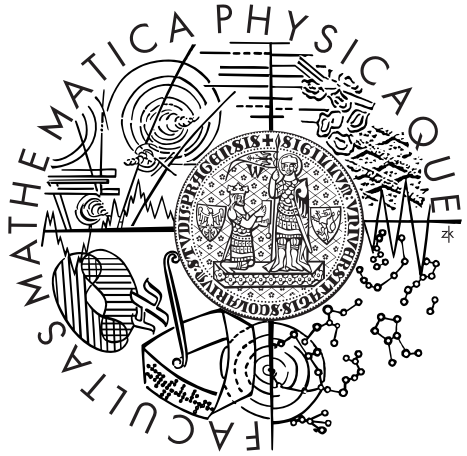
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Tomáš Reichel

Struktura nekomutativních těles

Katedra algebry

Vedoucí bakalářské práce:	Mgr. Jan Žemlička, Ph.D.
Studijní program:	Matematika
Studijní obor:	Obecná matematika

Praha 2015

Své poděkování chci věnovat Mgr. Janu Žemličkovi, Ph.D., který mou práci odborně a svědomitě vedl, věnoval mně a mé práci spoustu času a vždy byl ochoten mi poradit a pomoci.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora:

Název práce: Struktura nekomutativních těles

Autor: Tomáš Reichel

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: V této práci se budeme zabývat zněním a důkazem věty, jež nám umožňuje z cyklických rozšíření těles, která navíc splňují jisté další podmínky, zkonstruovat nekomutativní tělesa. Text od čtenáře vyžaduje základní znalosti z oblasti lineární algebry, okruhů a modulů a k použití věty je pak potřeba jistá zručnost v počítání Galoisových grup. Práce navíc přináší dva základní příklady, které ilustrují použití věty. Během důkazu se čtenář seznámí se strukturou tenzorového součinu a Brauerových grup.

Klíčová slova: nekomutativní těleso, tenzorový součin, Brauerova grupa

Title: Structure of division rings

Author: Tomáš Reichel

Department: Department of Algebra

Supervisor: Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This bachelor thesis deals with a theorem and its proof, which allows construction of division ring from cyclic field extension which satisfies certain conditions. The reader is expected to have basic knowledge of linear algebra, ring and module theory. For using this theorem the reader also needs some skills in counting Galois groups. In this work there are also included two basic examples of usage the theorem. During the proof we introduce a structure of tensor product and Brauer group.

Keywords: division ring, tensor product, Brauer group

Obsah

Úvod

Tato práce se zabývá konstrukcí nekomutativních těles. Ty, na rozdíl od komutativních těles, nejsou tak probádanou oblastí. Nejznámější nekomutativní těleso, tzv. „kvaterniony“, objevil v roce 1843 sir William Rowan Hamilton [6], když se snažil rozšířit komplexní čísla do tří složek namísto dvou.

Text je rozčleněn do čtyř kapitol a předmětem této práce je vyslovit a dokázat větu, která umožňuje nekomutativní tělesa konstruovat. Znění této věty je obsahem druhé kapitoly. Konstrukce se provádí následujícím způsobem: Nalezneme cyklické rozšíření těles, tedy Galoisovo rozšíření s cyklickou Galoisovou grupou, jejíž velikost je stejná jako stupeň rozšíření. Dále musíme nalézt prvek, splňující jisté podmínky, abychom ho mohli použít pro definici násobení. Pak těleso dostaneme jako vektorový prostor nad větším z těles.

Ve třetí a čtvrté kapitole se pak Věta dokazuje. K tomu je potřeba zavést Brauerovy grupy a k jejich zavedení je potřeba se seznámit s tenzorovým součinem. Tenzorovým součinem a Brauerovými grupami se zabývá třetí kapitola. Ve čtvrté se zavede kohomologická grupa, ovšem bez toho, abychom potřebovali znalosti kohomologické teorie, protože této oblasti matematiky bychom se rádi vyhnuli. Tedy pouze definujeme jeji nosnou množinu a operaci a ukážeme, že je definovaná struktura opravdu grupou.

Při práci jsme vycházeli z publikace Richarda S. Pierce: Associative Algebras [1], kde je konstrukční věta dokázána. Naší prací bylo text zjednodušit a přidat mu na čitelnosti, jelikož důkaz věty v knize využívá poznatky získané napříč celou knihou, používají se odkazy na dřívější tvrzení, která jsou zbytečně obecná. U Lemmatu 14 jsme vymysleli alternativní důkaz. Dále jsme doplnili text o důkazy, které autor knihy zřejmě považoval za zřejmé nebo je případně ponechával jako cvičení, například důkaz Věty 8. Poslední přínos je uvedení drobných příkladů v druhé kapitole – použití konstrukční věty ke zkonstruování kvaternionů a příklad, proč konstrukci nelze použít na konečná tělesa.

Kapitola 1

Základní definice a tvrzení

Definice. *Okruhem (s jednotkou) nazveme* $(D, +, -, 0, \cdot, 1)$ *splňující následující podmínky:*

- $(D, +, -, 0)$ *je abelovská grupa*
- $\forall a,b,c \in D : a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $1 \cdot a = a \cdot 1 = a$
- $\forall a,b,c \in D : (a + b) \cdot c = a \cdot c + b \cdot c$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Pokud okruh splňuje ještě podmínku

$$\forall a \in D \setminus \{0\} : \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1,$$

pak mluvíme o nekomutativním tělese (také division ring, skew field).

Poznámka. Nechť R je okruh s jednotkou a $a \in R$ má levou inverzi $b \in R$ a pravou inverzi $c \in R$. Pak $b = c$.

Platí totiž $b \cdot a = 1$ a $a \cdot c = 1$. Pak $b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c$

Poznámka. Tělesem budeme rozumět komutativní těleso.

Definice. *Nechť D je nekomutativní těleso. Pravým (levým) vektorovým prostorem zde budeme nazývat pravý (levý) D-modul.*

Oproti obvyklé definici vektorového prostoru nebudeme tedy požadovat komutativitu tělesa, nad kterým modul uvažujeme. Ve většině případů nebude mít tato změna vliv na platnost vět známých z lineární algebry ani na průběh jejich důkazů. Pouze poupravíme několik základních definic.

Definice. *Nechť V je pravý (levý analogicky) vektorový prostor nad D,* $v_1, \ldots, v_n \in V$.

$v_1, \ldots, v_n$ *jsou lineárně nezávislé, pokud* $\forall k \leq n, \forall d_1, \ldots, d_k \in D : \sum_{i=1}^{k} v_i d_i = 0$ *implikuje* $d_1 = \ldots = d_k = 0$.

$v_1, \ldots, v_n$ *generují V, pokud* $\forall v \in V, \exists d_1, \ldots, d_n \in D : \sum_{i=1}^{n} v_i d_i = v$.

$v_1, \ldots, v_n$ *tvoří bázi V, pokud jsou lineárně nezávislé a generují V.*

Nyní vyslovíme dvě lineárně algebraická lemmata, jejichž důkaz lze dohledat v publikaci prof. Bicana [4] jako tvrzení 2.21, 10.8 a 10.22.

Lemma 1. *Nechť V je vektorový prostor. Pak lze každou lineárně nezávislou množinu A rozšířit na bázi.*

Lemma 2. *Nechť V je vektorový prostor nad tělesem F dimenze k, $\{v_1, \ldots, v_k\}$ báze V a ϕ je endomorfismus na V. Pak ϕ je bijektivní právě tehdy, když matice M zobrazení ϕ vzhledem k $\{v_1, \ldots, v_k\}$ je regulární. Matice M^{-1} je pak maticí zobrazení ϕ^{-1} vzhledem k $\{v_1, \ldots, v_k\}$.*

Dále $End_F(V)$, tedy okruh endomorfismů $V \to V$, je izomorfní okruhu $M_k(F)$ čtvercových matic nad F.

Definice. *Nechť $(F, +, -, 0, \cdot, 1)$ je (komutativní) těleso a nechť $(R, +, -, 0, \cdot, 1)$ je okruh. R nazveme F-algebrou, pokud navíc splňuje axiomy vektorového prostoru nad F a platí:*

$$\forall a,b \in R, \forall k \in F : k \cdot (a \cdot b) = (k \cdot a) \cdot b = a \cdot (k \cdot b)$$

Poznámka. Písmenem F budeme zde vždy označovat komutativní těleso.

Značení. *Izomorfismus F-algeber A a B budeme značit $A \simeq B$.*

Příklad. Nechť A je F-algebra. Pak okruh endomorfismů $End_F(A)$ nese strukturu F-algebry. Násobení prvky F definujeme následujícím způsobem:

$$\phi \in End_F(A), x \in F : x \cdot \phi = (x\cdot) \circ \phi.$$

Definice. *Nechť $R \leq S$ jsou okruhy. Centralizátorem R v S rozumíme $C_S(R) = \{s \in S : r.s = s.r, \forall r \in R\}$. Centrem okruhu R rozumíme $Z(R) = C_R(R)$.*

Lemma 3. *Nechť D je nekomutativní těleso. Pak jeho centrum $Z(D) := \{d \in D : dr = rd, \forall r \in D\}$ je těleso.*

Důkaz: $Z(D)$ je podokruh D, takže je potřeba ověřit jen to, že: $a \in Z(D) \Rightarrow a^{-1} \in Z(D)$. Nechť $r \in D$, pak $a^{-1}r = a^{-1}ra^{-1}a = aa^{-1}ra^{-1} = ra^{-1}$.

□

Definice. *Nechť F je těleso a R je F-algebra. Pokud $Z(R) = \{1 \cdot k : k \in F\}$, pak se R nazývá centrální F-algebrou.*

Definice. *Nechť K je těleso a R je K-algebra. Pokud má R nad K konečnou dimenzi jakožto vektorový prostor, pak řekneme, že je R konečně dimenzionální.*

Definice. *Nechť $T \leq U$ je algebraické rozšíření těles. Jeho Galoisovou grupou nazveme grupu $Gal(U,T) := \{\sigma : U \to U, \sigma$ je T-izomorfismus$\}$.*

Definice. *Nechť $T \leq U$ je rozšíření těles, K jejich algebraický uzávěr. Řekneme, že $T \leq U$ je*

- *separabilní, pokud každé $a \in U$ je kořenem takového polynomu nad T, který nemá vícenásobné kořeny.*

- *normální, pokud* $\forall\phi$ *T-homomorfismus,* $\phi : K \to K$ *je* $\phi(U) = U$.
- *Galoisovo, pokud je normální, separabilní a konečného stupně.*
- *cyklické, pokud je Galoisovo a Gal(U,T) je cyklická grupa.*

Definice. *Okruh R se nazývá jednoduchý, pokud jeho oboustranné ideály jsou jen* $\{0\}$ *a R. K-algebra se nazývá jednoduchá, pokud je jednoduchá jakožto okruh. R-modul se nazývá jednoduchý, pokud jeho podmoduly jsou jen* $\{0\}$ *a M.*

Definice. *Nechť R je okruh a M je pravý (levý) R-modul. M se nazývá polojednoduchý (totálně rozložitelný), pokud existují takové jednoduché R-moduly* N_i*, že* $M \simeq \bigoplus N_i$*. Okruh R se nazveme polojednoduchým (totálně rozložitelným), pakliže je jakožto pravý (levý) R-modul polojednoduchý.*

V další kapitole vyslovíme větu, která nám umožní provést konstrukci nekomutativních těles. V důkazech se nám bude hodit Wedderburn-Artinova věta o rozkladu polojednoduchých okruhů, protože nám umožní nahlížet na složitější struktury jako na maticové okruhy. Zde uvedeme pouze znění, blíže je možno se s touto větou seznámit v literatuře [5]. Typicky je tato věta v literatuře využívá pro okruhy, funguje však stejným způsobem i pro F-algebry, jak za zněním ukážeme.

Věta 4 (Wedderburn-Artinova)**.** *Nechť A je polojednoduchý okruh. Pak existují* $n_1, \ldots, n_k \in \mathbb{N}$ *a nekomutativní tělesa* $D_1, \ldots, D_k$*, že*

$$A \simeq \bigoplus_{i=1}^{k} M_{n_i}(D_i).$$

Dvojice n_i *a* D_i *jsou až na pořadí a izomorfismus určeny jednoznačně.*

Pokud je A dokonce F-algebra, tak nekomutativní tělesa D_i *nesou také strukturu F-algebry a daný izomorfismus je izomorfismus F-algeber.*

$M_i(D_i)$ jsou totiž také F-algebry a jejich podprostor $I_n \cdot d$ $(= D_i)$, kde I_n je jednotková matice a $d \in D_i$, je F-algebra.

Důsledek. Pokud je navíc A jednoduchá, tak existuje $n \in \mathbb{N}$ a nekomutativní těleso se strukturou F-algebry D, že

$$A \simeq M_n(D).$$

Dvojice n a D je určena až na izomorfismus jednoznačně.

Definice. *Normou rozšíření těles* $F \leq E$ *s cyklickou Galoisovou grupou* $G = \langle\sigma\rangle$ *nazveme zobrazení* $N_{E/F} : E \to F^\star$ *definované jako* $N_{E/F}(d) := \prod_{i=0}^{|G|-1} \sigma^i(d)$.

Definice. *Nechť A je centrální, jednoduchá, konečně dimenzionální F-algebra a E je její podalgebrou. Řekneme, že E je ostře maximální podtěleso, jestliže je to těleso a* $dim_F(A) = [E : F]^2$.

Příklad. Kvaterniony $\mathbb{H} = \{a + bi + cj + dk : a,b,c,d \in \mathbb{R}\}$, kde $i^2 = j^2 = k^2 = ijk = -1$, $ij = k$, $jk = i$, $ki = j$, tvoří nekomutativní těleso.

Nyní uvedeme bez důkazu dvě věty z teorie okruhů a modulů. Budou nutné při práci s F-algebrami. Jejich důkazem se zabývá publikace R. Pierce [1] na stranách 220 a 230.

Věta 5 (Noether-Skolemova)**.** *Nechť A je centrální, jednoduchá a konečně dimenzionální F-algebra a B je její jednoduchá podalgebra. Nechť $\phi : B \to A$ je homomorfismus F-algeber.*

Pak existuje $x \in A^\star$ takové, že $\phi(y) = x^{-1}yx, \forall y \in B$.

Věta 6 (Jacobsonova o hustotě)**.** *Nechť A je okruh a M je jednoduchý levý A-modul. Nechť $u_1, \ldots, u_n$ je lineárně nezávislá množina v M jakožto vektorovém prostoru nad nekomutativním tělesem $End_A(M)$. Nechť $w_1, \ldots, w_n \in M$.*

Pak existuje $x \in A$ takové, že $xu_i = w_i, \forall i \in \{1, \ldots, n\}$.

Kapitola 2

Znění hlavní konstrukční věty

Jádrem celé práce je věta, pomocí níž je možné za jistých předpokladů zkonstruovat nekomutativní těleso. V této kapitole vyslovíme její znění a celý zbytek práce se bude zabývat jejím důkazem. Základem konstrukce jsou dvě komutativní tělesa F a E, kde $F < E$ je cyklické rozšíření. Výsledkem pak bude direktní suma kopií E, na její prvky tedy budeme smět nahlížet jako vektory nad tělesem E. Při násobení (které v hlavní větě definujeme) se na souřadnice levého činitele pouští prvky Galoisovy grupy $Gal(E,F)$. To způsobuje nekomutativitu násobení.

Značení. *Celočíselné dělení a div n budeme značit $a \div n$ a zbytek po dělení budeme značit a_n.*

Věta 7. *Nechť $F < E$ je cyklické rozšíření těles stupně n, $G = Gal(E,F) = \langle\sigma\rangle$ je jeho Galoisova grupa řádu n a nechť existuje $a \in F^\star$ takové, že $a^n \in N_{E/F}(E^\star)$ a $a^k \notin N_{E/F}(E^\star), \forall k \leq n$.*

Definujeme $A_\Phi := \bigoplus_{j=0}^{n-1} u^j E$ s násobením $\cdot : A_\Phi \times A_\Phi \to A_\Phi$ definovaným předpisem

$$\sum_{i=0}^{n-1} u^i c_i \cdot \sum_{j=0}^{n-1} u^j d_j = \sum_{i,j=0}^{n-1} u^{(i+j)\_n} \Phi(i,j) \sigma^j(c_i) d_j,$$

kde $\Phi : \{0,\ldots,n-1\}^2 \to F^\star$.

Pokud je $\Phi_a(i,j) := a^{(i+j)\div n}$, pak A_{Φ_a} tvoří nekomutativní těleso.

V literatuře se objekty A_Φ obvykle zvou „crossed product“.

Lemma 8. *Násobení v A_{Φ_a} je asociativní.*

Důkaz: Dokážeme, že zobrazení Φ_a splňuje kocyklickou podmínku, tzn.

$$\Phi_a(i,k)\Phi_a(i+j,k)^{-1}\Phi_a(j,i+k) = \sigma^k(\Phi_a(i,j)).$$

Protože $Im(\Phi_a) \subseteq F^\star$ a $\sigma^k \in Gal(E,F)$, tak $\sigma^k(\Phi_a(i,j)) = \Phi_a(i,j)$.

Protože $\Phi_a(i,j) = a^{(i+j)\div n}$, tak tedy potřebujeme

$$(i+k) \div n - (((i+j)\_n + k) \div n) + ((i+k)\_n + j) \div n = ((i+j) \div n),$$

což platí, protože $((i+j)\_n+k)\div n = (i+j+k)\div n - (i+j)\div n$ a $((i+k)\_n+j)\div n = (i+j+k)\div n - (i+k)\div n$.

Z kocyklické podmínky plyne asociativita, protože rozepíšeme-li násobení z definice, vyjde nám

$$\sum_{k=0}^{n-1} u^k b_k \cdot (\sum_{i=0}^{n-1} u^i c_i \cdot \sum_{j=0}^{n-1} u^j d_j)) =$$
$$= \sum_{k=0}^{n-1} u^k b_k \cdot \sum_{i,j=0}^{n-1} u^{(i+j)\_n} \Phi_a(i,j) \sigma^j(c_i) d_j =$$
$$= \sum_{i,j,k=0}^{n-1} u^{(i+j+k)\_n} \Phi_a((i+j)\_n,k) \Phi_a(i,j) \sigma^{(i+j)\_n}(b_k) \sigma^j(c_i) d_j =$$

Zde pak využijeme kocyklickou podmínku

$$= \sum_{i,j,k=0}^{n-1} u^{(i+j+k)\_n} \Phi_a((i+k)\_n,j) \Phi_a(i,k) \sigma^{(i+j)\_n)}(b_k) \sigma^j(c_i) d_j =$$
$$= \sum_{i,j,k=0}^{n-1} u^{(i+j+k)\_n} \Phi_a((i+k)\_n,j) \Phi_a(i,k) \sigma^j(\sigma^i(b_k) c_i) d_j =$$
$$= \sum_{k,i=0}^{n-1} u^{(k+i)\_n} \Phi_a(k,i) \sigma^i(b_k) c_i \cdot \sum_{j=0}^{n-1} u^j d_j =$$
$$= (\sum_{k=0}^{n-1} u^k b_k \cdot \sum_{i=0}^{n-1} u^i c_i) \cdot \sum_{j=0}^{n-1} u^j d_j.$$

□

Lemma 9. *V každém A_Φ platí pro každé $i,j \in \{0,\ldots,n-1\}$:*

$$(u^{i+j\_n})^{-1} u^i u^j = 1_{A_\Phi} \Phi(i,j).$$

Důkaz: Pro každé u^i existuje inverzní prvek: $(u^i)^{-1} = \Phi(i,n-i)^{-1} u^{n-i}$.

$$(u^{i+j\_n})^{-1} u^i u^j = (u^{i+j\_n})^{-1} (u^{i+j\_n}) \Phi(i,j) = \Phi(i,j).$$

□

Lemma 10. *V každém A_Φ platí pro každé $c \in E$ a pro každé $i \in \{0,\ldots,n-1\}$:*

$$\sigma^i(c) = (u^i)^{-1} c u^i,$$

neboli také:

$$c u^i = u^i \sigma^i(c).$$

Důkaz: Z Lemmatu 9 plyne, že $\Phi(i,0) = \Phi(0,i) = 1$. Pak

$$(u^i)^{-1} (u^0 c u^i) = (u^i)^{-1} (u^i) \Phi(i,0) \sigma^i(c) = \sigma^i(c).$$

□

Poznámka. Jednotka v okruhu A_{Φ_a} je $1_{A_{\Phi_a}} = u^0 \cdot 1_E$.

Pokud je Φ takové, že splňuje kocyklickou podmínku (tedy například Φ_a), pak maximální komutativní podtěleso A_Φ je E, tedy platí $C_{A_{\Phi_a}}(E) = E$.

Poznámka. Pokud je A_{Φ_a}, definované jako výše, nekomutativní těleso, $\{u^i\}$ jeho báze, pak inverzní prvek hledáme následujícím způsobem. Nechť $a \in A_{\Phi_a}$, $a \neq 0$, tzn. $a = \sum_{i=0}^{n-1} a_i u^i$. Pak zobrazení $a\cdot$ je automorfismus na A_{Φ_a}, protože $Ker(a\cdot) = \{0\}$ a $\forall b \in A_{\Phi_a} : a \cdot (a^{-1}b) = b$. Z Lemmatu 8 pak matice M_a zobrazení $a\cdot$ vzhledem k $\{u^i\}$, tedy s prvky $m_{ij} = \sigma^j(a_j).a^{(i+j)\div(n)}, \forall i,j \in \{0,\ldots,n-1\}$, je regulární. Matice $M_a^{-1} = M_{a^{-1}}$ je znovu z Lemmatu 8 matice zobrazení $a^{-1}\cdot$ vzhledem k $\{u^i\}$. Inverzním prvkem k a je pak $M_a^{-1} \cdot (1\,0\,\ldots\,0)^\top$.

Tvrzení 11. *A_Φ je jednoduchá F-algebra.*

Důkaz: Nechť $f : A_\Phi \to B$ je E-lineární epimorfismus F-algeber. Předpokládejme ke sporu, že jeho jádro je neprázdné. Pak vezměme minimální neprázdnou množinu $X \subseteq \mathbb{Z}_n$ takovou, že existují nenulová c_i tak, že $\sum_{i\in X} f(u^i)c_i = 0$.

Tedy i pro každé $e \in E$ platí rovnice:

$$e \cdot 0 = e\sum_{i\in X} f(u^i)c_i = \sum_{i\in X} f(u^i)\sigma^i(e)c_i.$$

Pak ale $\forall i,j, i \neq j : \sigma^i(e) = \sigma^j(e)$, kdyby totiž existovalo nějaké j, pro které by existovala nějaká neprázdná množina $K = \{k : \sigma^k(e) \neq \sigma^j(e)\}$, pak by

$$\sum_{i\in X}(\sigma^i(e) - \sigma^j(e))f(u^i)c_i = 0,$$

a tedy $X\backslash K \subset X$, což je ve sporu s minimalitou X.

Tedy $\sigma^i = \sigma^j, \forall i,j$ a tedy $|X| = 1$, jenže pak by $f(u^i)c_i = 0$, což je ve sporu s tím, že u^i je invertibilní.

Takže $Ker(f) = \emptyset$.

□

Jak konstrukční věta funguje, můžeme předvést na konstrukci nekomutativního tělesa kvaternionů s reálnými koeficienty. Větu použijeme na těleso reálných a těleso komplexních čísel.

Příklad (Konstrukce kvaternionů). Zvolíme $E := \mathbb{C}$ a $F := \mathbb{R}$. $\mathbb{C}/\mathbb{R}$ je cyklické rozšíření. Galoisova grupa $Gal(\mathbb{C},\mathbb{R}) = \{Id, \psi\}$, kde ψ je zobrazení, které komplexnímu číslu přiřadí jeho komplexně sdružené. $Gal(\mathbb{R},\mathbb{C})$ je cyklická řádu 2 a jejím generátorem je ψ.

Dále $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\star) = (0,\infty)$, protože pro $x + iy \in \mathbb{C}^\star$ platí

$$N_{E/F}(x + iy) = Id(x + iy).\psi(x + iy) = \sqrt{x^2 + y^2}$$

Vezmeme tedy za $a \in \mathbb{R}^\star$ nějaký záporný prvek $\mathbb{R}$ (vezmu $a = -1$), protože pak $a \notin (0,\infty)$, ale $a^2 \in (0,\infty)$. Pak

- $A_{\Phi_a} = \mathbb{H} = \mathbb{C} \oplus u\mathbb{C}$,
- $\mathbb{H}$ má nad $\mathbb{R}$ stupeň rozšíření 4, generátory jsou $\{1, i, u, iu\}$. Platí pro ně následující vztahy:

$$i\cdot i = -1, u\cdot u = u^{2mod(2)}\cdot(-1)^{2div(2)} = -1, iu\cdot iu = u^{2mod(2)}\cdot(-1)^{2div(2)}\cdot\bar{i}\cdot i = -1$$

$$i \cdot u = iu, u \cdot iu = i, iu \cdot i = u, i \cdot u \cdot iu = -1$$

- Inverze se spočítá následujícím způsobem. Nechť $h \in \mathbb{H}$, $h = a + bi + cu + dui$, $h \neq 0$. Pak $M_h = \binom{a+ib\ -c+id}{c+id\ a-ib}$. Prvek $\binom{1}{0} M_h^{-1}$ je inverzní k h.

Kvaterniony s racionálními koeficienty dostaneme konstrukcí z těles $\mathbb{Q}$ a $\mathbb{Q}(i)$.

Nyní si ukážeme, v jakém bodě konstrukce ztroskotá při použití na konečná tělesa, protože konečné nekomutativní těleso neexistuje.

Příklad. Nechť $\mathbb{F}_{p^n} \leq \mathbb{F}_{p^m}$, kde $m = n \cdot k$, je rozšíření konečných těles. $Gal(\mathbb{F}_{p^m}, \mathbb{F}_{p^n}) = \langle \phi \rangle$, kde ϕ je Frobeniův endomorfismus $x \mapsto x^{p^n}$. $Gal(\mathbb{F}_{p^m}, \mathbb{F}_{p^n})$ má řád k.

Není ale splněna poslední podmínka konstrukce. Platí, že multiplikativní grupy $\mathbb{F}_q^\star$ jsou cyklické ([3], Věta 3.3).

Nechť x je generátor $\mathbb{F}_{p^m}^\star$. Každý prvek $y \in \mathbb{F}_{p^m}^\star$ lze psát jako x^i pro nějaké $i \in \{0, \ldots, p^m - 2\}$ Pak

$$N_{\mathbb{F}_{p^m}/\mathbb{F}_{p^n}}(x) = \prod_{i=0}^{k-1} \phi^i(x) = \prod_{i=0}^{k-1} x^{p^{in}} = x^{\sum_{i=0}^{k-1} p^{in}} = x^{\frac{1-p^m}{1-p^n}}$$

Tedy z cykličnosti $\mathbb{F}_{p^m}^\star$: $N_{\mathbb{F}_{p^m}/\mathbb{F}_{p^n}}(\mathbb{F}_{p^m}^\star) = \{x^{i\frac{p^m-1}{p^n-1}}, i \in \{0, \ldots, p^m - 2\}\} \leq \mathbb{F}_{p^n}^\star$.

Protože ale $x^{p_m - 1} = x$, tak $\{x^{i\frac{p^m-1}{p^n-1}}, i \in \{0, \ldots, p^m - 2\}\}$ má právě $p^n - 2$ prvků, stejně jako $\mathbb{F}_{p^n}^\star$. Tedy $N_{\mathbb{F}_{p^m}/\mathbb{F}_{p^n}}(x) = \mathbb{F}_{p^n}^\star$.

Proto nám tato konstrukce nemůže zkonstruovat konečné nekomutativní těleso, které podle Wedderburnovy věty o konečných tělesech neexistuje.

Kapitola 3

Tenzorový součin a Brauerovy grupy

Nejobtížnější krok v důkazu toho, že A_{Φ_a} je skutečně nekomutativní těleso, je důkaz existence inverzního prvku. Žádné přímočaré řešení není vidět, proto na množině centrálních jednoduchých F-algeber definujeme strukturu abelovské grupy (tzn. Brauerova grupa). V této grupě je operace násobení definována pomocí tenzorového součinu, tak abychom mohli dokázat, že Brauerova grupa je opravdu abelovskou grupou, potřebujeme nejdříve definovat tenzorový součin a pak o něm dokázat několik tvrzení.

Definice. *Nechť A a B jsou F-algebry s bázemi $\{a_i\}$ a $\{b_j\}$. Pak tenzorový součin $A \otimes_F B$ (nebo jen $A \otimes B$) je F-algebra generovaná F-lineárními kombinacemi báze $\{a_i \otimes b_j\}$. Pro prvky $a = \sum_i f_i a_i \in A$, $b = \sum_j g_j b_j$ definujeme v $A \otimes B$ prvek $a \otimes b := \sum_{ij} f_i g_j a_i \otimes b_j$.*

Dále na $A \otimes B$ zavedeme multiplikativní operaci $\cdot$ definovanou na bázi jako:

$$(a_{i_1} \otimes b_{j_1}) \cdot (a_{i_2} \otimes b_{j_2}) = (a_{i_1} a_{i_2}) \otimes (b_{j_1} b_{j_2}),$$

která splňuje podmínku bilinearity, tedy

$$s(a \otimes b) = sa \otimes b = a \otimes sb, \forall s \in F, a \in A, b \in B,$$

$$(a_{i_1} + a_{i_2}) \otimes (b_j) = a_{i_1} \otimes b_j + a_{i_2} \otimes b_j,$$
$$a_i \otimes (b_{j_1} + b_{j_2}) = a_i \otimes b_{j_1} + a_i \otimes b_{j_2}.$$

Poznámka. Každý prvek $a \otimes b$ lze zapsat jako $(1 \otimes b)(a \otimes 1)$. Vezměme totiž jako první prvek báze A i báze B jednotku. Vyjádřeme si a,b vzhledem k bázím, tedy $a = \sum \alpha_i a_i$, $b = \sum \beta_i b_i$. Pak platí, že $1 \otimes b = \sum \beta_i (1 \otimes b_i)$ a stejně tak $a \otimes 1 = \sum \alpha_i (a_i \otimes 1)$. Celkem tedy

$$(1 \otimes b)(a \otimes 1) = \sum_{i,j} \alpha_i \beta_j (a_i \otimes b_j) = a \otimes b.$$

Definice. *Nechť $R = (R, +, -, 0, \cdot, 1)$ je okruh. Okruh $R^{op} := (R, +, -, 0, \times, 1)$, kde $x \times y = y \cdot x, \forall x,y \in R$ nazveme opačným okruhem k R.*

Lemma 12. *Nechť C je F-algebra a S, T jsou její konečně dimenzionální podalgebry. Nechť všechny prvky z S komutují se všemi prvky z T a nechť S je centrální jednoduchá F-algebra. Buďte $s_1, \ldots, s_n \in S$ lineárně nezávislé a $t_1, \ldots t_n \in T$ takové, že $s_1t_1 + \ldots + s_nt_n = 0$.*

Pak $t_1 = \ldots = t_n = 0$.

Důkaz: Chceme využít Jacobsonovu větu o hustotě, proto musíme splnit její požadavky. K jejímu použití potřebujeme jednoduchý levý modul, v tomto případě tuto roli hraje S jakožto jednoduchý (protože S je jednoduchý okruh) levý $S \otimes S^{op}$-modul. Dále $s_1, \ldots, s_n$ je lineárně nezávislá množina v S jakožto vektorovém prostoru nad $End_{S\otimes S^{op}}(S) = F$. Využijme tedy nyní n-krát Jacobsonovu větu o hustotě a tím pro každé $i \in \{1, \ldots, n\}$ získáme takové x_i, že $x_i s_i = 1$ a $x_i s_j = 0, \forall j \neq i$. Abychom mohli tyto x_i násobit s prvky z T, definujeme na C strukturu $S \otimes S^{op}$-T-bimodulu předpisem: $(s \otimes \tilde{s})c = \tilde{s}cs, \forall s, \tilde{s} \in S, c \in C$.

Bimodul je takto dobře definován, protože

$$s \otimes \tilde{s}(ct) = \tilde{s}(ct)s = (\tilde{s}cs)t = ((s \otimes \tilde{s})c)t, \forall s, \tilde{s} \in S, t \in T, c \in C.$$

Konečně můžeme vynásobit rovnici $s_1t_1 + \ldots + s_nt_n = 0$ postupně všemi prvky x_i a pro každé nám vyjde:

$$0 = x_i(s_1t_1 + \ldots + s_nt_n) = x_is_1t_1 + \ldots + x_is_nt_n = t_i.$$

A tedy $t_1 = \ldots = t_n = 0$.

□

Tvrzení 13. *Nechť A,B jsou centrální, jednoduché, konečně dimenzionální F-algebry. Pak $A \otimes B$ je centrální, jednoduchá, konečně dimenzionální F-algebra.*

Důkaz: Zvolme báze F-algeber $Z(A)$ resp. $Z(B)$ jako $\{a_1, \ldots, a_\nu\}$ resp. $\{b_1, \ldots, b_\mu\}$ a doplňme je do bází $\{a_1, \ldots, a_n\}$ a $\{b_1, \ldots, b_m\}$ F-algeber A a B.

Centrální: Chceme dokázat, že $Z(A \otimes B) = Z(A) \otimes Z(B)$. Nejprve dokážeme inkluzi $Z(A \otimes B) \supseteq Z(A) \otimes Z(B)$. Nechť $x \in Z(A) \otimes Z(B)$. Pak $x = \sum x_{i,j=1}^{\nu,\mu} a_i \otimes b_j$, tedy a_i a b_j komutují se všemi ostatními prvky bází. Nechť $y \in A \otimes B$, $y = \sum y_{ij} a_i \otimes b_j$. Pak $xy = \sum x_{ij}y_{kl}a_ia_k \otimes b_jb_l = \sum y_{kl}x_{ij}a_ka_i \otimes b_lb_j = yx$, takže $x \in Z(A \otimes B)$.

Nyní dokazujeme opačnou inkluzi. Platí, že $Z(A \otimes B) = C_{A\otimes B}(A \otimes F) \cap C_{A\otimes B}(F \otimes B)$, protože

$$\forall a \otimes b \in Z(A \otimes B), \forall c \otimes d \in A \otimes B : (a \otimes b)(c \otimes d) = (a \otimes b)(1 \otimes c)(d \otimes 1) =$$

$$= (1 \otimes c)(a \otimes b)(d \otimes 1) = (1 \otimes c)(d \otimes 1)(a \otimes b) = (c \otimes d)(a \otimes b).$$

Dokážeme, že $C_{A\otimes B}(A \otimes F) \subseteq Z(A) \otimes B$ (stejně tak analogicky $C_{A\otimes B}(F \otimes B) \subseteq A \otimes Z(B)$). Nechť $w \in C_{A\otimes B}(A \otimes F)$, $w = \sum x_j \otimes b_j$ pro nějaké $x_j \in A$. Pak $\forall x \in A : 0 = w(x \otimes 1) - (x \otimes 1)w = \sum (xx_j - x_jx) \otimes b_j$. Tedy $xx_j = x_jx$ a tedy $x_j \in Z(A), \forall x_j$.

Celkem tedy platí

$$Z(A \otimes B) = C_{A\otimes B}(A \otimes F) \cap C_{A\otimes B}(F \otimes B) = (Z(A) \otimes B) \cap (A \otimes Z(B)) = Z(A) \otimes Z(B).$$

Jednoduchá: Dokážeme, že každý nenulový homomorfismus F-algeber ϕ z $A \otimes B$ má nulové jádro. Nechť $\phi : A \otimes B \to C$, kde C je libovolná F-algebra, je homomorfismus F-algeber. Protože $A \otimes F \simeq A$ a $F \otimes B \simeq B$ jsou jednoduché algebry, tak $\phi|_{A\otimes F}$ a $\phi|_{F\otimes B}$ jsou prosté. Nechť $z \in Ker(\phi)$. Pak $\exists n \in \mathbb{N} : z = (a_1 \otimes b_1) + \ldots + (a_n \otimes b_n)$, kde $\{a_i\}$ jsou lineárně nezávislé prvky A. Tedy

$$\phi(z) = \phi((a_1 \otimes b_1) + \ldots + (a_n \otimes b_n)) = \phi((a_1 \otimes 1)(1 \otimes b_1) + \ldots + (a_n \otimes 1)(1 \otimes b_n)) =$$

$$= \phi((a_1 \otimes 1)\phi(1 \otimes b_1) + \ldots + \phi(a_n \otimes 1)\phi(1 \otimes b_n)) = 0.$$

Protože $\phi(A)$ je konečně generovaná F-algebra, tak z předchozího Lemmatu plyne, že

$$\phi(1 \otimes b_1) = \ldots = \phi(1 \otimes b_n) = 0.$$

A tedy, protože $(1 \otimes B)$ je jednoduchý, $1 \otimes b_1 = \ldots = 1 \otimes b_n = 0$. Proto také $z = 0$ a tedy $Ker(\phi) = \{0\}$.

Protože je každý nenulový homomorfismus z $A \otimes B$ prostý, tak $A \otimes B$ je jednoduchý. Kdyby nebyl jednoduchý, existoval by nějaký vlastní ideál I. Pro zobrazení $\psi : A \otimes B \in (A \otimes B)/I$ definované předpisem $\psi(x) = [x]_I$ platí $Ker(\psi) = I$, což je spor. Tedy $A \otimes B$ musí být jednoduchá.

Konečně dimenzionální: Protože $\{a_i\}$ i $\{b_j\}$ jsou konečné, tak i báze $\{a_i \otimes b_j\}$ F-algebry $A \otimes B$ je konečná.

□

Lemma 14. *Nechť D je F-algebra a nekomutativní těleso, pak*

$$M_a(F) \otimes M_b(D) \simeq M_{ab}(D).$$

Důkaz: Nechť $A = (f_{ij})_{i,j=1}^{a} \in M_a(F)$ a $B = (d_{ij})_{i,j=1}^{b} \in M_b(D)$ jsou libovolné matice.

Definujeme zobrazení $\phi : M_a(F) \otimes M_b(D) \to M_{ab}(D)$ na generující množině předpisem:

$$\phi(A \otimes B) = (A \cdot d_{ij})_{i,j=1}^{b}.$$

Dokážeme, že ϕ je izomorfismus F-algeber. Nejdříve ukážeme, že je to homomorfismus F-algeber. Využijeme při tom toho, že matice A má prvky z F, takže s prvky z D komutuje.

$$\phi(A\tilde{A} \otimes B\tilde{B}) = \phi(A\tilde{A} \otimes (\sum_{k=1}^{b} d_{ik}\tilde{d_{kj}})_{i,j=1}^{b}) = (A\tilde{A} \sum_{k=1}^{b} d_{ik}\tilde{d_{kj}})_{i,j=1}^{b} =$$

$$= (\sum_{k=0}^{b} A \cdot d_{ij} \cdot \tilde{A} \cdot \tilde{d_{ij}})_{i,j=1}^{b} = (A \cdot d_{ij})_{i,j=1}^{b}(\tilde{A} \cdot \tilde{d_{ij}})_{i,j=1}^{b} = \phi(A \otimes B)\phi(\tilde{A} \otimes \tilde{B}).$$

$$\phi(A+\tilde{A}\otimes B) = ((A+\tilde{A})d_{ij})_{i,j=1}^{b} = (A+d_{ij})_{i,j=1}^{b} + (\tilde{A}d_{ij})_{i,j=1}^{b} = \phi(A\otimes B)+\phi(\tilde{A}\otimes B).$$

$$\phi(A\otimes B+\tilde{B}) = (A(d_{ij}+\tilde{d_{ij}}))_{i,j=1}^{b} = (A+d_{ij})_{i,j=1}^{b} + (A\tilde{d_{ij}})_{i,j=1}^{b} = \phi(A\otimes B)+\phi(A\otimes\tilde{B}).$$

Protože $M_a(F)$ i $M_b(D)$ jsou jednoduché F-algebry, tak z Tvrzení 13 je i $M_a(F)\otimes M_b(D)$ jednoduchá F-algebra. Tím pádem homomorfismus ϕ musí být buď prostý, nebo nulový. A jelikož například $\phi(I_a \otimes I_b) = I_{ab} \neq 0$, tak ϕ je prostý.

Aby byl ϕ také na, stačí z lineárně algebraických důvodů, aby měly $M_a(F) \otimes M_b(D)$ a $M_{ab}(D)$ stejnou dimenzi nad F.

Nechť $dim_F(D) = n$, báze $M_a(F) = \{e_{11}, \ldots, e_{aa}\}$, báze $M_b(D) = \{d_{111}, \ldots, d_{bbn}\}$ a báze $M_{ab}(D) = \{f_{111}, \ldots, f_{ab,ab,n}\}$. Báze $M_a(F) \otimes M_b(D)$ je tedy $\{e_{11} \otimes d_{111}, \ldots, e_{aa} \otimes d_{bbn}\}$. $M_a(F) \otimes M_b(D)$ a $M_{ab}(D)$ jsou tedy oba vektorové prostory nad F dimenze a^2b^2n, takže ϕ je skutečně na a tedy izomorfismus.

□

Lemma 15 (Schur)**.** *Nechť R je okruh a M je jednoduchý R-modul. Pak $End_R(M)$ je nekomutativní těleso.*

Důkaz: Nechť ϕ je nenulový endomorfismus $M \to M$. $Ker(\phi) = \{0\}$, jinak by kvůli jednoduchosti muselo být $Ker(\phi) = M$ a ϕ by byl nulový. Stejně tak $Im(\phi) = M$, protože kdyby $Im(\phi) = \{0\}$, tak by ϕ byl nulový. Takže ϕ je izomorfismus, a tak existuje jeho inverze.

□

Nyní zavedeme pojem Brauerovy grupy. Na množině F-algeber definujeme pomocí tenzorového součinu strukturu grupy a následně v Tvrzení 16 dokážeme, že daná struktura je skutečně dobře definovanou grupou.

Definice (Brauerova grupa)**.** *Nechť F je těleso, na konečně dimenzionálních, centrálních, jednoduchých F-algebrách definujeme ekvivalenci $\sim$ předpisem:*

$A \sim B \equiv \exists D$ nekomutativní těleso a F-algebra a $\exists m,n \in \mathbb{N} : A \simeq M_n(D), B \simeq M_m(D)$

Pak definujeme grupu

$\boldsymbol{B}(F) = \{[A]_\sim : A$ je konečně dimenzionální, centrální, jednoduchá F-algebra$\}$

Násobení: $[A]_\sim \cdot [B]_\sim := [A \otimes B]_\sim$

Inverzní prvek: $[A]_\sim^{-1} = [A^{op}]_\sim$

Jednotka: $1_{\boldsymbol{B}(F)} = [F]_\sim$

Poznámka.

$$A \sim B \iff \exists n,m \in \mathbb{N} : A \otimes M_n(F) \simeq B \otimes M_m(F)$$

Důkaz: Pokud $A \sim B$, tedy $A \simeq M_m(D)$ a $B \simeq M_n(D)$, pak podle Lemmatu 14

$$A \otimes M_m(F) \simeq M_{nm}(D) \simeq B \otimes M_n(F).$$

Naopak nechť $\exists n,m \in \mathbb{N} : A \otimes M_n(F) \simeq B \otimes M_m(F)$. Z Wedderburnovy věty víme, že $\exists D_1,D_2$ nekomutativní tělesa a $s,t \in \mathbb{N}$, že $A \simeq M_s(D_1)$ a $B \simeq M_t(D_2)$. Tedy máme, že $M_{ns}(D_1) \simeq M_{mt}(D_2)$ a protože Wedderburnova věta říká, že D_1, D_2 jsou určeny jednoznačně, tak $D_1 \simeq D_2$.

□

Tvrzení 16. *Brauerova grupa je abelovská grupa.*

Důkaz: Tvrzení 13 nám říká, že pro každé A,B centrální jednoduché F-algebry je $A \otimes B$ centrální jednoduchá F-algebra.

Nyní dokážeme, že stačí je násobení v Brauerově grupě dobře definováno. Nechť $A \sim B$ a $C \sim D$. Pak chceme $A \otimes C \sim B \otimes D$. Z Poznámky víme, že $A \otimes M_a(F) \simeq B \otimes M_b(F)$, $C \otimes M_c(F) \simeq D \otimes M_d(F)$. Pak

$A \otimes C \otimes M_{ac}(F) \simeq A \otimes M_a(F) \otimes C \otimes M_c(F) \simeq B \otimes M_b(F) \otimes D \otimes M_d(F) \simeq B \otimes D \otimes M_{bd}(F)$, tedy znovu z Poznámky $A \otimes C \sim B \otimes D$.

Jednotka: $\forall A$ F-algebru s bází $\{a_i\}, a_0 = 1_A$ je $A \simeq (A \otimes F)$ pomocí izomorfismu $a_i \mapsto a_i \otimes 1$. To je zřejmě izomorfismus, protože F má jakožto F-algebra bázi $\{1\}$.

Asociativita: $\forall A,B,C$ F-algebry s bázemi $\{a_i\}, \{b_j\}, \{c_k\}, a_0 = 1_A, b_0 = 1_B, c_0 = 1_C$ je $A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C$ pomocí izomorfismu $a_i \otimes (b_j \otimes c_k) \mapsto (a_i \otimes b_j) \otimes c_k$.

Komutativita: $\forall A,B$ F-algebry s bázemi $\{a_i\}, \{b_j\}, a_0 = 1_A, b_0 = 1_B$ je $A \otimes B \simeq B \otimes A$ pomocí izomorfismu $a_i \otimes b_j \mapsto b_j \otimes a_i$.

Inverzní prvek: Chceme dokázat, že $\forall A$ F-algebru s bází $\{a_i\}, a_0 = 1_A$: $A \otimes A^{op} \simeq M_k(F)$. Nejprve dokážeme, že $A \otimes A^{op} \simeq End_F(A)$. Definujeme zobrazení $\Psi : A \otimes A^{op} \to End_F(A)$, které přiřadí prvku $\sum_{j,k=0}^{n-1} s_{jk} a_j \otimes a_k$ zobrazení $A \to A$ definované předpisem $x \mapsto \sum_{j,k=0}^{n-1} s_{jk} a_j x a_k$. Ověříme, že je Ψ dobře definovaný izomorfismus.

Potřebujeme ukázat, že $x \mapsto \sum_{j,k=0}^{n-1} s_{jk} a_j x a_k$ je endomorfismus F-algeber $A \to A$.

- $\forall x \in A : \sum_{j,k=0}^{n-1} s_{jk} a_j x a_k \in A$
- $\forall x,y \in A : \sum_{j,k=0}^{n-1} s_{jk} a_j (x+y) a_k = \sum_{j,k=0}^{n-1} s_{jk} a_j x a_k + \sum_{j,k=0}^{n-1} s_{jk} a_j y a_k$ z distributivity
- $\forall x \in A, f \in F : \sum_{j,k=0}^{n-1} s_{jk} a_j (xf) a_k = (\sum_{j,k=0}^{n-1} s_{jk} a_j x a_k) f$.

$\Psi(\sum_{j,k=0}^{n-1} s_{jk} a_j \otimes a_k + \sum_{j,k=0}^{n-1} t_{jk} a_j \otimes a_k) = \Psi(\sum_{j,k=0}^{n-1} (s_{jk} + t_{jk}) a_j \otimes a_k) = (x \mapsto \sum_{j,k=0}^{n-1} (s_{jk} + t_{jk}) a_j x a_k) = (x \mapsto \sum_{j,k=0}^{n-1} s_{jk} a_j x a_k) + (x \mapsto \sum_{j,k=0}^{n-1} t_{jk} a_j x a_k) = \Psi(\sum_{j,k=0}^{n-1} s_{jk} a_j \otimes a_k) + \Psi(\sum_{j,k=0}^{n-1} t_{jk} a_j \otimes a_k)$.

Při ověřování $\Psi(a.b) = \Psi(a) \circ \Psi(b)$ se využije převráceného násobení v opačné algebře.

$\Psi(\sum_{j,k=0}^{n-1} s_{jk} a_j \otimes a_k \cdot \sum_{\mu,\nu=0}^{n-1} t_{\mu\nu} a_\mu \otimes a_\nu) = \Psi(\sum_{j,k,\mu,\nu=0}^{n-1} s_{jk} \cdot t_{\mu\nu} a_j \cdot a_\mu \otimes a_\nu \cdot a_k) = (x \mapsto \sum_{j,k,\mu,\nu=0}^{n-1} s_{jk} \cdot t_{\mu\nu} a_j \cdot a_\mu x a_\nu \cdot a_k) = (x \mapsto \sum_{j,k=0}^{n-1} s_{jk} a_j (\sum_{\mu,\nu=0}^{n-1} t_{\mu\nu} a_\mu x a_\nu) a_k) = (x \mapsto \sum_{j,k=0}^{n-1} s_{jk} a_j \otimes a_k) \circ (x \mapsto \sum_{\mu,\nu=0}^{n-1} t_{\mu\nu} a_\mu \otimes a_\nu) = \Psi(\sum_{j,k=0}^{n-1} s_{jk} a_j \otimes a_k) \circ \Psi(\sum_{\mu,\nu=0}^{n-1} t_{\mu\nu} a_\mu \otimes a_\nu)$.

Bijekce: $Ker(\Psi)$ je ideál v $A \otimes A^{op}$, což je jednoduchá F-algebra, tedy $Ker(\Psi) = \{0\}$ nebo $Ker(\Psi) = A \otimes A^{op}$, ale $\Psi(a_0 \otimes a_0) = \Psi(1 \otimes 1) = (x \mapsto x) = Id \neq (x \mapsto 0)$, takže $Ker(\Psi) \neq A \otimes A^{op}$, takže $Ker(\Psi) = \{0\}$, což znamená, že Ψ je prosté. Naopak protože $Im(\Psi) \leq End_F(A)$, $dim_F(A \otimes A^{op}) = dim_F(End_F(A))$ a Ψ je prosté, tak je Ψ i na celé $End_F(A)$.

Z Lemmatu 2 plyne, že $End_F(A) \simeq M_n(F)$, kde n je takové, že $n^2 = dim_F(End_F(A))$.

□

Definice. *Nechť $F \leq E$ je rozšíření těles. Jádro homomorfismu $\kappa : \boldsymbol{B}(F) \to \boldsymbol{B}(E)$, $\kappa([A]) = [A \otimes_F E]$ nazveme relativní Brauerovou grupou a značíme $\boldsymbol{B}(E/F)$.*

Tvrzení 17. *$\boldsymbol{B}(E/F)$ je podgrupou $\boldsymbol{B}(F)$ a $[A_{\Phi_a}]_\sim$ je prvkem $\boldsymbol{B}(E/F)$.*

Důkaz: První část Tvrzení je zřejmá. V té druhé potřebujeme dokázat, že $A_{\Phi_a} \otimes_F E \simeq M_n(E)$. Připomeňme, že z definice A_{Φ_a} nám plyne $C_{A_{\Phi_a}}(E) = E$.

Nejprve $C_{A_{\Phi_a}}(E) \simeq End_{A_{\Phi_a} \otimes E}(A_{\Phi_a})$ pomocí izomorfismu $\rho : x \mapsto \rho_x = \cdot x$ pro $x \in C_{A_{\Phi_a}}(E)$. Platí, že A_{Φ_a} a $End_{A_{\Phi_a}}(A_{\Phi_a})$ jsou izomorfní jakožto F-algebry zobrazením $\rho : x \mapsto \rho_x = \cdot x$ pro $x \in A_{\Phi_a}$. $Ker(\rho) = \{0\}$, protože $a.x = 0, \forall a \in A_{\Phi_a}$ splňuje pouze 0, takže ρ je prosté. Je i na, protože $\forall \phi \in End_{A_{\Phi_a}}(A_{\Phi_a}) : \phi(x) = \phi(x \cdot 1) = x \cdot \phi(1)$ a tedy $\phi = \rho(\phi(1))$.

Na A_{Φ_a} definujeme strukturu levého $(A_{\Phi_a} \otimes E)$-modulu předpisem: $(b \otimes e) \cdot a = bae, \forall a,b \in A_{\Phi_a}, e \in E$. A_{Φ_a} splňuje axiomy $(A_{\Phi_a} \otimes E)$-modulu, protože:

$$(1) \quad a \otimes e, b \otimes f \in A_{\Phi_a} \otimes E, x \in A_{\Phi_a} : ((a \otimes e) + (b \otimes f))x =$$

$$= (\sum_{i,j,k=0}^{n-1} (a_{ijk} + b_{ijk})(u^i e_j \otimes e_k))x = \sum_{i,j,k=0}^{n-1} (a_{ijk} + b_{ijk})(u^i e_j x e_k) =$$

$$= \sum_{i,j,k=0}^{n-1} a_{ijk}(u^i e_j \otimes e_k) + \sum_{i,j,k=0}^{n-1} (b_{ijk})(u^i e_j \otimes e_k) = (a \otimes e)x + (b \otimes f)x$$

$$(2) \quad a \otimes e, b \otimes f \in A_{\Phi_a} \otimes E, x \in A_{\Phi_a} : ((a \otimes e)(b \otimes f))x =$$

$$= (\sum_{i,j,k,l,\mu,\nu=0}^{n-1} (a_{ij\mu} \cdot b_{kl\nu})(u^i e_j \cdot u^k e_l \otimes e_\mu \cdot e_\nu))x =$$

$$= (\sum_{i,j,k,l,\mu,\nu=0}^{n-1} (a_{ij\mu} \cdot b_{kl\nu})(u^i e_j \cdot u^k e_l x e_\mu \cdot e_\nu)) =$$

$$= (\sum_{i,j,k,l,\mu,\nu=0}^{n-1} (a_{ij\mu} \cdot b_{kl\nu})(u^i e_j \cdot u^k e_l x e_\nu \cdot e_\mu)) = (a \otimes e)((b \otimes f)x)$$

$$(3) \quad a \otimes e \in A_{\Phi_a} \otimes E, x,y \in A_{\Phi_a} : (a \otimes e)(x + y) = a(x + y)e = axe + aye$$

$$(4) \quad x \in A_{\Phi_a} : (1_{A_{\Phi_a}} \otimes 1)x = 1_{A_{\Phi_a}} xe = x$$

Dokážeme, že $\rho(C_{A_{\Phi_a}}(E)) \subseteq End_{A_{\Phi_a} \otimes E}(A)$. Nechť $x \in E, y \in C_{A_{\Phi_a}}(E) = E, a,b \in A_{\Phi_a}$. Pak $\rho_y((a \otimes x) \cdot b) = abxy = abyx = \rho_y(b) \cdot (a \otimes x)$.

Naopak vezmeme-li nějaký prvek $\rho_y \in End_{A_{\Phi_a} \otimes E}(A), y \in A_{\Phi_a}$, pak $\forall x \in E :$ $xy = \rho_y(x) = \rho_y((1 \otimes x) \cdot 1) = (1 \otimes x) \cdot \rho_y(1) = (1 \otimes x) \cdot y = yx$, a tedy $y \in C_{A_{\Phi_a}}(E) = E$.

Nakonec $A_{\Phi_a} = \bigoplus_1^k P$, $A_{\Phi_a} \otimes E = \bigoplus_1^n P$, kde P je jednoduchý modul, dále D označíme $End_{A_{\Phi_a} \otimes E}(P)$, což je nekomutativní těleso ze Schurova lemmatu.

$E = C_{A_{\Phi_a}}(E) \simeq End_{A_{\Phi_a} \otimes E}(A_{\Phi_a}) \simeq End_{A_{\Phi_a} \otimes E}(\bigoplus kP) \simeq M_k(D) \sim M_n(D) \simeq End_{A_{\Phi_a} \otimes E}(\bigoplus nP) \simeq End_{A_{\Phi_a} \otimes E}(A_{\Phi_a} \otimes E) = A_{\Phi_a} \otimes E$.

□

Kapitola 4

Kohomologické grupy a důkaz hlavní věty

V této kapitole pomocí již dokázaných vět a lemmat dokážeme hlavní větu této práce. Pomocí sady nerovností dokážeme rovnost tzn. stupně, indexu a exponentu naší zkonstruované F-algebry A_{Φ_a}. K důkazu jedné z nerovností je potřeba využít izomorfismu Brauerových grup a jistých kohomologických grup, ale protože se chceme vyhnout teorii algebraické topologie, tak definujeme jen jednu konkrétní grupu potřebnou pro provedení důkazu, aby nebylo třeba mít žádné znalosti kohomologie.

Lemma 18. *A_{Φ_a} má nad F dimenzi n^2.*

Důkaz: $A_{\Phi_a} = \bigoplus_{i=0}^{n-1} u^i E$ má nad E dimenzi n a $[E : F] = n$, protože $F \leq E$ je Galoisovo a tedy $[E : F] = |Gal(E,F)|$.

Nechť E má nad F bázi $\{e_1, \ldots, e_n\}$. Pak $\{u^i e_j\}$ je bází A nad F.

□

Definice. *Nechť A je konečně dimenzionální centrální jednoduchá F-algebra, F je těleso, tj. $A \simeq M_n(D)$ pro nějaké nekomutativní těleso s $Z(D) = F$. Pak*

- *Stupeň $Deg(A) := \sqrt{dim_F A}$,*
- *Index $Ind(A) := Deg(D)$,*
- *Exponent $Exp(A)$ je řád $[A]_\sim$ v Brauerově grupě $\boldsymbol{B}(F)$.*

Nyní je potřeba definovat kohomologické grupy.

Definice. *Nechť $F < E$ je cyklické rozšíření těles s Galoisovou grupou $G = \langle\sigma\rangle$ a A je F-algebra. Pak definujeme*

$C^k = \{\phi : \mathbb{Z}_n^k \to E^\star\}$,

$\delta^{(1)} : C^1 \to C^2, \delta^{(1)}_\Phi(i,j) = \Phi(j)\Phi(i+j)^{-1}\sigma^j(\Phi(i))$,

$\delta^{(2)} : C^2 \to C^3, \delta^{(2)}_\Phi(i,j,k) = \Phi(j,k)\Phi(i+j,k)^{-1}\Phi(i,j+k)(\sigma^k(\Phi(i,j)))^{-1}$.

Dále definujeme následující grupu $Z^2 = (Ker(\delta^{(2)}), \cdot, ^{-1}, 1)$, přičemž násobení $\cdot$ a inverze je v tělese E.

Normální podgrupou grupy Z^2 je $B^2 = Im(\delta^{(1)})$.

A nakonec definujme ještě faktorgrupu $H^2 = Z^2/B^2$.

Poznámka. Z^2 a B^2 jsou dobře definované abelovské grupy, jelikož operace v nich se počítají v tělese E.

Dále B^2 je podgrupou Z^2, protože $\delta^{(2)}_{\delta^{(1)}_\Phi}(i,j,k) = 1$, jak se snadno ukáže pouze dosazením.

Nakonec protože jsou Z^2 a B^2 abelovské grupy, tak je B^2 taky normální podgrupou. Tím pádem je i H^2 dobře definovaná grupa.

Následující lemma nebudeme dokazovat (viz závěr), v literatuře [1] se jím zabývá kapitola 14.3 na straně 256.

Lemma 19.

$$\forall \Phi,\Psi \in Z^2 : A_{\Phi\Psi} \sim A_\Phi \otimes A_\Psi.$$

Tvrzení 20. *H^2 a $\boldsymbol{B}(E/F)$ jsou izomorfní grupy. Izomorfismem mezi nimi je zobrazení $\theta : H^2 \to B(E/F)$, $\theta([\Phi]) = [A_\Phi]$.*

Důkaz: Dokážeme nejprve, že $[\Phi] \mapsto [A_\Phi]$ je dobře definovaná bijekce. Nechť $A_\Phi = \bigoplus_{i=0}^{n-1} u^i \cdot E$ a $A_\Psi = \bigoplus_{i=0}^{n-1} v^i \cdot E$. Zobrazení je dobře definované a prosté, jestliže platí

$$\forall \Phi,\Psi \in Z^2 = Ker(\delta^{(2)}) : \Phi\Psi^{-1} \in B^2 = Im(\delta^{(1)}) \iff A_\Phi \simeq A_\Psi.$$

Poznamenejme, že A_Φ a A_Ψ mají nad F stejnou dimenzi, proto $A_\Phi \simeq A_\Psi \iff A_\Phi \sim A_\Psi$.

Pokud Φ a Ψ splňují levou stranu ekvivalence, pak existuje $\Theta : \mathbb{Z}_n \to E^\star$ tak, že

$$\Phi(i,j)\Psi(i,j)^{-1} = \delta_\Theta(i,j) = \Theta(j)\Theta(i+j\_n)^{-1}\sigma^j(\Theta(i)), \forall i,j \in \mathbb{Z}_n.$$

Nyní chceme dokázat, že $A_\Phi \simeq A_\Psi$. Definujme tedy izomorfismus vektorových prostorů nad E $\phi : A_\Phi \to A_\Psi$ přiřazením $\phi(u^i) = v^i \cdot \Theta(i)$ a dokážeme, že je to také izomorfismus okruhů.

Nechť $u^i x, u^j y \in A_\Phi$. Pak

$$\phi(u^i x \cdot u^j y) = \phi(u^{i+j\_n}\Phi(i,j)\sigma^j(x)y) = v^{i+j\_n}\Theta(i+j\_n)\Phi(i,j)\sigma^j(x)y) =$$

$$= v^{i+j\_n}\Psi(i,j)\Theta(j)\sigma^j(\Theta(i))\sigma^j(x)y = v^{i+j\_n}\Psi(i,j)\sigma^j(\Theta(i)x)\Theta(j)y =$$

$$= (v^i\Theta(i)x) \cdot (v^j\Theta(j)y) = \phi(u^i x) \cdot \phi(u^j y).$$

Nyní ukážeme platnost obrácené implikace. Nechť $\phi : A_\Phi \to A_\Psi$ je takový izomorfismus, že $\forall c \in E : \phi(1_{A_\Phi} c) = 1_{A_\Psi} c$. Takový si můžeme zvolit díky Noether-Stokesově větě. Z Noether-Stokesovy věty totiž existuje $a \in A_\Phi$ tak, že $\phi(d) = a^{-1}da, \forall d \in E$. My si pak místo ϕ zvolíme izomorfismus $\tilde{\phi} = a\phi a^{-1}$.

Chceme najít takové $\Theta : \mathbb{Z}_n \to E^\star$, které by splňovalo

$$\Phi(i,j)\Psi(i,j)^{-1} = \delta_\Theta(i,j) = \Theta(j)\Theta(i+j\_n)^{-1}\sigma^j(\Theta(i)).$$

Mějme tedy prvek $i \in \{1,\ldots,n\}$. Připomeňme, že $C_{A_\Psi}(1_{A_\Psi}E) = 1_{A_\Psi}E$. Z Lemmatu 10 plyne $\sigma^i(c) = u_i^{-1}cu_i$, a tedy $1_{A_\Phi}\sigma^i(c) = u_i^{-1}1_{A_\Phi}cu_i$. Tedy také platí:

$$\phi(u_i)^{-1}(1_{A_\Psi}c)\phi(u_i) = \phi(u_i^{-1}1_{A_\Phi}cu_i) = \phi(1_{A_\Phi}\sigma^i(c)) =$$

$$= 1_{A_\Psi}\sigma^i(c) = u_v^{-1}1_{A_\Psi}cv_i.$$

Tedy platí $1_{A_\Psi} c\phi(u_i)v_i^{-1} = \phi(u_i)v_i^{-1}1_{A_\Psi}c, \forall c \in E$, takže $\phi(u_i)v_i^{-1}$ komutuje se všemi prvky z E, a proto $\phi(u_i)v_i^{-1} \in E$, což znamená, že existuje prvek $\Theta(i) \in E$: $\Theta(i)v_i = \phi(u_i)$. $\Theta(i) \neq 0$, protože $u_i \neq 0$ ani $v_i \neq 0$.

Zbývá ověřit, že $\Phi\Psi^{-1} = \delta^{(1)}_\Theta$.

$$1_{A_\Psi}\Phi(i,j)\Psi(i,j)^{-1} = \phi(1_{A_\Phi}\Phi(i,j))\Psi(i,j)^{-1} =$$

Zde použijeme Lemma 9.

$$= \phi(u^{-1}_{i+j\_n}u_iu_j)\Psi(i,j)^{-1} = 1_{A_\Psi}\Theta(i+j\_n)^{-1}v^{-1}_{i+j\_n}v_i\Theta(i)v_j\Theta(j)\Psi(i,j)^{-1} =$$

$$= 1_{A_\Psi}\Theta(i+j\_n)^{-1}v^{-1}_{i+j\_n}v_iv_j\sigma^j(\Theta(i))\Theta(j)\Psi(i,j)^{-1} =$$

$$= 1_{A_\Psi}\Theta(i+j\_n)^{-1}\Psi(i,j)\sigma^j(\Theta(i))\Theta(j)\Psi(i,j)^{-1} = 1_{A_\Psi}\Theta(j)\Theta(i+j\_n)^{-1}\sigma^j(\Theta(i)).$$

Zobrazení je také na, jak nyní dokážeme. Nechť $[A] \in B(E/F)$, tedy nechť A je jednoduchá, centrální, konečně dimenzionální F-algebra, která obsahuje E jako maximální podtěleso. Chceme dokázat, že pak existuje Φ_a takové, že $A \simeq A_\Phi$. Nejprve použijeme Noether-Stokesovu větu, která nám přinese existenci prvku $u \in A$, takového, že

$$\forall\sigma^i \in Gal(E,F), d \in E : \sigma^i(d) = (u^i)^{-1}du^i.$$

Ukážeme, že $U = \{u^0, \ldots, u^{n-1}\}$ je báze A. Jelikož E je ostře maximální v A, tedy $dim_E(A) = n$, tak stačí ukázat, že U je lineárně nezávislá. Zde zopakujeme stejný postup jako v důkaze Tvrzení 11. Předpokládejme, že je U lineárně závislá a vezměme tedy minimální množinu $X \subseteq \mathbb{Z}_n$ takovou, že existují nenulová c_i tak, že $\sum\limits_{i\in X} u^ic_i = 0$.

Tedy pro každé $e \in E^\star$ platí:

$$0 = e\sum_{i\in X} u^ic_i = \sum_{i\in X} u^i\sigma^i(e)c_i.$$

Pak ale $\forall i,j, i \neq j : \sigma^i(e) = \sigma^j(e)$, kdyby totiž existovalo nějaké j, pro které by existovala nějaká neprázdná množina $K = \{k : \sigma^k(e) \neq \sigma^j(e)\}$, pak by

$$\sum_{i\in X}(\sigma^i(e) - \sigma^j(e))u^ic_i = 0,$$

a tedy $X\backslash K \subset X$, což je ve sporu s minimalitou X.

Tedy $\sigma^i = \sigma^j, \forall i,j$ a tedy $|X| = 1$, jenže pak by $u^ic_i = 0$, což je ve sporu s tím, že u^i je invertibilní. U je tedy báze A a A tedy můžeme psát jako $\bigoplus\limits_{i=0}^{n-1} u^iE$.

Potřebujeme už jen najít správné a do Φ_a. Dokážeme, že pro $a = u^n$ platí $A \simeq A_{\Phi_{u^n}}$. Jelikož $(u^n)^{-1}du^n = \sigma^n(d) = d, \forall d \in E$, komutuje u^n se všemi prvky tělesa E. A protože $A = \bigoplus\limits_{i=0}^{n-1} u^iE$, tak $u^n \in Z(A) = F$.

Z Lemmatu 19 je zobrazení homomorfismem.

□

Nyní konečně uplatníme všechny dosažené výsledky a dokážeme konstrukční větu.

Důkaz: [Hlavní věta] Chceme dokázat sadu nerovností

$$n = Exp(A_{\Phi_a}) \leq Ind(A_{\Phi_a}) \leq Deg(A_{\Phi_a}) = n,$$

ze které tedy vyplývá rovnost $Ind(A_{\Phi_a}) = Deg(A_{\Phi_a})$, což platí právě tehdy, když A_{Φ_a} je nekomutativní těleso, protože $A_{\Phi_a} \simeq M_k(D)$ a $dim_F(A) = dim_F(D)$ a tedy $A_{\Phi_a} \simeq M_1(D) = D$.

Nejprve $n = Exp(A_{\Phi_a})$. To platí, protože $\boldsymbol{B}(E/F) \simeq F^\star/N_{E/F}(E^\star)$ izomorfismem $[a] \mapsto [A_{\Phi_a}]$ a $a^n \in N_{E/F}(E^\star)$ a zároveň $a^k \notin N_{E/F}(E^\star), \forall k < n$.

Dále $Ind(A_{\Phi_a}) \leq Deg(A_{\Phi_a})$ přímo z definice, protože $dim_F D \leq dim_F A_{\Phi_a}$ (dokonce $dim_F D \mid dim_F A_{\Phi_a}$).

Z Lemmatu 18 pak vyplývá $Deg(A_{\Phi_a}) = n$ $(= [E : F])$.

Nakonec $Exp(A_{\Phi_a}) \leq Ind(A_{\Phi_a})$, tedy pokud $Deg(D) = k \in \mathbb{N}$, kde D je nekomutativní těleso se strukturou F-algebry takové, že $A_{\Phi_a} \simeq M_m(D)$, pak $[A_{\Phi_a}]_\sim^k = 1_{\boldsymbol{B}(F)}$. Tedy $Deg(A) = mk$. D^m nese strukturu A_{Φ_a}-D-bimodulu a D^m je také vektorovým prostorem nad E. D^m má nad E dimenzi k, protože

$$dim_E(D^m) = \frac{dim_E(D^m)dim_F(E)}{mk} = \frac{dim_F(D^m)}{mk} = \frac{dim_D(D^m)dim_F(D)}{mk} = k.$$

Nechť $e_1, \ldots, e_k$ je tedy báze D^m jakožto vektorového prostoru nad E. Připomeňme, že A_{Φ_a} má nad E bázi $u^0, \ldots, u^{n-1}$.

Chceme nyní dokázat, že $[(\Phi_a)]^k = 1 \in H^2$. Tedy že $\Phi_a^k \in B^2$ $(= Im(\delta^{(1)}))$.

Vyjádříme každé $w_t u^i = \sum_{s=1}^{n} w_s \mu_{st}(i)$ a tím pro každé $i \in \{1, \ldots, n\}$ vytvoříme matici $M(i) = (\mu_{st}(i))_{s,t=1}^n$ s koeficienty v E.

Dále platí $M(i+j)\Phi_a(i,j) = M(j) \cdot \sigma^j(M(i))$, protože

$$\sum_{s=1}^{k} w_s \mu_{st}(ij)\Phi_a(i,j) = w_t u^{ij}\Phi_a(i,j) = w_t u^i u^j = \sum_{r=1}^{k} w_r \mu_{rt}(i) u^j =$$

$$= \sum_{r=1}^{k} w_r u^j \sigma^j \mu_{rt}(i) = \sum_{s=1}^{k} w_s (\sum_{r=1}^{k} \mu_{sr}(j)\sigma^j(\mu_{rt}(i))).$$

Protože jsme právě dokázali, že matice $M(i+j)\Phi_a(i,j)$ a $M(j) \cdot \sigma^j(M(i))$ se rovnají, rovnají se také i jejich determinanty, tedy

$$det(M(i+j))\Phi_a(i,j)^k = det(M(j)) \cdot det(\sigma^j(M(i))).$$

Připomeňme ještě, že $\Phi_a \in Z^2$, což jsme mimochodem dokázali, když jsme dokazovali asociativitu násobení A_{Φ_a} v Lemmatu 8. Dále platí, že $det(M) \in C^1$, protože $det(M) : Gal(E,F) \to E^\star$.

Můžeme si tedy povšimnout, že $\Phi_a^k = \delta^{(1)} det(M)$, a proto $\Phi_a^k \in B^2$, z čehož plyne, že $[\Phi_a]^k = 1 \in H^2$. To podle Tvrzení 20 znamená, že $[A_{\Phi_a}]_\sim^k = 1_{\boldsymbol{B}(F)}$.

□

Tím je dokázána konstrukční věta.

Závěr

V práci jsme dokázali konstrukční větu až na Lemma 19, které je velice technické, nepřehledné a došli jsme k závěru, že přestože nás lemma zajímá v konkrétním případě (v publikaci [1] je uvedeno pro libovolné Galoisovo rozšíření E/F a pro libovolné $\Phi,\Psi \in Z^2$, zatímco u nás má rozšíření E/F navíc cyklickou Galoisovu grupu a Φ_a, Φ_b máme přesně definované), tak ani tak nebude snadné ho nějak zjednodušit. Z tohoto a zejména také z časových důvodů jsme se rozhodli důkaz tohoto tvrzení vypustit. Je však možné si ho vyhledat v literatuře, kde je mu věnována kapitola 14.3 na straně 256.

Jinak je věta dokázána, přičemž jsme se vyhnuli homologické teorii. Dalším cílem této práce bylo zjednodušení značení, jelikož v původní publikaci bylo zavedeno vždy co nejobecněji, což se pro tuto práci nehodilo.

Na tuto práci by bylo možné navázat vytvořením sady příkladů, je pro to ale nutné umět počítat Galoisovy grupy a ani to nezaručuje úspěšnou konstrukci, jelikož se ještě musí najít správný prvek a splňující podmínky ve Větě 7.

Seznam použité literatury

[1] PIERCE, Richard. *Associative Algebras, Graduate Texts in Mathematics*. New York: Springer-Verlag. 1982, vol.88.

[2] STANOVSKÝ, David. *Základy algebry*. Praha: Matfyzpress. 2011.

[3] BARTO, Libor a TŮMA, Jiří. *Konečná tělesa* [online skripta]. 2008. Dostupné na: http://www.karlin.mff.cuni.cz/ barto/student/SkriptaKonTel.pdf.

[4] BICAN, Ladislav. *Lineární algebra a geometrie*. Praha: Academia. 2002.

[5] ANDERSON, Frank a FULLER, Kent. *Rings and Categories of Modules*. New York: Springer-Verlag. 1992.

[6] BEČVÁŘ, Jindřich. *150 let od objevu kvaternionů*. Jednota matematiků a fyziků, Pokroky matematiky, fyziky a astronomie. 1993. vol.33 no.6.