

UNIVERZITA PALACKÉHO V OLOMOUCI

PŘÍRODOVĚDECKÁ FAKULTA

Katedra algebry a geometrie



Vybrané aplikace teorie těles

DIPLOMOVÁ PRÁCE

Vedoucí diplomové práce:

Doc. RNDr. Petr Emanovský, Ph.D.

Datum odevzdání: 8. dubna 2011

Vypracoval:

Tomáš Tábořský

F–M, 2. ročník

Olomouc 2011

Prohlášení

Prohlašuji, že jsem předloženou diplomovou 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 8. dubna 2011

Tomáš Táborský

Poděkování

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

Obsah

Úvod	6
1 Normální rozšíření těles	7
Řešené příklady	10
Cvičení	13
2 Separabilní rozšíření těles	14
Řešené příklady	18
Cvičení	31
3 Galoisovy grupy a jejich vlastnosti	33
Řešené příklady	38
Cvičení	44
4 Galoisovo cyklické rozšíření	46
Řešené příklady	48
Cvičení	54
5 Eukleidovské konstrukce a jejich algebraické interpretace	55
5.1 Eukleidovské konstrukce	55
5.2 Důkazy neřešitelnosti tří antických úloh	57
Řešené příklady	59
Cvičení	61
6 Úvod do problematiky algebraického kódování	62
6.1 Dvojkové symetrické kanály	62
6.2 Blokový kód	63
6.3 Objevování a opravování chyb blokových kódů	64
6.4 Lineární (maticové) kódy	64
6.5 Grupové kódy	67
6.6 Polynomické kódy	68
Řešené příklady	70
Cvičení	77

Závěr	78
Seznam použitých symbolů	79
Seznam použité literatury	80

Úvod

Moderní algebra studuje problematiku algebraických struktur (grup, okruhů, těles, atd.). Klasická algebra se zabývá řešením rovnic a jejich soustav, používá číselnou symboliku. Klíčovým algebraickým problémem bylo nalezení řešení algebraických rovnic. Algebraické rovnice prvního a druhé stupně uměli řešit již babylónští matematici. Teprve v roce 1545 ve spisu *Ars magna* byly publikovány Girolamem Cardanem (1501 – 1576) postupy při řešení algebraických rovnic třetího a čtvrtého stupně. Matematici se dále snažili nalézt řešení algebraických rovnic pátého a vyššího stupně. Norský matematik Niels Henrik Abel (1802 – 1829) v roce 1824 provedl důkaz neexistence řešení obecné algebraické rovnice pátého stupně v radikálech. Évariste Galois (1811 – 1832) uvedl ve svých spisech nutnou a postačující podmínku řešitelnosti algebraických rovnic v radikálech. Jeho metody a myšlenky mají podstatný vliv na rozvoj algebry, ale i celé matematiky.

S rozvojem moderní algebry souvisí i následná aplikace této teorie. Díky poznatkům moderní algebry byly formulovány důkazy o neřešitelnosti tří klasických problémů antické matematiky. Tyto poznatky se také uplatnily při hledání konstrukcí pravidelných n -úhelníků. Důkaz věty o sestrojitelnosti pravidelných n -úhelníků provedl roku 1796 Karl Friedrich Gauss (1777 – 1855).

V důsledku rozvoje moderní algebry dochází k rozvoji nových technologií, např. kódování a dekódování informací, počítačových technologií a mnoha dalších.

Diplomová práce obsahově navazuje na bakalářskou práci [18]. Práce je zaměřena na základní problematiku teorie těles, tj. algebraické a transcendentní rozšíření těles, hledání rozkladových těles polynomů a základní vlastnosti konečných těles. Diplomová práce se rovněž zabývá problematikou Galoisovy teorie, k jejímu zavedení je potřebné zavést normální a separabilní rozšíření těles. Na závěr práce je uvedena geometrická aplikace teorie těles a základní vlastnosti teorie algebraického kódování.

Jednotlivé kapitoly obsahují vždy teoretickou část, v této části jsou uvedeny základní definice a věty. Věty jsou většinou dokázány nebo je uveden odkaz na příslušnou literaturu, v níž je důkaz proveden. Součástí každé kapitoly jsou řešené úlohy a také cvičení pro samostatné řešení, jednotlivé příklady jsou uvedeny s výsledky pro následnou kontrolu.

1 Normální rozšíření těles

V úvodu této kapitoly připomene definice algebraického a transcendentního rozšíření těles. Dále se budeme zabývat normálním rozšířením těles, uvedeme základní vlastnosti. Tato problematika navazuje na algebraické a transcendentní rozšíření těles.

Definice 1.1. Nechť $\mathbb{K}$ je podtěleso tělesa $\mathbb{F}$ a nechť B je libovolná podmnožina tělesa $\mathbb{F}$. Průnik všech podoborů integrity tělesa $\mathbb{F}$ obsahujících $\mathbb{K} \cup B$ nazveme **podoborem integrity generovaným** B nad $\mathbb{K}$ a značíme jej $\mathbb{K}[B]$. Podobně průnik všech podtěles tělesa $\mathbb{F}$ obsahujících $\mathbb{K} \cup B$ nazveme **podtělesem generovaným** B nad $\mathbb{K}$ a značíme jej $\mathbb{K}(B)$.

Definice 1.2. Nechť $\mathbb{K}$ 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 $\mathbb{F}$, nazveme **transcendentním** prvkem nad $\mathbb{F}$.

Definice 1.3. 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 normálního rozšíření tělesa.

Definice 1.4. Těleso $\mathbb{K}$ se nazývá **normální rozšíření** tělesa $\mathbb{F}$, je-li $\mathbb{K}$ algebraické rozšíření $\mathbb{F}$ a každý ireducibilní polynom $f \in \mathbb{F}[x]$ mající v $\mathbb{K}$ alespoň jeden kořen, má v $\mathbb{K}$ všechny své kořeny.

Následně budou uvedeny dvě věty bez důkazů, které využijeme při důkazu věty 1.3. Důkazy těchto vět lze najít např. v [4].

Věta 1.1. *Nechť $\mathbb{F}$ je nadtěleso tělesa $\mathbb{K}$ a nechť $\alpha \in \mathbb{F}$ je algebraický prvek nad $\mathbb{K}$. Je-li $f \in \mathbb{K}[x]$ minimální polynom prvku α , pak f je ireducibilní. Pro polynom $g \in \mathbb{K}[x]$ platí, že $g(\alpha) = 0$, právě když $f|g$.*

Věta 1.2. *Nechť $\mathbb{F}$ je nadtěleso tělesa $\mathbb{K}$ a $B \subseteq \mathbb{F}$ množina algebraických prvků nad $\mathbb{K}$. Pak $\mathbb{K}(B) = \mathbb{K}[B]$ je algebraické rozšíření tělesa $\mathbb{K}$.*

Dále budou uvedeny dvě věty, pomocí nichž můžeme rozhodnout, zda dané rozšíření je normální či nikoliv.

Věta 1.3. *Nadtěleso $\mathbb{F}$ tělesa $\mathbb{K}$ je normální rozšíření tělesa $\mathbb{K}$ právě tehdy, když $\mathbb{F}$ je rozkladovým tělesem libovolné neprázdné množiny $B \subseteq \mathbb{K}[x]$.*

Důkaz. Předpokládejme, že $\mathbb{F}$ je normální rozšíření tělesa $\mathbb{K}$. Položme $B = \{f \in \mathbb{K}[x] : f \text{ je ireducibilní, } f \text{ má kořen v } \mathbb{F}\}$. Každý polynom $f \in B$ má dle předpokladu všechny kořeny v $\mathbb{F}$, proto je rozkladové těleso $\mathbb{M}$ množiny B obsaženo v $\mathbb{F}$. Nechť $\alpha \in \mathbb{F}$ je libovolný prvek a nechť $g \in \mathbb{K}[x]$ je minimální polynom prvku α . Z věty 1.1 vyplývá, že polynom g je ireducibilní nad $\mathbb{K}$, tedy $g \in B$. Proto $\alpha \in \mathbb{M}$ a $\mathbb{F} = \mathbb{M}$ je rozkladové těleso množiny B .

Naopak předpokládejme, že těleso $\mathbb{F}$ je rozkladové těleso nějaké množiny B polynomů z $\mathbb{K}[x]$. Označme C množinu všech kořenů polynomů z B . Dle věty 1.2 platí, že $\mathbb{F} = \mathbb{K}(C) = \mathbb{K}[C]$ je algebraickým rozšířením tělesa $\mathbb{K}$. Nechť $f \in \mathbb{K}[x]$ je libovolný ireducibilní polynom, jehož kořen je $\alpha \in \mathbb{F}$. Z věty 32.4 z [4] plyne existence polynomu $h(x_1, x_2, \dots, x_n) \in \mathbb{K}[x_1, x_2, \dots, x_n]$. Zřejmě existují prvky $\alpha_1, \alpha_2, \dots, \alpha_n$ takové, že $\alpha = h(\alpha_1, \alpha_2, \dots, \alpha_n) \in C$. Vzhledem k tomu, jak je množina C definována, existuje pro každé α_i ($i = 1, \dots, n$) polynom $g_i \in B$, pro nějž platí $g_i(\alpha_i) = 0$. Označme $g = g_1 g_2 \dots g_n$ a nechť $\beta_1, \beta_2, \dots, \beta_m$ ($m \in \mathbb{N}$) jsou všechny kořeny polynomu g . Jelikož polynomy $g_1, g_2, \dots, g_n$ mají dle předpokladu všechny kořeny v $\mathbb{F}$, leží všechny kořeny $\beta_1, \beta_2, \dots, \beta_m$ polynomu g rovněž v tělese $\mathbb{F}$. Tedy $\mathbb{K}(\beta_1, \beta_2, \dots, \beta_m) \subseteq \mathbb{F}$. Je zřejmé, že $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq \{\beta_1, \beta_2, \dots, \beta_m\}$, proto $\alpha \in \mathbb{K}(\beta_1, \beta_2, \dots, \beta_m)$. Nechť β je libovolný kořen polynomu f . Z toho, že každá dvě kořenová nadtělesa ireducibilního polynomu jsou izomorfní, vyplývá existence izomorfismu $\phi : \mathbb{K}(\alpha) \rightarrow \mathbb{K}(\beta)$, který lze rozšířit na $\mathbb{K}$ -izomorfismus $\psi : \mathbb{K}(\alpha, \beta_1, \beta_2, \dots, \beta_m) \rightarrow \mathbb{K}(\beta, \beta_1, \beta_2, \dots, \beta_m)$. Prvek $\alpha \in \mathbb{K}(\beta_1, \beta_2, \dots, \beta_m)$ a platí $[\mathbb{K}(\beta_1, \beta_2, \dots, \beta_m) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta_1, \beta_2, \dots, \beta_m) : \mathbb{K}] = [\mathbb{K}(\beta, \beta_1, \beta_2, \dots, \beta_m) : \mathbb{K}] = [\mathbb{K}(\beta, \beta_1, \beta_2, \dots, \beta_m) : \mathbb{K}(\beta_1, \beta_2, \dots, \beta_m)] \cdot [\mathbb{K}(\beta_1, \beta_2, \dots, \beta_m) : \mathbb{K}]$. Tedy $[\mathbb{K}(\beta, \beta_1, \beta_2, \dots, \beta_m) : \mathbb{K}(\beta_1, \beta_2, \dots, \beta_m)] = 1$. Proto $\beta \in \mathbb{K}(\beta_1, \beta_2, \dots, \beta_m) \subseteq \mathbb{F}$ [4].

□

Věta 1.4. *Nechť těleso $\mathbb{F}$ je konečným rozšířením tělesa $\mathbb{K}$. Pak $\mathbb{F}$ je normálním rozšířením tělesa $\mathbb{K}$ právě tehdy, když $\mathbb{F}$ je rozkladovým tělesem nějakého polynomu $f \in \mathbb{K}[x]$.*

Důkaz. Z předchozí věty plyne, že rozkladové těleso polynomu f je normálním rozšířením tělesa $\mathbb{K}$. Nechť $\mathbb{F}$ je normální rozšíření tělesa $\mathbb{K}$. Těleso $\mathbb{F}$ je konečným rozšířením $\mathbb{K}$, proto existují prvky $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}$ takové, že $\mathbb{F} = \mathbb{K}(\alpha_1, \alpha_2, \dots, \alpha_n)$. Označme $f_i \in \mathbb{K}[x]$

minimální polynom prvku α_i , $i = 1, 2, \dots, n$ a položíme $f = f_1 f_2 \dots f_n$. Rozkladové těleso $\mathbb{L}$ polynomu f zřejmě obsahuje prvky $\alpha_1, \alpha_2, \dots, \alpha_n$, proto $\mathbb{F} \subseteq \mathbb{L}$. Z druhé strany $\mathbb{F}$ je normální nad $\mathbb{K}$, proto $\mathbb{F}$ obsahuje všechny kořeny polynomu f_i , kde $i = 1, \dots, n$, tedy všechny kořeny polynomu f a $\mathbb{L} \subseteq \mathbb{F}$ [4]. $\square$

V následujících větách budou uvedeny základní vlastnosti normálních rozšíření těles.

Věta 1.5. *Nechť $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ jsou tělesa. Je-li $\mathbb{L}$ normální nad $\mathbb{F}$, pak $\mathbb{L}$ je normální nad $\mathbb{K}$.*

Důkaz. Dle věty 1.3 existuje podmnožina $B \subseteq \mathbb{F}[x]$ taková, že $\mathbb{L}$ je rozkladovým tělesem množiny B . Jelikož $\mathbb{F} \subseteq \mathbb{K}$, je $B \subseteq \mathbb{K}[x]$ a z věty 1.3 plyne, že $\mathbb{L}$ je normální nad $\mathbb{K}$ [4]. $\square$

Věta 1.6. *Nechť $\mathbb{F}$ a $\mathbb{L}$ jsou normální rozšíření tělesa $\mathbb{K}$. Je-li $\mathbb{M}$ nejmenší nadtěleso tělesa $\mathbb{K}$ obsahující $\mathbb{F}$ a $\mathbb{L}$, pak $\mathbb{M}$ je normální rozšíření tělesa $\mathbb{K}$.*

Důkaz. Podle věty 1.3 je $\mathbb{F}$ rozkladovým tělesem nějaké množiny polynomů $A \subseteq \mathbb{K}[x]$ a $\mathbb{L}$ rozkladovým tělesem nějaké množiny polynomů $B \subseteq \mathbb{K}[x]$. Označme C množinu všech kořenů polynomů z A a D množinu všech kořenů polynomů z B . Pak $\mathbb{F} = \mathbb{K}(C)$, $\mathbb{L} = \mathbb{K}(D)$ a $\mathbb{M} = \mathbb{K}(C \cup D)$. To znamená, že $\mathbb{M}$ je rozkladovým tělesem množiny $A \cup B \subseteq \mathbb{K}[x]$ a $\mathbb{M}$ je normálním rozšířením tělesa $\mathbb{K}$ [4]. $\square$

Věta 1.7. *Nechť $\mathbb{K}$ je normální rozšíření tělesa $\mathbb{L}$ a $\mathbb{M}$ libovolné rozšíření tělesa $\mathbb{L}$. Pak nejmenší nadtěleso $\mathbb{F}$ tělesa $\mathbb{L}$ obsahující $\mathbb{K}$ i $\mathbb{M}$ je normální rozšíření tělesa $\mathbb{M}$.*

Důkaz věty 1.7 lze nalézt např. v [4].

Věta 1.8. *Nechť $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ a nechť $\mathbb{K}$ je normální rozšíření tělesa $\mathbb{L}$ a $\mathbb{L}$ je normální rozšíření tělesa $\mathbb{F}$. Pak $\mathbb{K}$ je normální rozšíření tělesa $\mathbb{F}$.*

Důkaz. Nechť $\mathbb{K}$ je normální rozšíření tělesa $\mathbb{L}$ a $\mathbb{L}$ je normální rozšíření tělesa $\mathbb{F}$. Dle věty 1.3 existuje $B \subseteq \mathbb{L}[x]$ takové, že $\mathbb{K}$ je rozkladovým tělesem polynomů z B . Dále dle věty 1.3 existuje $C \subseteq \mathbb{F}[x]$ takové, že $\mathbb{L}$ je rozkladovým tělesem polynomů z C . Platí, že $C \subseteq \mathbb{F}[x] \subseteq B \subseteq \mathbb{L}[x]$, tedy $C \subseteq B$. Je zřejmé, že $\mathbb{K}$ je rozkladovým tělesem polynomů $C \subseteq \mathbb{F}[x]$. Proto $\mathbb{K}$ je normální rozšíření tělesa $\mathbb{F}$. $\square$

Řešené příklady

Příklad 1.1. Rozhodněte, zda daná rozšíření nad uvedenými tělesy jsou normální.

- a) $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$,
- b) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}i)$ nad $\mathbb{Q}$,
- c) $\mathbb{Q}(i + \frac{3}{4})$ nad $\mathbb{Q}$,
- d) $\mathbb{Q}(\pi)$ nad $\mathbb{Q}$,
- e) $\mathbb{Q}(\sqrt[3]{3})$ nad $\mathbb{Q}$.

Řešení:

- a) $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$.

Využijeme věty 1.4, dle které stačí nalézt polynom z $\mathbb{Q}[x]$ takový, že $\mathbb{Q}(\sqrt{2})$ je jeho rozkladovým tělesem.

Uvažujme polynom $f = x^2 - 2$, zřejmě $f \in \mathbb{Q}[x]$.

Polynom f následně upravíme

$$f = (x - \sqrt{2})(x + \sqrt{2}).$$

Pro prvky platí:

$$\begin{aligned}\sqrt{2} &\in \mathbb{Q}(\sqrt{2}), \\ -\sqrt{2} &\in \mathbb{Q}(\sqrt{2}).\end{aligned}$$

Zřejmě těleso $\mathbb{Q}(\sqrt{2})$ je rozkladovým tělesem polynomu f . Tedy rozšíření $\mathbb{Q}(\sqrt{2})$ tělesa $\mathbb{Q}$ je normální.

- b) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}i)$ nad $\mathbb{Q}$.

Řešení je analogické jako v případě a).

Uvažujme polynom $f = x^3 - 3$. Polynom f můžeme psát ve tvaru

$$f = (x - \sqrt[3]{3})(x^2 + \sqrt[3]{3}x + \sqrt[3]{9}).$$

Zbývající dva kořeny polynomu f nalezneme dle známého vztahu

$$x_{2,3} = \frac{-\sqrt[3]{3} \pm \sqrt{\sqrt[3]{9} - 4\sqrt[3]{9}}}{2} = \frac{-\sqrt[3]{3} \pm \sqrt{-3\sqrt[3]{3}}}{2} = \frac{-\sqrt[3]{3} \pm i\sqrt{3}\sqrt[3]{3}}{2}.$$

Zřejmě těleso $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}i)$ je rozkladovým tělesem polynomu f . Tedy těleso $\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}i)$ je normálním rozšířením tělesa $\mathbb{Q}$.

c) $\mathbb{Q}(i + \frac{3}{4})$ nad $\mathbb{Q}$.

Zřejmě $\mathbb{Q}(i + \frac{3}{4}) = \mathbb{Q}(i)$. Uvažujme polynom $f = x^2 - 1$, polynom f můžeme rozložit do následujícího tvaru

$$f = (x + i)(x - i).$$

Tedy těleso $\mathbb{Q}(i + \frac{3}{4})$ je rozkladovým tělesem polynomu f a těleso $\mathbb{Q}(i + \frac{3}{4})$ je normální rozšíření tělesa $\mathbb{Q}$.

d) $\mathbb{Q}(\pi)$ nad $\mathbb{Q}$.

Prvek π je transcendentní nad tělesem $\mathbb{Q}$. Tedy $\mathbb{Q}(\pi)$ je transcendentní rozšíření tělesa $\mathbb{Q}$, proto $\mathbb{Q}(\pi)$ není normální rozšíření tělesa $\mathbb{Q}$.

e) $\mathbb{Q}(\sqrt[3]{3})$ nad $\mathbb{Q}$.

Uvažujme polynom $f = x^3 - 3$. Polynom f můžeme psát ve tvaru

$$f = (x - \sqrt[3]{3})(x^2 + \sqrt[3]{3}x + \sqrt[3]{9}).$$

Prvek $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{3})$ je kořenem polynomu f , ale zbývající dva kořeny polynomu f neleží v $\mathbb{Q}(\sqrt[3]{3})$ (viz b)). Z definice 1.4 vyplývá, že $\mathbb{Q}(\sqrt[3]{3})$ není normální rozšíření tělesa $\mathbb{Q}$.

Příklad 1.2. Rozhodněte, zda daná rozšíření konečných těles jsou normální.

a) $\mathbb{Z}_3(\sqrt{2} + \bar{1})$ nad $\mathbb{Z}_3$,

b) $\mathbb{Z}_5(\sqrt[4]{2})$ nad $\mathbb{Z}_5$.

Řešení:

a) $\mathbb{Z}_3(\sqrt{2} + \bar{1})$ nad $\mathbb{Z}_3$.

Zřejmě $\mathbb{Z}_3(\sqrt{2} + \bar{1}) = \mathbb{Z}_3(\sqrt{2})$. Při řešení využijeme věty 1.4, tedy stačí nalézt jediný polynom $f \in \mathbb{Z}_3[x]$, pro který platí, že $\mathbb{Z}_3(\sqrt{2} + \bar{1})$ je jeho rozkladovým tělesem. Uvažujme polynom $f = x^2 + \bar{1}$, zřejmě $f \in \mathbb{Z}_3[x]$.

Polynom f následně upravíme

$$f = (x - \sqrt{2})(x + \sqrt{2}).$$

Tedy $\mathbb{Z}_3(\sqrt{2} + \bar{1})$ je rozkladovým tělesem polynomu f a dle věty 1.4 je $\mathbb{Z}_3(\sqrt{2} + \bar{1})$ normální rozšíření tělesa $\mathbb{Z}_3$.

b) $\mathbb{Z}_5 \left(\sqrt[4]{2} \right)$ nad $\mathbb{Z}_5$.

Řešení je analogické jako v části za a). Tedy stačí nalézt libovolný polynom $f \in \mathbb{Z}_5[x]$, pro nějž platí, že jeho rozkladovým tělesem je $\mathbb{Z}_5 \left(\sqrt[4]{2} \right)$.

Uvažujme polynom $f = x^4 - \bar{2}$. Polynom f následně rozložíme

$$\begin{aligned} f = x^4 - \bar{2} &= \left(x^2 + \sqrt{2} \right) \left(x^2 - \sqrt{2} \right) = \left(x^2 - \bar{4}\sqrt{2} \right) \left(x^2 - \sqrt{2} \right) = \\ &= \left(x - \bar{2}\sqrt[4]{2} \right) \left(x + \bar{2}\sqrt[4]{2} \right) \left(x - \sqrt[4]{2} \right) \left(x + \sqrt[4]{2} \right). \end{aligned}$$

Je evidentní, že $\mathbb{Z}_5 \left(\sqrt[4]{2} \right)$ je rozkladovým tělesem polynomu f , tedy $\mathbb{Z}_5 \left(\sqrt[4]{2} \right)$ je normálním rozšířením tělesa $\mathbb{Z}_5$.

Příklad 1.3. Rozhodněte, zda těleso $\mathbb{Q}(\alpha, \sqrt[3]{\alpha})$ je normální rozšíření tělesa $\mathbb{Q}$, kde α je kořen polynomu $f = x^4 - 1$.

Řešení:

Při řešení využijeme větu 1.8. Tedy stačí dokázat, že $\mathbb{Q}(\alpha, \sqrt[3]{\alpha})$ je normální rozšíření tělesa $\mathbb{Q}(\alpha)$ a $\mathbb{Q}(\alpha)$ je normální rozšíření tělesa $\mathbb{Q}$.

Zřejmě těleso $\mathbb{Q}(\alpha, \sqrt[3]{\alpha})$ je rozkladovým tělesem polynomu

$$g = x^3 - \alpha$$

nad $\mathbb{Q}(\alpha)$, proto $\mathbb{Q}(\alpha, \sqrt[3]{\alpha})$ je normální rozšíření tělesa $\mathbb{Q}(\alpha)$.

Těleso $\mathbb{Q}(\alpha)$ je zřejmě rozkladovým tělesem polynomu f nad tělesem $\mathbb{Q}$, proto $\mathbb{Q}(\alpha)$ je normální rozšíření tělesa $\mathbb{Q}$.

Tedy $\mathbb{Q}(\alpha, \sqrt[3]{\alpha})$ je normální rozšíření tělesa $\mathbb{Q}$.

Cvičení

Cvičení 1.1. Rozhodněte, zda rozšíření uvedených těles jsou normální.

- a) $\mathbb{Q}(\sqrt{3} + 2)$ nad $\mathbb{Q}$,
- b) $\mathbb{Q}(\sqrt[4]{2}, i)$ nad $\mathbb{Q}$,
- c) $\mathbb{C}$ nad $\mathbb{R}$,
- d) $\mathbb{Q}(e)$ nad $\mathbb{Q}$.

[a) těleso $\mathbb{Q}(\sqrt{3} + 2) = \mathbb{Q}(\sqrt{3})$ a je zřejmě rozkladovým tělesem polynomu $f = x^2 - 3$, tedy $\mathbb{Q}(\sqrt{3} + 2)$ je normální rozšíření tělesa $\mathbb{Q}$; b) těleso $\mathbb{Q}(\sqrt[4]{2}, i)$ je rozkladovým tělesem polynomu $f = x^4 - 2$, těleso $\mathbb{Q}(\sqrt[4]{2}, i)$ je normálním rozšířením tělesa $\mathbb{Q}$; c) těleso $\mathbb{C} = \mathbb{R}(i)$ je rozkladovým tělesem polynomu $f = x^2 - 1$, těleso $\mathbb{C}$ je normálním rozšířením tělesa $\mathbb{R}$; d) $\mathbb{Q}(e)$ je transcendentní rozšířením tělesa $\mathbb{Q}$, proto $\mathbb{Q}(e)$ není normální rozšíření tělesa $\mathbb{Q}$]

Cvičení 1.2. Rozhodněte, zda daná rozšíření konečných těles jsou normální.

- a) $\mathbb{Z}_{11}(\sqrt{\bar{7}} - \bar{1})$ nad $\mathbb{Z}_{11}$,
- b) $\mathbb{Z}_5(\sqrt[4]{\bar{3}} + \bar{4})$ nad $\mathbb{Z}_5$.

[a) těleso $\mathbb{Z}_{11}(\sqrt{\bar{7}} - \bar{1}) = \mathbb{Z}_{11}(\sqrt{\bar{7}})$ je zřejmě rozkladovým tělesem polynomu $f = x^2 - \bar{7}$, těleso $\mathbb{Z}_{11}(\sqrt{\bar{7}} - \bar{1})$ je normálním rozšířením tělesa $\mathbb{Z}_{11}$; b) těleso $\mathbb{Z}_5(\sqrt[4]{\bar{3}} + \bar{4}) = \mathbb{Z}_5(\sqrt[4]{\bar{3}})$ je rozkladovým tělesem polynomu $f = x^4 - \bar{3}$, těleso $\mathbb{Z}_5(\sqrt[4]{\bar{3}} + \bar{4})$ je tedy normálním rozšířením tělesa $\mathbb{Z}_5$]

2 Separabilní rozšíření těles

Tato kapitola bude věnována dalšímu typu rozšíření těles tzv. separabilnímu. Budeme definovat nové pojmy, jako je separabilní polynom, separabilní rozšíření, dokonalé těleso, atd. Všechny tyto pojmy využijeme při zavedení Galoisova rozšíření tělesa.

Definice 2.1. Ireducibilní polynom $f \in \mathbb{F}[x]$ se nazývá **separabilní**, má-li všechny kořeny jednoduché. V opačném případě se polynom f nazývá **neseperabilní**.

Definice 2.2. Prvek α z nadtělesa $\mathbb{F}$ tělesa $\mathbb{K}$ se nazývá **separabilní nad $\mathbb{K}$** , je-li α algebraický nad $\mathbb{K}$ a jeho minimální polynom je separabilní. Je-li minimální polynom neseperabilní, řekneme, že prvek α je **neseperabilní nad $\mathbb{K}$** .

Definice 2.3. Konečné rozšíření $\mathbb{F}$ tělesa $\mathbb{K}$ se nazývá **separabilní**, je-li jeho každý prvek separabilní nad $\mathbb{K}$.

Pomocí následující věty budeme schopni na základě největšího společného dělitele polynomu a jeho první derivace rozhodnout o separabilnosti daného polynomu nad uvedeným tělesem. Důkaz této věty lze nalézt např. v [9].

Věta 2.1. *Nechť f je ireducibilní polynom nad tělesem $\mathbb{F}$ a dále $NSD(f, f')$ je největší společný dělitel polynomu f a jeho derivace f' . Jestliže $NSD(f, f') = 1$, pak f je separabilní nad $\mathbb{F}$. V opačném případě f je neseperabilní.*

Z předchozí věty vyplývá.

Důsledek 2.1. *Ireducibilní polynom je separabilní, jestliže jeho první derivace je různá od nuly.*

Důsledek 2.2. *Každý ireducibilní polynom nad tělesem s charakteristikou 0 je separabilní.*

Níže uvedené definice zavádí pojem redukovaný stupeň polynomu a nadtělesa. V následující větě ukážeme souvislost mezi redukovaným stupněm nadtělesa a stupněm nadtělesa.

Definice 2.4. **Redukovaným stupněm** ireducibilního polynomu $f \in \mathbb{F}[x]$ budeme rozumět počet navzájem různých kořenů polynomu f , což budeme značit $st_r f$.

Definice 2.5. Necht $\mathbb{K}$ je nadtěleso tělesa $\mathbb{F}$ a $\alpha \in \mathbb{K}$ je algebraický prvek nad $\mathbb{F}$. Pak **redukovaným stupněm nadtělesa** $\mathbb{F}(\alpha)$ nad $\mathbb{F}$ rozumíme redukovaný stupeň minimálního polynomu prvku α . Redukovaný stupeň nadtělesa $\mathbb{F}(\alpha)$ nad $\mathbb{F}$ budeme označovat $[\mathbb{F}(\alpha) : \mathbb{F}]_r$.

Věta 2.2. Necht $\mathbb{K}$ je nadtěleso tělesa $\mathbb{F}$ a $\alpha \in \mathbb{K}$ je algebraický prvek nad $\mathbb{F}$. Pak platí, že prvek α je separabilní nad $\mathbb{F}$, právě když $[\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}]_r$.

Definice 2.6. Řekneme, že těleso $\mathbb{F}$ je **algebraicky uzavřené**, jestliže libovolný polynom $f \in \mathbb{F}[x]$ má v $\mathbb{F}$ alespoň jeden kořen.

Definice 2.7. Nadtěleso $\mathbb{K}$ tělesa $\mathbb{F}$ nazveme **algebraickým uzávěrem** tělesa $\mathbb{F}$, je-li algebraicky uzavřené a algebraické nad $\mathbb{F}$.

V následující větě uvedeme jednu z vlastností, která je analogická pro stupně rozšíření těles.

Věta 2.3. Necht $\mathbb{M}$ je algebraický uzávěr tělesa $\mathbb{F}$ a necht $\mathbb{K}, \mathbb{L}$ jsou dvě mezitělesa konečného stupně nad $\mathbb{F}$ taková, že $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. Pak

$$[\mathbb{L} : \mathbb{F}]_r = [\mathbb{L} : \mathbb{K}]_r \cdot [\mathbb{K} : \mathbb{F}]_r.$$

Důkaz věty 2.2 i věty 2.3 lze nalézt např. v [4].

V níže uvedených větách bude dále charakterizováno separabilní rozšíření těles.

Věta 2.4. Necht $\mathbb{K}$ je konečné rozšíření tělesa $\mathbb{F}$ charakteristiky p . Pak existuje celé nezáporné číslo l takové, že

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}]_r \cdot p^l.$$

Důkaz. Necht $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ je báze vektorového prostoru $\mathbb{K}$ nad $\mathbb{F}$. Budeme postupovat úplnou indukcí podle k . Pro $k = 1$ platí tvrzení dle věty 2.1. Necht tedy $k > 1$, předpokládejme, že tvrzení platí pro $k - 1$. Označme $\mathbb{L} = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{k-1})$, pak $\mathbb{K} = \mathbb{F}(\alpha_k)$. Podle indukčního předpokladu existují $s, t \in \mathbb{N}_0$ taková, že $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{F}]_r \cdot p^s$ a $[\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{L}]_r \cdot p^t$. Položme $l = s + t$, pak platí $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{F}] = [\mathbb{K} : \mathbb{L}]_r \cdot p^t \cdot [\mathbb{L} : \mathbb{F}]_r \cdot p^s = [\mathbb{K} : \mathbb{F}]_r \cdot p^l$ [4]. $\square$

Věta 2.5. Necht $\mathbb{F}$ je nadtěleso tělesa $\mathbb{K}$ charakteristiky p . Je-li prvek $\alpha \in \mathbb{F}$ separabilní nad $\mathbb{K}$, pak těleso $\mathbb{K}(\alpha)$ je separabilním rozšířením tělesa $\mathbb{K}$.

Důkaz. Necht β je prvek z $\mathbb{K}(\alpha)$. Ukážeme, že β je separabilní nad $\mathbb{K}$. Z věty 2.3 vyplývá, že existují prvky $s, t \in \mathbb{N}_0$ takové, že $[\mathbb{K}(\beta) : \mathbb{K}] = [\mathbb{K}(\beta) : \mathbb{K}]_r \cdot p^s$ a $[\mathbb{K}(\alpha) : \mathbb{K}(\beta)] = [\mathbb{K}(\alpha) : \mathbb{K}(\beta)]_r \cdot p^t$. Zřejmě platí $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}(\beta)] \cdot [\mathbb{K}(\beta) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}(\beta)]_r \cdot p^t \cdot [\mathbb{K}(\beta) : \mathbb{K}]_r \cdot p^s = [\mathbb{K}(\alpha) : \mathbb{K}]_r \cdot p^{t+s}$. Podle věty 2.1 platí $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}]_r$, proto $s + t = s = t = 0$. Tedy $[\mathbb{K}(\beta) : \mathbb{K}] = [\mathbb{K}(\beta) : \mathbb{K}]_r$ z toho plyne, že β je separabilní nad $\mathbb{K}$ (dle věty 2.1) [4]. $\square$

Věta 2.6. *Konečné rozšíření $\mathbb{F}$ tělesa $\mathbb{K}$ je separabilní, právě když $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}]_r$.*

Důkaz. Necht $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ je báze vektorového prostoru $\mathbb{K}$ nad $\mathbb{F}$. Budeme postupovat úplnou indukcí vzhledem ke k . Pro $k = 1$ platí tvrzení dle věty 2.1. Necht tedy $k > 1$, předpokládejme, že tvrzení platí pro $k - 1$. Označme $\mathbb{L} = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{k-1})$. Je-li $\mathbb{F}$ separabilní nad $\mathbb{K}$, je zřejmě $\mathbb{F}$ separabilní nad $\mathbb{L}$ a $\mathbb{L}$ separabilní nad $\mathbb{K}$. Dle indukčního předpokladu platí $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_r$ a $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}]_r$, tedy $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}]_r \cdot [\mathbb{L} : \mathbb{K}]_r = [\mathbb{F} : \mathbb{K}]_r$.

Necht tedy naopak $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}]_r$. Dokážeme, že libovolný prvek α je separabilní nad $\mathbb{K}$. Z věty 2.3 plyne existence $s, t \in \mathbb{N}_0$ takových, že $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}]_r \cdot p^s$ a $[\mathbb{F} : \mathbb{K}(\alpha)] = [\mathbb{F} : \mathbb{K}(\alpha)]_r \cdot p^t$. Zřejmě platí $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}(\alpha)]_r \cdot [\mathbb{K}(\alpha) : \mathbb{K}]_r \cdot p^{t+s} = [\mathbb{F} : \mathbb{K}]_r \cdot p^{t+s} = [\mathbb{F} : \mathbb{K}]_r$, tedy $s + t = s = t = 0$. Proto $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}]_r$ z toho plyne, že α je separabilní nad $\mathbb{K}$ [4]. $\square$

Důkaz následující věty lze najít např. v [4].

Věta 2.7. *Necht těleso $\mathbb{L}$ je separabilní rozšíření tělesa $\mathbb{F}$ a těleso $\mathbb{K}$ je separabilní rozšíření tělesa $\mathbb{L}$. Pak těleso $\mathbb{K}$ je separabilní rozšíření tělesa $\mathbb{F}$.*

Důsledek 2.3. *Necht $\mathbb{K}$ je separabilní rozšíření tělesa $\mathbb{F}$. Uvažujme prvky $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{K}$ takové, že α_i je separabilní nad $\mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_{i-1})$ pro každé $i = 1, \dots, n$. Pak těleso $\mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_n)$ je separabilní rozšíření tělesa $\mathbb{F}$. Jsou-li prvky $\alpha_1, \alpha_2, \dots, \alpha_n$ separabilní nad $\mathbb{F}$, pak $\mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_n)$ je separabilní rozšíření tělesa $\mathbb{F}$.*

Následně zavedeme pojem dokonalé těleso a dále budou uvedeny jeho vlastnosti.

Definice 2.8. Těleso $\mathbb{F}$ se nazývá **dokonalé**, jestliže každý ireducibilní polynom $f \in \mathbb{F}[x]$ je separabilní.

Věta 2.8. *Těleso $\mathbb{F}$ je dokonalé, právě když každé jeho algebraické rozšíření je separabilní.*

Důkaz. Nechť $\mathbb{F}$ je dokonalé těleso a nechť α je prvek z libovolného algebraického rozšíření $\mathbb{K}$ tělesa $\mathbb{F}$. Minimální polynom prvku α je separabilní nad $\mathbb{F}$, proto $\mathbb{K}$ je separabilní nad $\mathbb{F}$.

Naopak předpokládejme, že každé algebraické rozšíření tělesa $\mathbb{F}$ je separabilní. Nechť $f \in \mathbb{F}[x]$ je ireducibilní. Rozkladové těleso $\mathbb{K}$ polynomu f je separabilní nad $\mathbb{F}$, jelikož polynom f je až na násobek nenulovým prvkem z $\mathbb{F}$ minimálním polynomem libovolného svého kořene α z $\mathbb{K}$. Tedy f je separabilní nad $\mathbb{F}$ [4]. $\square$

Věta 2.9. *Každé algebraicky uzavřené těleso je dokonalé.*

Důkaz. Pro všechny ireducibilní polynomy nad libovolným algebraicky uzavřeným tělesem platí, že jsou prvního stupně. A tyto polynomy jsou zřejmě separabilní [4]. $\square$

Věta 2.10. *Každé těleso charakteristiky nula je dokonalé.*

Důkaz. Pro tělesa charakteristiky nula platí, že všechny ireducibilní polynomy nad tímto tělesem mají všechny kořeny jednoduché. Tyto polynomy jsou zřejmě separabilní. $\square$

Věta 2.11. *Těleso $\mathbb{F}$ charakteristiky p je dokonalé, právě když pro každý prvek $a \in \mathbb{F}$ má polynom $x^p - a$ kořen v $\mathbb{F}$.*

Větu 2.11 využijeme při důkazu následující věty, důkaz této věty lze nalézt např. v [4].

Lemma 2.1. *Nechť $\mathbb{F}$ je těleso charakteristiky p . Pak pro libovolné přirozené číslo k a libovolné dva prvky $a, b \in \mathbb{F}$ platí $(a + b)^{p^k} = a^{p^k} + b^{p^k}$.*

Věta 2.12. *Každé konečné těleso je dokonalé.*

Důkaz. Nechť p je charakteristika tělesa $\mathbb{F}$. Zobrazení $f : \mathbb{F} \rightarrow \mathbb{F}$ definované předpisem $f(a) = a^p$ je homomorfismus, neboť dle předchozího lemmatu platí $f(a + b) = (a + b)^p = a^p + b^p = f(a) + f(b)$ a $f(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = f(a) \cdot f(b)$. Zobrazení f je monomorfismus, jelikož $f(a) = a^p = 0$, právě když $a = 0$. Zobrazení f je izomorfismus vzhledem k tomu, že $\mathbb{F}$ má konečný počet prvků. Nechť $a \in \mathbb{F}$ je libovolný prvek, pak existuje prvek $\alpha \in \mathbb{F}$ takový, že $f(\alpha) = \alpha^p = a$. Prvek α je tedy kořenem polynomu $x^p - a$ a nyní stačí využít předchozí větu [4]. $\square$

Řešené příklady

Příklad 2.1. Rozhodněte, zda uvedený polynom je nad daným tělesem separabilní.

- a) $f = x^2 - 2$ nad $\mathbb{Q}$,
- b) $g = x^4 - x^2 - 6$ nad $\mathbb{Q}$,
- c) $h = x^6 + 8x^4 + 20x^2 + 16$ nad $\mathbb{Q}$,
- d) $k = x^4 + 4x^3 + 2x - 2$ nad $\mathbb{Q}$.

Řešení:

- a) $f = x^2 - 2$ nad $\mathbb{Q}$.

Při řešení využijeme definice 2.1, dle které je ireducibilní polynom nad daným tělesem separabilní, jestliže má všechny kořeny jednoduché.

Polynom f můžeme zapsat ve tvaru

$$f = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Polynom f je zřejmě ireducibilní nad $\mathbb{Q}$ a má všechny kořeny jednoduché. Tedy dle definice 2.1 je polynom f nad $\mathbb{Q}$ separabilní.

- b) $g = x^4 - x^2 - 6$ nad $\mathbb{Q}$.

Řešení bude analogické jako v části a).

Uvažujme substituci $y = x^2$. Tedy $g = y^2 - y - 6$, zřejmě platí

$$g = (y - 3)(y - 2).$$

Po zpětném dosazení do substituce dostaneme

$$g = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3}).$$

Polynom g má všechny kořeny jednoduché, ale není nad $\mathbb{Q}$ ireducibilní, jelikož

$$g = (x^2 - 2)(x^2 - 3).$$

Tedy polynom g není nad $\mathbb{Q}$ separabilní.

- c) $h = x^6 + 8x^4 + 20x^2 + 16$ nad $\mathbb{Q}$.

Nejprve ověříme, zda polynom h nemá vícenásobné kořeny. Určíme největšího společného dělitele polynomů h a h' , pokud tyto dva polynomy jsou nesoudělné, pak polynom h

má všechny kořeny jednoduché. Největší společný dělitel polynomu h a jeho první derivace určíme s využitím Euklidova algoritmu. (Symbolem $\sim$ budeme značit relaci být asociovaný na množině všech polynomů.)

Derivace polynomu je

$$h' = 6x^5 + 32x^3 + 40x \sim 3x^5 + 16x^3 + 20x.$$

Následně je popsán Euklidův algoritmus pro určení $\text{NSD}(h, h')$.

$$\begin{array}{r} (3x^6 + 24x^4 + 60x^2 + 48) : (3x^5 + 16x^3 + 20x) = x \\ \underline{-3x^6 - 16x^4 - 20x^2} \\ 8x^4 + 40x^2 + 48 \sim x^4 + 5x^2 + 6 \end{array}$$

$$\begin{array}{r} (3x^5 + 16x^3 + 20x) : (x^4 + 5x^2 + 6) = 3x \\ \underline{-3x^5 - 15x^3 - 18x} \\ x^3 + 2x \end{array}$$

$$\begin{array}{r} (x^4 + 5x^2 + 6) : (x^3 + 2x) = x \\ \underline{-x^4 - 2x^2} \\ 3x^2 + 6 \sim x^2 + 2 \end{array}$$

$$\begin{array}{r} (x^3 + 2x) : (x^2 + 2) = x \\ \underline{-x^3 - 2x} \\ 0 \end{array}$$

Tedy $\text{NSD}(h, h') = x^2 + 2$, proto polynom f má vícenásobné kořeny a není separabilní nad $\mathbb{Q}$.

d) $k = x^4 + 4x^3 + 2x - 2$ nad $\mathbb{Q}$.

Z Eisensteinova kritéria ireducibility plyne, že k je ireducibilní nad $\mathbb{Q}$ (hledané prvočíslo $p = 2$). Dále postupujeme analogicky jako v části c). Určíme $\text{NSD}(k, k')$.

Derivace polynomu je

$$k' = 4x^3 + 12x^2 + 2 \sim 2x^3 + 6x^2 + 1.$$

Níže je popsán Euklidův algoritmus pro určení $\text{NSD}(k, k')$.

$$\begin{array}{r}
(x^4 + 4x^3 + 2x - 2) : (2x^3 + 6x^2 + 1) = \frac{1}{2}x + \frac{1}{2} \\
\underline{-x^4 - 3x^3 - \frac{1}{2}x} \\
x^3 + \frac{3}{2}x - 2 \\
\underline{-x^3 - 3x^2 - \frac{1}{2}} \\
-3x^2 + \frac{3}{2}x - \frac{5}{2} \sim 6x^2 - 3x + 5
\end{array}$$

$$\begin{array}{r}
(6x^3 + 18x^2 + 3) : (6x^2 - 3x + 5) = x + \frac{7}{2} \\
\underline{-6x^3 + 3x^2 - 5x} \\
21x^2 - 5x + 3 \\
\underline{-21x^2 + \frac{21}{2}x - \frac{35}{2}} \\
\frac{11}{2}x - \frac{29}{2} \sim 11x - 29
\end{array}$$

$$\begin{array}{r}
(6x^2 - 3x + 5) : (11x - 29) = \frac{6}{11}x + \frac{141}{121} \\
\underline{-6x^2 + \frac{174}{11}x} \\
\frac{141}{11}x + 5 \\
\underline{-\frac{141}{11}x + \frac{4089}{121}} \\
\frac{8783}{121} \sim 1
\end{array}$$

Tedy $\text{NSD}(k, k') = 1$, proto polynom k má všechny kořeny jednoduché. Polynom k je dle definice 2.1 separabilní nad $\mathbb{Q}$.

Příklad 2.2. Rozhodněte, zda polynom $f = x^3 + 2u$ je separabilní nad tělesem $\mathbb{Q}(u)$, kde u je kořen polynomu $g = x^2 + x + 1$.

Řešení:

Při řešení postupujeme analogicky jako v předcházejícím případě.

Polynom g je zřejmě ireducibilní nad $\mathbb{Q}$, proto ani $\sqrt[3]{2u}$ není prvkem tělesa $\mathbb{Q}(u)$. Tedy polynom f je ireducibilní nad $\mathbb{Q}(u)$.

Rovnice $f = 0$ je binomickou rovnicí. Tato rovnice má zřejmě všechny kořeny různé, proto polynom f má všechny kořeny jednoduché.

Tedy polynom f je separabilní nad $\mathbb{Q}$.

Příklad 2.3. Rozhodněte, zda uvedený prvek je separabilní nad uvedeným tělesem.

- a) $\alpha = \sqrt{1 + \sqrt{2}}$ nad $\mathbb{Q}$,
- b) $\beta = \sqrt[3]{1 + 2u}$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$,

- c) $\gamma = \sqrt[6]{u^2 + \bar{2}u}$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$,
d) $\delta = v^2 + \bar{2}$ nad $\mathbb{Z}_3$, kde v je kořen ireducibilního polynomu $f = x^2 + x + \bar{2}$.

Řešení:

a) $\alpha = \sqrt{1 + \sqrt{2}}$ nad $\mathbb{Q}$.

Při řešení využijeme definice 2.2. Nejprve nalezneme minimální polynom pro daný prvek a rozhodneme, zda tento polynom je separabilní nebo nikoliv. Při hledání minimálního polynomu budeme postupovat jak bylo uvedeno v [18].

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

Minimální polynom pro prvek α nad $\mathbb{Q}$ je $f = x^4 - 2x^2 - 1$. Následně hledáme kořeny polynomu f .

Zavedeme substituci $y = x^2$ a určíme kořeny polynomu $f = y^2 - 2y - 1$ vzhledem k y . Kořeny polynomu f vzhledem k y jsou

$$y_{1,2} = 1 \pm \sqrt{2}.$$

Polynom f má kořeny

$$x_{1,2,3,4} = \pm \sqrt{1 \pm \sqrt{2}}.$$

Odtud plyne, že polynom f je ireducibilní nad $\mathbb{Q}$ a má všechny kořeny jednoduché. Tedy je separabilní nad $\mathbb{Q}$, proto dle definice 2.2 je prvek α separabilní nad $\mathbb{Q}$.

b) $\beta = \sqrt[3]{\bar{1} + \bar{2}u}$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$.

Řešení je analogické jako v předcházejícím případě. Nejprve nalezneme minimální polynom pro prvek β nad $\mathbb{Z}_3(u)$.

$$\begin{aligned}\beta^0 &= \bar{1} \\ \beta^1 &= \sqrt[3]{\bar{1} + \bar{2}u} \\ \beta^2 &= \sqrt[3]{(\bar{1} + \bar{2}u)^2} \\ \beta^3 &= \bar{1} + \bar{2}u\end{aligned}$$

Odtud minimální polynom pro prvek β nad $\mathbb{Z}_3(u)$ je $f = x^3 + \bar{2} + u$. Zřejmě platí

$$f = x^3 + \bar{2} + u = x^3 + \sqrt[3]{(\bar{2} + u)^3} = \left(x + \sqrt[3]{\bar{2} + u}\right)^3.$$

Polynom f je nad tělesem $\mathbb{Z}_3(u)$ ireducibilní, ale má trojnásobný kořen, proto je nad $\mathbb{Z}_3(u)$ neseperabilní. Tedy i prvek β je nad $\mathbb{Z}_3(u)$ neseperabilní.

c) $\gamma = \sqrt[6]{u^2 + \bar{2}u}$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$,

Řešení je analogické jako v předcházejících případech.

$$\begin{aligned}\gamma^0 &= \bar{1} \\ \gamma^1 &= \sqrt[6]{u^2 + \bar{2}u} \\ \gamma^2 &= \sqrt[6]{(u^2 + \bar{2}u)^2} \\ \gamma^3 &= \sqrt[6]{(u^2 + \bar{2}u)^3} \\ \gamma^4 &= \sqrt[6]{(u^2 + \bar{2}u)^4} \\ \gamma^5 &= \sqrt[6]{(u^2 + \bar{2}u)^5} \\ \gamma^6 &= u^2 + \bar{2}u\end{aligned}$$

Minimální polynom pro prvek γ nad $\mathbb{Z}_3(u)$ je $f = x^6 - u^2 - \bar{2}u$.

Zřejmě platí

$$\begin{aligned}f &= x^6 - (u^2 + \bar{2}u) = \left(x^3 + \sqrt{u^2 + \bar{2}u}\right) \left(x^3 - \sqrt{u^2 + \bar{2}u}\right) = \\ &= \left(x + \sqrt[3]{\sqrt{u^2 + \bar{2}u}}\right)^3 \left(x + \sqrt[3]{\bar{2}\sqrt{u^2 + \bar{2}u}}\right)^3.\end{aligned}$$

Minimální polynom pro prvek γ nad $\mathbb{Z}_3(u)$ je neseperabilní, tedy i prvek γ je neseperabilní nad tělesem $\mathbb{Z}_3(u)$.

d) $\delta = v^2 + \bar{2}$ nad $\mathbb{Z}_3$, kde v je kořen ireducibilního polynomu $f = x^2 + x + \bar{2}$.

Nejprve nalezneme minimální polynom pro prvek δ nad $\mathbb{Z}_3$. Při úpravách využijeme toho, že prvek v je kořenem polynomu f , odtud $v^2 = \bar{2}v + \bar{1}$.

$$\begin{aligned}\delta^0 &= \bar{1} \\ \delta^1 &= v^2 + \bar{2} = (\bar{2}v + \bar{1}) + \bar{2} = \bar{2}v \\ \delta^2 &= (\bar{2}v)^2 = v^2 = \bar{2}v + \bar{1} = \delta^1 + \bar{1}\end{aligned}$$

Tedy minimální polynom pro prvek δ nad $\mathbb{Z}_3$ je $f = x^2 + \bar{2}x + \bar{2}$.

Ověříme, zda polynom f je ireducibilní nad $\mathbb{Z}_3$.

$$f(\bar{0}) = \bar{2}$$

$$f(\bar{1}) = \bar{2}$$

$$f(\bar{2}) = \bar{1}$$

Odtud plyne, že polynom f je ireducibilní nad $\mathbb{Z}_3$. Kořeny polynomu f jsou

$$x_{1,2} = \bar{2} \pm \sqrt{\bar{2}}.$$

Tedy polynom f je separabilní nad $\mathbb{Z}_3$, proto prvek δ je též separabilní nad $\mathbb{Z}_3$.

Příklad 2.4. Určete redukovaný stupeň polynomů nad uvedenými tělesy.

a) $f = x^6 + \bar{1}$ nad $\mathbb{Z}_3$,

b) $g = x^{10} + \bar{2}x^5 + \bar{1}$ nad $\mathbb{Z}_5$,

c) $h = \bar{2}x^6 + u$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$.

Řešení:

a) $f = x^6 + \bar{1}$ nad $\mathbb{Z}_3$.

Při řešení budeme vycházet z definice 2.4, podle které redukovaným stupněm polynomu rozumíme počet navzájem různých kořenů ireducibilního polynomu.

Nejprve rozhodneme, zda polynom f je ireducibilní nad $\mathbb{Z}_3$.

$$f(\bar{0}) = \bar{1}$$

$$f(\bar{1}) = \bar{2}$$

$$f(\bar{2}) = \bar{2}$$

Odtud plyne, že polynom f je ireducibilní nad $\mathbb{Z}_3$. Následně určíme kořeny polynomu f .

Zřejmě platí

$$\begin{aligned} f &= x^6 + \bar{1} = x^6 - \bar{2} = (x^3 - \sqrt{\bar{2}})(x^3 + \sqrt{\bar{2}}) = \\ &= \left(x^3 + \sqrt[3]{(\sqrt{\bar{2}})^3}\right) \left(x^3 + \sqrt[3]{(\bar{2}\sqrt{\bar{2}})^3}\right) = \left(x + \sqrt[3]{\sqrt{\bar{2}}}\right)^3 \left(x + \sqrt[3]{\bar{2}\sqrt{\bar{2}}}\right)^3. \end{aligned}$$

Polynom f má dva navzájem různé kořeny, tedy $st_r f = 2$.

b) $g = x^{10} + \bar{2}x^5 + \bar{1}$ nad $\mathbb{Z}_5$.

Budeme postupovat analogicky jako v časti a). Nejprve rozhodneme, zda polynom g je ireducibilní nad $\mathbb{Z}_5$.

$$f(\bar{0}) = \bar{1}$$

$$f(\bar{1}) = \bar{3}$$

$$f(\bar{2}) = \bar{2}$$

$$f(\bar{3}) = \bar{3}$$

$$f(\bar{4}) = \bar{1}$$

Odtud plyne, že polynom g je ireducibilní nad $\mathbb{Z}_5$. Následně budeme hledat kořeny polynomu g .

Zavedme substituci $y = x^5$. Polynom g můžeme přepsat do tvaru

$$g = y^2 + y + \bar{1}.$$

Nalezneme kořeny polynomu g vzhledem k y .

$$y_{1,2} = \frac{-\bar{1} \pm \sqrt{\bar{1} - \bar{4}}}{\bar{2}} = \frac{-\bar{1} \pm \sqrt{\bar{2}} \bar{3}}{\bar{2}} = \bar{2} \pm \bar{3}\sqrt{\bar{2}}$$

Tedy platí

$$g = (y - \bar{2} - \bar{3}\sqrt{\bar{2}})(y - \bar{2} + \bar{3}\sqrt{\bar{2}}).$$

Po dosazení do substituce dostaneme

$$g = (x^5 - \bar{2} - \bar{3}\sqrt{\bar{2}})(x^5 - \bar{2} + \bar{3}\sqrt{\bar{2}}) = \left(x + \sqrt[5]{\bar{3} + \bar{2}\sqrt{\bar{2}}}\right)^5 \left(x - \sqrt[5]{\bar{3} + \bar{2}\sqrt{\bar{2}}}\right)^5.$$

Zřejmě $st_r g = 2$.

c) $h = \bar{2}x^6 + u$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$.

Polynom h je zřejmě ireducibilní nad $\mathbb{Z}_3(u)$. Následně budeme hledat kořeny polynomu h pomocí postupných algebraických úprav.

$$\begin{aligned} g &= \bar{2}x^6 + u = \bar{2}(x^6 + \bar{2}u) = \bar{2}(x^6 - u) = \\ &= \bar{2}(x^3 - \sqrt{u})(x^3 + \sqrt{u}) = \bar{2}\left(x + \sqrt[3]{\bar{2}\sqrt{u}}\right)^3 \left(x + \sqrt[3]{\sqrt{u}}\right)^3. \end{aligned}$$

Polynom g má zřejmě dva různé kořeny, tedy $st_r g = 2$.

Příklad 2.5. Určete redukovaný stupeň nadtělesa nad uvedenými tělesy.

- a) $\mathbb{Z}_3(\alpha)$ nad $\mathbb{Z}_3$, kde $\alpha = \sqrt[4]{2} + \bar{1}$,
- b) $\mathbb{Z}_3(u, \beta)$ nad $\mathbb{Z}_3(u)$, kde $\beta = \sqrt[3]{u} + \bar{2}$, u je algebraický prvek nad $\mathbb{Z}_3$,
- c) $\mathbb{Z}_3(u, \gamma)$ nad $\mathbb{Z}_3(u)$, kde $\gamma = \sqrt[6]{u} + \bar{1}$, u je algebraický prvek nad $\mathbb{Z}_3$.

Řešení:

- a) $\mathbb{Z}_3(\alpha)$ nad $\mathbb{Z}_3$, kde $\alpha = \sqrt[4]{2} + \bar{1}$.

Při řešení vyjdeme z definice 2.5, podle které stačí najít redukovaný stupeň příslušného minimálního polynomu.

Nejprve určíme minimální polynom pro α nad $\mathbb{Z}_3$.

$$\begin{aligned}\alpha^0 &= \bar{1} \\ \alpha^1 &= \sqrt[4]{2} + \bar{1} \\ \alpha^2 &= \sqrt[4]{2^2} + \bar{2}\sqrt[4]{2} + \bar{1} \\ \alpha^3 &= \sqrt[4]{2^3} + \bar{2}\sqrt[4]{2^2} + \sqrt[4]{2} + \sqrt[4]{2^2} + \bar{2}\sqrt[4]{2} + \bar{1} = \sqrt[4]{2^3} + \bar{1} \\ \alpha^4 &= \bar{2} + \sqrt[4]{2} + \sqrt[4]{2^3} + \bar{1} + \underbrace{\sqrt[4]{2^3} + \bar{1}}_{\alpha^3} + \underbrace{\sqrt[4]{2} + \bar{1}}_{\alpha} + \bar{1} = \alpha^3 + \alpha + \bar{1}\end{aligned}$$

Odtud minimální polynom pro prvek α nad $\mathbb{Z}_3$ je

$$f = x^4 + \bar{2}x^3 + \bar{2}x + \bar{2}.$$

Derivace polynomu f je

$$f' = x^3 + \bar{2}.$$

Následně určíme $\text{NSD}(f, f')$.

$$\begin{array}{r} (x^4 + \bar{2}x^3 + \bar{2}x + \bar{2}) : (x^3 + \bar{2}) = x + \bar{2} \\ \hline -x^4 \qquad \qquad -\bar{2}x \\ \hline \qquad +\bar{2}x^3 \qquad \qquad +\bar{2} \\ \qquad -\bar{2}x^3 \qquad \qquad -\bar{1} \\ \hline \qquad \qquad \qquad \qquad \bar{1} \end{array}$$

Odtud plyne, že $\text{NSD}(f, f') = \bar{1}$. Tedy polynom f má všechny kořeny jednoduché a redukovaný stupeň minimálního polynomu prvku α nad $\mathbb{Z}_3$ je čtyři. Z čehož plyne, že $[\mathbb{Z}_3(\alpha) : \mathbb{Z}_3]_r = 4$.

b) $\mathbb{Z}_3(u, \beta)$ nad $\mathbb{Z}_3(u)$, kde $\beta = \sqrt[3]{u} + \bar{2}$,

Řešení bude analogické jako v části a). Nejprve nalezneme minimální polynom pro prvek β nad $\mathbb{Z}_3(u)$.

$$\beta^0 = \bar{1}$$

$$\beta^1 = \sqrt[3]{u} + \bar{2}$$

$$\beta^2 = \sqrt[3]{u^2} + \sqrt[3]{u} + \bar{1}$$

$$\beta^3 = u + \sqrt[3]{u^2} + \sqrt[3]{u} + \bar{2}\sqrt[3]{u^2} + \bar{2}\sqrt[3]{u} + \bar{2} = u + \bar{2}$$

Minimální polynom pro prvek β je

$$f = x^3 - u - \bar{2} = x^3 + \bar{2}u + \bar{1}.$$

Dále platí

$$f = x^3 + \bar{2}u + \bar{1} = \left(x + \sqrt[3]{\bar{2}u + \bar{1}}\right)^3.$$

Redukovaný stupeň polynomu f je jedna, tedy $[\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r = 1$.

c) $\mathbb{Z}_3(u, \gamma)$ nad $\mathbb{Z}_3(u)$, kde $\gamma = \sqrt[6]{u} + \bar{1}$.

Nalezneme minimální polynom pro prvek γ nad $\mathbb{Z}_3(u)$,

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

$$\gamma^1 = \sqrt[6]{u} + \bar{1}$$

$$\gamma^2 = \sqrt[6]{u^2} + \bar{2}\sqrt[6]{u} + \bar{1}$$

$$\gamma^3 = \sqrt[6]{u^3} + \bar{2}\sqrt[6]{u^2} + \sqrt[6]{u} + \sqrt[6]{u^2} + \bar{2}\sqrt[6]{u} + \bar{1} = \sqrt[6]{u^3} + \bar{1}$$

$$\gamma^4 = \sqrt[6]{u^4} + \sqrt[6]{u} + \sqrt[6]{u^3} + \bar{1}$$

$$\gamma^5 = \sqrt[6]{u^5} + \sqrt[6]{u^2} + \sqrt[6]{u^4} + \sqrt[6]{u} + \sqrt[6]{u^4} + \sqrt[6]{u} + \sqrt[6]{u^3} + \bar{1} = \sqrt[6]{u^5} + \bar{2}\sqrt[6]{u^4} + \sqrt[6]{u^3} + \bar{2}\sqrt[6]{u} + \bar{1}$$

$$\begin{aligned} \gamma^6 &= u + \bar{2}\sqrt[6]{u^5} + \sqrt[6]{u^4} + \sqrt[6]{u^3} + \sqrt[6]{u^2} + \sqrt[6]{u} + \sqrt[6]{u^5} + \bar{2}\sqrt[6]{u^4} + \sqrt[6]{u^3} + \sqrt[6]{u^2} + \bar{2}\sqrt[6]{u} + \bar{1} = \\ &= \bar{2}(\underbrace{\sqrt[6]{u^3} + \bar{1}}_{\alpha^3}) + u + \bar{2} = \bar{2}\alpha^3 + u + \bar{2} \end{aligned}$$

Minimální polynom pro γ nad $\mathbb{Z}_3(u)$ je

$$f = x^6 + x^3 + \bar{2}u + \bar{1}.$$

Následně budeme hledat kořeny polynomu f . Zavedme substituci $y = x^3$. Pak platí

$$f = y^2 + y + \bar{2}u + \bar{1}.$$

Kořeny polynomu f vzhledem k y jsou

$$y_{1,2} = \frac{-\bar{1} \pm \sqrt{\bar{1} - (\bar{2}u + \bar{1})}}{\bar{2}} = \frac{\bar{2} \pm \sqrt{u}}{\bar{2}} \frac{\bar{2}}{\bar{2}} = \bar{1} \pm \bar{2}\sqrt{u}.$$

Po dosazení do substituce dostaneme

$$f = (x^3 - \bar{2}\sqrt{u} - \bar{1}) (x^3 + \bar{2}\sqrt{u} - \bar{1}).$$

Odtud

$$f = \left(x + \sqrt[3]{\bar{2} + \sqrt{u}}\right)^3 \left(x + \sqrt[3]{\bar{2} + \bar{2}\sqrt{u}}\right)^3.$$

Polynom f má právě dva různé kořeny, tedy $[\mathbb{Z}_3(u, \gamma) : \mathbb{Z}_3(u)]_r = 2$.

Příklad 2.6. Určete redukovaný stupeň nadtělesa $\mathbb{Z}_3(u, \alpha, \beta)$ nad tělesem $\mathbb{Z}_3(u)$, kde $\alpha = \sqrt[3]{u + \bar{1}}$ a $\beta = \sqrt[6]{u} + \bar{1}$. Dále ověřte, zda je splněno tvrzení věty 2.4, a rozhodněte, zda dané rozšíření je separabilní.

Řešení:

Při řešení využijeme věty 2.3, podle které platí

$$[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)]_r = [\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)]_r \cdot [\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r.$$

Tedy stačí najít $[\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r$ a $[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)]_r$.

i) Určíme $[\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r$.

Nejprve hledáme minimální polynom pro α nad $\mathbb{Z}_3(u)$.

$$\begin{aligned}\alpha^0 &= \bar{1} \\ \alpha^1 &= \sqrt[3]{u + \bar{1}} \\ \alpha^2 &= \sqrt[3]{(u + \bar{1})^2} \\ \alpha^3 &= u + \bar{1}\end{aligned}$$

Minimální polynom pro α nad $\mathbb{Z}_3(u)$ je

$$f = x^3 + \bar{2}u + \bar{2} = \left(x + \sqrt[3]{\bar{2}u + \bar{2}}\right)^3.$$

Odtud $[\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r = 1$.

ii) Určíme $[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)]_r$.

Využijeme výsledku z předešlého příkladu, podle kterého minimální polynom pro prvek β nad $\mathbb{Z}_3(u, \alpha)$ můžeme zapsat ve tvaru

$$f = \left(x + \sqrt[3]{2 + \sqrt{u}}\right)^3 \left(x + \sqrt[3]{2 + 2\sqrt{u}}\right)^3.$$

Odtud plyne, že $[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)]_r = 2$.

S využitím dvou předcházejících výsledků dostaneme

$$[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)]_r = [\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)]_r [\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r = 1 \cdot 2 = 2.$$

Zbývá ověření věty 2.4. Při aplikaci věty na tento příklad dostaneme

$$[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)] = [\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)]_r \cdot 3^l. \quad (*)$$

Musíme dokázat, že existuje $l \in \mathbb{N}_0$ splňující předcházející vztah.

Nejprve určíme $[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)]$. Podle věty o vícenásobném rozšíření, uvedené v [18], platí

$$[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)] = [\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)] \cdot [\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)].$$

Minimální polynom pro prvek α nad $\mathbb{Z}_3(u)$ je třetího stupně, tedy $[\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)] = 3$. Minimální polynom pro prvek β nad $\mathbb{Z}_3(u, \alpha)$ je šestého stupně, tedy $[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u, \alpha)] = 6$.

Z předešlého plyne, že $[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)] = 6 \cdot 3 = 18$.

Po dosazení do vztahu (*) dostaneme

$$18 = 2 \cdot 3^l,$$

$$9 = 3^l,$$

$$l = 2.$$

Tedy hledané přirozené číslo l existuje a je rovno dvěma.

Posledním úkolem je rozhodnout, zda $\mathbb{Z}_3(u, \alpha, \beta)$ je separabilní rozšíření tělesa $\mathbb{Z}_3(u)$.

Dle věty 2.6 je konečné rozšíření separabilní, právě když je roven stupeň rozšíření redukovanému stupni rozšíření.

Dále platí

$$[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)] = 18,$$

$$[\mathbb{Z}_3(u, \alpha, \beta) : \mathbb{Z}_3(u)]_r = 2.$$

Je zřejmé, že stupeň rozšíření $\mathbb{Z}_3(u, \alpha, \beta)$ tělesa $\mathbb{Z}_3(u)$ je různý od příslušného redukovaného stupně rozšíření. Tedy dle věty 2.6 $\mathbb{Z}_3(u, \alpha, \beta)$ není separabilní rozšíření tělesa $\mathbb{Z}_3(u)$.

Příklad 2.7. Rozhodněte, zda $\mathbb{Z}_5(\alpha)$ je separabilní rozšíření tělesa $\mathbb{Z}_5$, kde $\alpha = \sqrt[3]{2} + \bar{1}$.

Řešení:

Řešení bude vycházet z věty 2.6. Nejprve nalezneme minimální polynom pro prvek α nad $\mathbb{Z}_5$.

$$\alpha^0 = \bar{1}$$

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

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

$$\alpha^3 = \bar{2} + \bar{3}\sqrt[3]{2^2} + \bar{3}\sqrt[3]{2} + \bar{1} = \underbrace{\bar{3}\sqrt[3]{2^2} + \sqrt[3]{2} + \bar{3}}_{\bar{3}\alpha^2} + \bar{3} + \underbrace{\bar{2}\sqrt[3]{2} + \bar{2}}_{\bar{2}\alpha} = \bar{3}\alpha^2 + \bar{2}\alpha + \bar{3}$$

Minimální polynom pro α nad $\mathbb{Z}_5$ je

$$f = x^3 + \bar{2}x^2 + \bar{3}x + \bar{2}.$$

Polynom f je třetího stupně, tedy $[\mathbb{Z}_5(\alpha) : \mathbb{Z}_5] = 3$.

Následně určíme derivaci polynomu f .

$$f' = \bar{3}x^2 + \bar{4}x + \bar{3}.$$

Dále určíme NSD(f, f').

$$\begin{array}{r} (x^3 + \bar{2}x^2 + \bar{3}x + \bar{2}) : (\bar{3}x^2 + \bar{4}x + \bar{3}) = \bar{2}x + \bar{3} \\ \hline -x^3 - \bar{3}x^2 - x \\ \hline \bar{4}x^2 + \bar{2}x + \bar{2} \\ \hline -\bar{4}x^2 - \bar{2}x - \bar{4} \\ \hline \bar{3} \sim \bar{1} \end{array}$$

Odtud plyne, že $\text{NSD}(f, f') = \bar{1}$, proto polynom f má všechny kořeny jednoduché, a tedy $[\mathbb{Z}_5(\alpha) : \mathbb{Z}_5]_r = 3$.

Rozšíření $\mathbb{Z}_5(\alpha)$ tělesa $\mathbb{Z}_5$ je separabilní, jelikož jsou splněny podmínky věty 2.6.

Příklad 2.8. Rozhodněte, zda těleso $\mathbb{Z}_3$ je dokonalé.

Řešení:

Při řešení využijeme větu 2.11. Z této věty plyne, že každý z polynomů

$$x^3, x^3 + \bar{1}, x^3 + \bar{2}$$

musí mít kořen v $\mathbb{Z}_3$.

Zřejmě platí

$\bar{0} \in \mathbb{Z}_3$ je kořenem polynomu x^3 ,

$\bar{1} \in \mathbb{Z}_3$ je kořenem polynomu $x^3 + \bar{2}$,

$\bar{2} \in \mathbb{Z}_3$ je kořenem polynomu $x^3 + \bar{1}$.

Z věty 2.11 plyne, že těleso $\mathbb{Z}_3$ je dokonalé.

Cvičení

Cvičení 2.1. Rozhodněte, zda uvedený polynom je separabilní nad uvedeným tělesem.

- a) $f = x^3 - 7x - 6$ nad $\mathbb{Q}$,
- b) $g = x^6 - 3$ nad $\mathbb{Q}$,
- c) $h = x^6 + x^3 + u$ nad $\mathbb{Z}_3(u)$, kde u je algebraický prvek nad $\mathbb{Z}_3$,
- d) $k = \bar{2}x^4 + \bar{2}x^2 + x + \bar{2}$ nad $\mathbb{Z}_3$.

[a) kořenem polynomu f je zřejmě $1 \in \mathbb{Q}$, polynom f není ireducibilní nad $\mathbb{Q}$, tedy polynom f není separabilní nad $\mathbb{Q}$; b) rovnice $g = 0$ je binomickou rovnicí, jejíž všechny kořeny jsou různé, ani jeden z těchto kořenů není prvkem tělesa $\mathbb{Q}$, tedy polynom g je separabilní nad $\mathbb{Q}$; c) kořeny polynomu h jsou $\bar{2}\sqrt[3]{\bar{2} + \sqrt{\bar{1} + \bar{2}u}}$, $\bar{2}\sqrt[3]{\bar{2} + \bar{2}\sqrt{\bar{1} + \bar{2}u}}$, tyto kořeny jsou trojnásobné, polynom je zřejmě ireducibilní nad $\mathbb{Z}_3(u)$, tedy polynom h je neseperabilní nad $\mathbb{Z}_3(u)$; d) polynom k je ireducibilní nad $\mathbb{Z}_3$, $\text{NSD}(k, k') = \bar{1}$, tedy polynom k je separabilní nad $\mathbb{Z}_3$]

Cvičení 2.2. Rozhodněte, zda daný prvek je separabilní nad uvedeným tělesem.

- a) $\alpha = \sqrt{2} + \sqrt{3}$ nad $\mathbb{Q}$,
- b) $\beta = \sqrt[3]{u} + \bar{2}u$ nad $\mathbb{Z}_3(u)$,
- c) $\gamma = \sqrt{\bar{2}} + v$ nad $\mathbb{Z}_3$, kde v je kořenem ireducibilního polynomu $f = x^2 + x + \bar{2}$ nad $\mathbb{Z}_3$.

[a) minimální polynom pro α nad $\mathbb{Q}$ je polynom $f = x^4 - 10x^2 + 1$, který je separabilní nad $\mathbb{Q}$, tedy prvek α je separabilní nad $\mathbb{Q}$; b) polynom $g = x^3 + u^2 + \bar{2}u$ je minimální polynom pro prvek β nad $\mathbb{Z}_3(u)$, polynom g je neseperabilní, tedy prvek β je neseperabilní nad $\mathbb{Z}_3(u)$; c) polynom $h = x^4 + x^2 + x$ je minimální polynom pro prvek γ nad $\mathbb{Z}_3$, polynom h je reducibilní, proto není separabilní nad $\mathbb{Z}_3$, tedy prvek γ není separabilní nad $\mathbb{Z}_3$]

Cvičení 2.3. Určete všechny polynomy třetího stupně ze $\mathbb{Z}_3[x]$, které jsou nad $\mathbb{Z}_3$ separabilní.

$[x^3 + \bar{2}x + \bar{1}, x^3 + \bar{2}x + \bar{2}, x^3 + x^2 + \bar{2}, x^3 + x^2 + x + \bar{2}, x^3 + x^2 + \bar{2}x + \bar{1}, x^3 + \bar{2}x^2 + \bar{1}, x^3 + \bar{2}x^2 + x + \bar{1}, x^3 + \bar{2}x^2 + \bar{2}x + \bar{2}]$

Cvičení 2.4. Určete redukovaný stupeň polynomu nad uvedeným tělesem.

- a) $f = x^5 + 5$ nad $\mathbb{Q}$,

b) $g = x^6 + \bar{2}x^3 + \bar{2}$ nad $\mathbb{Z}_3$,

c) $h = x^3 - u$ nad $\mathbb{Z}_3(u)$.

[a) $st_r f = 5$; b) $st_r g = 2$; c) $st_r h = 1$]

Cvičení 2.5. Určete redukovaný stupeň nadtělesa nad uvedeným tělesem.

a) $\mathbb{Z}_3(u, \alpha)$ nad $\mathbb{Z}_3(u)$, kde $\alpha = \sqrt[3]{u+1}$, u je algebraický prvek nad $\mathbb{Z}_3$,

b) $\mathbb{Z}_3(u, \beta)$ nad $\mathbb{Z}_3(u)$, kde $\beta = \sqrt[6]{u-2}$, u je algebraický prvek nad $\mathbb{Z}_3$.

[a) $[\mathbb{Z}_3(u, \alpha) : \mathbb{Z}_3(u)]_r = 1$; b) $[\mathbb{Z}_3(u, \beta) : \mathbb{Z}_3(u)]_r = 2$]

3 Galoisovy grupy a jejich vlastnosti

V této kapitole využijeme pojmů z předešlých dvou kapitol k zavedení Galoisova rozšíření tělesa. Uvedeme vlastnosti automorfizmů, na základě nichž budeme konstruovat Galoisovu grupu. V následující definici bude zaveden pojem Galoisovo rozšíření.

Definice 3.1. Každé konečné separabilní normální rozšíření $\mathbb{K}$ tělesa $\mathbb{F}$ nazveme **Galoisovým rozšířením** tělesa $\mathbb{F}$.

Nechť $\mathbb{K}$ je rozšíření tělesa $\mathbb{F}$. Označme $G(\mathbb{K}, \mathbb{F})$ množinu všech automorfizmů tělesa $\mathbb{K}$, pro které platí, že všechny prvky z tělesa $\mathbb{F}$ zobrazí identicky na sebe. Takové automorfizmy nazveme **$\mathbb{F}$ -automorfizmy**. Je zřejmé, že $G(\mathbb{K}, \mathbb{F})$ je grupou vzhledem k operaci skládání zobrazení.

Definice 3.2. Grupou $G(\mathbb{K}, \mathbb{F})$ všech $\mathbb{F}$ -automorfizmů Galoisova rozšíření $\mathbb{K}$ tělesa $\mathbb{F}$ nazveme **Galoisovou grupou** $\mathbb{K}$ nad $\mathbb{F}$.

Definice 3.3. Řekneme, že prvky α, β z nadtělesa $\mathbb{K}$ tělesa $\mathbb{F}$ jsou **konjugované** nad $\mathbb{F}$, jestliže mají stejné minimální polynomy.

Ve větách 3.1 a 3.2 bude popsán vztah mezi prvky Galoisovy grupy a konjugovanými prvky.

Věta 3.1. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a nechť $\varphi \in G(\mathbb{K}, \mathbb{F})$. Pak pro každý prvek $\alpha \in \mathbb{K}$ platí, že prvky $\alpha, \varphi(\alpha)$ jsou konjugované nad $\mathbb{F}$.*

Důkaz. Nechť $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{F}[x]$ je minimální polynom prvku α . Pak $f(\varphi(\alpha)) = a_n(\varphi(\alpha))^n + \dots + a_1(\varphi(\alpha)) + a_0 = \varphi(f(\alpha)) = 0$. Tedy f je minimální polynom prvku $\varphi(\alpha)$ a prvky $\alpha, \varphi(\alpha)$ jsou konjugované nad $\mathbb{F}$ [4]. $\square$

Lemma 3.1. *Nechť $\mathbb{K}$ je algebraické rozšíření nekonečného tělesa $\mathbb{F}$ a nechť prvky $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ jsou separabilní nad $\mathbb{F}$. Je-li $\beta \in \mathbb{K}$, pak existuje prvek $\vartheta \in \mathbb{K}$ takový, že $\mathbb{F}(\alpha_1, \dots, \alpha_n, \beta) = \mathbb{F}(\vartheta)$.*

Definice 3.4. Prvek ϑ z předchozího lemmatu nazveme **primitivním prvkem** tělesa $\mathbb{F}(\alpha_1, \dots, \alpha_n, \beta)$ nad $\mathbb{F}$.

Věta 3.2. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a prvky $\alpha, \beta \in \mathbb{K}$ jsou konjugované nad $\mathbb{F}$. Pak existuje prvek $\varphi \in G(\mathbb{K}, \mathbb{F})$ takový, že $\beta = \varphi(\alpha)$.*

Důkaz. Předpokládejme, že prvky $\alpha, \beta \in \mathbb{K}$ jsou konjugované nad $\mathbb{F}$. Pak tělesa $\mathbb{F}(\alpha), \mathbb{F}(\beta)$ jsou kořenová tělesa minimálního polynomu prvků α, β . Každá dvě kořenová nad tělesa ireducibilního polynomu nad $\mathbb{F}$ jsou $\mathbb{F}$ -izomorfní. Proto existuje $\mathbb{F}$ -izomorfismus $\eta : \mathbb{F}(\alpha) \rightarrow \mathbb{F}(\beta)$ takový, že $\eta(\alpha) = \beta$. Jelikož $\mathbb{K}$ je konečné separabilní rozšíření tělesa $\mathbb{F}(\alpha)$, existuje podle lematu 3.1 primitivní prvek ϑ tělesa $\mathbb{K}$ nad $\mathbb{F}(\alpha)$. Nechť f je minimální polynom prvku ϑ nad $\mathbb{F}(\alpha)$ a nechť $\psi : \mathbb{F}(\alpha)[x] \rightarrow \mathbb{F}(\beta)[x]$ izomorfismus indukovaný izomorfismem η , pro nějž platí $\psi(h) = \eta(a_0)x^0 + \dots + \eta(a_n)x^n$ pro $h \in \mathbb{F}(\alpha)[x]$. Je-li g minimální polynom prvku ϑ nad $\mathbb{F}$, pak $f|g$ v $\mathbb{F}(\alpha)[x]$ a $\psi(f)|g$ vzhledem k tomu, že $\psi(g) = g$. Jelikož polynom g má kořen ϑ v $\mathbb{K}$, leží všechny kořeny polynomu g a všechny kořeny polynomu $\psi(f)$ v tělese $\mathbb{K}$. Tedy existuje izomorfismus $\varphi : \mathbb{F}(\alpha, \vartheta) \rightarrow \mathbb{F}(\beta, \vartheta')$ takový, že $\varphi|_{\mathbb{F}(\alpha)} = \eta$ a $\varphi(\vartheta) = \vartheta'$, kde ϑ' je nějaký kořen polynomu $\psi(f)$. Jelikož $\mathbb{F}(\alpha, \vartheta) = \mathbb{K}$, platí $\varphi \in G(\mathbb{K}, \mathbb{F})$ [4]. $\square$

Následující dvě věty charakterizují Galoisovy grupy, určují počet prvků a jejich řád.

Věta 3.3. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$. Pak $|G(\mathbb{K}, \mathbb{F})| = [\mathbb{K} : \mathbb{F}]$.*

Důkaz. Nechť ϑ je primitivní prvek tělesa $\mathbb{K}$ nad $\mathbb{F}$ a $\vartheta_1, \dots, \vartheta_n$ jsou kořeny minimálního polynomu f prvku ϑ nad $\mathbb{F}$. Nechť φ je libovolný prvek z $G(\mathbb{K}, \mathbb{F})$. Dle věty 3.1 $\varphi(\vartheta) = \vartheta_j$, pro některé $j = 1, \dots, n$, tedy $|G(\mathbb{K}, \mathbb{F})| \leq n = [\mathbb{K} : \mathbb{F}]$. Na druhé straně dle věty 3.2 pro každé $j = 1, \dots, n$ existuje prvek $\varphi \in G(\mathbb{K}, \mathbb{F})$ takový, že $\varphi(\vartheta) = \vartheta_j$. Proto $[\mathbb{K} : \mathbb{F}] = n \leq |G(\mathbb{K}, \mathbb{F})|$, tedy $|G(\mathbb{K}, \mathbb{F})| = [\mathbb{K} : \mathbb{F}]$ [4]. $\square$

Věta 3.4. *Nechť $\mathbb{K}$ je normální rozšíření stupně n nad tělesem $\mathbb{F}$. Pak $G(\mathbb{K}, \mathbb{F})$ je konečná grupa řádu n .*

Důkaz. Nechť $\mathbb{K}$ je normální rozšíření stupně n nad tělesem $\mathbb{F}$. Pak existuje prvek β takový, že $\mathbb{K} = \mathbb{F}(\beta)$. Nechť n je stupeň minimálního polynomu f prvku β nad $\mathbb{F}$. Stupeň rozšíření $\mathbb{K}$ nad $\mathbb{F}$ je n a každý prvek $\alpha \in \mathbb{K}$ lze zapsat ve tvaru

$$\alpha = a_0 + a_1\beta + \dots + a_{n-1}\beta^{n-1}, \quad a_0, \dots, a_{n-1} \in \mathbb{F}.$$

Každý automorfismus $\varphi \in G(\mathbb{K}, \mathbb{F})$ zobrazí kořen β na některý kořen polynomu f . Tedy každému $\varphi \in G(\mathbb{K}, \mathbb{F})$ odpovídá některý kořen polynomu f .

Předpokládejme, že β' je některý kořen polynomu f . Jelikož $\mathbb{K}$ je normální rozšíření a $\beta \in \mathbb{K}$, tak i $\beta' \in \mathbb{K}$. Uvažujme zobrazení $\psi : \mathbb{K} \rightarrow \mathbb{K}$ definované vztahem

$$\psi(\alpha) = a_0 + a_1\beta' + \dots + a_{n-1}\beta'^{n-1}, \quad a_0, \dots, a_{n-1} \in \mathbb{F}.$$

Zřejmě $\psi \in G(\mathbb{K}, \mathbb{F})$.

Existuje tedy bijekce mezi automorfizmy z $G(\mathbb{K}, \mathbb{F})$ a kořeny polynomu f , tedy řád $G(\mathbb{K}, \mathbb{F})$ je roven počtu kořenů f , tj. n [12]. $\square$

Definice 3.5. Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a nechť H je podgrupa Galoisovy grupy $G(\mathbb{K}, \mathbb{F})$. Množinu $\mathbb{K}(G, H) = \{\alpha \in \mathbb{K} : \varphi(\alpha) = \alpha \ \forall \varphi \in H\}$ nazveme **invariantním tělesem** podgrupy H .

Dále budou uvedeny dvě věty bez důkazu, které využijeme k důkazu věty 3.7. Důkazy těchto vět lze nalézt např. v [4].

Věta 3.5. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a nechť H je podgrupa Galoisovy grupy $G(\mathbb{K}, \mathbb{F})$. Pak $\mathbb{K}(G, H)$ je podtěleso tělesa $\mathbb{K}$ obsahující $\mathbb{F}$. Je-li H normální podgrupa grupy G , pak $\mathbb{K}(G, H)$ je normální rozšíření tělesa $\mathbb{F}$.*

Věta 3.6. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a nechť $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ je meztěleso. Je-li $G(\mathbb{K}, \mathbb{F})$ Galoisova grupa tělesa $\mathbb{K}$ nad $\mathbb{F}$, pak $G(\mathbb{K}, \mathbb{L}) = \{\varphi \in G(\mathbb{K}, \mathbb{F}); \varphi|_{\mathbb{L}} = 1_{\mathbb{L}}\}$ je podgrupa grupy $G(\mathbb{K}, \mathbb{F})$. Je-li $\mathbb{L}$ normální rozšíření tělesa $\mathbb{F}$, pak $G(\mathbb{K}, \mathbb{L})$ je normální podgrupa v $G(\mathbb{K}, \mathbb{F})$ a $G(\mathbb{L}, \mathbb{F}) \cong G(\mathbb{K}, \mathbb{F})/G(\mathbb{K}, \mathbb{L})$.*

Následně bude uvedena hlavní věta Galoisovy teorie. Význam této věty je značný, jelikož převádí zkoumání normálních rozšíření na zkoumání podgrup Galoisovy grupy.

Věta 3.7. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a $G(\mathbb{K}, \mathbb{F})$ Galoisova grupa $\mathbb{K}$ nad $\mathbb{F}$. Nechť Φ je zobrazení množiny všech podgrup grupy $G(\mathbb{K}, \mathbb{F})$ do množiny všech meztěles $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ definované pro $H \leq G(\mathbb{K}, \mathbb{F})$ předpisem $\Phi(H) = \mathbb{K}(G, H) = \{\alpha \in \mathbb{K} : \varphi(\alpha) = \alpha \text{ pro každé } \varphi \in H\}$. Nechť Ψ je zobrazení množiny všech meztěles $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ do množiny všech podgrup grupy $G(\mathbb{K}, \mathbb{F})$ dané předpisem $\Psi(\mathbb{L}) = G(\mathbb{K}, \mathbb{L})$.*

Pak platí:

- i) Φ a Ψ jsou bijekce, které jsou navzájem inverzní,*
- ii) Φ a Ψ indukují vzájemně jednoznačná zobrazení mezi množinami všech normálních podgrup grupy $G(\mathbb{K}, \mathbb{F})$ a všech meztěles normálních nad $\mathbb{F}$,*
- iii) $[\Phi(H) : \mathbb{F}] = [G : H]$, $[\mathbb{K} : \Phi(H)] = |H|$ pro každou podgrupu H grupy $G(\mathbb{K}, \mathbb{F})$,*
- iv) $[\mathbb{L} : \mathbb{F}] = [G : \Psi(\mathbb{L})]$, $[\mathbb{K} : \mathbb{L}] = |\Psi(\mathbb{L})|$ pro každé meztěleso $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$.*

Důkaz.

a) Jelikož $\Psi(\mathbb{L}) = G(\mathbb{K}, \mathbb{L})$, je dle věty 3.3 $|\Psi(\mathbb{L})| = [\mathbb{K} : \mathbb{L}]$.

b) Ukážeme, že pro každou podgrupu $H \leq G(\mathbb{K}, \mathbb{F})$ je $[\mathbb{K} : \Phi(H)] = |H|$. Označme $\mathbb{L} = \Phi(H)$. Je-li $K = G(\mathbb{K}, \mathbb{L})$ Galoisova grupa $\mathbb{K}$ nad $\mathbb{L}$, pak zřejmě $H \leq K$. Necht' dále ϑ je primitivní prvek tělesa $\mathbb{K}$ nad $\mathbb{L}$. Uvažujme polynom $f \in \mathbb{L}[x]$ stupně n , který je minimálním polynomem prvku ϑ . Zřejmě platí $[\mathbb{K} : \mathbb{L}] = n$ a z věty 3.3 plyne $[\mathbb{K} : \mathbb{L}] = |K|$. Je-li $H = \{1 = \varphi_1, \varphi_2, \dots, \varphi_h\}$ a $g = \prod_{i=1}^h (x - \varphi_i(\vartheta))$, pak pro každé $\varphi \in H$ platí $H = \{\varphi\varphi_1, \varphi\varphi_2, \dots, \varphi\varphi_h\}$. Označme $\Psi : \mathbb{K}[x] \rightarrow \mathbb{K}[x]$ izomorfismus indukovaný φ . Platí $\Psi(g) = \prod_{i=1}^h (x - \varphi\varphi_i(\vartheta)) = g$, a tedy $g \in \mathbb{L}[x]$. Polynom g je dělitelný polynomem f , jelikož $g(\vartheta) = 0$. Tedy $st f = |K| \leq st g = |H|$. Odtud $H = K$, tudíž $[\mathbb{K} : \Phi(H)] = [\mathbb{K} : \mathbb{L}] = |K| = |H|$.

c) Dle věty 3.3 je $[\mathbb{K} : \mathbb{F}] = |G|$ a dle a) platí $[\mathbb{K} : \mathbb{L}] = |\Psi(\mathbb{L})|$. Odtud dostaneme

$$[\mathbb{L} : \mathbb{F}] = \frac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{K} : \mathbb{L}]} = \frac{|G|}{|\Psi(\mathbb{L})|} = [G : \Psi(\mathbb{L})].$$

Tím bylo dokázáno tvrzení *iv*).

d) Dle b) je $[\mathbb{K} : \Psi(H)] = |H|$, z čeho vyplývá

$$[\Psi(H) : \mathbb{F}] = \frac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{K} : \Psi(H)]} = \frac{|G|}{|H|} = [G : H].$$

Tím bylo dokázáno tvrzení *iii*).

e) Nyní již lze snadno dokázat tvrzení *i*). Necht' $\Psi\Phi(H) = \{\varphi \in G(\mathbb{K}, \mathbb{F}) : \varphi \upharpoonright_{\Phi(H)} = 1_{\Phi(H)}\} = \{\varphi \in G(\mathbb{K}, \mathbb{F}) : \varphi(\alpha) = \alpha \text{ pro každé } \alpha \in \Phi(H)\} \supseteq H$ a $\Phi\Psi(\mathbb{L}) = \{\alpha \in \mathbb{K} : \varphi(\alpha) = \alpha \text{ pro každé } \varphi \in \Phi(\mathbb{L})\} \supseteq \mathbb{L}$. Podle *iii*) a *iv*) platí

$$[\Psi\Phi(H) : H] = \frac{[G : H]}{[G : \Psi\Phi(H)]} = \frac{[G : H]}{[\Phi(H) : \mathbb{F}]} = \frac{[G : H]}{[G : H]} = 1,$$

$$[\Phi\Psi(\mathbb{L}) : \mathbb{L}] = \frac{[\mathbb{K} : \mathbb{L}]}{[\mathbb{K} : \Phi\Psi(\mathbb{L})]} = \frac{[\mathbb{K} : \mathbb{L}]}{|\Psi(\mathbb{L})|} = \frac{[\mathbb{K} : \mathbb{L}]}{[\mathbb{K} : \mathbb{L}]} = 1.$$

Tedy pro každou podgrupu H grupy $G(\mathbb{K}, \mathbb{F})$ je $\Psi\Phi(H) = H$ a pro každé meztěleso $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ je $\Phi\Psi(\mathbb{L}) = \mathbb{L}$.

f) Tvrzení *ii*) vyplývá z tvrzení *i*) a z vět 3.5 a 3.6 [4].

□

Důsledek 3.1. *Nechť $\mathbb{K}$ je Galoisovo rozšíření tělesa $\mathbb{F}$ a nechť $G(\mathbb{K}, \mathbb{F})$ je Galoisova grupa tělesa $\mathbb{K}$ nad $\mathbb{F}$. Pak prvek $\alpha \in \mathbb{K}$ leží v $\mathbb{F}$, právě když $\varphi(\alpha) = \alpha$ pro každé $\varphi \in G(\mathbb{K}, \mathbb{F})$.*

Následující věta dále charakterizuje zobrazení z věty 3.7. Důkaz této věty lze najít např. v [9].

Věta 3.8. *Zobrazení $\Psi : \mathbb{L} \rightarrow G(\mathbb{K}, \mathbb{L})$ (z věty 3.7) zobrazuje svaz všech meztěles $\mathbb{L}_1, \mathbb{L}_2, \dots$ na svaz všech podgrup grupy $G(\mathbb{K}, \mathbb{F})$. Jestliže $\mathbb{L}_1 \subset \mathbb{L}_2$, pak $G(\mathbb{K}, \mathbb{L}_1) \supset G(\mathbb{K}, \mathbb{L}_2)$.*

Řešené příklady

Příklad 3.1. Nalezněte konjugované prvky k daným prvkům nad uvedeným tělesem.

- a) $\alpha = \sqrt[3]{3} + 1$ nad $\mathbb{Q}$,
- b) $\beta = \sqrt[3]{4}$ nad $\mathbb{Z}_5$,
- c) $\gamma = \sqrt[3]{1 + \sqrt{3}}$ nad $\mathbb{Q}$.

Řešení:

- a) $\alpha = \sqrt[3]{3} + 1$ nad $\mathbb{Q}$.

Dle definice 3.3 konjugované prvky jsou ty, které nad daným tělesem mají stejné minimální polynomy.

Nejprve určíme minimální polynom pro α nad $\mathbb{Q}$.

$$\begin{aligned}\alpha^0 &= 1 \\ \alpha^1 &= \sqrt[3]{3} + 1 \\ \alpha^2 &= \sqrt[3]{3^2} + 2\sqrt[3]{3} + 1 \\ \alpha^3 &= 3 + 3\sqrt[3]{3^2} + 3\sqrt[3]{3} + 1 = 3(\underbrace{\sqrt[3]{3^2} + 2\sqrt[3]{3} + 1}_{\alpha^2}) - 3\sqrt[3]{3} + 1 = 3\alpha^2 - 3(\underbrace{\sqrt[3]{3} + 1}_{\alpha}) + 4 = \\ &= 3\alpha^2 - 3\alpha + 4\end{aligned}$$

Minimální polynom pro prvek α nad $\mathbb{Q}$ je

$$f = x^3 - 3x^2 + 3x - 4.$$

Kořeny polynomu f jsou

$$\begin{aligned}x_1 &= \sqrt[3]{3} + 1, \\ x_2 &= \sqrt[3]{3} \left(\frac{-1+i\sqrt{3}}{2} \right) + 1, \\ x_3 &= \sqrt[3]{3} \left(\frac{-1-i\sqrt{3}}{2} \right) + 1.\end{aligned}$$

Z věty 3.1 plyne, že prvky x_1, x_2, x_3 jsou konjugované s prvkem α nad $\mathbb{Q}$.

- b) $\beta = \sqrt[3]{4}$ nad $\mathbb{Z}_5$.

Při řešení postupujeme analogicky jako v předcházejícím případě.

Určíme minimální polynom pro prvek β nad $\mathbb{Z}_5$.

$$\begin{aligned}\beta^0 &= \bar{1} \\ \beta^1 &= \sqrt[3]{4}\end{aligned}$$

$$\beta^2 = \sqrt[3]{4^2}$$

$$\beta^3 = \bar{4}$$

Minimální polynom pro prvek β nad $\mathbb{Z}_5$ je $g = x^3 - \bar{4}$, který můžeme rozložit do následujícího tvaru

$$g = \left(x - \sqrt[3]{\bar{4}}\right) \left(x^2 + \sqrt[3]{\bar{4}}x + \sqrt[3]{\bar{4}^2}\right).$$

Kořeny polynomu g jsou

$$x_1 = \sqrt[3]{\bar{4}},$$

$$x_{2,3} = \frac{-\sqrt[3]{\bar{4}} \pm \sqrt{\sqrt[3]{\bar{4}^2} - \bar{4} \sqrt[3]{\bar{4}^2}}}{2} = \frac{-\sqrt[3]{\bar{4}} \pm \sqrt{2} \sqrt[3]{\bar{4}}}{2} \cdot \frac{\bar{3}}{\bar{3}} = \sqrt[3]{\bar{4}} \left(\bar{2} \pm \bar{3}\sqrt{\bar{2}}\right).$$

Prvky x_1, x_2, x_3 jsou konjugované s prvkem β nad $\mathbb{Z}_5$, dle věty 3.1.

$$\text{c) } \gamma = \sqrt[3]{1 + \sqrt{3}} \text{ nad } \mathbb{Q}.$$

Určíme minimální polynom pro prvek γ nad $\mathbb{Q}$.

$$\gamma^0 = 1$$

$$\gamma^1 = \sqrt[3]{1 + \sqrt{3}}$$

$$\gamma^2 = \sqrt[3]{(1 + \sqrt{3})^2}$$

$$\gamma^3 = 1 + \sqrt{3}$$

$$\gamma^4 = \sqrt[3]{(1 + \sqrt{3})^4}$$

$$\gamma^5 = \sqrt[3]{(1 + \sqrt{3})^5}$$

$$\gamma^6 = 1 + 2\sqrt{3} + 3 = 2(\underbrace{1 + \sqrt{3}}_{\gamma^3}) + 2 = 2\gamma^3 + 2$$

Minimální polynom pro prvek γ nad $\mathbb{Q}$ je

$$h = x^6 - 2x^3 - 2.$$

Kořeny polynomu h jsou

$$x_1 = \sqrt[3]{1 + \sqrt{3}},$$

$$x_2 = \sqrt[3]{1 - \sqrt{3}},$$

$$x_3 = \sqrt[3]{1 + \sqrt{3}} \left(\frac{-1+i\sqrt{3}}{2}\right),$$

$$x_4 = \sqrt[3]{1 + \sqrt{3}} \left(\frac{-1-i\sqrt{3}}{2}\right),$$

$$x_5 = \sqrt[3]{1 - \sqrt{3}} \left(\frac{-1+i\sqrt{3}}{2}\right),$$

$$x_6 = \sqrt[3]{1 - \sqrt{3}} \left(\frac{-1-i\sqrt{3}}{2}\right).$$

Tedy prvky $x_1, \dots, x_6$ jsou konjugované s prvkem γ nad $\mathbb{Q}$.

Příklad 3.2. Určete Galoisovu grupu uvedeného rozšíření. Dále určete zobrazení z věty 3.7 mezi všemi podgrupami a podtělesy.

- a) $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ nad $\mathbb{Q}$,
- b) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$.

Řešení:

- a) $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ nad $\mathbb{Q}$.

Dle věty 3.1 každý $\mathbb{Q}$ -automorfismus, tedy prvek Galoisovy grupy $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}), \mathbb{Q})$, musí zobrazit $\sqrt[3]{2}$ na prvek s ním konjugovaný a $i\sqrt{3}$ na prvek s ním konjugovaný.

1. Určíme všechny konjugované prvky s prvkem $i\sqrt{3}$ nad $\mathbb{Q}$.

Minimální polynom pro prvek $i\sqrt{3}$ nad $\mathbb{Q}$ je

$$f = x^2 + 3.$$

Kořeny polynomu f jsou

$$x_{1,2} = \pm i\sqrt{3}.$$

Odtud prvky x_1, x_2 jsou konjugované s prvkem $i\sqrt{3}$ nad $\mathbb{Q}$.

2. Určíme všechny konjugované prvky s $\sqrt[3]{2}$ nad $\mathbb{Q}(i\sqrt{3})$.

Minimální polynom pro $\sqrt[3]{2}$ nad $\mathbb{Q}(i\sqrt{3})$ je

$$g = x^3 - 2.$$

Kořeny polynomu g jsou

$$\begin{aligned} x_1 &= \sqrt[3]{2}, \\ x_{2,3} &= \sqrt[3]{2} \left(\frac{-1 \pm i\sqrt{3}}{2} \right). \end{aligned}$$

Tedy prvky x_1, x_2, x_3 jsou konjugované s prvkem $\sqrt[3]{2}$ nad $\mathbb{Q}(i\sqrt{3})$.

Odtud prvky Galoisovy grupy $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}), \mathbb{Q})$ zřejmě jsou

$$\begin{aligned} \varphi_1 &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ i\sqrt{3} \mapsto i\sqrt{3} \end{cases}, & \varphi_2 &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ i\sqrt{3} \mapsto -i\sqrt{3} \end{cases}, \\ \varphi_3 &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \left(\frac{-1+i\sqrt{3}}{2} \right) \\ i\sqrt{3} \mapsto i\sqrt{3} \end{cases}, & \varphi_4 &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \left(\frac{-1+i\sqrt{3}}{2} \right) \\ i\sqrt{3} \mapsto -i\sqrt{3} \end{cases}, \end{aligned}$$

$$\varphi_5 = \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \left(\frac{-1-i\sqrt{3}}{2} \right) \\ i\sqrt{3} \mapsto i\sqrt{3} \end{cases}, \quad \varphi_6 = \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \left(\frac{-1-i\sqrt{3}}{2} \right) \\ i\sqrt{3} \mapsto -i\sqrt{3} \end{cases}.$$

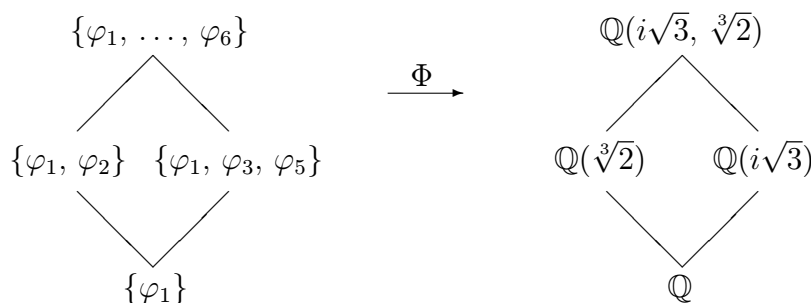
Níže bude uvedena tabulka pro operaci skládání zobrazení mezi prvky Galoisovy grupy $G(\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}), \mathbb{Q})$.

$\circ$	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_1	φ_4	φ_3	φ_6	φ_5
φ_3	φ_3	φ_4	φ_5	φ_6	φ_1	φ_2
φ_4	φ_4	φ_3	φ_6	φ_5	φ_2	φ_1
φ_5	φ_5	φ_6	φ_1	φ_2	φ_3	φ_4
φ_6	φ_6	φ_5	φ_2	φ_1	φ_4	φ_3

Z výše uvedené tabulky určíme všechny podgrupy Galoisovy grupy $G(\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}), \mathbb{Q})$.

- a) jednoprvková $(\{\varphi_1\}, \circ)$,
- b) dvouprvková $(\{\varphi_1, \varphi_2\}, \circ)$,
- c) tříprvková $(\{\varphi_1, \varphi_3, \varphi_5\}, \circ)$,
- d) šestiprvková $(\{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}, \circ) = G(\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}), \mathbb{Q})$.

Posledním úkolem je najít zobrazení Φ ze svazu všech podgrup do svazu všech meztěles.



Vztah mezi podgrupou a meztělesem v zobrazení Φ je takový, že všechny prvky z dané podgrupy Galoisovy grupy $G(\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}), \mathbb{Q})$ „nechají na místě“ všechny prvky z příslušného meztělesa.

Tedy zřejmě platí

$$\begin{aligned} \Phi(\{\varphi_1\}) &= \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}), & \Phi(\{\varphi_1, \varphi_3, \varphi_5\}) &= \mathbb{Q}(i\sqrt{3}), \\ \Phi(\{\varphi_1, \varphi_2\}) &= \mathbb{Q}(\sqrt[3]{2}), & \Phi(\{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}) &= \mathbb{Q}. \end{aligned}$$

b) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$.

1. Určíme všechny konjugované prvky s $\sqrt{2}$ nad $\mathbb{Q}$.

Minimální polynom pro prvek $\sqrt{2}$ nad $\mathbb{Q}$ je

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

Kořeny polynomu f jsou

$$x_{1,2} = \pm\sqrt{2}.$$

Odtud prvky x_1, x_2 jsou konjugované s prvkem $\sqrt{2}$ nad $\mathbb{Q}$.

2. Určíme všechny konjugované prvky s $\sqrt{3}$ nad $\mathbb{Q}(\sqrt{2})$.

Minimální polynom pro $\sqrt{3}$ nad $\mathbb{Q}(\sqrt{2})$ je

$$g = x^2 - 3.$$

Kořeny polynomu g jsou

$$x_{1,2} = \pm\sqrt{3}.$$

Tedy prvky x_1, x_2 jsou konjugované s prvkem $\sqrt{3}$ nad $\mathbb{Q}(\sqrt{2})$.

Odtud prvky Galoisovy grupy $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$ jsou

$$\varphi_1 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \varphi_2 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases},$$

$$\varphi_3 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \varphi_4 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

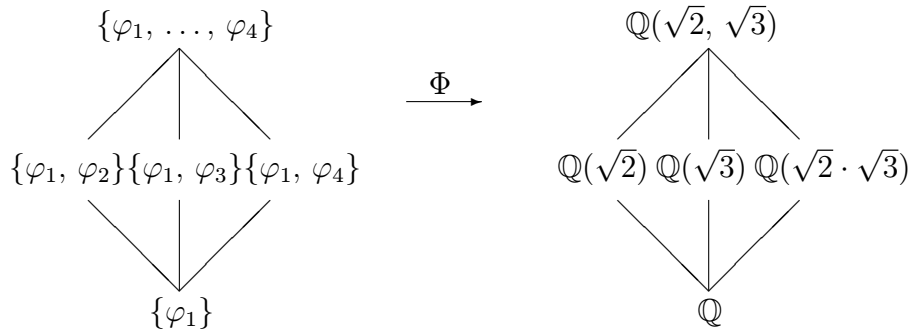
Následně bude uvedena tabulka pro operaci skládání zobrazení mezi prvky Galoisovy grupy $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$.

$\circ$	φ_1	φ_2	φ_3	φ_4
φ_1	φ_1	φ_2	φ_3	φ_4
φ_2	φ_2	φ_1	φ_4	φ_3
φ_3	φ_3	φ_4	φ_1	φ_2
φ_4	φ_4	φ_3	φ_2	φ_1

Z výše uvedené tabulky určíme všechny podgrupy Galoisovy grupy $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$.

- a) jednoprvková $(\{\varphi_1\}, \circ)$,
- b) dvouprvkové $(\{\varphi_1, \varphi_2\}, \circ)$, $(\{\varphi_1, \varphi_3\}, \circ)$, $(\{\varphi_1, \varphi_4\}, \circ)$,
- c) čtyřprvková $(\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}, \circ)$.

Posledním úkolem je najít zobrazení Φ ze svazu všech podgrup do svazu všech meztěles.



Vzhledem k definici zobrazení Φ z věty 3.7 platí

$$\begin{aligned} \Phi(\{\varphi_1\}) &= \mathbb{Q}(\sqrt{2}, \sqrt{3}), & \Phi(\{\varphi_1, \varphi_2\}) &= \mathbb{Q}(\sqrt{2}), \\ \Phi(\{\varphi_1, \varphi_3\}) &= \mathbb{Q}(\sqrt{3}), & \Phi(\{\varphi_1, \varphi_4\}) &= \mathbb{Q}(\sqrt{2} \cdot \sqrt{3}), \\ \Phi(\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}) &= \mathbb{Q}. \end{aligned}$$

Cvičení

Cvičení 3.1. Určete konjugované prvky k daným prvkům nad uvedeným tělesem.

- a) $\alpha = \sqrt[4]{2}$ nad $\mathbb{Q}$,
- b) $\beta = \sqrt[3]{1 + \sqrt{2}}$ nad $\mathbb{Z}_5$,
- c) $\gamma = \bar{2}\sqrt{2} + \bar{2}$ nad $\mathbb{Z}_3$.

[a) prvky $x_{1,2} = \pm \sqrt[4]{2}$, $x_{3,4} = \pm i \sqrt[4]{2}$ jsou konjugované s prvkem α nad $\mathbb{Q}$; b) prvky $x_{1,2} = \sqrt[3]{1 \pm \sqrt{2}}$, $x_{3,4} = \sqrt[3]{1 \pm \sqrt{2}} (\bar{2} + \bar{3}\sqrt{2})$, $x_{5,6} = \sqrt[3]{1 \pm \sqrt{2}} (\bar{2} - \bar{3}\sqrt{2})$ jsou konjugované s prvkem β nad $\mathbb{Z}_5$; c) prvky $x_{1,2} = \bar{2} \pm \sqrt{2}$ jsou konjugované s prvkem γ nad $\mathbb{Z}_3$]

Cvičení 3.2. Určete Galoisovu grupu uvedeného rozšíření. Dále určete zobrazení z věty 3.7 mezi všemi podgrupami a podtělesy.

- a) $\mathbb{Z}_5 \left(\sqrt{2}, \sqrt[3]{2} \right)$ nad $\mathbb{Z}_5$,
- b) $\mathbb{Z}_3 \left(\sqrt[4]{2} \right)$ nad $\mathbb{Z}_3$.

[a) prvky Galoisovy grupy $G \left(\mathbb{Z}_3 \left(\sqrt{2}, \sqrt[3]{2} \right), \mathbb{Z}_3 \right)$ jsou

$$\varphi_1 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases}, \quad \varphi_2 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}(\bar{2} + \bar{3}\sqrt{2}) \end{cases}, \quad \varphi_3 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}(\bar{2} - \bar{3}\sqrt{2}) \end{cases},$$

$$\varphi_4 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases}, \quad \varphi_5 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}(\bar{2} + \bar{3}\sqrt{2}) \end{cases}, \quad \varphi_6 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}(\bar{2} - \bar{3}\sqrt{2}) \end{cases}.$$

Podgrupy Galoisovy grupy $G \left(\mathbb{Z}_5 \left(\sqrt{2}, \sqrt[3]{2} \right), \mathbb{Z}_5 \right)$ jsou

$$(\{\varphi_1\}, \circ), (\{\varphi_1, \varphi_4\}, \circ), (\{\varphi_1, \varphi_2, \varphi_3\}, \circ), (\{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}, \circ).$$

Pro zobrazení Φ platí

$$\begin{aligned} \Phi(\{\varphi_1\}) &= \mathbb{Z}_5 \left(\sqrt{2}, \sqrt[3]{2} \right), & \Phi(\{\varphi_1, \varphi_4\}) &= \mathbb{Z}_5 \left(\sqrt[3]{2} \right), \\ \Phi(\{\varphi_1, \varphi_2, \varphi_3\}) &= \mathbb{Z}_5 \left(\sqrt{2} \right), & \Phi(\{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}) &= \mathbb{Z}_5. \end{aligned}$$

b) prvky Galoisovy grupy $G \left(\mathbb{Z}_3 \left(\sqrt[4]{2} \right), \mathbb{Z}_3 \right)$ jsou

$$\begin{aligned} \varphi_1 : \sqrt[4]{2} &\mapsto \sqrt[4]{2} & \varphi_2 : \sqrt[4]{2} &\mapsto -\sqrt[4]{2}, \\ \varphi_3 : \sqrt[4]{2} &\mapsto \sqrt{2}\sqrt[4]{2}, & \varphi_4 : \sqrt[4]{2} &\mapsto -\sqrt{2}\sqrt[4]{2}. \end{aligned}$$

Podgrupy Galoisovy grupy $G\left(\mathbb{Z}_5\left(\sqrt[4]{2}\right), \mathbb{Z}_5\right)$ jsou

$$(\{\varphi_1\}, \circ), (\{\varphi_1, \varphi_2\}, \circ), (\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}, \circ).$$

Pro zobrazení Φ platí

$$\begin{aligned}\Phi(\{\varphi_1\}) &= \mathbb{Z}_3\left(\sqrt[4]{2}\right), & \Phi(\{\varphi_1, \varphi_2\}) &= \mathbb{Z}_3\left(\sqrt{2}\right), \\ \Phi(\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}) &= \mathbb{Z}_3.\end{aligned}$$

4 Galoisovo cyklické rozšíření

V této kapitole se budeme zabývat vlastnostmi Galoisovy grupy separabilních polynomů. Dále budeme studovat vlastnosti Galoisových cyklických grup a Galoisova cyklického rozšíření.

Definice 4.1. Galoisovou grupou separabilního polynomu $f \in \mathbb{F}[x]$ rozumíme Galoisovu grupu rozkladového tělesa $\mathbb{K}$ polynomu f nad $\mathbb{F}$.

Definice 4.2. Galoisovo rozšíření $\mathbb{K}$ tělesa $\mathbb{F}$ nazveme **Galoisovým komutativním rozšířením**, je-li příslušná Galoisova grupa $G(\mathbb{K}, \mathbb{F})$ abelovská.

Definice 4.3. Galoisovo rozšíření $\mathbb{K}$ tělesa $\mathbb{F}$ nazveme **Galoisovým cyklickým rozšířením**, je-li příslušná Galoisova grupa $G(\mathbb{K}, \mathbb{F})$ cyklická.

Definice 4.4. Těleso, které nemá žádná vlastní podtělesa, nazveme **prvotělesem**.

Nyní bude uvedena věta bez důkazu, kterou využijeme k důkazu věty 4.2.

Věta 4.1. *Nechť $\mathbb{F}$ je prvotěleso, n přirozené číslo, pro které platí, že není dělitelné charakteristikou tělesa $\mathbb{F}$. Dále nechť $\mathbb{K}$ je rozkladové těleso polynomu $f = x^n - 1$. Pak množina všech kořenů polynomu f tvoří cyklickou podgrupu multiplikativní grupy tělesa $\mathbb{K}$ generovanou libovolnou primitivní n -tou odmocninou z jedné.*

Důkaz věty 4.1 lze nalézt např. v [4].

Definice 4.5. Zobrazení $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ udávající počet všech přirozených čísel menších než n a současně nesoudělných s n nazveme **Eulerovou funkcí**.

Věta 4.2. *Nechť $\mathbb{F}$ je těleso a n je přirozené číslo, které není dělitelné charakteristikou tělesa $\mathbb{F}$. Galoisova grupa polynomu $f = x^n - 1$ je izomorfní s některou podgrupou grupy všech jednotek okruhu $\mathbb{Z}_n$. Rozkladové těleso $\mathbb{K}$ polynomu f je komutativním rozšířením tělesa $\mathbb{F}$. Je-li $\mathbb{F} = \mathbb{Q}$, pak Galoisova grupa polynomu f je izomorfní s multiplikativní grupou všech jednotek okruhu $\mathbb{Z}_n$ a má řád $\varphi(n)$, kde φ je Eulerova funkce.*

Důkaz. Nechť ϑ je primitivní n -tá odmocnina z jedné. Zřejmě $\mathbb{K} = \mathbb{F}(\vartheta)$. Nechť $\varrho \in G(\mathbb{K}, \mathbb{F})$, pak $\varrho(\vartheta)$ je konjugovaný prvek k prvku ϑ . Tedy $\varrho(\vartheta)$ je primitivní n -tá odmocnina z jedné. Zřejmě z předcházející věty a z věty 17.5 z [3] plyne existence $k \in \mathbb{N}$

nesoudělného s n , pro které platí $\varrho(\vartheta) = \vartheta^k$. Označme $\bar{k}$ třídu $k + \{n\}$ faktorového okruhu $\mathbb{Z}_n$ obsahující k a položme $\Phi(\varrho) = \bar{k}$, kde Φ je zobrazení grupy $G(\mathbb{K}, \mathbb{F})$ do grupy všech jednotek okruhu $\mathbb{Z}_n$. Nechť $\psi \in G(\mathbb{K}, \mathbb{F})$ je libovolný další prvek, $\psi(\vartheta) = \vartheta^l$, kde $l \in \mathbb{N}$. Tedy $\varrho\psi(\vartheta) = \varrho(\vartheta^l) = \vartheta^{kl}$. Odtud $\Phi(\varrho\psi) = \overline{k^l} = \overline{k}^l = \Phi(\varrho)\Phi(\psi)$ a tedy Φ je homomorfismus. Je-li ϱ takový prvek, že $\Phi(\varrho) = \bar{1}$, je $\varrho(\vartheta) = \vartheta$ a $\varrho = 1_{\mathbb{K}}$. Tedy $\text{Ker } \Phi = \{1\}$.

Zbývá dokázat, že pro $\mathbb{F} = \mathbb{Q}$ je homomorfismus Φ surjektivní. Nechť $\bar{k} \in \mathbb{Z}_n$ je libovolná jednotka. Zřejmě $\text{NSD}(n, k) = 1$, proto ϑ^k je primitivní n -tá odmocnina z jedné. Nechť $\alpha_1, \alpha_2, \dots, \alpha_k$ jsou právě všechny n -té odmocniny z jedné. Uvažujme polynom $f_n = (x - \alpha_1)(x - \alpha_2) \cdot \dots \cdot (x - \alpha_k)$. Tento polynom je ireducibilní (to dokazuje věta 39.16 z [4]). Jelikož polynom f_n je ireducibilní, pak prvky ϑ a ϑ^k jsou konjugované nad $\mathbb{Q}$. Z věty 3.2 plyne existence prvku $\varrho \in G(\mathbb{K}, \mathbb{F})$, pro který platí $\varrho(\vartheta) = \vartheta^k$. Proto $\Phi(\varrho) = \bar{k}$ a rovnost $|G(\mathbb{K}, \mathbb{F})| = \varphi(n)$ plyne z definice Eulerovy funkce [4]. $\square$

V následující větě je charakterizováno za jaké podmínky je příslušné rozkladové těleso polynomu cyklické rozšíření. Tato věta bude uvedena bez důkazu, jelikož je přímým důsledkem předcházející věty.

Věta 4.3. *Nechť $\mathbb{F}$ je těleso a q prvočíslo, různé od charakteristiky tělesa $\mathbb{F}$. Pak rozkladové těleso $\mathbb{K}$ polynomu $x^q - 1$ je cyklickým rozšířením tělesa $\mathbb{F}$. Je-li $\mathbb{F} = \mathbb{Q}$, pak Galoisova grupa polynomu $x^q - 1$ je izomorfní s multiplikativní grupou tělesa $\mathbb{Z}_q$.*

Řešené příklady

Příklad 4.1. Určete Galoisovu grupu separabilního polynomu nad uvedeným tělesem.

a) $f = x^4 - 2x^2 + 2$ nad $\mathbb{Q}(i)$,

b) $g = x^6 - \bar{3}$ nad $\mathbb{Z}_5$.

Řešení:

a) $f = x^4 - 2x^2 + 2$ nad $\mathbb{Q}(i)$.

Dle definice 4.1 Galoisovou grupou separabilního polynomu nad uvedeným tělesem rozumíme Galoisovu grupu rozkladového tělesa tohoto polynomu nad daným tělesem.

1. Určíme rozkladové těleso polynomu f nad $\mathbb{Q}(i)$.

Nejprve nalezneme kořeny polynomu f .

Zavedme substituci $y = x^2$. Tedy $f = y^2 - 2y + 2$.

Kořeny polynomu f vzhledem k proměnné y jsou

$$y = 1 \pm i.$$

Po zpětném dasazení do substituce dostaneme kořeny polynomu f vzhledem k x , tj.

$$x_{1,2} = \pm\sqrt{1+i},$$

$$x_{3,4} = \pm\sqrt{1-i}.$$

Označme $\alpha = \sqrt{1+i}$, $\beta = \sqrt{1-i}$.

Tedy rozkladové těleso polynomu f je $\mathbb{Q}(i, \alpha, \beta)$.

2. Určíme prvky Galoisovy grupy $G(\mathbb{Q}(i, \alpha, \beta), \mathbb{Q}(i))$.

i) Minimální polynom pro prvek α nad $\mathbb{Q}(i)$ je

$$f_1 = x^2 - (1+i).$$

Kořeny polynomu f_1 jsou

$$x_{1,2} = \pm\alpha.$$

ii) Minimální polynom pro prvek β nad $\mathbb{Q}(i)$ je

$$f_2 = x^2 - (1-i).$$

Kořeny polynomu f_2 jsou

$$x_{1,2} = \pm\beta.$$

Odtud prvky Galoisovy grupy $G(\mathbb{Q}(i, \alpha, \beta), \mathbb{Q}(i))$ jsou

$$\begin{aligned}\varphi_1 &= \begin{cases} \alpha \mapsto \alpha \\ \beta \mapsto \beta \end{cases}, & \varphi_2 &= \begin{cases} \alpha \mapsto \alpha \\ \beta \mapsto -\beta \end{cases}, \\ \varphi_3 &= \begin{cases} \alpha \mapsto -\alpha \\ \beta \mapsto \beta \end{cases}, & \varphi_4 &= \begin{cases} \alpha \mapsto -\alpha \\ \beta \mapsto -\beta \end{cases}.\end{aligned}$$

Tabulka pro operaci skládání zobrazení mezi prvky grupy $G(\mathbb{Q}(i, \alpha, \beta), \mathbb{Q}(i))$ je ve tvaru.

$\circ$	φ_1	φ_2	φ_3	φ_4
φ_1	φ_1	φ_2	φ_3	φ_4
φ_2	φ_2	φ_1	φ_4	φ_3
φ_3	φ_3	φ_4	φ_1	φ_2
φ_4	φ_4	φ_3	φ_2	φ_1

b) $g = x^6 - \bar{3}$ nad $\mathbb{Z}_5$.

Budeme postupovat analogicky jako v části a).

1. Určíme rozkladové těleso polynomu g nad $\mathbb{Z}_5$.

Nejprve nalezneme kořeny polynomu g .

Zřejmě lze polynom g rozložit do následujícího tvaru

$$g = x^6 - \bar{3} = (x^3 - \sqrt{\bar{3}})(x^3 + \sqrt{\bar{3}}).$$

Dále platí

$$g = (x - \sqrt[6]{\bar{3}})(x^2 + \sqrt[6]{\bar{3}}x + \sqrt[6]{\bar{3}^2})(x + \sqrt[6]{\bar{3}})(x^2 - \sqrt[6]{\bar{3}}x + \sqrt[6]{\bar{3}^2}).$$

Odtud kořeny polynomu g jsou

$$\begin{aligned}x_1 &= \sqrt[6]{\bar{3}}, \\ x_{2,3} &= \frac{-\sqrt[6]{\bar{3}} \pm \sqrt{\sqrt[6]{\bar{3}^2} - 4\sqrt[6]{\bar{3}^2}}}{2} = \sqrt[6]{\bar{3}} \left(\frac{-1 \pm \sqrt{2}}{2} \right) \cdot \frac{\bar{3}}{3} = \sqrt[6]{\bar{3}} \left(2 \pm \bar{3}\sqrt{2} \right), \\ x_4 &= -\sqrt[6]{\bar{3}},\end{aligned}$$

$$x_{5,6} = \frac{\sqrt[6]{3} \pm \sqrt{\sqrt[6]{3^2} - 4\sqrt[6]{3^2}}}{2} = \sqrt[6]{3} \left(\frac{1 \pm \sqrt{2}}{2} \right) \cdot \frac{3}{3} = \sqrt[6]{3} \left(\bar{3} \pm \bar{3}\sqrt{2} \right).$$

Tedy rozkladové těleso polynomu g je $\mathbb{Z}_5 \left(\sqrt{2}, \sqrt[6]{3} \right)$.

2. Určíme prvky Galoisovy grupy $G \left(\mathbb{Z}_5 \left(\sqrt{2}, \sqrt[6]{3} \right), \mathbb{Z}_5 \right)$.

i) Minimální polynom pro $\sqrt{2}$ nad $\mathbb{Z}_5$ je

$$g_1 = x^2 - \bar{2}.$$

Kořeny polynomu g_1 jsou

$$x_{1,2} = \pm \sqrt{2},$$

ii) Minimální polynom pro $\sqrt[6]{3}$ je

$$g_2 = x^6 - \bar{3}.$$

Kořeny polynomu g_2 jsou

$$\begin{aligned} x_1 &= \sqrt[6]{3}, \\ x_2 &= \sqrt[6]{3} \left(\bar{2} + \bar{3}\sqrt{2} \right), \\ x_3 &= \sqrt[6]{3} \left(\bar{2} - \bar{3}\sqrt{2} \right), \\ x_4 &= -\sqrt[6]{3}, \\ x_5 &= \sqrt[6]{3} \left(\bar{3} + \bar{3}\sqrt{2} \right), \\ x_6 &= \sqrt[6]{3} \left(\bar{3} - \bar{3}\sqrt{2} \right). \end{aligned}$$

Zřejmě prvky Galoisovy grupy $G \left(\mathbb{Z}_5 \left(\sqrt{2}, \sqrt[6]{3} \right), \mathbb{Z}_5 \right)$ jsou

$$\begin{aligned} \varphi_1 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3} \end{cases}, & \varphi_2 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[6]{3} \mapsto -\sqrt[6]{3} \end{cases}, \\ \varphi_3 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(\bar{2} + \bar{3}\sqrt{2}) \end{cases}, & \varphi_4 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(\bar{2} - \bar{3}\sqrt{2}) \end{cases}, \\ \varphi_5 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(\bar{3} + \bar{3}\sqrt{2}) \end{cases}, & \varphi_6 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(\bar{3} - \bar{3}\sqrt{2}) \end{cases}, \\ \varphi_7 &= \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3} \end{cases}, & \varphi_8 &= \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[6]{3} \mapsto -\sqrt[6]{3} \end{cases}, \end{aligned}$$

$$\varphi_9 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(2 + 3\sqrt{2}) \end{cases}, \quad \varphi_{10} = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(2 - 3\sqrt{2}) \end{cases},$$

$$\varphi_{11} = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(3 + 3\sqrt{2}) \end{cases}, \quad \varphi_{12} = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[6]{3} \mapsto \sqrt[6]{3}(3 - 3\sqrt{2}) \end{cases}.$$

Tabulka pro skládání zobrazení mezi prvky Galoisovy grupy $G\left(\mathbb{Z}_5\left(\sqrt{2}, \sqrt[6]{3}\right), \mathbb{Z}_5\right)$ je ve tvaru.

$\circ$	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8	φ_9	φ_{10}	φ_{11}	φ_{12}
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8	φ_9	φ_{10}	φ_{11}	φ_{12}
φ_2	φ_2	φ_1	φ_6	φ_5	φ_4	φ_3	φ_8	φ_7	φ_{12}	φ_{11}	φ_{10}	φ_9
φ_3	φ_3	φ_6	φ_4	φ_1	φ_2	φ_5	φ_9	φ_{12}	φ_{10}	φ_7	φ_8	φ_{11}
φ_4	φ_4	φ_5	φ_1	φ_3	φ_6	φ_2	φ_{10}	φ_{11}	φ_7	φ_9	φ_{12}	φ_8
φ_5	φ_5	φ_4	φ_2	φ_6	φ_3	φ_1	φ_{11}	φ_{10}	φ_8	φ_{12}	φ_9	φ_7
φ_6	φ_6	φ_3	φ_5	φ_2	φ_1	φ_4	φ_{12}	φ_9	φ_{11}	φ_8	φ_7	φ_{10}
φ_7	φ_7	φ_8	φ_9	φ_{10}	φ_{11}	φ_{12}	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_8	φ_8	φ_7	φ_{12}	φ_{11}	φ_{10}	φ_9	φ_2	φ_1	φ_6	φ_5	φ_4	φ_3
φ_9	φ_9	φ_{12}	φ_{10}	φ_7	φ_8	φ_{11}	φ_3	φ_6	φ_4	φ_1	φ_2	φ_5
φ_{10}	φ_{10}	φ_{11}	φ_7	φ_9	φ_{12}	φ_8	φ_4	φ_5	φ_1	φ_3	φ_6	φ_2
φ_{11}	φ_{11}	φ_{10}	φ_8	φ_{12}	φ_9	φ_7	φ_5	φ_4	φ_2	φ_6	φ_3	φ_1
φ_{12}	φ_{12}	φ_9	φ_{11}	φ_8	φ_7	φ_{10}	φ_6	φ_3	φ_5	φ_2	φ_1	φ_4

Příklad 4.2. Rozhodněte, zda dané Galoisovo rozšíření je komutativní, resp. cyklické.

- $\mathbb{Z}_5\left(\sqrt[4]{2}\right)$ nad $\mathbb{Z}_5$,
- $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ nad $\mathbb{Q}$.

Řešení:

- $\mathbb{Z}_5\left(\sqrt[4]{2}\right)$ nad $\mathbb{Z}_5$.

Dle definice 4.3 platí, že Galoisovo rozšíření je cyklické, jestliže Galoisova grupa rozšíření je cyklická.

Nejprve určíme prvky Galoisovy grupy $G\left(\mathbb{Z}_5\left(\sqrt[4]{2}\right), \mathbb{Z}_5\right)$.

Minimální polynom pro prvek $\sqrt[4]{2}$ nad $\mathbb{Z}_5$ je

$$f = x^4 - \bar{2}.$$

Polynom f lze rozložit do následujícího tvaru

$$f = (x^2 - \sqrt{2})(x^2 - \bar{4}\sqrt{2}) = (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x + \bar{2}\sqrt[4]{2})(x - \bar{2}\sqrt[4]{2}).$$

Odtud prvky Galoisovy grupy $G(\mathbb{Z}_5(\sqrt[4]{2}), \mathbb{Z}_5)$ jsou

$$\varphi_1 : \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad \varphi_2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2},$$

$$\varphi_3 : \sqrt[4]{2} \mapsto \bar{2}\sqrt[4]{2}, \quad \varphi_4 : \sqrt[4]{2} \mapsto -\bar{2}\sqrt[4]{2}.$$

Tabulka pro operaci skládání zobrazení mezi prvky grupy $G(\mathbb{Z}_5(\sqrt[4]{2}), \mathbb{Z}_5)$ je ve tvaru

$\circ$	φ_1	φ_2	φ_3	φ_4
φ_1	φ_1	φ_2	φ_3	φ_4
φ_2	φ_2	φ_1	φ_4	φ_3
φ_3	φ_3	φ_4	φ_2	φ_1
φ_4	φ_4	φ_3	φ_1	φ_2

Zřejmě Galoisova grupa $G(\mathbb{Z}_5(\sqrt[4]{2}), \mathbb{Z}_5)$ je abelovská a dále má dvě jednoprvkové množiny generátorů $\{\varphi_3\}$, $\{\varphi_4\}$, proto je cyklická. Tedy dle definic 4.2 a 4.3 je Galoisovo rozšíření $\mathbb{Z}_5(\sqrt[4]{2})$ tělesa $\mathbb{Z}_5$ komutativní a cyklické.

b) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ nad $\mathbb{Q}$.

Při řešení budeme postupovat analogicky jako v části a).

Minimální polynomy pro prvky $\sqrt{5}$, $\sqrt{7}$ nad $\mathbb{Q}$ jsou

$$f = x^2 - 5, \quad g = x^2 - 7.$$

Odtud určíme prvky Galoisovy grupy $G(\mathbb{Q}(\sqrt{5}, \sqrt{7}), \mathbb{Q})$.

$$\varphi_1 = \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ \sqrt{7} \mapsto \sqrt{7} \end{cases}, \quad \varphi_2 = \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ \sqrt{7} \mapsto -\sqrt{7} \end{cases},$$

$$\varphi_3 = \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ \sqrt{7} \mapsto \sqrt{7} \end{cases}, \quad \varphi_4 = \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ \sqrt{7} \mapsto -\sqrt{7} \end{cases}.$$

Tabulka pro operaci skládání zobrazení mezi prvky grupy $G(\mathbb{Q}(\sqrt{5}, \sqrt{7}), \mathbb{Q})$ je ve tvaru

$\circ$	φ_1	φ_2	φ_3	φ_4
φ_1	φ_1	φ_2	φ_3	φ_4
φ_2	φ_2	φ_1	φ_4	φ_3
φ_3	φ_3	φ_4	φ_1	φ_2
φ_4	φ_4	φ_3	φ_2	φ_1

Galoisova grupa $G(\mathbb{Q}(\sqrt{5}, \sqrt{7}), \mathbb{Q})$ je abelovská, ale nemá žádné jednoprvkové množiny generátorů, proto není cyklická. Tedy Galoisovo rozšíření $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ tělesa $\mathbb{Q}$ je komutativní, ale není cyklické.

Cvičení

Cvičení 4.1. Určete Galoisovu grupu separabilního polynomu nad uvedeným tělesem.

a) $f = x^4 - 5$ nad $\mathbb{Q}$,

b) $g = x^7 - 5$ nad $\mathbb{Q}(\xi)$, kde ξ je primitivní sedmá odmocnina z jedné.

[a) rozkladové těleso polynomu f nad $\mathbb{Q}$ je $\mathbb{Q}(i, \sqrt[4]{5})$, prvky Galoisovy grupy $G(\mathbb{Q}(i, \sqrt[4]{5}), \mathbb{Q})$ jsou ve tvaru

$$\begin{aligned}\varphi_1 &= \begin{cases} \sqrt[4]{5} \mapsto \sqrt[4]{5} \\ i \mapsto i \end{cases}, & \varphi_2 &= \begin{cases} \sqrt[4]{5} \mapsto -\sqrt[4]{5} \\ i \mapsto i \end{cases}, & \varphi_3 &= \begin{cases} \sqrt[4]{5}i \mapsto \sqrt[4]{5} \\ i \mapsto i \end{cases}, \\ \varphi_4 &= \begin{cases} \sqrt[4]{5} \mapsto -i\sqrt[4]{5} \\ i \mapsto i \end{cases}, & \varphi_5 &= \begin{cases} \sqrt[4]{5} \mapsto \sqrt[4]{5} \\ i \mapsto -i \end{cases}, & \varphi_6 &= \begin{cases} \sqrt[4]{5} \mapsto -\sqrt[4]{5} \\ i \mapsto -i \end{cases}, \\ \varphi_7 &= \begin{cases} \sqrt[4]{5}i \mapsto \sqrt[4]{5} \\ i \mapsto -i \end{cases}, & \varphi_8 &= \begin{cases} \sqrt[4]{5} \mapsto -i\sqrt[4]{5} \\ i \mapsto -i \end{cases}.\end{aligned}$$

b) rozkladové těleso polynomu g nad $\mathbb{Q}(\xi)$ je $\mathbb{Q}(\xi, \sqrt[7]{5})$, prvky Galoisovy grupy $G(\mathbb{Q}(\xi, \sqrt[7]{5}), \mathbb{Q}(\xi))$ jsou ve tvaru

$$\begin{aligned}\varphi_1 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}, & \varphi_2 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}\xi, & \varphi_3 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}\xi^2, \\ \varphi_4 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}\xi^3, & \varphi_5 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}\xi^4, & \varphi_6 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}\xi^5, \\ \varphi_7 : \sqrt[7]{5} &\mapsto \sqrt[7]{5}\xi^6.\end{aligned}$$

Cvičení 4.2. Rozhodněte, zda Galoisovo rozšíření $\mathbb{Q}(i\sqrt{2})$ tělesa $\mathbb{Q}$ je cyklické.

[Prvky Galoisovy grupy $G(\mathbb{Q}(i\sqrt{2}), \mathbb{Q})$ jsou ve tvaru

$$\varphi_1 : i\sqrt{2} \mapsto i\sqrt{2}, \quad \varphi_2 : i\sqrt{2} \mapsto -i\sqrt{2}.$$

Zřejmě jednoprvková množina $\{\varphi_2\}$ je generátorem grupy $G(\mathbb{Q}(i\sqrt{2}), \mathbb{Q})$, proto tato grupa je cyklická. Tedy rozšíření $\mathbb{Q}(i\sqrt{2})$ tělesa $\mathbb{Q}$ je cyklické.]

5 Eukleidovské konstrukce a jejich algebraické interpretace

Tato kapitola je zaměřena na aplikaci algebry polynomů a teorie algebraického rozšíření těles na geometrické problémy. Budeme se zabývat eukleidovskou konstrukcí a dále se podíváme na důkazy neřešitelnosti tří antických úloh.

5.1 Eukleidovské konstrukce

Eukleides ve svém díle *Základy* uvažuje jen takové konstrukce, které lze rozložit na postupné provádění následujících dvou elementárních konstrukcí:

E_1) jsou-li dány v rovině dva různé body A, B , lze sestrojit přímku procházející body A, B ;

E_2) je dán v rovině bod A a úsečka délky r . Pak lze sestrojit kružnici k se středem v bodě A a poloměrem r [12].

Definice 5.1. Každou konstrukci, kterou lze složit postupným prováděním elementárních konstrukcí E_1 a E_2 , nazveme **eukleidovskou konstrukcí**.

Definice 5.2. Základními konstrukcemi rozumíme:

K_1) průnik dvou přímek (pokud existuje);

K_2) průnik přímky a kružnice (pokud existuje);

K_3) průnik dvou kružnic (pokud existuje).

Každou eukleidovskou konstrukci lze rozložit na postupné provádění tří základních konstrukcí K_1, K_2, K_3 [12].

Věta 5.1. *Konstrukční úlohu lze provést eukleidovsky právě tehdy, když lze souřadnice hledaných bodů vypočítat ze souřadnic daných bodů pomocí racionálních operací a druhé odmocniny.*

Důkaz.

1. „ $\Rightarrow$ “

ad E_1) Nechť $A = [a_1, a_2]$, $B = [b_1, b_2]$ jsou dva body určené souřadnicemi v kartézské souřadné soustavě, kde $a_1 \neq b_1$. Přímku p určenou body A, B lze v popsat rovnicí pomocí

racionálních operací a souřadnic těchto bodů ve tvaru

$$p : y = \frac{b_2 - a_2}{b_1 - a_1}x + \frac{a_2b_1 - a_1b_2}{b_1 - a_1},$$

po snadné úpravě se dostaneme k obecnému vyjádření přímky v rovině $ax + by + c = 0$.

ad E₂) Je-li dán bod $A = [a_1, a_2]$ a úsečka CD délky r , kde $C = [c_1, c_2]$, $D = [d_1, d_2]$. Pak rovnici kružnice k se středem v bodě A o poloměru r lze získat ze souřadnic bodů A, C, D pomocí racionálních operací ve tvaru

$$k : (x - a_1)^2 + (y - a_2)^2 = r^2,$$

kde $r = \sqrt{(c_1 - d_1)^2 + (c_2 - d_2)^2}$. Opět lze vyjádřit v obecném tvaru $x^2 + y^2 + ax + by + c = 0$.

Eukleidovskou konstrukci můžeme rozložit na konstrukce K_1 , K_2 , K_3 .

ad K₁) Máme sestavit průsečík dvou přímek, jejichž rovnice jsme získali ze souřadnic daných bodů pomocí racionálních operací. Tedy máme řešit soustavu dvou lineárních rovnic

$$ax + by + c = 0, \quad dx + ey + f = 0.$$

Obě přímky se protínají, jestliže má soustava právě jedno řešení, které lze určit z a, b, c, d, e, f pomocí racionálních operací, tj. pomocí racionálních operací ze souřadnic bodů určujících dané přímky.

ad K₂) Máme najít průsečík resp. průsečíky přímky s kružnicí, tedy budeme řešit soustavu rovnic

$$x^2 + y^2 + ax + by + c = 0, \quad dx + ey + f = 0.$$

Předpokládejme, že průsečík existuje, tzn. že soustava má řešení. Pak soustavu řešíme tak, že z druhé rovnice vyjádříme jednu neznámou a dosadíme do první rovnice. Získáme kvadratickou rovnici, jejíž koeficienty byly získány pomocí racionálních úprav. Při řešení kvadratické rovnice využíváme pouze racionálních operací a druhé odmocniny. Tedy řešení původní soustavy určíme pomocí uvedených operací ze souřadnic zadaných bodů.

ad K₃) Máme najít průsečík, resp. průsečíky dvou kružnic, tedy řešíme soustavu dvou rovnic druhého stupně

$$x^2 + y^2 + ax + by + c = 0, \quad x^2 + y^2 + dx + ey + f = 0.$$

Soustavu řešíme tak, že od druhé rovnice odečteme první. Soustavu jsme převedli na tvar z části ad K_2). Tedy opět souřadnice průsečíků získáme ze souřadnic zadaných bodů pomocí racionálních operací a druhé odmocniny.

2. „ $\Leftarrow$ “

Nechť jsou dány úsečky a , b , kde $b \neq 0$. Stačí dokázat, že jsme schopni sestrojit úsečky následujících délek

$$a + b, a - b, a \cdot b, \frac{a}{b}, \sqrt{a}.$$

Konstrukce součtu a rozdílu úseček je triviální. Konstrukce součinu a podílu úseček se provádí na základě podobnosti trojúhelníku s využitím redukčního úhlu. Při konstrukci úsečky o délce $\sqrt{a}$ využijeme Eukleidovu větu o výšce [12].

□

Důkaz následující věty lze nalézt např. v [12].

Věta 5.2. *Nechť je dáno r úseček o délkách $a_1, \dots, a_r$. Nechť $\mathbb{F}$ je těleso, které vznikne z $\mathbb{Q}$ adjunkcí čísel $a_1, \dots, a_r$. Nechť β je kořen ireducibilního polynomu*

$$f = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$$

nad $\mathbb{F}$. Lze-li úsečku o velikosti β sestrojit eukleidovsky, pak stupeň polynomu f je mocninou dvojky.

5.2 Důkazy neřešitelnosti tří antických úloh

V této části budou uvedeny tři známé antické úlohy, jejichž konstrukce nelze provést eukleidovsky. Důkazy o neřešitelnosti těchto úloh byly provedeny až s využitím poznatků moderní algebry.

1. Delfská úloha – duplikace krychle

Znění úlohy: „Nechť je dána krychle o hraně a . Sestrojte eukleidovsky úsečku délky x tak, že krychle o hraně x má dvojnásobný objem než původní krychle o hraně a .“

Důkaz. Musí platit $x^3 = 2a^3$. Zvolme $a = 1$, pak řešíme rovnici $x^3 - 2 = 0$. Polynom $x^3 - 2$ je podle Eisensteinova kritéria ireducibility ireducibilní nad $\mathbb{Q}$. Tento polynom je třetího stupně, což není mocnina dvojky. Tedy dle věty 5.2 nelze eukleidovsky zkonstruovat úsečku délky x [12].

□

2. Trisekce úhlu

Znění úlohy: „*Je dán úhel β . Sestrojte eukleidovsky úhel $\frac{\beta}{3}$.*“

Důkaz. Zvolme v rovině pravoúhlou soustavu souřadnic. Úhel β umístíme tak, aby vrchol ležel v počátku soustavy souřadnic a jeho rameno na ose x . Pak úhel β je určen body

$$[0, 0], [1, 0], [\cos \beta, \sin \beta].$$

Rozdělit úhel na třetiny znamená sestrojít bod o souřadnicích $[\cos \frac{\beta}{3}, \sin \frac{\beta}{3}]$. Jelikož platí $\sin \alpha = \sqrt{1 - \cos^2 \alpha}$, stačí zkonstruovat úsečku délky $\cos \frac{\beta}{3}$.

Dle vzorce známého z trigonometrie platí vztah

$$4 \cos^3 \frac{\beta}{3} - 3 \cos \frac{\beta}{3} = \cos \beta.$$

Položme $\cos \beta = a$ a $\cos \frac{\beta}{3} = x$, pak platí

$$4x^3 - 3x - a = 0,$$

kde $4x^3 - 3x - a$ je polynom nad $\mathbb{Q}(a)$. Tento polynom je pro některé hodnoty zřejmě reducibilní nad $\mathbb{Q}(a)$ např. pro $a = 0, -1$. Tedy jsme schopni provést trisekci úhlu $90^\circ, 180^\circ$. Stačí ukázat, že obecná eukleidovská konstrukce neexistuje, tj. existují úhly, které nelze eukleidovsky dělit na třetiny. Např. položme $\cos \beta = a = \frac{3}{5}$. Pak rovnici $4x^3 - 3x - a = 0$ můžeme přepsat do následujícího tvaru

$$20x^3 - 15x - 3 = 0,$$

kde polynom $20x^3 - 15x - 3$ je ireducibilní dle Eisensteinova kritéria nad $\mathbb{Q}$. Tento polynom je třetího stupně, tedy dle věty 5.2 nelze úsečku délky $\cos \frac{\beta}{3}$ sestrojít eukleidovsky [12]. $\square$

3. Kvadratura kruhu

Znění úlohy: „*Je dána kružnice k o poměru r . Sestrojte eukleidovsky čtverec o straně a , který má stejný obsah jako vnitřek kružnice k .*“

Důkaz. Zvolme poloměr $r = 1$. Pak vnitřek kružnice má obsah $S_\circ = \pi$. Hledáme čtverec o obsahu $S_\square = \pi$, odtud jeho strana je délky $\sqrt{\pi}$. Jelikož π je transcendentní nad $\mathbb{Q}$, nejsme schopni eukleidovsky zkonstruovat úsečku délky $\sqrt{\pi}$ [12]. $\square$

Řešené příklady

Příklad 5.1. Dokažte, že následující konstrukce jsou eukleidovské.

- a) Sestrojte tečny z bodu A ke kružnici k o středu S a poloměru r , bod A leží vně kružnice k .
- b) Je dán úhel α , sestrojte úhel o velikosti $\frac{\alpha}{2}$.

Řešení:

- a) Sestrojte tečny z bodu A ke kružnici k o středu S a poloměru r , bod A leží vně kružnice k .

Při řešení využijeme definice 5.2, podle které platí, že daná konstrukce je eukleidovská, jestliže lze složit z postupného provádění elementárních konstrukcí.

Tato konstrukce se skládá z následujících kroků:

- i) sestrojíme kružnici l_1 se středem v A o poloměru $|AS|$ (konstrukce E_2);
- ii) sestrojíme kružnici l_2 se středem v S o poloměru $|AS|$ (konstrukce E_2), průsečíky kružnic l_1, l_2 označme X, Y ;
- iii) sestrojíme přímku p procházející body X, Y (konstrukce E_1);
- iv) sestrojíme přímku q procházející body A, S (konstrukce E_1), průsečík přímek p, q označme O ;
- v) sestrojíme kružnici k_t se středem O a poloměrem $|OS|$ (konstrukce E_1), průsečíky kružnic k_t, k označme $T_{1,2}$;
- vi) sestrojíme přímky t_1, t_2 procházející body A, T_1 a A, T_2 (konstrukce E_1); t_1, t_2 jsou hledané tečny.

Tedy dle definice 5.2 je tato konstrukce eukleidovská.

- b) Je dán úhel α , sestrojte úhel o velikosti $\frac{\alpha}{2}$.

Dle věty 5.1 platí, že danou úlohu lze zkonstruovat eukleidovsky právě tehdy, když lze ze souřadnic zadaných bodů určit souřadnice hledaných bodů pomocí racionálních operací a druhé odmocniny.

Úhel α umístíme do počátku pravoúhlé soustavy souřadné a nechť jedno rameno leží na ose x . Pak úhel α je určen body

$$A = [1, 0], B = [0, 0], C = [\cos \alpha, \sin \alpha].$$

Sestrojit úhel o velikosti $\frac{\alpha}{2}$ znamená sestrojit bod X o souřadnicích

$$X = \left[\cos \frac{\alpha}{2}, \sin \frac{\alpha}{2} \right],$$

tzn. sestrojit úsečky o délkách $\cos \frac{\alpha}{2}, \sin \frac{\alpha}{2}$.

Dle vzorců známých z trigonometrie platí

$$\cos \frac{\alpha}{2} = \sqrt{\frac{1 + \cos \alpha}{2}}, \sin \frac{\alpha}{2} = \sqrt{\frac{1 - \cos \alpha}{2}}.$$

Tato konstrukce je eukleidovská, jelikož jsme schopni ze souřadnic zadaných bodů určit souřadnice bodu X pomocí racionálních operací a druhé odmocniny.

Příklad 5.2. Nechť je dán úhel α , pro který platí, že $\cos \alpha = \frac{3}{10}$. Rozhodněte, zda lze eukleidovsky sestrojit úhel o velikosti $\frac{\alpha}{3}$.

Řešení:

Abychom daný úhel mohli roztřít, musel by být polynom na levé straně rovnice

$$4 \cos^3 \frac{\alpha}{3} - 3 \cos \frac{\alpha}{3} - \cos \alpha = 0$$

reducibilní nad $\mathbb{Q}(\cos \alpha)$.

Položme $\cos \frac{\alpha}{3} = x$ a dosaďme za $\cos \alpha = \frac{3}{10}$, pak

$$4x^3 - 3x - \frac{3}{10} = 0.$$

Rovnici upravíme do následujícího tvaru

$$40x^3 - 30x - 3 = 0.$$

Z Eisensteinova kritéria ireducibility plyne, že polynom $40x^3 - 30x - 3$ je ireducibilní nad $\mathbb{Q}(\frac{3}{10}) = \mathbb{Q}$, proto nelze provést trisekci tohoto úhlu.

Cvičení

Cvičení 5.1. Dokažte, že konstrukce těžiště trojúhelníka je eukleidovskou konstrukcí.

[uvažujme trojúhelník ABC v rovině, jehož vrcholy mají souřadnice $A = [a_1, a_2]$, $B = [b_1, b_2]$, $C = [c_1, c_2]$. Z analytické geometrie víme, že pro souřadnice těžiště trojúhelníka vzhledem k souřadnicím vrcholů platí

$$T = \left[\frac{a_1 + b_1 + c_1}{3}, \frac{a_2 + b_2 + c_2}{3} \right],$$

tedy dle věty 5.1 je daná konstrukce eukleidovská.]

Cvičení 5.2. Rozhodněte, zda lze eukleidovsky sestrojít trisekce následujících úhlů.

- a) $\frac{\pi}{3}$,
- b) $\frac{3\pi}{2}$.

[po dosazení do rovnice $4 \cos^3 \frac{\alpha}{3} - 3 \cos \frac{\alpha}{3} = \cos \alpha$ a zavedení substituce $\cos \frac{\alpha}{3} = x$ dostaneme:

- a) rovnici $8x^3 - 6x - 1 = 0$. snadno lze ověřit, že rovnice nemá racionální kořen ve tvaru $\frac{p}{q}$ takový, že $p \nmid 1$ a $q \nmid 8$, proto nelze provést eukleidovsky trisekci úhlu o velikosti $\frac{\pi}{3}$,
- b) rovnici $4x^3 - 3x = 0$, polynom $4x^3 - 3x$ je reducibilní nad $\mathbb{Q}$ ($\cos \frac{3\pi}{2} = 0$), tedy lze provést eukleidovsky trisekci úhlu o velikosti $\frac{3\pi}{2}$.]

6 Úvod do problematiky algebraického kódování

V této kapitole se budeme věnovat problematice kódování číslíkových informací. Typický je případ přenosu informace, která se skládá z řetězce znaků nějaké konečné abecedy. Tato abeceda může např. obsahovat $0, 1 \in \mathbb{Z}_2$,¹ nebo se může skládat z malých a velkých písmen latinské abecedy, z arabských číslic, případně může obsahovat číslice i písmena. Dále se budeme zabývat vlastnostmi blokových, maticových, grupových a polynomických kódů.

6.1 Dvojkové symetrické kanály

Přenos informace představuje přenos znaků konečné abecedy nějakým oznamovacím (komunikačním) kanálem. Nedokonalost oznamovacích kanálů (ať už to jsou dráty v případě telefoního spojení či kosmický prostor v systémech spojovaných družic) má za následek to, že s pravděpodobností q vznikne při přenosu chyba a příjemce zachytí znak nepřesně.

Návrhy komunikačních systémů se hodnotí matematickými metodami využívající zjednodušené modely oznamovacích kanálů. Nejjednodušší, ale přitom realistický model takového oznamovacího kanálu se v případě použití dvojkové abecedy se signály 0 a 1 nazývá **dvojkový symetrický kanál**.

Předpokládejme, že dvojkové signály, které budeme označovat 0 a 1, se po jednom přenášejí k příjemci. Nechť p je pravděpodobnost, že příjemce přečte přenášený signál správně. A nechť $q = 1 - p$ je pravděpodobnost, že příjemce přečte signál chybně. Předpokládejme, že chyby při postupném přenášení číslic vznikají nezávisle na sobě ve smyslu následující definice [8].

Definice 6.1. Nechť $\epsilon_1, \epsilon_2, \epsilon_3, \dots$ je posloupnost některých jevů a nechť $\mathcal{T}$ je vlastnost, kterou každé ϵ_i může, ale nemusí mít. Označme p_i pravděpodobnost, že ϵ_i má vlastnost $\mathcal{T}$, a nechť $q_i = 1 - p_i$ je pravděpodobnost, že ϵ_i nebude mít vlastnost $\mathcal{T}$. Potom jsou uvedené jevy nezávislé vzhledem k $\mathcal{T}$. Pro každé dvě disjunktní podmnožiny indexů I, J součin $\prod_I p_i \prod_J q_j$ znamená pravděpodobnost toho, že každé ϵ_i ($i \in I$) má vlastnost $\mathcal{T}$ a současně žádné ϵ_j ($j \in J$) nemá vlastnost $\mathcal{T}$.

¹Pozn. V této kapitole budeme prvky tělesa $\mathbb{Z}_2$ značit 0, 1.

Věta 6.1. *Pravděpodobnost, že při přenosu n -bitové informace (tj. informace o n binárních symbolech) dvojkovým symetrickým kanálem vznikne přesně k chyb, je*

$$P_k = \binom{n}{k} p^{n-k} q^k = \binom{n}{k} p^{n-k} (1-p)^k = \binom{n}{k} (1-q)^{n-k} q^k.$$

Důkaz věty 6.1 lze nalézt např. v [8].

Definice 6.2. **Binární (m, n) -kód** je složen z kódovací funkce $E : 2^m \rightarrow 2^n$ a dekódovací funkce $D : 2^n \rightarrow 2^m$, kde 2^n je množina všech n -tic složených z prvků ze $\mathbb{Z}_2$.²

Kódy dělíme na **samoopravné**, jejichž úkolem je opravit chyby způsobené šumem v přenosovém kanálu, a **kódy zjišťující chyby**, které mají jen odhalit přítomnost chyb.

6.2 Blokový kód

Blokový kód definujeme jako kód, který blokům složeným z pevného počtu m symbolů (tj. slovům délky m) přiřazuje bloky s větším počtem symbolů určené na přenos signálů.

Dále budeme předpokládat, že přenášená posloupnost znaků je složená jen z nul a jedniček. Blokový kód je pak určený kódovací funkcí E a dekódovací funkcí D , přičemž platí

$$E : 2^m \rightarrow 2^n, D : 2^n \rightarrow 2^m, \quad m \leq n.$$

To znamená, že E zakóduje slova složená z m číslic na slova složená z n číslic a D přiřazuje každé posloupnosti n číslic posloupnost m číslic. Každý takový kód nazveme **binárním blokovým (m, n) -kódem**.

Předpokládejme, že kódované slovo $\mathbf{a}$ je složené po řadě z číslic $a_1, a_2, \dots, a_n$, což budeme zapisovat $\mathbf{a} = (a_1, \dots, a_n)$. Pak číslice $a_1, a_2, \dots, a_n$ nazveme **souřadnicemi kódovaného slova $\mathbf{a}$** .

Uvažujme kódovaná slova $\mathbf{a} = (a_1, \dots, a_n)$ a $\mathbf{b} = (b_1, \dots, b_n)$ s n souřadnicemi. **Vzdálenost** dvou kódovaných slov $\mathbf{a}, \mathbf{b}$ definujeme jako počet indexů i , pro které platí, že $a_i \neq b_i$. Vzdálenost dvou kódovaných slov $\mathbf{a}, \mathbf{b}$ budeme značit $d(\mathbf{a}, \mathbf{b})$ [8].

Definice 6.3. Nechť $\mathbf{a} = (a_1, \dots, a_n)$ je binární kódované slovo. Pak **váhou** kódovaného slova $\mathbf{a}$ budeme rozumět počet jedniček mezi jeho souřadnicemi, což budeme značit $w(\mathbf{a})$.

²Pozn. V této kapitole budeme předpokládat, že $m, n \in \mathbb{N}$.

Poznámka 6.1. Nechť $\mathbf{a}$, $\mathbf{b}$ jsou dvě binární slova délky n . Pak pro **vzdálenost** binárních slov $\mathbf{a}$, $\mathbf{b}$ platí, že je rovna váze jejich binárního součtu, tedy $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} + \mathbf{b})$.

Definice 6.4. Řekneme, že dvě binární slova jsou **sousední**, jestliže se liší právě v jedné souřadnici.

6.3 Objevování a opravování chyb blokových kódů

Uvažujme blokový binární (m, n) -kód s kódovací funkcí $E : 2^m \rightarrow 2^n$. Označme M množinu všech kódovaných slov. Tedy $2^n \setminus M$ je množina všech nekódovaných slov. Předpokládejme, že vysíláme slova z M a přijímáme slova z množiny 2^n . Pokud jsme přijali nekódované slovo, říkáme, že jsme objevili chybu. Je-li přijaté slovo kódované, pak buď nedošlo k chybě nebo jsme ji neobjevili. Řekneme, že došlo ke **k -násobné chybě**, jestliže počet chybných míst je nejvýše k [1].

Definice 6.5. Řekneme, že **kód objevuje k -násobné chyby**, jestliže při vyslání kódovaného slova a při vzniku k -násobné chyby je přijaté slovo vždy nekódované.

Definice 6.6. **Minimální vzdálenost** kódu rozumíme nejmenší vzdálenost dvou různých kódovaných slov.

Definice 6.7. Řekneme, že kód **opravuje k -násobné chyby**, jestliže při vyslání kódovaného slova $\mathbf{a}$ a při k -násobné chybě má přijaté slovo $\mathbf{b}$ vzdálenost od slova $\mathbf{a}$ menší než je jeho vzdálenost od libovolného jiného kódovaného slova.

Důkazy následujících dvou vět lze nalézt např. v [8].

Věta 6.2. *Kód může zjišťovat nejvýše k -násobné chyby právě tehdy, když minimální vzdálenost mezi každými dvěma kódovanými slovy je alespoň $k + 1$.*

Věta 6.3. *Blokový kód může opravovat nejvýše k -násobné chyby právě tehdy, když minimální vzdálenost mezi dvěma kódovanými slovy je alespoň $2k + 1$.*

6.4 Lineární (maticové) kódy

V této kapitole se budeme zabývat metodou kódování slov založenou na násobení maticí. Výhodou tohoto kódování je, že vyžaduje mnohem menší paměť oproti blokovým kódům.

Definice 6.8. Binární kód se nazývá **lineární (maticový)**, jestliže je podprostorem lineárního prostoru 2^m . Je-li jeho dimenze n mluvíme o (m, n) -kódu.

Definice 6.9. Lineární (m, n) -kód je určen libovolnou bází $b_1, \dots, b_n$. Pak matici

$$\mathbf{G} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

nazveme **kódovací maticí** daného kódu.

Vlastnosti kódovací matice plynoucí z předcházející definice

- a) každý řádek matice je kódovaným slovem,
- b) každé kódované slovo je lineární kombinací řádků,
- c) řádky matice jsou lineárně nezávislé.

Poznámka 6.2. Binární lineární kód K s kódovací maticí $\mathbf{G} = ||g_{ij}||$ nad $\mathbb{Z}_2$ přiřazuje každému slovu $\mathbf{a}$ kódované slovo $\mathbf{b}$ takové, že platí

$$\mathbf{b} = \mathbf{a} \cdot \mathbf{G}.$$

Důkazy vět 6.4 a 6.5 lze nalézt např. v [8].

Věta 6.4. *Nechť $\mathbf{G}$ je kódovací matice a nechť $\mathbf{I}_m$ je dílčí matice $\mathbf{G}$ typu $m \times n$, která vznikne z matice $\mathbf{G}$ vynecháním $m + 1, \dots, n$ -tého sloupce. Je-li matice $\mathbf{I}_m$ jednotková, pak všechna kódovaná slova jsou různá.*

Věta 6.5. *Nechť $\mathbf{G}$ je kódovací matice typu $m \times n$, která obsahuje jednotkovou dílčí matici $\mathbf{I}_m$ (zavedenou v přecházející větě). Pak (m, n) -kódovací funkce $\mathbf{a} \mapsto \mathbf{a} \cdot \mathbf{G}$ je monomorfismus aditivní grupy původních m -bitových slov do aditivní grupy kódovaných slov.*

V následující definici zavedeme pojem kontrolní matice lineárního kódu.

Definice 6.10. Řekneme, že matice $\mathbf{H}$ je kontrolní maticí lineárního kódu K , jestliže pro každé $\mathbf{a} \in K$ platí

$$\mathbf{H} \cdot \mathbf{a}^T = \mathbf{o}^T,$$

kde $\mathbf{o}$ je nulový vektor.

Poznámka 6.3. Pro kódovací matici $\mathbf{G}$ a kontrolní matici $\mathbf{H}$ lineárního kódu platí

$$\mathbf{H} \cdot \mathbf{G}^T = \mathbf{N},$$

kde $\mathbf{N}$ je nulová matice příslušného typu.

V následující definici zavedeme pojem ekvivalentní kódy.

Definice 6.11. Řekneme, že kód C je **ekvivalentní** s kódem C' , jestliže existuje bijekce mezi kódovanými slovy z C a kódovanými slovy z C' , která zachovává vzdálenosti.

Věta 6.6. *Nechť $\mathbf{G}$ je kódovací matice a nechť $\mathbf{G}'$ je matice, která vznikne pomocí následujících operací nebo jejich kombinací:*

- a) permutací řádků matice $\mathbf{G}$,
- b) permutací sloupců matice $\mathbf{G}$,
- c) přičtením násobku jednoho řádku k jinému řádku matice $\mathbf{G}$.

Pak matice $\mathbf{G}'$ je kódovací maticí generující kód ekvivalentní s kódem generovaným maticí $\mathbf{G}$.

Důkaz věty 6.6 vychází z definice 6.11.

Věta 6.7 ukazuje výhodnější postup při hledání kontrolní matice lineárního kódu než pomocí definice 6.10.

Věta 6.7. *Lineární kód s kódovací maticí $\mathbf{G} = (\mathbf{E}|\mathbf{B})$ má kontrolní matici*

$$\mathbf{H} = (-\mathbf{B}^T|\mathbf{E}'),$$

kde $\mathbf{E}$, $\mathbf{E}'$ jsou jednotkové matice příslušného typu.

Důkaz. Nechť K je lineární (m, n) -kód s kódovací maticí $\mathbf{G} = (\mathbf{E}|\mathbf{B})$ a kontrolní maticí $\mathbf{H}$. Máme ověřit, že K je lineární prostor shodný s prostorem K' všech řešení rovnic $\mathbf{H} \cdot \mathbf{a}^T = \mathbf{o}^T$ ($\mathbf{a} \in K$). Platí

$$\mathbf{H} \cdot \mathbf{G}^T = (-\mathbf{B}^T|\mathbf{E}') \cdot \begin{pmatrix} \mathbf{E} \\ \mathbf{B}^T \end{pmatrix} = -\mathbf{B}^T \cdot \mathbf{E} + \mathbf{E}' \cdot \mathbf{B}^T = -\mathbf{B}^T + \mathbf{B}^T = \mathbf{N}.$$

Pro každý řádek $\mathbf{a}$ matice $\mathbf{G}$ platí $\mathbf{G} \cdot \mathbf{a}^T = \mathbf{o}^T$. Prostor K' obsahuje celou bázi prostoru K , tedy K je podprostorem prostoru K' .

Dále stačí ověřit, že prostory K , K' mají stejnou dimenzi. Matice $\mathbf{G}$ a tedy i matice $\mathbf{B}$ mají n řádků. Jednotková matice $\mathbf{E}'$ je řádu $m - n$, tedy platí $h(\mathbf{H}) = m - n$. Odtud plyne, že prostor K' má dimenzi $m - h(\mathbf{H}) = n$, tedy $K = K'[1]$. $\square$

6.5 Grupové kódy

V této části definujeme grupové kódy, uvedeme jejich základní vlastnosti a budeme se zabývat problematikou dekódování.

Definice 6.12. Blokový kód, pro který platí, že kódovaná slova tvoří aditivní grupu, nazveme **grupovým kódem**.

Věta 6.8. *Nechť je dán grupový kód, který obsahuje kódovaná slova $\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_{2^m-1}$. Pak minimální vzdálenost $d(\mathbf{b}_i, \mathbf{b}_j)$ (pro $i \neq j$) mezi dvěma kódovanými slovy je rovna minimální váze $w(\mathbf{b}_k)$ některého nenulového kódovaného slova.*

Důkaz. Uvažujme kódovaná slova $\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_{2^m-1}$, zřejmě tvoří aditivní grupu. Dále minimální vzdálenost $d(\mathbf{b}_i, \mathbf{b}_j)$ pro nějaké $\mathbf{b}_i, \mathbf{b}_j$ ($\mathbf{b}_i \neq \mathbf{b}_j$). Jelikož $\mathbf{b}_i + \mathbf{b}_j$ je též kódované slovo, tedy položíme $\mathbf{b}_k = \mathbf{b}_i + \mathbf{b}_j$. Z definic váhy a vzdálenosti kódovaných slov plyne, že $w(\mathbf{b}_k) = d(\mathbf{b}_i, \mathbf{b}_j)$ [8]. $\square$

Následně se budeme zabývat optimalizací dekódování grupového kódu $\mathbf{G} \mapsto \mathbf{a} \cdot \mathbf{G}$ ($\mathbf{G}$ je kódovací matice typu $m \times n$). Budeme se snažit o snížení pravděpodobnosti neodhazitelných chyb (tj. pravděpodobnosti $D(\mathbf{a} \cdot \mathbf{G}) \neq \mathbf{a}$). Dekódovací funkce závisí na všech slovech, která mohou být přijata. Zřejmě kódovaná slova tvoří podgrupu B (obsahující prvky $\{\mathbf{0}, \mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{2^m-1}\}$) grupy C všech možných slov, která mohou být přijata. Sestrojíme tabulku množiny C tak, že v prvním řádku budou všechny prvky množiny B , přičemž začneme prvkem $\mathbf{0}$:

$$\mathbf{0} \quad \mathbf{b}_1 \quad \mathbf{b}_2 \quad \dots \quad \mathbf{b}_{2^m-1}$$

Druhý řádek dostaneme tak, že budeme vybírat nějaké $\mathbf{c}_i \in C$ a ke každému $\mathbf{b}_i \in B$ přičteme $\mathbf{c}_i$.

$$\begin{array}{ccccccc} \mathbf{0} & \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_{2^m-1} \\ \mathbf{0} + \mathbf{c}_i & \mathbf{b}_1 + \mathbf{c}_i & \mathbf{b}_2 + \mathbf{c}_i & \dots & \mathbf{b}_{2^m-1} + \mathbf{c}_i \end{array}$$

Řádek upravíme tak, že vlevo napíšeme slovo $\mathbf{b}_j + \mathbf{c}_i$ s nejmenší váhou, označme jej $\mathbf{c}_1$. Dále přepíšeme do tvaru

$$\begin{array}{ccccccc} \mathbf{0} & \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_{2^m-1} \\ \mathbf{c}_1 & \mathbf{b}_1 + \mathbf{c}_1 & \mathbf{b}_2 + \mathbf{c}_1 & \dots & \mathbf{b}_{2^m-1} + \mathbf{c}_1 \end{array}$$

Následně vybereme další kódované slovo z C , které nepatří do žádného z obou řádků a napíšeme třetí řádek. Pak z něj vybere prvek s nejmenší váhou, označme jej $\mathbf{c}_2$. Celý řádek přepíšeme tak, aby $\mathbf{c}_2$ byl na prvním místě. Postupujeme tak dlouho, dokud tabulka neobsahuje všechna slova z C . Konečná tabulka má tvar

$\mathbf{0}$	$\mathbf{b}_1$	$\mathbf{b}_2$	$\dots$	$\mathbf{b}_{2^m-1}$
$\mathbf{c}_1$	$\mathbf{b}_1 + \mathbf{c}_1$	$\mathbf{b}_2 + \mathbf{c}_1$	$\dots$	$\mathbf{b}_{2^m-1} + \mathbf{c}_1$
$\mathbf{c}_2$	$\mathbf{b}_1 + \mathbf{c}_2$	$\mathbf{b}_2 + \mathbf{c}_2$	$\dots$	$\mathbf{b}_{2^m-1} + \mathbf{c}_2$
$\vdots$				
$\mathbf{c}_{2^m-n-1}$	$\mathbf{b}_1 + \mathbf{c}_{2^m-n-1}$	$\mathbf{b}_2 + \mathbf{c}_{2^m-n-1}$	$\dots$	$\mathbf{b}_{2^m-1} + \mathbf{c}_{2^m-n-1}$

Při dekódování vyhledáme v tabulce přijaté slovo $\mathbf{c} = \mathbf{b}_i + \mathbf{c}_j$ a za výsledné kódované slovo zvolíme $\mathbf{b}_i$ [8].

6.6 Polynomické kódy

V této části se budeme zabývat **polynomickými kódy**, které chápeme jako speciální třídu grupových kódů. Jsou to (m, n) -kódy, které ztotožňují původní slova délky m s polynomy, a tyto polynomy se pak násobí pevně zvoleným polynomem. Tak dostaneme kódovaná slova délky n .

Mezi m -bitovými slovy $\mathbf{a} = a_0a_1 \dots a_{m-1}$ a polynomy stupně $m-1$ (tedy délky m) existuje přirozená bijekce taková, že platí

$$\mathbf{a} \leftrightarrow a = a_0 + a_1x + \dots + a_{m-1}x^{m-1}.$$

Např. slovu 110101 odpovídá polynom

$$1x^0 + 1x^1 + 0x^2 + 1x^3 + 0x^4 + 1x^5.$$

V následujících definicích definujeme polnomický kód a kódovací matici.

Definice 6.13. Nechť $\mathbb{F}$ je libovolné konečné těleso a nechť

$$g = g_0 + g_1x + \dots + g_kx^k \in \mathbb{F}[x] \quad (g_0 \neq 0, g_k \neq 0)$$

je polynom stupně k . **Polynomický kód** s kódovacím polynomem g přiřazuje každému slovu $\mathbf{a} = a_0a_1 \dots a_{m-1}$ kódované slovo $\mathbf{b} = b_0b_1 \dots b_{n-1}$, které odpovídá polynomu

$$b = b_0 + b_1x + \dots + b_{n-1}x^{n-1} = ag.$$

Definice 6.14. Nechť je dán m -bitový polynomický kód s kódovacím polynomem

$$g = g_0 + g_1x + \dots + g_kx^k.$$

Pak matice

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \dots & g_k & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{k-1} & g_k & \dots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & 0 & \dots & g_0 & \dots & g_{k-1} & g_k \end{pmatrix}$$

typu $m \times (m + k)$ je **kódovací maticí** tohoto polynomického kódu.

Poznámka 6.4. Nenulové prvky v j -tém řádku kódovací matice $\mathbf{G}$ z předcházející definice tvoří blok $g_0g_1 \dots g_k$, který leží na j -tém až $(j + k)$ -tém místě tohoto řádku.

Věta 6.9. *Nechť je dán polynom s koeficienty ze $\mathbb{Z}_2$, který je dělitelný polynomem $1 + x$. Pak má sudý počet nenulových koeficientů.*

Důkaz. Nechť je dán polynom $f = a_0 + a_1x + \dots + a_nx \in \mathbb{Z}_2[x]$ a nechť pro nějaký polynom h platí $f = (x + 1)h$. Pro $x = 1$, platí

$$f(1) = (1 + 1)h(1) = 0.$$

Dále $f(1) = a_0 + a_1 + \dots + a_n$, tedy počet nenulových koeficientů musí být sudý [8]. $\square$

Věta 6.10. *Minimální vzdálenost dvou kódovaných slov v polynomickém kódu je rovna minimální váze kódovaných slov různých od nuly.*

Důkaz věty 6.10 je analogický s důkazem věty 6.8.

Řešené příklady

Příklad 6.1. Blokový $(2, 3)$ -kód je určený funkcí

$$E : \begin{array}{ll} \mathbf{a}_1 = 00 \mapsto \mathbf{b}_1 = 001, & \mathbf{a}_2 = 01 \mapsto \mathbf{b}_2 = 011, \\ \mathbf{a}_3 = 10 \mapsto \mathbf{b}_3 = 100, & \mathbf{a}_4 = 11 \mapsto \mathbf{b}_4 = 111. \end{array}$$

- a) Určete vzdálenosti mezi kódovanými slovy $d(\mathbf{a}_1, \mathbf{a}_4)$, $d(\mathbf{b}_2, \mathbf{b}_4)$.
- b) Určete váhu kódovaných slov $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4$.
- c) Určete sousední slova kódovaného slova $\mathbf{b}_2$.

Řešení:

a)

Vzdálenost mezi dvěma kódovanými slovy $\mathbf{a}, \mathbf{b}$ je rovna počtu indexů, pro které platí $a_i \neq b_i$.

i) Určíme $d(\mathbf{a}_1, \mathbf{a}_4)$.

Pro souřadnice kódovaných slov $\mathbf{a}_1, \mathbf{a}_4$ platí

$$\begin{array}{l} a_{11} \neq a_{41}, \\ a_{12} \neq a_{42}. \end{array}$$

Odtud $d(\mathbf{a}_1, \mathbf{a}_4) = 2$.

ii) Určíme $d(\mathbf{b}_2, \mathbf{b}_4)$.

Pro souřadnice kódovaných slov $\mathbf{b}_2, \mathbf{b}_4$ platí

$$\begin{array}{l} b_{21} \neq b_{41}, \\ b_{22} = b_{42}, \\ b_{23} = b_{43}. \end{array}$$

Odtud $d(\mathbf{b}_2, \mathbf{b}_4) = 1$.

b)

Váha kódovaného slova je dle definice 6.3 rovna počtu jednotek mezi jeho souřadnicemi.

Tedy platí

$$\begin{array}{ll} w(\mathbf{b}_1) = 1, & w(\mathbf{b}_2) = 2, \\ w(\mathbf{b}_3) = 1, & w(\mathbf{b}_4) = 3. \end{array}$$

c)

Dle definice 6.4 dvě kódovaná slova jsou sousední, liší-li se právě v jedné souřadnici.

Zřejmě kódovaná slova $\mathbf{b}_1$, $\mathbf{b}_4$ jsou sousední slova s $\mathbf{b}_2$.

Příklad 6.2. Blokový (2, 6)-kód určený funkcí

$$E : \begin{aligned} \mathbf{a}_1 = 00 &\mapsto \mathbf{b}_1 = 000000, & \mathbf{a}_2 = 01 &\mapsto \mathbf{b}_2 = 010101, \\ \mathbf{a}_3 = 10 &\mapsto \mathbf{b}_3 = 101010, & \mathbf{a}_4 = 11 &\mapsto \mathbf{b}_4 = 111111. \end{aligned}$$

Určete kolikanásobné chyby může zjišťovat a opravovat tento blokový kód.

Řešení:

Při řešení využijeme vět 6.2 a 6.3. Podle těchto vět platí, že daný kód zjišťuje k -násobné chyby, právě když minimální vzdálenost mezi každými dvěma kódovanými slovy je alespoň $k + 1$. Opravuje k -násobné chyby, právě když minimální vzdálenost mezi každými dvěma kódovanými slovy je alespoň $2k + 1$.

Určíme vzdálenosti každých dvou kódovaných slov:

$$\begin{aligned} d(\mathbf{b}_1, \mathbf{b}_2) &= 3, & d(\mathbf{b}_2, \mathbf{b}_3) &= 6, \\ d(\mathbf{b}_1, \mathbf{b}_3) &= 3, & d(\mathbf{b}_2, \mathbf{b}_4) &= 3, \\ d(\mathbf{b}_1, \mathbf{b}_4) &= 6, & d(\mathbf{b}_3, \mathbf{b}_4) &= 3. \end{aligned}$$

Odtud minimální vzdálenost mezi kódovanými slovy je 3.

Tedy tento blokový kód může zjišťovat nejvýše dvojnásobné chyby a opravovat jednoduché chyby.

Příklad 6.3. Dokažte, že každá grupová translace $\tau : \mathbf{x} \mapsto \mathbf{x} + \mathbf{c}$ grupy $(\mathbb{Z}_2^r, +)$ zachovává vzdálenosti mezi kódovanými slovy (převzato z [8]).

Řešení:

Nechť $\mathbf{c}$ je ve tvaru

$$\mathbf{c} = (c_1, \dots, c_r).$$

Pro každá dvě slova $\mathbf{a}_1 = (a_{11}, \dots, a_{1r})$, $\mathbf{a}_2 = (a_{21}, \dots, a_{2r})$ z $\mathbb{Z}_2^r$ platí

$$\begin{aligned} \mathbf{a}_1 &= (a_{11}, \dots, a_{1r}) \mapsto \mathbf{b}_1 = (a_{11} + c_1, \dots, a_{1r} + c_r), \\ \mathbf{a}_2 &= (a_{21}, \dots, a_{2r}) \mapsto \mathbf{b}_2 = (a_{21} + c_1, \dots, a_{2r} + c_r). \end{aligned}$$

Pro vzdálenosti slov $\mathbf{a}_1$, $\mathbf{a}_2$ a $\mathbf{b}_1$, $\mathbf{b}_2$ platí

$$d(\mathbf{a}_1, \mathbf{a}_2) = w(\mathbf{a}_1 + \mathbf{a}_2) = w(a_{11} + a_{21}, \dots, a_{1r} + a_{2r}),$$

$$\begin{aligned} d(\mathbf{b}_1, \mathbf{b}_2) &= w(\mathbf{b}_1 + \mathbf{b}_2) = w(a_{11} + c_1 + a_{22} + c_1, \dots, a_{1r} + c_r + a_{2r} + c_r) = \\ &= w(a_{11} + a_{22}, \dots, a_{1r} + a_{2r}). \end{aligned}$$

Odtud $d(\mathbf{a}_1, \mathbf{a}_2) = d(\mathbf{b}_1, \mathbf{b}_2)$, tedy grupová translace zachovává vzdálenosti mezi kódovanými slovy.

Příklad 6.4. Uvažujme lineární $(3, 5)$ -kód s kódovací maticí

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Rozhodněte, zda všechna kódovaná slova tohoto maticového kódu jsou různá, a určete je.

Řešení:

Při řešení využijeme větu 6.4. Matice $\mathbf{I}_m$ je dílčí maticí matice $\mathbf{G}$ (dle věty 6.4) ve tvaru

$$\mathbf{I}_m = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Matice $\mathbf{I}_m$ je zřejmě jednotková, proto dle věty 6.4 jsou všechna kódovaná slova různá.

Dále určíme všechna kódovaná slova. Maticový kód s kódovací maticí $\mathbf{G}$ přiřazuje každému slovu $\mathbf{a}$ kódované slovo $\mathbf{a} \cdot \mathbf{G}$, odtud

$$\begin{array}{ll} 000 \mapsto 00000, & 100 \mapsto 10011, \\ 001 \mapsto 00100, & 101 \mapsto 10111, \\ 010 \mapsto 01001, & 110 \mapsto 11010, \\ 011 \mapsto 01101, & 111 \mapsto 11110. \end{array}$$

Příklad 6.5. Určete kontrolní matici lineárního kódu K s kódovací maticí

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Dále ověřte, že pro kontrolní a kódovací matici lineárního kódu K platí $\mathbf{H} \cdot \mathbf{G}^T = \mathbf{0}$ (upraveno podle [8]).

Řešení:

Při řešení tohoto příkladu využijeme větu 6.7, podle které platí, že matice $(-\mathbf{B}^T|\mathbf{E}')$ je kontrolní maticí kódu K , je-li kódovací matice kódu K ve tvaru $(\mathbf{E}|\mathbf{B})$.

Nejprve upravíme matici $\mathbf{G}$ do tvaru $\mathbf{G}' = (\mathbf{E}|\mathbf{B})$, která je kódovací maticí kódu K' ekvivalentního s K . Stačí provést permutaci

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 8 & 4 & 5 & 2 & 1 & 3 \end{pmatrix}$$

na sloupce matice $\mathbf{G}$.

Odtud

$$\mathbf{G}' = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right).$$

Zřejmě platí

$$\mathbf{B}' = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Tedy kontrolní matice kódu K' je dle věty 6.7 ve tvaru

$$\mathbf{H}' = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Po provedení inverzní permutace $\pi' = \pi$ získáme kontrolní matici původního kódu

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Na závěr zbývá ověřit platnost

$$\mathbf{H} \cdot \mathbf{G}^T = \mathbf{0}.$$

Po dosazení do předcházejícího vztahu dostaneme

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Příklad 6.6. Určete dekódovací tabulku pro grupový $(2, 4)$ -kód určený kódovací maticí

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Řešení:

V prvním řádku dekódovací tabulky jsou všechna kódovaná slova daného grupového kódu, první slovo v řádku je slovo s nejmenší vahou. Nejprve určíme všechna kódovaná slova daného grupového kódu.

$$\begin{array}{ll} 00 \mapsto 0000, & 10 \mapsto 1010, \\ 01 \mapsto 0111, & 11 \mapsto 1101. \end{array}$$

Dále označme B množinu všech kódovaných slov a C množinu všech slov, která mohou být přijata.

První řádek tabulky je zřejmě ve tvaru

$$\mathbf{0000} \quad \mathbf{0111} \quad \mathbf{1010} \quad \mathbf{1101}$$

Druhý řádek tabulky dostaneme tak, že vybereme libovolné slovo z množiny C , které není v prvním řádku, a že každému slovu z prvního řádku jej přičteme. Např. zvolme 1111 a dostaneme druhý řádek v následujícím tvaru.

$$\begin{array}{cccc} \mathbf{0000} & \mathbf{0111} & \mathbf{1010} & \mathbf{1101} \\ \hline 1111 & 1000 & 0101 & 0010 \end{array}$$

Druhý řádek upravíme tak, že vlevo napíšeme slovo s nejmenší vahou a zbytek řádku určíme tak, že toto slovo přičítáme ke slovům z prvního řádku (analogicky jak je uvedeno v podkapitole 6.5).

Odtud

0000	0111	1010	1101
1000	1111	0010	0101

Třetí řádek dostaneme analogicky jako druhý, zvolíme slovo z C , které není ještě obsaženo v tabulce, např. 0100. Tedy platí

0000	0111	1010	1101
1000	1111	0010	0101
0100	0011	1110	1001

Třetí řádek je již ve tvaru, kdy na prvním místě je slovo s nejnižší váhou, tedy nemusíme jej dále upravovat. Dále určíme čtvrtý řádek, zvolme např. slovo 0001 a postupujeme analogicky jako v předcházejících případech:

0000	0111	1010	1101
1000	1111	0010	0101
0100	0011	1110	1001
0001	0110	1011	1100

Čtvrtý řádek je též ve tvaru, kde na prvním místě je slovo s nejnižší váhou v řádku.

Zřejmě všechna slova z C jsou uvedena v tabulce. Tedy výše uvedená tabulka je dekódovací tabulkou daného grupového kódu.

Příklad 6.7. Určete kódovací matici a minimální vzdálenost kódovaných slov trojbitového polynomického kódu s kódovacím polynomem $x^2 + x + 1$. Dále určete kolikanásobné chyby může tento kód opravovat.

Řešení:

Kódovací matice pro tento polynomický kód je dle definice 6.14 v následujícím tvaru

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Minimální vzdálenost kódovaných slov určíme s využitím věty 6.10, podle které je rovna minimální váze všech nenulových kódovaných slov. Určíme všechna kódovaná slova a jejich váhu.

$\mathbf{a}_1 = 000 \mapsto \mathbf{b}_1 = 00000$	
$\mathbf{a}_2 = 001 \mapsto \mathbf{b}_2 = 00111$	$w(\mathbf{b}_2) = 3$
$\mathbf{a}_3 = 010 \mapsto \mathbf{b}_3 = 01110$	$w(\mathbf{b}_3) = 3$
$\mathbf{a}_4 = 011 \mapsto \mathbf{b}_4 = 01001$	$w(\mathbf{b}_4) = 2$
$\mathbf{a}_5 = 100 \mapsto \mathbf{b}_5 = 11100$	$w(\mathbf{b}_5) = 3$
$\mathbf{a}_6 = 101 \mapsto \mathbf{b}_6 = 11011$	$w(\mathbf{b}_6) = 4$
$\mathbf{a}_7 = 110 \mapsto \mathbf{b}_7 = 10010$	$w(\mathbf{b}_7) = 2$
$\mathbf{a}_8 = 111 \mapsto \mathbf{b}_8 = 10101$	$w(\mathbf{b}_8) = 3$

Zřejmě minimální váha nenulových kódovaných slov je 2, proto i minimální vzdálenost kódovaných slov je 2. Tedy tento kód zjišťuje jednoduché chyby.

Cvičení

Cvičení 6.1. Blokový (1, 6)-kód je určený funkcí

$$E : \mathbf{a}_1 = 0 \mapsto \mathbf{b}_1 = 000000,$$

$$\mathbf{a}_2 = 1 \mapsto \mathbf{b}_2 = 111110.$$

a) Určete $d(\mathbf{b}_1, \mathbf{b}_2)$, $w(\mathbf{b}_1)$, $w(\mathbf{b}_2)$.

b) Určete kolikanásobné chyby tento blokový kód může zjišťovat a opravovat.

[a) $d(\mathbf{b}_1, \mathbf{b}_2) = 5$, $w(\mathbf{b}_1) = 0$, $w(\mathbf{b}_2) = 5$; b) tento blokový kód zjišťuje čtyřnásobné a opravuje dvojnásobné chyby, jelikož minimální vzdálenost mezi kódovanými slovy je 5]

Cvičení 6.2. Určete kontrolní matice následujících lineárních kódů.

a) Lineární kód K s kódovací maticí

$$\mathbf{G}_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

b) Lineární kód L s kódovací maticí

$$\mathbf{G}_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

$$\left[\text{a) } \mathbf{H}_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} ; \text{ b) } \mathbf{H}_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \right]$$

Cvičení 6.3. Polynomický dvoubitový kód s kódovacím polynomem $x^2 + 1$. Určete kódovací matici a dekódovací tabulku.

$$\left[\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} ; \begin{array}{cc|cc} \mathbf{0000} & \mathbf{0101} & \mathbf{1010} & \mathbf{1111} \\ \hline 0001 & 0100 & 1011 & 1110 \\ 0010 & 0111 & 1000 & 1101 \\ 0011 & 0110 & 1001 & 1100 \end{array} \right]$$

Závěr

Teorie těles se uplatňuje v mnoha oblastech. Využíváme ji při řešení algebraických rovnic, s tím souvisí i celá Galoisova teorie. Další využití našla v eukleidovské geometrii, kdy na základě této teorie byl objasněn problém tří antických úloh, mj. i při řešení problematiky sestrojování pravidelných mnohoúhelníků. Uplatňuje se i v novodobých technologiích, s čímž souvisí mj. problematika kódování dat. S teorií kódování se setkáváme v běžném životě, ať už jsou to rodná čísla, ISBN kódy, atd.

Tato problematika je rozsáhlá, proto není možné v této práci zpracovat všechny již zmíněné oblasti. Část práce je zaměřena na Galoisovu teorii, které předchází zavedení normálního a separabilního rozšíření. Její hlavní význam je značný při řešení algebraických rovnic vyššího stupně pomocí radikálů. S využitím této teorie jsme schopni převést určité problémy z teorie těles do teorie grup.

Další část je věnována základní problematice algebraického kódování. V této části je nastíněn pouhý úvod do této teorie, který by měl demonstrovat, jak je v této oblasti aplikována teorie těles. Pro hlubší studování této teorie lze doporučit ke studiu [1], [8].

Tato práce obsahuje řešené i neřešené úlohy. Příklady jsou koncipovány tak, aby ilustrovaly jednotlivé pojmy. Neřešené úlohy jsou uvedeny ve cvičeních, kde čtenář nalezne jejich řešení. Při řešení těchto úloh je předpokládána znalost základů algebry a zájem se touto problematikou zabývat.

Seznam použitých symbolů

Symbol	Použití	Význam
$\forall$	$\forall x$	pro každé x – obecný kvantifikátor
$\exists$	$\exists x$	existuje x – existenční kvantifikátor
$\circ$	$\circ$	operace skládání zobrazení
$\Rightarrow$	$A \Rightarrow B$	výrok A implikuje výrok B
$\Leftrightarrow$	$A \Leftrightarrow B$	výrok A je ekvivalentní s výrokem B
$\in$	$x \in M$	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
B	B	matice B
	B ^T	transponovaná matice k matici B
	G, H	kódovací a kontrolní matice
	E, N	jednotková a nulová matice
	(A B)	matice složená z prvků matic A, B uspořádaných za sebou
	$\left(\begin{array}{c} \mathbf{A} \\ \mathbf{B} \end{array} \right)$	matice složená z prvků matic A, B uspořádaných pod sebou
a	a	kódované slovo a
	a = ($a_1, \dots, a_n$)	souřadnice kódovaného slova a
$\mathbb{N}$	$\mathbb{N}$	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
f	f	polynom f
	$st f$	stupeň polynomu f
	$st_r f$	redukovaný stupeň polynomu f
()	$(x_1, x_2, \dots, x_n)$	uspořádaná n -tice
[]	$\mathbb{F}[x]$	obor integrity polynomů jedné neurčité nad $\mathbb{F}$
	$[\mathbb{F} : \mathbb{L}]$	stupeň rozšíření $\mathbb{F}$ nad $\mathbb{L}$
	$[\mathbb{F} : \mathbb{L}]_r$	redukovaný stupeň rozšíření $\mathbb{F}$ nad $\mathbb{L}$
{ }	$\{x_1, x_2, \dots, x_n\}$	n -prvková množina

Seznam použité literatury

- [1] ADÁDEK, J. *Kódování a teorie informace*. Praha: ČVUT v Praze, 1994.
- [2] AIGNER, M., ZIEGLER, G. M. *Proofs from the book*. Berlin, Heidelberg, New York: Springer–Verlag, 2004. ISBN 3540404600.
- [3] BICAN, L. *Algebra I*. 1. vyd. Praha: SPN, 1977. 186 s.
- [4] BICAN, L. *Algebra II*. 1. vyd. Praha: SPN, 1982. 259 s.
- [5] BICAN, L. *Algebra (pro učitelské studium)*. 1. vyd. Praha : Academia, 2001. 110 s. ISBN 8020008608.
- [6] BICAN, L., KEPKA, T., NĚMEC, P. *Úvod do teorie konečných těles a lineárních kódů*. Praha: SPN, 1982.
- [7] BIGGS, N. L. *Discrete mathematics*. Oxford: Oxford University Press, 1994.
- [8] BIRKHOFF, G., BARTEE, T. O. *Aplikovaná algebra*. Z angl. orig. přel. Jaroslav Smítal. 1. vyd. Bratislava: Alfa, 1981. 389 s.
- [9] BIRKHOFF, G., MAC LANE, S. *Prehľad modernej algebry*. Z angl. orig. přel. Štefan Znám a Jaroslav Smítal. 1. vyd. Bratislava: Alfa, 1979. 468 s.
- [10] BLAŽEK, J., et al. *Algebra a teoretická aritmetika. II. díl*. 1.vyd. Praha: SPN, 1985. 258 s.
- [11] DIVIŠOVÁ, Z., KOSTRA, J., VAVROŠ, M. *Algebraické rozšíření a jejich aplikace*. 1. vyd. Ostrava: Ostravská univerzita v Ostravě, 2003. 98 s.
- [12] CHAJDA, I. *Vybrané kapitoly z algebry*. 2. vyd. Olomouc: Univerzita Palackého v Olomouci, 2000. 78 s. ISBN 802440205.
- [13] KATRIŇÁK, T., et al. *Algebra a teoretická aritmetika. 1*. 1. vyd. Bratislava: Alfa, 1985. 349 s.
- [14] POSTNIKOV, M. M. *Teorija Galua*. Moskva: Gosudarstvennoje izdatel'stvo fiziko-matematičeskoj literatury, 1963. 218 s.

- [15] PROCHÁZKA, L., et al. *Algebra*. 1. vyd. Praha: Academia, 1990. 560 s. ISBN 8020003010.
- [16] RACHŮNEK, J. *Grupy a okruhy*. 1. vyd. Olomouc: Univerzita palackého v Olomouci, 2005. 106 s. ISBN 8024409984.
- [17] SVÄTOKRIŽNÝ, P., et al. *Aritmetika a algebra pre pedagogické fakulty. [Diel] 2*. 1. vyd. Bratislava: Slovenské pedagogické nakladateľstvo, 1978. 463 s.
- [18] TÁBORSKÝ, T. *Základy teorie těles v úlohách*. Olomouc, 2009. 54 s. Vedoucí bakalářské práce Doc. RNDr. Petr Emanovský, Ph.D.
- [19] VAŠÍČEK, K. Evariste Galois. *Veda.cz* [online]. 17.6.2005, [cit. 2010-08-07]. Dostupný z WWW: <<http://www.veda.cz/article.do?articleId=11062>>.