Division algebras of higher degree over rational function fields in one variable

A thesis submitted to the
University of Hyderabad
for the degree of

Doctor of Philosophy

in

Mathematics

by

Sudeep Singh Parihar

Department of Mathematics and Statistics
School of Mathematics and Computer/Information Sciences
University of Hyderabad
Hyderabad - 500 046
INDIA

March 2009

DECLARATION

Date: March 2009

I, **Sudeep Singh Parihar** hereby declare that the work embodied in the present thesis entitled **Division algebras of higher degree over rational function fields in one variable** has been carried out by me under the supervision of Prof. V. Suresh, Department of Mathematics and Statistics, University of Hyderabad, Hyderabad, India, as per the Ph.D ordinance of the university.

I declare that, to the best of my knowledge, no part of this thesis was earlier submitted for the award of research degree of any university or institution.

Sudeep Singh Parihar
(Reg. No: 02MMPP02)

CERTIFICATE

Department of Mathematics and Statistics
School of MCIS
University of Hyderabad
Hyderabad- 500 046

Date: March 2009

This is to certify that Mr. **Sudeep Singh Parihar** (Regd. No. 02MMPP02) has carried out the research work embodied in the present thesis entitled **Division algebras of higher degree over rational function fields in one variable**, for the full period prescribed under Ph.D. ordinance of the university.

No part of this thesis was earlier submitted by him for the award of research degree of any university or institution.

Prof. V. Suresh
Supervisor

Prof. T. Amaranath
Dean of the School

Prof. R. Tandon
Head of the Department

Preface

The aim of this thesis is to study the structure of $Br(k(t))$ in terms of the residue maps and the $Br(k)$. We also studied the u-invariant of hermitian forms. This work is made possible due to the invaluable guidance of Professor V. Suresh. I express my gratitude and indebtedness to my supervisor Prof. V. Suresh for giving me the opportunity to work with him. In particular, I am thankful for his constant and never tiring guidance. Learning and working with him has been one of the most enriching and fruitful experiences of my life.

I would like to thank *Council for Scientific and Industrial research* (CSIR INDIA) for their financial support.

Last but not the least, I am grateful to my family members for their encouragement and support.

- Sudeep Singh Parihar

Table of Contents

Introduction

Let k be a field and $Br(k)$ be the Brauer group of k. The structure of these Brauer groups is well understood for special fields, e.g. number fields, p-adic fields and function fields of p-adic curves. However very little is known for general fields. In the first part of this thesis, we make a little contribution to understand the structure of $Br(k(t))$ in terms of the residue maps and the $Br(k)$.

In the second part of the thesis we consider the hermitian forms over central simple algebras with involutions. It is known that there is a bound for the u-invariant of hermitian forms in terms of the u-invariant of the quadratic forms over the field k. In this thesis we give a different bound and show that our bound is sharper than the known bounds for certain class of central simple algebras.

We now describe the results proved in this thesis.

Let k be a field of characteristic zero. Let $X(k)$ be the character group $Hom(\Gamma_k, \mathbf{Q}/\mathbf{Z})$ of the continuous Galois group Γ_k of k. Let $k(t)$ be the function field of the projective line $\mathbb{P}^1_k$. For every closed point P of $\mathbb{P}^1_k$, let $k(P)$ denote the residue field at P and $\partial_P : Br(k(t)) \to X(k(P))$ be the residue homomorphism at P. We have the following exact sequence of Faddeev ([5]):

$$0 \to Br(k) \to Br(k(t)) \stackrel{\oplus\partial_P}{\to} \oplus_P X(k(P)) \stackrel{\Sigma cor}{\to} X(k) \to 0,$$

where Σcor is the sum of the corestriction (or norm) maps $X(k(P)) \to X(k)$ and the sum is over the set of closed points of $\mathbb{P}^1_k$. If the characteristic of k is p, the above exact sequence of Faddeev still holds, if we replace the Brauer groups and character groups by their subgroups of prime to p-torsion.

In [9], Rowen-Sivatski-Tignol, tried to obtain information on the index of Brauer classes in $Br(k(t))$ from their images under the ramification map $\oplus\partial_P$. For an element $\alpha \in Br(k(t))$, the ramification degree is defined as $\sum[k(P) : k]$, where the sum is taken over all the closed points P of $\mathbb{P}^1_k$ with $\partial_P(\alpha) \neq 0$. They studied 2-torsion elements in $Br(k(t))$ with ramification degree at most 3 ($\text{char}(k) \neq 2$). In this thesis we extend their results to the elements of l-torsion for any prime number l not equal to the characteristic of k.

Let $\mathcal{R}_l = \text{Ker}(\Sigma cor_P : \oplus_P\ {}_lX(k(P)) \to\ {}_lX(k))$. For $\rho = (\chi_P) \in \mathcal{R}$, the *support* of ρ is

$$\text{supp}(\rho) = \{P \mid \chi_P \neq 0\},$$

and χ_P is called the *component* of ρ at P. The *degree* of ρ, denoted by $\deg(\rho)$, defined as:

$$\deg(\rho) = \sum_{P \in \text{supp}(\rho)} deg(P),$$

where $\deg(P)$ is the degree of the extension $k(P)/k$ of fields.

In the first part of the thesis, we have proved the following results.

Theorem 0.1 Let $\rho \in \mathcal{R}_l$. Suppose that $\text{degsupp}(\rho) = 2$. If $\text{supp}(\rho) = \{P_1, P_2\}$ (two distinct rational points), then there exist $\lambda, a, b \in k^*$ such that $\rho = (\partial_P((\lambda, (t-a)(t-b)^{l-1})_l))$.

Theorem 0.2 Let $\rho \in \mathcal{R}_l$. Suppose that $l \geq 3$ and $\text{degsupp}(\rho) = 2$. If $\text{supp}(\rho) = \{P\}$ ($\deg P = 2$), then there exists $a \in k$ such that $\rho = (\partial_Q((t, t^2 + at + 1)_l))$.

Theorem 0.3 Let $\rho \in \mathcal{R}_l$. Suppose that degsupp$(\rho) = 3$. If supp$(\rho) = \{P_1, P_2, P_3\}$ (three distinct rational points), then there exist $a_1, a_2 \in k^*$ such that $\rho = (\partial_P((t, (t-a_1)(t-a_2)(t-a_1a_2)^{l-1})_l))$.

Theorem 0.4 Let $\rho \in \mathcal{R}_l$. Suppose that degsupp$(\rho) = 3$. If supp$(\rho) = \{P_1, P_2\}$ (deg$P_1 = 1$ and deg$P_2 = 2$), then there exist $\lambda, a, b, c \in k^*$ such that $\rho = (\partial_P((\lambda, (t^2+at+b)(t-c)^{l-2})_l)$ or $\rho = (\partial_P((t, (t^2+at+b)(t-c))_l))$.

Theorem 0.5 Let $\rho \in \mathcal{R}_l$. Suppose that degsupp$(\rho) = 3$. If supp$(\rho) = \{P\}$ (deg$P = 3$), then there exist $\lambda, a, b, c, \in k^*$ such that $\rho = (\partial_P((\lambda, (t^3+at^2+bt+c))_3))$ ($l = 3$) or $\rho = (\partial_P((t, (t^3+at^2+bt+c))_l))$.

Theorem 0.6 For every central simple k-algebra A,

$$\text{index}(A \otimes (a,b)_l) \in \{\frac{1}{l}\,\text{index}(A), \text{index}(A), l\,\text{index}(A)\}.$$

Theorem 0.7 For any central simple k-algebra A and $g(t)$ a polynomial of degree l,

$$\text{index}(A \otimes (\lambda, g(t))_l) = \text{index}(A) \text{ or } l\,\text{index}(A).$$

Theorem 0.8 For any central simple k-algebra A,

$$index(A \otimes (t, t^2+at+1)_l) = \text{index}(A) \text{ or } l\,\text{index}(A).$$

Theorem 0.9 For any central simple k-algebra A,

$$\text{index}(A \otimes (t, (t-a)g(t))_l) = \text{index}(A) \text{ or } l\,\text{index}(A).$$

Let K be a field of characteristic not equal 2 and A a central simple algebra over K with an involution σ. Let $\epsilon \in \{\pm 1\}$ and (V, h), or simply h, an ϵ-hermitian form over A with respect to σ. We say that h is *isotropic* if there is exists a $v \in V$, $v \neq 0$ such that $h(v, v) = 0$. If h is not isotropic, then we say that h is *anisotropic*. The u invariant of ϵ-hermitian forms over A with respect to σ is defined as the supremum of dimensions of anisotropic ϵ-hermitian forms over A with respect to σ and denoted by $u(A, \sigma, \epsilon)$. In ([8]), a bound for $u(A, \sigma, \epsilon)$ was given in terms of $u(K)$, where $u(K) = u(K, identity, +1)$ is the classical u-invariant of the quadratic forms over the field K. In the second part of the thesis, we proved the following results.

Theorem 0.10 Let k be a field of characteristic not equal to 2 and K/k a quadratic extension. Let A_0 be a central simple algebra over k with an involution τ. Let $A = A_0 \otimes_k K$ and $\sigma = \tau \otimes id$, where id is the identity of K. Then we have

$$u(A, \sigma, \epsilon) \leq \frac{3}{2} u(A_0, \tau, \epsilon).$$

Theorem 0.11 Let k be a field of characteristic not equal to 2 and K/k a quadratic extension. Let A_0 be a central simple algebra over k with an involution τ. Let $A = A_0 \otimes_k K$ and $\sigma = \tau \otimes -$, where $-$ is the non-trivial automorphism of K/k. Then we have

$$u(A, \sigma, \epsilon) \leq minimum\{u(A_0, \tau, \epsilon) + \frac{1}{2} u(A_0, \tau, -\epsilon), u(A_0, \tau, -\epsilon) + \frac{1}{2} u(A_0, \tau, \epsilon)\}.$$

Corollary 0.12 Let k be a field of characteristic not equal to 2 and K/k a quadratic extension. Let H be a quaternion algebra over K with an involution σ of second kind. Then $u(H, \sigma, \epsilon) \leq \frac{7}{8} u(k)$.

Corollary 0.13 Let A be a central simple k-algebra of degree 4 with an orthogonal involution σ. Then $u(A, \sigma, -1) \leq \frac{17}{16} u(k)$.

Corollary 0.14 Let A be a central simple k-algebra of degree 4 with an orthogonal involution σ. Then $u(A, \sigma, 1) \leq \frac{29}{16} u(k)$.

Remark 0.15 Our bounds are sharper than the bounds given in ([8]).

Chapter 1

Some basic definitions and results

This chapter, which is preliminary in nature, contains a rapid review of some of the basic definitions and results used in this thesis. The references for definitions and results recalled in the thesis are from [2], [4], [7], [6], [10].

1.1 The Brauer group

In this section we recall the definition of Brauer group, ramification map and an exact sequence of Faddeev (see [6]).

Let R be a commutative ring with unity. By an R-*algebra* we mean a ring A which is also a unitary R module such that

$$a(xy) = (ax)y = x(ay)$$

for all a in R and x, y in A. We say that two R-algebras A and B are isomorphic if there exists an isomorphism $\phi : A \to B$ of rings which is also R-linear. Let k be a field. Let A be a k-algebra. Since k is a field, the map $k \to A$ given by $a \mapsto a \cdot 1$ is injective. Hence we identify k as a sub ring of A.

We say that an R-algebra A is *simple* if the ring A is simple i.e., A has no two sided ideals other than (0) and A. A finite dimensional simple k-algebra with center a field k is called a *central simple algebra* over k. Let D be a division ring and k be the center of D. If D is finite dimensional over k, then D is a central simple k-algebra and we call D a *central division* k-algebra.

Let k be a field. By the classical theorem of Wedderburn, we know that every central simple k-algebra is isomorphic to a matrix algebra $M_n(D)$ for some central division k-algebra D. We also know that if $M_n(D)$ is isomorphic to $M_{n'}(D')$ for some central divsion k-algebras D and D', then $n = n'$ and $D \simeq D'$. Let A be a central simple k-algebra. Then $A \simeq M_n(D)$ for some n and a central division k-algebra D. Let $L \subset D$ be a maximal subfield. Then we have $D \otimes_k L \simeq M_d(L)$. In particular, the dimension of a central simple k-algebra is a square. The square root of the dimension of a central simple k-algebra is called the *degree* and denoted by $deg(A)$. Let A be a cental simple k-algebra. Then $A \simeq M_n(D)$ for some central division k-algebra. The degree of D is called the *index* of A and denoted by $ind(A)$.

Two central simple k-algebras A and B are called *similar*, denoted by $A \sim B$, if $M_m(A)$ and $M_n(B)$ are isomorphic for some m, n. It is easy to see that this is an equivalence relation on the set of isomorphic classes of central simple k-algebras. The set of equivalence classes of central simple k-algebras is denoted by $Br(k)$. By the Wedderburn theorem, $Br(k)$ can be identified with the set of isomorphism classes of central division k-algebras. For a central simple k-algebra A, let $[A]$ denote the equivalence class containing A. Let A and B be two central simple k-algebras of same dimension. Then $[A] = [B]$ if and only if $A \simeq B$.

Let A and B be two central simple k-algebras. Then $A \otimes_k B$ is a central simple algebra over k. The tensor product of central simple algebras induces a group structure on $Br(k)$. This group $Br(k)$ is called the *Brauer group* of k. The equivalence class $[M_n(k)]$ is the identity element of $Br(k)$. For a central simple k-algebra A, the class $[A^o]$ is the inverse of the class $[A]$, where for any ring B, B^o denotes the opposite ring. Since $A \otimes_k B \simeq B \otimes_k A$, the Brauer group $Br(k)$ is abelian. Let A be a central simple k-algebra. It is known that $deg(A) \cdot [A] = 0$. In particular every element of $Br(k)$ is a torsion element. The order of the class $[A]$ in $Br(k)$ is called the *exponent* of A.

Let L/k be an extension of fields. Let A be a central simple k-algebra. Then $A \otimes_k L$ is a central simple L-algebra and this induces a homomorphism $Br(k) \to Br(L)$.

The l-torsion subgroup of $Br(k)$, denoted by ${}_lBr(k)$, is defined as ${}_lBr(k) = \{[\text{A}] |\ [A]^{\otimes l} = [k]\}$.

Let F be a field. Let $\Gamma_F = Gal(F_s/F)$ denote the absolute Galois group of F, where F_s is the separable closure of F. Let $X(F) = Hom(\Gamma_F, \mathbb{Q}/\mathbb{Z})$ be the character group of continuous homomorphisms from Γ_F to $\mathbb{Q}/\mathbb{Z}$.

For any abelian group G and positive integer n, let ${}_nG$ be the subgroup of G consisting of all those elements of G whose order divides n, i.e.

$${}_nG = \{g \in G \mid g^n = e\}.$$

Let R be a discrete valuation ring with residue field k. Let K be the field of fractions of R. Let l be a prime number not equal to the characteristic of k. Then we have a homomorphism $\partial :\ {}_lBr(K) \to\ {}_lX(k)$, called the *residue map* at R.

Let C be a nonsingular projective curve over a field k and $k(C)$ its function field. Then for each closed point p of C, the local ring $\mathcal{O}_{C,p}$ at p is a discrete valuation ring with field of fractions $k(C)$ and residue field $k(p)$ a finite extension of k. Let v_p denote the discrete valuation at p with valuation ring $\mathcal{O}_{C,p}$. Let l be a prime number not equal to the characteristic of k. Let $p \in C$ be a closed point of C. Then we have the residue map $\partial_p : {}_lBr(k(t)) \to {}_lX(k(p))$. Since $k(p)$ is a finite extension of k, the absolute Galois group $\Gamma_{k(p)}$ is a subgroup of Γ_k of finite index. Hence we have a homomorphism $cor_p : {}_lX(k(p)) \to {}_lX(k)$, called the *corestriction* (or *norm*) map.

We have the following exact sequence of Faddeev (see Corollary 6.4.6 in [6]):

$$0 \longrightarrow {}_lBr(k) \longrightarrow {}_lBr(k(t)) \xrightarrow{\oplus\partial_p} \bigoplus_{p\in\mathbb{P}^1_k} {}_lX(k(p)) \xrightarrow{\sum cor_p} {}_lX(k) \longrightarrow 0$$

where $\sum cor_p$ is the sum of the corestriction (norm) maps ${}_lX(k(p)) \longrightarrow_l X(k)$ and ${\mathbb{P}^1_k}^{(1)}$ denotes the set of closed points on the projective line $\mathbb{P}^1_k$.

Let $\mathfrak{R}$ be the kernel of the homomorphism

$$\sum cor_p : \bigoplus_{p\in{\mathbb{P}^1_k}^{(1)}} X(k(p)) \longrightarrow X(k)).$$

The elements in $\mathfrak{R}$ are called *ramification sequences.* Let $\rho = (\chi_p) \in \mathfrak{R}$. The set $\{p \in {\mathbb{P}^1_k}^{(1)} | \chi_p \neq 0\}$ is called the *support* of ρ and denoted by supp(ρ). The element $\chi_p \in X(k(p))$ is called the *component* of ρ at p. The *degree* of the support of ρ, denoted by deg supp(ρ), is defined as :

$$\deg \operatorname{supp}(\rho) = \sum_{p\in supp(\rho)} \deg(p),$$

where $\deg(p)$ is the degree of the finite extension $k(p)$ over k.

If p is a rational point (i.e., $k(p) = k$), then $cor_p : X(k(p)) \longrightarrow X(k)$ is the identity map. Therefore, the support of a ramification sequence cannot consist of a single rational point. Hence deg supp$(\rho) \geq 2$ for all $\rho \in \mathfrak{R}$.

1.2 The cyclic algebra

To construct a *cyclic* algebra we start with a Galois extension L/K of degree n such that the Galois group $G = G(L/K)$ is cyclic. Let σ be a generator of G. Let $a \in K^* = K - \{0\}$. Now we construct an algebra A which is denoted by $(L/K, \sigma, a)$ as follows : Let A be a L-vector space of dimension n. Choose a basis of A and denote it by $1, e, ..., e^{n-1}$. We have

$$A = L.1 \oplus Le \oplus ... \oplus Le^{n-1}.$$

Define the multiplication on A as follows:

$$e^n = a.1,\ \lambda e^i \mu e^j = \lambda\mu e^{i+j} \text{ and } e(\lambda\,.1) = \sigma(\lambda)\, e \qquad \text{for } \lambda, \mu \in L.$$

We denote this algebra A by $(L/K, \sigma, a)$. It is well know that $(L/K, \sigma, a)$ is a central simple algebra over K. Since L is a maximal subfield of $(L/K, \sigma, a)$ and L/K a cyclic extension, we call this algebra a *cyclic algebra*.

For a finite extension L/K, let $N_{L/K} : L \to K$ be the norm map. Let L/K be a Cyclic extension, σ be a generator of $G(L/K)$ and $a, b \in K^*$. We have the following:

Theorem 1.2.1: $(L/K, \sigma, a) \simeq (L/K, \sigma, b)$ if and only if $ba^{-1} \in N_{L/K}(L^*)$.

Corollary 1.2.2: If the degree of L/K is a prime number, then $(L/K, \sigma, a)$ is a division algebra if and only if a does not belong to $N_{L/K}(L^*)$.

Let K be a field and l a prime number not equal to the characteristic of K. Suppose that K contains a primitive l^{th} root of unity ζ. Let $a \in K^*$. If a is not an l^{th} power in K, then $L = K(\sqrt[l]{a})$ is a cyclic extension of degree l and the automorphism of L given by $\sigma(\sqrt[l]{a}) = \zeta\sqrt[l]{a}$ is a generator of the Galois group

$G(L/K)$. For any $b \in K^*$, the cyclic algebra $(L/K, \sigma, b)$ is denoted by $(a, b)_l$ and called an *l-symbol algebra*.

Let R be a discrete valuation ring, K its field of fractions and k the residue field of R. Let l be a prime number not equal to the characteristic of k. Assume that k contains a primitive l^{th} root of unity. Fix a primitive l^{th} root of unity ζ in k. We identify the l-torsion subgroup ${}_lX(k)$ of $X(k)$ with k^*/k^{*^l}. Assume also that K contains a primitive l^{th} root of unity. Fix an l^{th} root of unity in K which maps to the fixed primitive l^{th} root of unity of k. Let $\partial : {}_lBr(K) \to {}_lX(k)$ be the residue homomorphsim. For an l-symbol algebra $(a, b)_l$, where $a, b \in K^*$, we have

$$\partial((a, b)_l) = (-1)^{v(a)v(b)}\overline{a^{v(b)}b^{-v(a)}}\, k^{*l} \in k^*/k^{*l}$$

where v is the discrete valuation of K and $^{-}$denotes the residue map from the discrete valuation ring R to its residue field k. In particular, if a and b are units in R, then $\partial((a, b)_l) = 1$. If a is a unit and b is a parameter in R, then $\partial((a, b)_l)) = \overline{a}k^{*l}$.

Let E/k be a finite extension. Assume that k contains a primitive l^{th} root of unity. Fix a primitive l^{th} root of unity ζ in k^*. As we mentioned above, we identify ${}_lX(E)$ with E^*/E^{*l} and ${}_lX(k)$ with k^*/k^{*l}. Under this identification, the map $cor : {}_lX(E) \to {}_lX(k)$ is given by the norm map $N : E^* \to k^*$.

1.3 Transformations of the projective line

In this section we recall a few facts about the transformations of the projective line from [9].

A choice of projective coordinates in the projective line $\mathbb{P}^1_F$ over an arbitrary field F is an identification $\mathbb{P}^1_F = Proj(F[u,v])$ where u, v are indeterminates of degree 1 over F. When projective coordinates are chosen, the rational points of $\mathbb{P}^1_F$ are identified with $F \cup \infty$ in such a way that $a \in F$ corresponds to the homogeneous ideal $(u - av)F[u,v]$, and ∞ to $vF[u,v]$. We call the point ∞ to be the *point at infinity.* We identify the field of rational functions on $\mathbb{P}^1_F$ with $F(t)$, where $t = uv^{-1}$, and $\mathbb{P}^1_F \setminus \{\infty\} = \mathbb{A}^1_F = Spec(F[t])$.

It is well known that the group of transformations of $\mathbb{P}^1_F$ is simply transitive on the triples of the rational points (see [2]).

Proposition 1.3.1 Let p, $p^{'}$ be two rational points on $\mathbb{P}^1_F$ and q, $q^{'}$ be two closed points of degree 2. The projective transformations of $\mathbb{P}^1_F$ which map p to $p^{'}$ and q to $q^{'}$ are in one-to-one correspondence with the F-isomorphisms from F_q to $F_{q'}$.

Proof: Since the group of transformation of $\mathbb{P}^1_F$ acts transitively on the triple of rational points, after applying a projective transformation we may assume that $p = p'$. Choose projective coordinates of $\mathbb{P}^1_F$ such that p is the point at infinity. Then projective transformations which leave p invariant are the transformations of the affine line $\mathbb{A}^1_F$. We view q and q' as closed points of degree 2 on $\mathbb{A}^1_F = Spec(F[t])$. Then q corresponds to a maximal ideal $(f(t))$ and q' corresponds to a maximal ideal $(g(t))$ in $F[t]$ where $f(t)$ and $g(t)$ are monic irreducible polynomials of degree 2. The affine transformation $t \mapsto at + b$ (with a,$b \in F$,$a \neq 0$) maps q to q' if and only if the ideals $(f(at + b)) = (g(t))$.

It is clear that if $(f(at + b)) = (g(t))$ then the map $t \mapsto at + b$ induces an F-isomorphism from F_q to $F_{q'}$. Conversely, assume $\psi : \frac{F[t]}{(f(t))} \to \frac{F[t]}{(g(t))}$ is an F-isomorphism. Let θ and $\theta^{'}$ be the images of t in $F_q = \frac{F[t]}{(f(t))}$ and $F_{q'} = \frac{F[t]}{(g(t))}$ respectively. Since $f(\theta) = 0$,we have $f(\psi(\theta)) = 0$. Since any element of $\frac{F[t]}{(g(t))}$ is of the form $a\theta^{'}+b$,we have $\psi(\theta)=a\theta^{'}+b$ and hence $f(a\theta^{'}+b)=0$. Since $g(t)$ is the minimal polynomial of $\theta^{'}$, so $g(t)$ divides $f(at+b)$. Since f and g are irreducible polynomials of degree 2, we have $f(at+b)=\lambda g(t)$ for some λ in F and hence the ideals $(f(at+b))=(g(t))$. □

Proposition 1.3.2 Let r,r' be closed points of degree 3 on $\mathbb{P}^1_F$. The projective transformation of $\mathbb{P}^1_F$ which maps r to r' are in one-to-one correspondence with the F-isomorphisms from F_r to $F_{r'}$.

Proof: Choose coordinates to represent $\mathbb{P}^1_F$ as $Proj(F[u,v])$, where u,v are indeterminates of degree 1. We may then find homogeneous irreducible polynomials f,$g\in F[u,v]$ of degree 3 such that r corresponds to the maximal ideal $(f(u,v))$ and r' corresponds to the maximal ideal $(g(u,v))$. After scaling, we may assume the coefficients of u^3 in f and g are 1. The projective transformation $u\mapsto au+bv$, $v\mapsto cu+dv$ (where $a,b,c,d\in F$ and $ad-bc\neq 0$) maps r to r' iff the ideals

$$(f(au+bv,cu+dv))=(g(u,v))$$

or, after de-homogenizing,

$$(f(at+b,ct+d))=(g(t,1))$$

It is clear that if $(f(at+b,ct+d))=(g(t,1))$ then the map $t\mapsto at+b$ and $1\mapsto ct+d$ induces an F-isomorphism from F_r to $F_{r'}$. Conversely, assume $\psi:\frac{F[t]}{(f(t,1))}\rightarrow\frac{F[t]}{(g(t,1))}$ is an F-isomorphism. Let θ and α be the images of t in $F_r=\frac{F[t]}{(f(t,1))}$ and $F_{r'}=\frac{F[t]}{(g(t,1))}$ respectively. Since $f(\theta,1)=0$, we have $f(\psi(\theta),1)=0$.

We first show that for any $x\in F_{r'}$ such that $x\notin F$, there exist $a,b,c,d\in F$, uniquely determined up to a scalar factor, such that $x=\frac{a\alpha+b}{c\alpha+d}$ and $ad-bc\neq 0$. Since $\alpha\notin F$ and $x\neq 0$, we have

$$dim_F(F+F\alpha)=dim_F(x(F+F\alpha))=2$$

Since, $dim_F F_{r'}=3$, we have

$$dim_F((F+F\alpha)\cap x(F+F\alpha))\geqslant 1$$

which implies, $x = \frac{a\alpha+b}{c\alpha+d}$ for some $a, b, c, d \in F$. Since $x \notin F$ it follows that $ad - bc \neq 0$.

Suppose $dim_F((F + F\alpha) \cap x(F + F\alpha)) = 2$ then

$$F + F\alpha = x(F + F\alpha) \text{ .....(1)}$$

hence, $x \in (F + F\alpha)$ and thus $F + F\alpha = F + Fx$.

Now, we show that $F + F\alpha$ is a subalgebra of $F(\alpha) \simeq F_{r'}$. It suffices to show that $\alpha^2 \in F + F\alpha$. Since $F + F\alpha = F + Fx$ we have $\alpha \in F + Fx$. Let $\alpha = a' + b'x$. Now $(a' + b'x)(F + F\alpha) = (F + F\alpha) + x(F + F\alpha)$, from equation (1) we have $(a' + b'x)(F + F\alpha) = F + F\alpha$, and thus $\alpha^2 \in F + F\alpha$. Therefore $F + F\alpha$ is a subalgebra of $F(\alpha)$ and hence a subfield, which is a contradiction. Hence $dim_F((F + F\alpha) \cap x(F + F\alpha)) = 1$. It follows that x can be uniquely expressed as $\frac{a\alpha+b}{c\alpha+d}$, which proves our claim.

In particular $\psi(\theta) = \frac{a\alpha+b}{c\alpha+d}$. Hence $f(\psi(\theta), 1) = 0$ implies that $f(a\alpha + b, c\alpha + d) = 0$. Since $g(t, 1)$ is the minimal polynomial of α, $g(t, 1)$ divides $f(at+b, ct+d)$. Since f and g are irreducible polynomials of degree 3, $f(at + b, ct + d) = \lambda g(t, 1)$ for some λ in F and hence the ideals $(f(at + b, ct + d)) = (g(t, 1))$. □

From (1.3.1) and (1.3.2) and from the second fundamental theorem of projective geometry (see [2]) we can deduce the following facts:

Corollary 1.3.3 (i) Let p_1, p_2, p_3 be three distinct rational points on $\mathbb{P}^1_F$ and let $\lambda_1, \lambda_2, \lambda_3 \in F[u, v]$ be homogeneous polynomials of degree 1 which are pairwise distinct up to scalars.There is a choice of projective coordinates $\mathbb{P}^1_F = Proj(F[u, v])$ such that

$$p_1 = \lambda_1 F[u, v], p_2 = \lambda_2 F[u, v], p_3 = \lambda_3 F[u, v].$$

(ii) Let p be a rational point on $\mathbb{P}^1_F$ and q be a closed point of degree 2 on $\mathbb{P}^1_F$. Let $\lambda \in F[u, v]$ be a homogeneous polynomial of degree 1 and $f(u, v) \in F[u, v]$

be a homogeneous polynomial of degree 2 such that $F_q \simeq F[t]/(f(t,1)$. There is a choice of projective coordinates $\mathbb{P}^1_F = Proj(F[u,v])$ such that

$$p = \lambda F[u,v], q = f(u,v)F[u,v].$$

(iii) Let r be a closed point of degree 3 on $\mathbb{P}^1_F$ and $f(u,v) \in F[u,v]$ be a homogeneous polynomial of degree 3 such that $F_r \simeq F[t]/(f(t,1)$.There is a choice of projective coordinates $\mathbb{P}^1_F = Proj(F[u,v])$ such that

$$r = f(u,v)F[u,v].$$

1.4 Central simple algebras with a constant slot.

This section is taken from [9]. Let E be a finite-dimensional central division algebra over an arbitrary field K and x be an indeterminate over K. The ring $E[x] = E \otimes_K K[x]$ is a PID with Ore ring of fractions $E(x) = E \otimes_K K(x)$. Let α be an automorphism of finite order n of $E[x]$ and $g \in K[x]$. Consider the algebra

$$\Delta(E(x), \alpha, g) = E(x) \oplus E(x)y \oplus ... \oplus E(x)y^{n-1}$$

where multiplication is defined by

$$y^n = g \text{ and } yf = \alpha(f)y \text{ for } f \in E(x).$$

This algebra can be viewed as the quotient ring of the skew-polynomial ring $E(x)[y;\alpha]$ by the ideal generated by $y^n - g$.

Let F be a field and l a prime number not equal to the characteristic of F. Let D be a central division algebra over F. Let $a \in F^*$. Suppose that there is no element λ in D with $\lambda^l = a$. Then $E = D \otimes_F F(\sqrt[l]{a})$ is a central division algebra over $K = F(\sqrt[l]{a})$. Assume that F contains a primitive l^{th} root of unity. Fix an

l^{th} root of unity $\zeta \in F^*$. The automorphism of K/F given by $\sqrt[l]{a} \mapsto \zeta\sqrt[l]{a}$ extends to an automorphism α of E which is identity on D. Let t be an indeterminate over F and $g \in F[t]$.

1.5 Hermitian Forms and the u-invariant

Throughout this section k denotes a field of characteristic not equal to 2.

Let A be a central simple algebra over a field k. By an *involution* on A we mean a map $\sigma : A \to A$ such that $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(b)\sigma(a)$ and $\sigma^2(a) = a$ for all $a, b \in A$.

Let A be a central simple algebra over a field k with an involution σ on A. Let $\varepsilon = \pm 1$. An *ε-hermitian form* over (A, σ) is a pair (V, h) consisting of a right A-module V and a bi-additive map $h : V \times V \to A$ such that $h(xa, yb) = \sigma(a)h(x, y)b$ and $h(y, x) = \varepsilon\sigma(h(x, y))$ for all $x, y \in V$ and for all $a, b \in A$. Let $V^* = Hom_A(V, A)$ be the dual of V. The form h induces a map $\widetilde{h} : V \to V^*$ which we call the adjoint of h. The left A-module V^* is regarded as a right A-module through the involution σ on A. Then $\widetilde{h} : V \to V^*$ is A-linear. We say that h is *non-degenerate* if $\widetilde{h}$ is an isomorphism. A non-degenerate ε-hermitian form is also called an *ε-hermitian space*. We remark that if the map $\widetilde{h} : V \to V^*$ is injective, then it is an isomorphism (comparing the k-dimension of V and V^*).

Let (V, h) and (V', h') be two ε-hermitian forms. We say that (V, h) and (V', h') are *isometric* if there exists an A-module isomorphism $f : V \to V'$ such that $h'(f(x), f(y)) = h(x, y)$ for all $x, y \in V$.

Let (V, h) and (V', h') be two ε-hermitian forms. The orthogonal sum $(V, h) \oplus$

(V', h') is by definition the form $(V \oplus V', h \oplus h')$, where $(h \oplus h')(v+v', w+w') = h(v,w) + h'(v', w')$. Let $Gr^{\varepsilon}(A, \sigma)$ be the Grothendieck group of the isometric classes of non-degenerate ε-hermitian spaces with respect to the orthogonal sums. Let (V, h) be an ε-hermitian space and W a submodule of V. The subset $W^{\perp} = \{v \in W | h(v, w) = 0 \text{ for all } w \in W\}$ is a subspace of V and called the perpendicular of W. An ε-hermitian space (V, h) is said to be hyperbolic if there exists a sub module W of V such that $W = W^{\perp}$. Let W be an A-module and $V = W \oplus W^*$. Define $h : V \times V \to A$ by $h(x+f, y+g) = f(y) + \varepsilon\sigma(g(x))$ for all $x, y \in W$ and $f, g \in W^*$. Then it is easy to see that (V, h) is an hyperbolic ε-hermitian space over (V, σ). This form is denoted by $\mathbf{h}_W$.

Let (V, h) be an ε-hermitian space over (A, σ) and W a A-submodule of V. Then h restricted to W is an ε-hermitian form and it is denoted by $h \mid_W$. This form need not be non-degenerate in general. If $(W, h \mid_W)$ is non-degenerate, then $h \simeq h \mid_W \perp h'$ for some ε-hermitian space h' over (A, σ).

The *Witt group* $W^{\varepsilon}(A, \sigma)$ is the quotient of $Gr^{\varepsilon}(A, \sigma)$ by the subgroup generated by hyperbolic spaces. If $\varepsilon = 1$, an ε-hermitian space is said to be a hermitian space and if $\varepsilon = -1$, then an ε-hermtian space is called a skew-hermitian space.

Let D be a central division k-algebra with an involution σ. Let (V, h) be an ε-hermitian space over (D, σ). Suppose that either D is non-commutative or $\varepsilon \neq -1$. Then there exists a basis $\{e_1, \cdots, e_n\}$ of V such that $h(e_i, e_j) = 0$ for all $i \neq j$. Let $\lambda_i = h(e_i, e_i)$. We write $h =< \lambda_1, \cdots, \lambda_n >$.

Let A be a central simple algebra with an involution σ. Let (V, h) be an ε-hermitian space. When there is no confusion, we drop V and simply say that h is an hermitian space. Write $A = M_n(D)$ for some central division k-algebra. Then we now that $\dim_k V$ is a multiple of $\dim_k(D) \cdot n$. The quotient $\dim_k V / \dim_k(D) \cdot n$

is called the *dimension of* h and denoted by $\dim(h)$. If $A = D$ is a central division k-algebra, then $\dim(h) = \dim_D V$. By the definition, the dimension of any hyperbolic form is even.

We say that h is *isotropic* is there exists $x \in V$, $x \neq 0$, such that $h(x, x) = 0$. If h is not isotropic, then we say that h is *anisotropic*. The *u-invariant* of an ε-hermitian spaces over (A, σ), denoted by $u(A, \sigma, \varepsilon)$, is defined as

$$\sup\{\dim(h) | h \text{ is an anisotropic } \varepsilon\text{−hermitian space over}(A, \sigma)\}.$$

If $A = k$, $\epsilon = 1$ and σ is the identity map, then a hermitian form is just a quadratic form and $u(A, \sigma, 1) = u(k)$ is the classical u-invariant of quadratic forms over the field k.

Let (V, h) be an ε-hermitian space over (A, σ). Then $h = h_a n \perp \mathbf{h}$ for some anisotropic form $h_a n$ and hyperbolic form $\mathbf{h}$. The isometry class of $h_a n$ is depends only on h. Since $\mathbf{h}$ is hyperbolic, its dimension is even. The *Witt index* of h is defined as the $\dim(\mathbf{h})/2$.

Let W be an A-submodule of V. If h restricted to V is anisotropic, then $(W, h\mid_W)$ is non-degenerate. In particular, if h is anisotropic, then for any submodule W of V, we have $h \simeq h\mid_W \perp h'$.

Let A be a central simple algebra with an involution σ. Suppose $A = M_n(D)$ for some central division k-algebra. Then by Morita equivalance, there exists an involution τ on D such that $u(A, \sigma, \varepsilon) = u(D, \sigma, \varepsilon)$.

Let A be a central simple algebra over K with an involution σ. We say that σ is of *first kind* if σ is the identity map on K and σ is of *second kind* if σ is not identity on K. Since K is the center of A, it is easy to see that $\sigma(K) = K$. If σ is of second kind, then $k = \{a \in K | \sigma(a) = a\}$ is a subfield of K and the degree of K/k is 2.

Let k be a field and $K = k(\sqrt{d})$ a quadratic extension. Let A be a central simple algebra over K with an involution σ of second kind such that $\sigma(\sqrt{d}) = -\sqrt{d}$. Let h be an ε-hermitian form on (A, σ). Then $\sqrt{d}\, h$ is a $-\varepsilon$-hermitian form on (A, σ). Since $\sqrt{d}$ is in the center of A, it is easy to see that h is isotropic if and only if $\sqrt{d}\, h$ is isotropic. We also have $\dim h = \dim \sqrt{d}\, h$. Therefore $u(A, \sigma, \varepsilon) = u(A, \sigma, -\varepsilon)$.

Let A be a central simple algebra over k with an involution σ of first kind. Let n be the degree of A. For $\varepsilon = \pm 1$, let

$$S(\sigma, \varepsilon) = \{x \in A | \sigma(x) = \epsilon x\}.$$

We know that $S(\sigma, \varepsilon)$ is a subspace of the k-vector space A and

$$\dim_k S(\sigma, \varepsilon) = \frac{n(n+1)}{2} \text{ or } \frac{n(n-1)}{2}.$$

We say that σ is *orthogonal* if $\dim_k S(\sigma, +1) = \frac{n(n+1)}{2}$ and *symplectic* if $\dim_k S(\sigma, +1) = \frac{n(n-1)}{2}$.

Let σ and τ be two involutions of first kind on a central simple k-algebra A. Then we have $\tau = int(u)\sigma$ for some unit $u \in A$ with $\sigma(u) = \pm u$, where $int(u)$ is the inner automorphism of A given by $x \mapsto uxu^{-1}$. Let $\eta \in \{\pm 1\}$ be such that $\sigma(u) = \eta u$. Let h be an ε-hermitian form over (A, σ). Let $h'(x, y) = uh(x, y)$. Then we have

$$\begin{aligned} \tau h'(x, y) &= \tau(uh(x, y)) \\ &= \tau(h(x, y))\tau(u) \\ &= int(u)(\sigma(h(x, y)))(int(u)\sigma)(u) \\ &= u\varepsilon h(y, x)u^{-1}u\eta u u^{-1} \\ &= \varepsilon\eta u h(y, x). \end{aligned}$$

Thus it is easy to see that $h' = uh$ is an $\varepsilon\eta$-hermitian form over (A, τ). It is easy to see that h is isotropic if and only if h' is isotropic. Hence we have

$u(A,\sigma,\varepsilon) = u(A,\tau,\varepsilon\eta)$. Thus to study $u(A,\sigma,\varepsilon)$ for all σ and ε, it is enough to study $u(A,\sigma,\varepsilon)$ for a fixed σ and all ε. In particular, if σ and τ are either both orthogonal or both symplectic, then $u(A,\sigma,\varepsilon) = u(A,\tau,\varepsilon)$.

Let A be a central simple algebra over K with an involution τ (first or second kind). Assume that there exist $\lambda, \mu \in A^*$ such that $\tau(\lambda) = -\lambda$, $\tau(\mu) = -\mu$, $\mu\lambda = -\lambda\mu$ and $L = K(\lambda)$ is a quadratic extension of K. Let $\widetilde{A}$ be the centralizer of L in A. Let τ_1=$\tau \mid_{\widetilde{A}}$ and let τ_2 be the involution $int(\mu^{-1})\tau_1$ on $\widetilde{A}$. Then τ_1 is an involution of second kind and τ_2 is an involution of first kind. We have $A = \widetilde{A} \oplus \mu\widetilde{A}$. Let $\pi : A \to \widetilde{A}$ be the L-linear projections given by $\pi_1(x+\mu y) = x$ and $\pi_2(x+\mu y) = y$. Let $h : V \times V \to A$ be an ε-hermitian space over (A,τ). Let $h_i : V \times V \to \widetilde{A}$ be defined by $h_i = \pi_i h$. Then h_1 is an ε-hermitian space over $(\widetilde{A},\tau_1)$ and h_2 is a $-\varepsilon$-hermitian space over $(\widetilde{A},\tau_2)$.

Theorem 1.5.1 With the notation as above, we have the following exact sequence

$W^{\varepsilon}(A,\tau) \xrightarrow{\pi_1} W^{\varepsilon}(\tilde{A},\tau_1) \xrightarrow{\rho} W^{-\varepsilon}(A,\tau) \xrightarrow{\pi_2} W^{\varepsilon}(\tilde{A},\tau_2)$ for a suitable map ρ.

This is proved in an appendix to [3] by Parimala, Sridharan and Suresh.

The following is proved in ([8]):

Corollary 1.5.2 Let A, $\tilde{A}$, τ, τ_1 and τ_2 be as above. Then $u(A,\tau,\varepsilon) \leq \frac{1}{2}u(\tilde{A},\tau_2,-\varepsilon) + u(\tilde{A},\tau_1,\varepsilon)$.

Let Q be a central simple algebra over k of degree 2. Then we call Q a *quaternion algebra*. Since the characteristic of k is not equal to 2, it is easy to see that $Q = (a,b)_2$ for some $a, b \in k^*$. Let $x, y \in Q$ be such that $x^2 = a$,

$y^2 - b$ and $xy + yx = 0$. Then every element in Q can be uniquely written as $\lambda_0 + \lambda_1 x + \lambda_2 y + \lambda_2 xy$ for some $\lambda_i \in k$. The map on Q, denoted by $-$, given by $\lambda_0 + \lambda_1 x + \lambda_2 y + \lambda_2 xy \mapsto \lambda_0 - \lambda_1 x - \lambda_2 y - \lambda_2 xy$ is an involution on Q and called the *canonical* involution.

Let A_0 be a central simple k-algebra with an involution σ of first kind. Let $Q = (a, b)$ be a quaternion algebra over k. Let $\lambda, \mu \in Q$ be such that $\lambda^2 = a$ and $\mu^2 = b$. Let $A = A_0 \otimes Q$ and $\tau = \sigma \otimes \bar{}$, where $\bar{}$ is the canonical involution on Q. Then A, λ, μ and τ are as in the paragraph before (1.6). In this case we have $\tilde{A} = A_0 \otimes k(\lambda)$, $\tau_1 = \sigma \otimes \bar{}$ and $\tau_2 = \sigma \otimes id$, where $\bar{}$ is the non-trivial automorphism of $k(\lambda)$ and id is the identity map of $k(\lambda)$. In this thesis, we use (1.6) and (1.7) in the situation described just now without any further reference.

In [8] the following theorem is proved.

Theorem 1.5.3 Let $Q = (a, b)_K$ be a quaternion division algebra over a field K. Let $-$ be the canonical involution of Q and $\wedge$ an orthogonal involution of Q and let $L = K(\sqrt{a}) \subset Q$ which is stable under $-$, then we have:
$u(Q, \wedge) = u(Q, -, -1) \leq min\{\frac{1}{2}u(L) + u(L, -), u(L) + \frac{1}{2}u(L, -)\}$,
$u(Q, -) = u(Q, \wedge, -1) \leq \frac{1}{2}u(L, -)$. □

By using above theorem we can deduce:

Theorem 1.5.4 Let k be a field of characteristic not equal to 2. Let H be a quaternion algebra over k and $\bar{}$ the canonical involution on H. Then $u(H, \bar{}, 1) \leq \frac{1}{4}u(k)$ and $u(H, \bar{}, -1) \leq \frac{5}{4}u(k)$.

□

Chapter 2

Division algebras of higher degree over rational function fields in one variable

2.1 Some Preliminaries

Let k be a field and $Br(k)$ be the Brauer group of division algebras over k. Let $X(k)$ be the character group $Hom(\Gamma_k, \mathbf{Q}/\mathbf{Z})$ of the continuous Galois group Γ_k of k. Let $k(t)$ be the function field of the projective line $\mathbb{P}^1_k$. For every closed point P of $\mathbb{P}^1_k$, let $k(P)$ denote the residue field at P and $\partial_P : Br(k(t)) \to X(k(P))$ be the residue homomorphism at P. If l is a prime not equal to the characteristic of k, we have the following exact sequence of Faddeev ([6]):

$$0 \longrightarrow {}_lBr(k) \longrightarrow {}_lBr(k(t)) \xrightarrow{\oplus\partial_p} \bigoplus_{P\in\mathbb{P}^1_k} {}_lX(k(P)) \xrightarrow{\sum cor} {}_lX(k) \longrightarrow 0$$

where Σcor is the sum of the corestriction (or norm) maps ${}_lX(k(P)) \to {}_lX(k)$ and the sum is over the set of closed points of $\mathbb{P}^1_k$.

In ([9]), Rowen-Sivatski-Tignol, tried to obtain information on the index of Brauer classes in $Br(k(t))$ from their images under the ramification map $\oplus\partial_P$. For an element $\alpha \in Br(k(t))$, the ramification degree is defined as $\sum[k(P) : k]$, where the sum is taken over all the closed points P of $\mathbb{P}^1_k$ with $\partial_P(\alpha) \neq 0$. They studied 2-torsion elements in $Br(k(t))$ with ramification degree at most 3. In this chapter we extend their results to the elements of l-torsion for any prime number l not equal to the characteristic of k.

We now recall a class of central simple algebras. Let D be a finite dimensional central division algebra over an arbitrary field K and x be an indeterminate over K. The ring $D[x] = D \otimes K[x]$ is a left principal domain with Ore ring of fractions $D(x) = D \otimes K(x)$. Let α be an automorphism of finite order n of $D[x]$ and $g \in K[x]$. Consider the algebra

$$\Delta(D(x), \alpha, g) = D(x) \oplus D(x)y \oplus \cdots \oplus D(x)y^{n-1}$$

where the multiplication defined by $y^n = g$ and $yf = \alpha(f)y$ for $f \in D(x)$. This algebra can be viewed as the quotient ring of the skew-polynomial ring $D(x)[y; \alpha]$ by the ideal generated by $y^n - g$.

Theorem 2.1.1 ([9], Th.1.1) Suppose n is a prime number and α does not restrict to the identity on $K[x]$. The algebra $\Delta(D(x), \alpha, g)$ is a division algebra if and only if there is no $f \in D[x]$ such that $\alpha^{n-1}(f) \cdots \alpha(f)f = g$.

2.2 l-torsion ramification sequences

In this section k denotes a field and l a prime number not equal to the characteristic of k. We assume that k contains a primitive l^{th} root of unity. We fix a primitive l^{th} root of unity ζ in k.

Let $X(k)$ be the group of characters of the absolute Galois group of k. Since l is not equal to the characteristic of k and k contains a primitive l^{th} root of unity, by fixing a primitive l^{th} root of unity in k, we identify ${}_lX(k(P))$ with $k(P)^*/k(P)^{*^l}$ for every closed point P of $\mathbb{P}^1_k$. Thus an l-torsion ramification sequence $\rho \in \mathcal{R}_l$ can be viewed as an element of $\oplus_{P \in \mathbb{P}^1_k{}^{(1)}} k(P)^*/k(P)^{*^l}$ which is in the kernel of the norm map

$$\oplus_{P\in\mathbb{P}^1_k{}^{(1)}} k(P)^*/k(P)^{*^l} \to k^*/k^{*^l}.$$

Let ρ be a non-trivial element of ${}_l\mathcal{R}$. As we already mentioned in chapter 1 $\mathrm{degsupp}(\rho) \geq 2$.

Theorem 2.2.1 Let $\rho \in \mathcal{R}_l$. Suppose that $\mathrm{degsupp}(\rho) = 2$. If $\mathrm{supp}(\rho) = \{P_1, P_2\}$ (two distinct rational points), then there exist $\lambda, a, b \in k^*$ such that $\rho = (\partial_P((\lambda, (t-a)(t-b)^{l-1})_l))$.

Proof. Suppose that $\mathrm{degsupp}(\rho) = 2$ and $\mathrm{supp}(\rho) = \{P_1, P_2\}$. Since P_1 and P_2 are two rational points of $\mathbb{P}^1_k$, we choose an affine line $\mathbb{A}^1_k$ in $\mathbb{P}^1_k$ such that P_1 and P_2 correspond to the maximal ideals $(t-a)$ and $(t-b)$ for some $a, b \in k^*$. Write $\rho = (\chi_P)$. Since P_1 and P_2 are rational points, $[k(P_1) : k] = [k(P_2) : k] = 1$. Since $\mathrm{supp}(\rho) = \{P_1, P_2\}$, by Faddeev's exact sequence we have $N_{k(P_1)/k}(\chi_{P_1}).N_{k(P_2)/k}(\chi_{P_2}) = 1$ where $N_{k(P_i)/k}$ are the norm maps from $k(P_i)$ to k for $i = 1, 2$. So $\chi_{P_1} = \chi_{P_2}^{-1} \in k^*/k^{*^l}$ and $\chi_P = 1$ for all $P \neq P_i$. Let $\lambda \in k^*$ represents χ_{P_1}.

Let $\beta = (\lambda, (t-a)(t-b)^{l-1})_l$. We claim that $\rho = (\partial_P(\beta))$. If P is any closed point of the affine line $\mathbb{A}^1_k$ not equal to P_1 and P_2, then $t-a$ and $t-b$ are units at P and hence $\partial_P(\beta) = 1$. If P is the point out side the affine line, then it easy to see that $v_P((t-a)(t-b)^{l-1}) = -l$. In particular $\partial_P(\beta) = 1$. Now, $\partial_{P_1}(\beta) = (-1)^{v_{P_1}(\lambda)v_{P_1}((t-a)(t-b)^{l-1})}\overline{\lambda^{v_{P_1}((t-a)(t-b)^{l-1})}((t-a)(t-b)^{l-1})^{-v_{P_1}(\lambda)}}\, k^{*l} \in k^*/k^{*l}$. Since $v_{P_1}(\lambda) = 0$ and $v_{P_1}((t-a)(t-b)^{l-1}) = 1$, we have $\partial_{P_1}(\beta) = \lambda k^{*^l} = \chi_{P_1}$ and $\partial_{P_2}(\beta) = \lambda^{l-1}k^{*^l} = \lambda^{-1}k^{*^l} = \chi_{P_1}^{-1} = \chi_{P_2}$. Hence $\rho = (\partial_P(\beta))$ □

Theorem 2.2.2 Let $\rho \in \mathcal{R}_l$. Suppose that $l \geq 3$ and degsupp$(\rho) = 2$. If supp$(\rho) = \{P\}$ (deg$P = 2$), then there exists $a \in k$ such that $\rho = (\partial_Q((t, t^2 + at + 1)_l))$.

Proof. Suppose that degsupp$(\rho) = 2$ and supp$(\rho) = \{P\}$. Since deg$P = 2$, $k(P)/k$ is a degree two extension. Let $\lambda \in k(P)$ representing χ_P in $k(P)^*/k(P)^{*^l}$. Let N be the norm map from $k(P)$ to k. Since $cor_P(\rho) = \sum cor_Q(\rho) = 1$, $N(\chi_P) = b^l$ for some $b \in k^*$. Since l is odd and $[k(P) : k] = 2$, replacing λ by $b^{-\frac{l(l+1)}{2}}\lambda^{l+1}$, we assume that $N(\lambda) = 1$.

If $\lambda \in k^*$, then $N(\lambda) = \lambda^2 = 1$ and hence $\lambda = \pm 1$. Since l is odd, we have $\lambda = \lambda^l$. Since ρ is non-trivial, this is a contradiction. Hence λ is not in k^*. Since $N(\lambda) = 1$, the minimal polynomial of λ is of the form $t^2 + at + 1$. By the change of projective coordinates (see Corollary 1.3.3*(ii)*), we assume that there is an affine line $\mathbb{A}^1_k$ in $\mathbb{P}^1_k$ containing P such that P corresponds to the maximal ideal $(t^2 + at + 1)$.

Let $\beta = (t, t^2 + at + 1)_l$. If Q' is a rational point of the affine line $\mathbb{A}^1_k$ corresponding to the maximal ideal (t) then $v_{Q'}(t) = 1$ and $v_{Q'}(t^2 + at + 1) = 0$. Hence we have $\partial_{Q'}(\beta) = \overline{(-1)^{v_{Q'}(t)v_{Q'}(t^2+at+1)}t^{v_{Q'}(t^2+at+1)}(t^2 + at + 1)^{-v_{Q'}(t)}}\, k^{*l} \in k^*/k^{*l}$. Thus $\partial_{Q'}(\beta) = \overline{(t^2 + at + 1)^{-1}} = 1$. If Q'' is any closed point on the affine line other than P and Q' then clearly, $\partial_{Q''}(\beta) = 1$. If P_∞ is the point out side the affine line, then $v_{P_\infty}(t) = -1$, $v_{P_\infty}(t^2 + at + 1) = -2$ and

$\partial_{P_\infty}(\beta) = \overline{(-1)^{v_{P_\infty}(t)v_{P_\infty}(t^2+at+1)}t^{v_{P_\infty}(t^2+at+1)}(t^2 + at + 1)^{-v_{P_\infty}(t)}}\, k(P_\infty)^{*l}$

Hence $\partial_{P_\infty}(\beta) = 1$. We have $\partial_P(\beta)$ equal to the image of t in $k(P)^*/k(P)^{*^l}$. Since P corresponds to the maximal ideal $(t^2 + at + 1)$, the image of t in $k(P) = k[t]/(t^2 + at + 1)$ is λ. Hence $\rho = (\partial_Q(\beta))$. □

Theorem 2.2.3 Let $\rho \in \mathcal{R}_l$. Suppose that degsupp$(\rho) = 3$. If supp$(\rho) = \{P_1, P_2, P_3\}$ (three distinct rational points), then there exist $a_1, a_2 \in k^*$ such that $\rho = (\partial_P((t, (t-a_1)(t-a_2)(t-a_1a_2)^{l-1})_l))$.

Proof. Suppose that degsupp$(\rho) = 3$ and supp$(\rho) = \{P_1, P_2, P_3\}$. Let $a_i \in k(P_i)$ be such that $\chi_{P_i} = a_i k(P)^{*^l}$, for $i = 1, 2, 3$. Since $(cor_P(\rho)) = 1$ and cor_{P_i} are identity functions, we have $a_1a_2a_3 \in k^{*^l}$.

By the change of projective coordinates (see Corollary 2*(i)* of Chapter 1), we can assume that there is an affine line in $\mathbb{P}^1_k$ containing all P_i and each P_i corresponds to the maximal ideal $(t-a_i)$, $i = 1, 2$ and P_3 corresponds to $(t-a_1a_2)$. Let $\beta = (t, (t-a_1)(t-a_2)(t-a_1a_2)^{l-1})_l$. Then we have $\partial_{P_i}(\beta) = a_i$ for $i = 1, 2$ and $\partial_{P_3}(\beta) = (a_1a_2)^{l-1} = a_3$ module k^{*^l}. If Q is closed point of $\mathbb{P}^1_k$ not equal to P_i, $i = 1, 2, 3$, then it easy see that $\partial_P(\beta) = 1$. Hence $\rho = (\partial_P(\beta))$. □

Theorem 2.2.4 Let $\rho \in \mathcal{R}_l$. Suppose that degsupp$(\rho) = 3$. If supp$(\rho) = \{P_1, P_2\}$ (deg$P_1 = 1$ and deg$P_2 = 2$), then there exist $\lambda, a, b, c \in k^*$ such that $\rho = (\partial_P((\lambda, (t^2+at+b)(t-c)^{l-2})_l)$ or $\rho = (\partial_P((t, (t^2+at+b)(t-c))_l))$.

Proof. Suppose that degsupp$(\rho) = 3$ and supp$(\rho) = \{P_1, P_2\}$ with deg$P_1 = 1$ and deg$(P_2) = 2$.

Let $\lambda_1 \in k(P_1)$ and $\lambda_2 \in k(P_2)$ be such that $\chi_{P_1} = \lambda_1 k(P_1)^{*^l}$ and $\chi_{P_2} = \lambda_2 k(P_2)^{*^l}$.

Suppose that $\lambda_2 \in k^* k(P_2)^{*^l}$. Let $\lambda \in k^*$ be such that $\lambda_2 = \lambda$ modulo $k(P_2)^{*^l}$. Let $N : k(P_2) \to k$ be the norm map. Since $\sum cor_Q(\rho) = 1$, we have $\lambda_1 N(\lambda_2) \in k^{*^l}$. Choose an affine line in $\mathbb{P}^1_k$ containing P_1 and P_2, so that P_1

corresponds to a maximal ideal $(t-c)$ and P_2 corresponds to a maximal ideal t^2+at+b. Let $\beta = (\lambda, (t^2+bt+c)(t-c)^{l-2})_l$. Let P be a closed point of $\mathbb{P}^1_k$. If P is not equal to either P_1 or P_2, then it is easy see that $\partial_P(\beta) = 1$. We have $\partial_{P_1}(\beta) = \lambda^{l-2}$ and $\partial_{P_2}(\beta) = \lambda$. Since $\lambda = \lambda_2$ module $k(P_2)^{*^l}$ and $\lambda^{l-2} = \lambda_2^{l-1} = \lambda_2^{-2} = \lambda_1$ modulo k^{*^l}, $\rho = (\partial_P(\beta))$.

Assume that $\lambda_2 \notin k^*k(P_2)^{*^l}$. In particular, $\lambda_2 \notin k$ and $k(P_2) = k(\lambda_2)$. Let t^2+at+b be the minimal polynomial of λ_2 over k. Note that b is the norm of λ_2 from $k(P_2)$ to k.

Once again by Corollary 1.3.3*(i)*, we assume that there is an affine line in $\mathbb{P}^1_k$ such that P_1 corresponds to a maximal ideal $(t-c)$, $c \neq 0$, and P_2 corresponds to the maximal ideal t^2+at+b.

Let $\beta = (t, (t^2+at+b)(t-c))_l$. It is clear that $\partial_{P_1}(\beta) = \lambda_1$ and $\partial_{P_2}(\beta) = \lambda_2$. If P is any point which in the affine line and not equal to P_1, P_2 and the closed point P_0 corresponding to the maximal ideal (t), then it is easy to see that $\partial_P(\beta) = 1$. We have $\partial_{P_0}(\beta) = (\lambda_1 N(\lambda_2))^{-1} = 1$ modulo k^{*^l}. If the P_∞ is the point out side the affine line, then $\partial_{P_\infty}(\beta) = 1$. Hence $\rho = (\partial_P(\beta))$. □

Theorem 2.2.5 Let $\rho \in \mathcal{R}_l$. Suppose that degsupp$(\rho) = 3$. If supp$(\rho) = \{P\}$ (deg$P = 3$), then there exist $\lambda, a, b, c, \in k^*$ such that $\rho = (\partial_P((\lambda, (t^3+at^2+bt+c))_3))$ ($l=3$) or $\rho = (\partial_P((t, (t^3+at^2+bt+c))_l))$.

Proof. Suppose that degsupp$(\rho) = 3$ and supp$(\rho) = \{P\}$. Let $\lambda \in k(P)$ be such that $\chi_P = \lambda$ modulo $k(P)^{*^l}$. Let N be the norm map from $k(P)^*$ to k^*.

Suppose $\lambda \in k^*k(P)^{*^l}$. Multiplying λ by an l^{th} power of an element in $k(P)$, we assume that $\lambda \in k^*$. Then $N(\lambda) = \lambda^3 \in k^{*^l}$. If $l > 3$, then $\lambda \in k^{*^l}$. This is contradiction as ρ is non-trivial. Hence $l = 3$. Choose an affine line in $\mathbb{P}^1_k$ containing P so that P corresponds to a maximal ideal $(t^3 + at^2 + bt + c)$. Let $\beta = (\lambda, t^3 + at^2 + bt + c)_3$. Then it easy to see that $\rho = (P_Q(\beta))$.

Assume that $\lambda \notin k^*k(P)^{*^l}$. Then $k(P) = k(\lambda)$. Let $t^3 + at^2 + bt + c$ be the minimal polynomial of λ over k. We choose an affine line in $\mathbb{P}^1_k$ containing P such that P corresponds to the maximal ideal $t^3 + at^2 + bt + c$. Let $\beta = (t, t^3 + at^2 + bt + c)_l$. If Q is a point not equal to either P or the point P_0 corresponding to the maximal ideal (t) or the point P_∞ out side the affine line, then $\partial_Q(\beta) = 1$. It is clear that $\partial_P(\beta) = \lambda$. We have $\partial_{P_0}(\beta) = c^{-1}$ modulo k^{*^l}. Since $t^3 + at^2 + bt + c$ is the minimal polynomial of λ, we have $c = -N(\lambda)$, which is an l^{th} power. Hence $\partial_{P_0}(\beta) = 1$. It is easy to see that $\partial_{P_\infty}(\beta) = 1$. Hence $\rho = (\partial_Q(\beta))$. □

2.3 The l-symbol algebras

Let k be a field and l a prime number not equal to the characteristic of k. Assume that k contains a primitive l^{th} root of unity. Fix a primitive l^{th} root of unity ζ in k. Let D be a central division algebra over k and $a \in k^*$. Then $E = D \otimes k(\sqrt[l]{a})$ is a division algebra if and only if D does not contain an l^{th} root of a (see [4] §9 Corollary 9).

Suppose that D does not contain an l^{th} root of a. Let σ be the automorphism of $k(\sqrt[l]{a})$ given by $\sigma(\sqrt[l]{a}) = \zeta\sqrt[l]{a}$. Then $E = D \otimes k(\sqrt[l]{a})$ is a division algebra and the automorphism σ extends to an automorphism of α of E which is the identity on D.

Proposition 2.3.1 Let D and a be as above. Let $g \in k[t]$. Then $\Delta(E(t), \alpha, g) \simeq D \otimes_k (a, g)_l$.

Proof. We have $\Delta(E(t), \alpha, g) = E(t) \oplus E(t)y \oplus \cdots \oplus E(t)y^{l-1}$, with multiplication defined by $y^l = g$ and $yf = \alpha(f)y$ for $f \in E(t)$. We can consider D as subalgebra of E and hence of $\Delta(E(t), \alpha, g)$. Let $x = \sqrt[l]{a} \in k(\sqrt[l]{a}) \subset E \subset \Delta(E(t), \alpha, g)$. We have $x^l = a$, $y^l = g$ and $yx = \alpha(x)y = \zeta xy$. Hence the $k(t)$-subalgebra of $\Delta(E(t), \alpha, g)$ generated by x and y is isomorphic to $(a, g)_l$. Since α is identity on D, for any $d \in D$ we have $yd = \alpha(d)y = dy$. We also have $xd = dx$ for all $d \in D$, because $k(\sqrt[l]{a})$ is the center of $E = D \otimes k(\sqrt[l]{a})$. Hence, every element of D and every element of the subalgebra generated by x and y commute. Now define a map $\phi : D \otimes (a, g)_l \to \Delta(E(t), \alpha, g)$ such that $\phi(b \otimes c) = bc$. So, $\phi((b_1 \otimes c_1)(b_2 \otimes c_2)) = \phi(b_1 b_2 \otimes c_1 c_2) = b_1 b_2 c_1 c_2$. Since the elements of D and $(a, g)_l$ commute therefore, $b_2 c_1 = c_1 b_2$. So,$\phi((b_1 \otimes c_1)(b_2 \otimes c_2)) = b_1 c_1 b_2 c_2 = \phi((b_1 \otimes c_1)\phi((b_2 \otimes c_2)$. Hence, there is a $k(t)$-algebra homomorphism $\phi : D \otimes (a, g)_l \to \Delta(E(t), \alpha, g)$. Since $D \otimes (a, g)_l$ is simple, ϕ is injective. By the dimension count, it follows that ϕ is an isomorphism. □

Corollary 2.3.2 Let D, E and a be as above. Let $g \in k[t]$. Then $D \otimes_k (a, g)_l$ is not a division algebra if and only there exits $f \in E[t]$ such that $\alpha^{l-1}(f) \cdots \alpha(f) f = g$.

Proof. Follows from Theorem(2.1.1) and Proposition(2.3.1). □

Corollary 2.3.3 Let D be a central division algebra over k and $a \in k^*$. Suppose that D does not contain an l^{th} root of a. Then, for every $g \in k[t]$ of degree co-prime with l, $D \otimes_k (a, g)_l$ is a division algebra.

Proof. By Corollary 2.3.2, $D \otimes_k (a, g)_l$ is a division algebra if and only if there is no $f \in E[t]$ such that $\alpha^{l-1}(f) \cdots \alpha(f) f = g$. Since deg $\alpha^i(f) =$ deg f for any i we get, l deg $f =$ deg g. So, l divides deg g. □

Proposition 2.3.4 Let D be a central division algebra and $g \in k[t]$. Then

$$\Delta(D(x), \alpha, g(x^l)) \simeq D \otimes_k (t, g(t))_l,$$

where $x^l = t$ and α is the automorphism of $D(x)$ defined by $\alpha(x) = \zeta x$ and $\alpha(d) = d$ for all $d \in D$.

Proof. Let $t = x^l \in \Delta(D(x), \alpha, g(x^l))$. Since $\alpha(t) = t$, we see that $yt = \alpha(t)y = ty$ and hence for any i, $y^i t = \alpha(t) y^i = t y^i$. Thus, t commutes with every element of $\Delta(D(x), \alpha, g(x^l))$. So, t is in the center of $\Delta(D(x), \alpha, g(x^l))$. We have $y \in \Delta(D(x), \alpha, g(x^l))$ with $y^l = g(x^l) = g(t)$. The sub-algebra of $\Delta(D(x), \alpha, g(x^l))$ generated by x and y is clearly isomorphic to $(t, g(t))$ and commutes with D. Hence we have a homomorphism $D \otimes_k (t, g(t)) \to \Delta(D(x), \alpha, g(x^l))$. By dimension count, it is an isomorphism. □

Corollary 2.3.5 Let $g \in k[t]$. The algebra $\Delta(E(t), \alpha, g) \simeq D \otimes_k (t, g)_l$ is not a division algebra if and only there exits $f \in D[t]$ such that $\alpha^{n-1}(f) \cdots \alpha(f) f = g(t^l)$.

Proof. Follows from Theorem(2.1.1) and Proposition(2.3.4). □

Theorem 2.3.6 Let D be a central division algebra over k. Let and $\lambda \in k^*$ and $g \in k[t]$ be a separable polynomial of degree l which is reducible. Suppose that D does not contain an l^{th} root of λ. The tensor product $D \otimes (\lambda, g(t))_l$ is not a division algebra if and only if $g(t) = b(t-a)^l$ and there exists $\theta \in D \otimes k(\sqrt[l]{\lambda})$ such that $\alpha^{l-1}(\theta) \cdots \alpha(\theta)\theta = b$.

Proof. Suppose $D \otimes (\lambda, g(t))_l$ is not a division algebra. Let $p(t)$ be a monic irreducible factor of g. Since g is reducible and of degree l, the degree of $p(t)$ is co-prime to l. Let $F = k[t]/(p(t))$. Since $[F : k] = deg(p(t))$, which is co-prime to l, $D \otimes_k F$ is a division algebra and there is no element in D whose l^{th} power is λ. By (2.3.1), there exists $f \in (D \otimes F)[t]$ such that $\alpha^{l-1}(f) \cdots \alpha(f)f = g(t)$. Since g is a polynomial of degree l, by comparing the degrees of both sides, we see that $\deg(f) = 1$. Since p has a root in F, g has a root a in F. Since a is a central element, by substituting $t = a$ both sides, we get that $f(a) = 0$. Hence $f(t) = \theta(t-a)$ for some $\theta \in D \otimes F \otimes k(\sqrt[l]{\lambda})$. We have

$$g(t) = \alpha^{l-1}(f) \cdots \alpha(f)f = \alpha^{l-1}(\theta) \cdots \alpha(\theta)\theta(t-a)^l.$$

Since g is separable, we have $p(t) = t - a$ and hence $F = k$. Therefore $g(t) = \alpha^{l-1}(\theta) \cdots \alpha(\theta)\theta(t-a)^l$ for some $\theta \in D \otimes k(\sqrt[l]{\lambda})$. Conversely, suppose that $g(t) = \alpha^{l-1}(\theta) \cdots \alpha(\theta)\theta(t-a)^l$. Then $(\lambda, g(t))_l = (\lambda, b(t-a)^l)_l = (\lambda, b)$, where $b = \alpha^{l-1}(\theta) \cdots \alpha(\theta)\theta$. Since $\theta \in D \otimes k(\sqrt[l]{\lambda})$, $D \otimes (\lambda, b)_l$ is not a division algebra by Corollary (2.3.2) and hence $D \otimes (\lambda, g(t))_l$ is not a division algebra. □

Let $b, c \in k$ and α and β are roots of the polynomial $t^2 + bt + c$ in an extension of k. Then we have $\alpha + \beta = -b$ and $\alpha\beta = c$. Using these equalities and binomial expansion, it is easy to see that, for any odd natural number l,

$$\alpha^l + \beta^l = -\{b^l + {}^lC_1 c(\alpha^{l-2} + \beta^{l-2}) + {}^lC_2 c^2(\alpha^{l-4} + \beta^{l-4}) + \cdots + {}^lC_{\frac{l-1}{2}} c^{\frac{l-1}{2}}(\alpha + \beta)\}.$$

By induction, it easy to see that $\alpha^l + \beta^l \in k$ and is a polynomial in b and c with integer coefficients. Let $h_l(b, c) = \alpha^l + \beta^l \in k$.

Theorem 2.3.7 Let D be a central division algebra over k and $a \in k^*$. The tensor product $D \otimes (t, t^2 + at + 1)_l$ is not a division algebra if and only if there exist $u \in D$ and $v \in k$ an l^{th} root of unity such that $h_l(u, v) = a$.

Proof. Suppose $D \otimes (t, t^2 + at + 1)_l$ is not a division algebra. Then, by (2.3.5), there exists $f \in D[t]$ such that $\alpha^{l-1}(f) \cdots \alpha(f) f = t^{2l} + at^l + 1$, where α is identity on D and $\alpha(t) = \rho t$. By considering the degree on the both sides, we see that $f(t) = \theta t^2 + ut + v$ for some $\theta, u, v \in D$. By comparing the coefficients, we get that $\theta^l = v^l = 1$. Since k contains a primitive l^{th} root of unity, $\theta, v \in k$. Since k is the center of D, we can divide the polynomial f by θ and assume that $\theta = 1$. Thus we have $f(t) = t^2 + ut + v$, with $u \in D$ and $v \in k$. Since u and v commute, by comparing the coefficient of t^l both sides, we get that $h_l(u, v) = a$.

Conversely, suppose that there exist $u \in D$ and $v \in k$ an l^{th} root of unity such that $h_l(u, v) = a$. Let $f(t) = t^2 + ut + v$. Then it is not difficult to see that $\alpha^{l-1}(f) \cdots \alpha(f) f = t^{2l} + at^l + 1$. By Corollary (2.3.5), the algebra $D \otimes (t, t^2 + at + 1)_l$ is not division. □

Theorem 2.3.8 Let D be a central division algebra over k, $a \in k^*$ and $g(t) \in k[t]$. If a is not an l^{th} power in D and $t^l - a$ does not divide $g(t^l)$ in $k[t]$, then the tensor product $D \otimes (t, (t - a)g(t))_l$ is a division algebra.

Proof. Assume that a is not an l^{th} power in D and $t^l - a$ does not divide $g(t^l)$. Suppose that $D \otimes (t, (t - a)g(t))_l$ is not a division algebra. Then, by Corollary

(2.3.5), there exists $f(t) \in D[t]$ such that $\alpha^{l-1}(f)\cdots\alpha(f)f = (t^l - a)g(t^l)$. Since a is not an l^{th} power in D, $t^l - a$ is an irreducible element of $(D \otimes k(\sqrt[l]{a}))[t]$. $D \otimes k(\sqrt[l]{a})[t]$ is principal domain so, $t^l - a$ is a prime element.Hence, $t^l - a$ divides $\alpha^i(f)$ for some i. Therefore, $f = (t^l - a)u$ for some $u \in D \otimes k(\sqrt[l]{a})[t]$ and $\alpha^i(f) = (t^l - a)\alpha^i(u)$ for all i.Therefore, $(t^l - a)^l \alpha^{l-1}(u)\cdots\alpha(u)u = (t^l - a)g(t^l)$. Hence $t^l - a$ divides $g(t^l)$, which is a contradiction. □

Theorem 2.3.9 For every central simple k-algebra A

$$index(A \otimes (a,b)_l) \in \{\tfrac{1}{l}\, indA, indA, l\, indA\}.$$

Proof. Let $d = \text{ind}(A \otimes (a,b)_l)$. We know that for two central simple k-algebras A and B, $ind(A \otimes B)$ divides (ind A) (ind B). Thus d divides l ind(A). Write l ind$(A) = dd'$ for some d'. Since $A \otimes (a,b) \otimes (a, b^{l-1}) \sim A$, the ind$(A)$ divides indld. Write $ld = \text{ind}(A)l'$ for some l'. We have $l^2\, \text{ind}(A) = \text{ind}(A)l'd'$. Since l is a prime, we have $d' = 1$ or l or l^2. Hence $index(A \otimes (a,b)_l) \in \{\frac{1}{l}\, indA, indA, l\, indA\}$. □

Theorem 2.3.10 For any central simple k-algebra A

$$index(A \otimes (\lambda, g(t))_l) = indA \text{ or } l\, indA,$$

where degree of $g(t)$ is l.

Proof. Let $A' = (A \otimes (\lambda, g(t))_l)$. By (2.3.9), $index(A') \in \{\frac{1}{l}\, indA, indA, l\, indA\}$. Let D (respectively D') be a division algebra Brauer-equivalent to A (respectively $(A \otimes (\lambda, g(t))_l)$. We have $[D'] = [A][(\lambda, g(t))_l] = [D][(\lambda, g(t))_l] = [D \otimes (\lambda, g(t))_l]$. Hence $D \otimes (\lambda, g(t))_l$ is division algebra if and only if $ind(A') = l\, ind(A)$. Suppose $D \otimes (\lambda, g(t))_l$ is not division algebra. Then, by (2.3.9), $index(A \otimes (\lambda, g(t))_l) =$

$indA$ or $\frac{1}{l}$ $indA$. By (2.3.6), we have $g(t) = b(t-a)^l$ and there exists $\theta \in D \otimes k(\sqrt[l]{\lambda})$ such that $\alpha^{l-1}(\theta) \cdots \alpha(\theta)\theta = b$. Hence $A' = (A \otimes (\lambda, b)_l)$. Assume that index $A' = \frac{1}{l}$ index A. Then deg $D' = \frac{1}{l}$ index A and $deg_{k(t)}(D(t)) = deg_k(D)$ and hence deg $D(t) =$ deg $(D' \otimes_{k(t)} (\lambda, b)_l)$. Since $D(t)$ and $D' \otimes_{k(t)} (\lambda, b)_l$ are Brauer-equivalent, it follows $D(t) \simeq (D' \otimes_{k(t)} (\lambda, b)_l)$. Hence $D(t)$ contains a subalgebra isomorphic to $(\lambda, b)_l$. So that $D(t)$ contains elements f,h such that $fh = \xi hf$, $f^l = \lambda$ and $h^l = b$. We may find f_0,$h_0 \in k[t]$ and f_1,$h_1 \in D[t]$ such that $f = f_1 f_0^{-1}$ and $h = h_1 h_0^{-1}$. Then clearing denominators,

$$f_1 h_1 = \xi h_1 f_1 \text{ and } h_1^l = b h_0^l \text{ where } \xi \text{ is } l^{\text{th}}\text{-root of unity.}$$

From these equations, it follows that the leading coefficient of h_1 is in k and that it does not commute with the leading coefficient of f_1 which is in D. This is a contradiction as k is the center of D. Therefore, $index(A \otimes (\lambda, g(t))_l) = indA$. □

Theorem 2.3.11 For any central simple k-algebra A

$$index(A \otimes (t, t^2 + at + 1)_l) = indA \text{ or } l\ indA.$$

Proof. Let $A' = (A \otimes (t, t^2 + at + 1)_l)$. By (2.3.9), $index(A') \in \{\frac{1}{l}\, indA, indA, l\ indA\}$. Suppose index $A' = \frac{1}{l}$ index A. As in the proof of (2.3.10), $D(t)$ contains a subalgebra isomorphic to $(t, t^2 + at + 1)_l$. Hence $D(t)$ contains elements f, h such that $fh = \xi hf$, $f^l = t$ and $h^l = t^2 + at + 1$. We may find f_0,$h_0 \in k[t]$ and f_1,$h_1 \in D[t]$ such that $f = f_1 f_0^{-1}$ and $h = h_1 h_0^{-1}$. Then by clearing denominators, we have

$$f_1^l = t f_0^l\ ,\ f_1 h_1 = \xi h_1 f_1 \text{ and } h_1^l = (t^2 + at + 1) h_0^l$$

where ξ is an l^{th}-root of unity.

From these equations, it follows that the leading coefficient of f_1 is in k and that it does not commute with the leading coefficient of h_1 which is in D. This is a contradiction as k is the center of D. Therefore, $index(A \otimes (t, t^2 + at + 1)_l) = indA$ or $l\ indA$. Now, $index(A \otimes (t, t^2 + at + 1)_l) = indA$ if and only if $D \otimes (t, t^2 + at + 1)_l)$ is not a division algebra. By (2.3.7), $D \otimes (t, t^2 + at + 1)_l$ is not a division algebra if and only if there exists $u \in D$ and $v \in k$ an l^{th} root of unity such that $h_l(u, v) = a$. Otherwise $index(A \otimes (t, t^2 + at + 1)_l = l\ indA$ □

Theorem 2.3.12 For any central simple k-algebra A

$$index(A \otimes (t, (t-a)g(t))_l) = indA \text{ or } l\ indA.$$

Proof. Let $A' = (A \otimes (t, (t-a)g(t))_l)$. By (2.3.8) ind $A' = l$ ind A if a is not an l^{th} power in D and $t^l - a$ does not divide $g(t^l)$ in $k[t]$. Otherwise ind $A' =$ ind A. □

Chapter 3

Hermitian forms and the u-invariant

Throughout this chapter k and K denote fields of characteristic not equal to 2.

Let A be a central simple K-algebra with an involution σ. Let $\varepsilon \in \{\pm 1\}$ and

$$S(\sigma, \varepsilon) = \{x \in A | \sigma(x) = \varepsilon x\}.$$

Let $r = \dim_k S(\sigma, \varepsilon)$ and $k = \{\lambda \in K | \sigma(\lambda) = \lambda\}$.

By a theorem of Mahmoudi ([8]) we have

$$u(A, \sigma, \varepsilon) \leq \frac{r(r+1)}{2m^2[K:k]} u(k)$$

where m is the degree of A over K.

In this chapter we give a better bound for $u(A, \sigma, \varepsilon)$ when the degree of A is at most 4.

Let $K = k(\sqrt{d})$ be a quadratic field extension of k and θ a k-automorphism of K. Note that there is only one non-trivial k-automorphism K. If θ is non-trivial, then $\theta(\sqrt{d}) = -\sqrt{d}$. Let $\eta \in \{\pm 1\}$ be such that $\theta(\sqrt{d}) = \eta\sqrt{d}$. Let A_0 be a central simple algebra k with an involution τ of first kind. Let $A = A_0 \otimes K$ and $\sigma = \tau \otimes \theta$. Then A is a central simple algebra over K and σ is an involution on A. The involution σ on A is of first kind if $\eta = 1$ and second kind if $\eta = -1$.

Identify A_0 as a subalgebra of A. Then we have $A = A_0 \oplus A_0\sqrt{d}$. Let $\pi_i : A \to A_0$ be the projections given by $\pi_1(x + y\sqrt{d}) = x$ and $\pi_2(x + y\sqrt{d}) = y$ for all $x, y \in A_0$. Let $h : V \times V \to A$ be an ε-hermitian form over (A, σ). Let $h_i = \pi_i h : V \times V \to A_0$. Then $h(x, y) = h_1(x, y) + h_2(x, y)\sqrt{d}$. We have

$$h_1(x,y) + h_2(x,y)\sqrt{d} = h(x,y) = \varepsilon\sigma(h(y,x)) = \varepsilon\tau(h_1(y,x)) + \varepsilon\eta h_2(x,y)\sqrt{d}.$$

Now it is easy to check that h_1 is an ε-hermitian form over (A_0, τ) and h_2 is a $\eta\varepsilon$-hermitian form over (A_0, τ). The assignments $h \mapsto h_i$ induces homomorphisms

$$\pi_1 : W^\varepsilon(A, \sigma) \to W^\varepsilon(A_0, \tau)$$

and

$$\pi_2 : W^\varepsilon(A, \sigma) \to W^{\eta\varepsilon}(A_0, \tau).$$

Let $h_0 : V_0 \times V_0 \to A_0$ be an ε-hermitian space over (A_0, τ). Let $V = V_0 \otimes_{A_0} A$. Then we can write $V = V_0 \oplus V_0\sqrt{d}$. Define $h : V \times V \to A$ by

$$h(x_1 + y_1\sqrt{d}, x_2 + y_2\sqrt{d}) = h_0(x_1, x_2) + \eta d h_0(y_1, y_2) + (\eta h_0(x_1, y_2) + h_0(y_1, x_2))\sqrt{d}.$$

Then it can be checked that h is an ε-hermitian form over (A, σ) and the assignment $h_0 \mapsto h$ induces a homomorphism $\rho : W^\varepsilon(A_0, \tau) \to W^\varepsilon(A, \sigma)$.

Lemma 3.1 Let K/k, A_0, A, σ, τ, ρ and π_2 as above. Then $\pi_2 \circ \rho = 0$.

Proof. Let (V_0, h_0) be an ε-hermitian space over (A_0, τ). We have $\rho(h_0) = (V, h)$, where $V = V_0 \oplus \sqrt{d}V_0$ and h is as defined above. Let $W = \{x + \sqrt{d}\ 0 | x \in V_0\} \subset V$. Then we have

$$\pi_2\rho(h_0)(x_1 + \sqrt{d}\ 0, x_2 + \sqrt{d}\ 0) = \pi_2(h_0(x_1, x_2) + \sqrt{d}\ 0) = 0.$$

Thus $W \subset W^{\perp}$. Let $x + \sqrt{y} \in W^{\perp}$. Then we have $0 = \pi_2\rho(h_0)(z + \sqrt{d}\ 0, x + \sqrt{d}y) = \eta h_0(z, y)$ for all $z \in V_0$. Since h_0 is non-degenerate, we have $y = 0$. Hence $W = W^{\perp}$ and $\pi_2\rho(h_0)$ is hyperbolic. □

Theorem 3.2 Let K/k, A_0, A, σ, τ, ρ and π_2 as above. Let (V, h) be an anisotropic ε-hermitian space over (A, σ). Suppose that $\pi_2(h) = h' \perp \mathbf{h}$ for some hyperbolic space $\mathbf{h}$. Then there exist an ε-hermitian space h_1 over (A, σ) and an ε-hermitian space h_2 over (A_0, τ) such that

$$h = h_1 \perp \rho(h_2) \quad \text{and} \quad \pi_2(h_1) = h'.$$

Proof. We prove this by induction on dim$\mathbf{h}$. If the dim$(\mathbf{h}) = 0$, i.e. there is no $\mathbf{h}$, then we take $h_1 = h$ and we are done. Assume that dim$(\mathbf{h}) = m \geq 1$. In particular $\pi_2(h)$ is isotropic. Then there exists $z \in V$, $z \neq 0$, such that $\pi_2(h)(z, z) = 0$. Let $V_0 = zA_0$ be the A_0-submodule of V generated by z. Since $\pi_2(h(z, z)) = 0$, we have $h(z, z) \in A_0$. Let $a, b \in A_0$. Then $h(za, zb) = \sigma(a)h(z, z) = \tau(a)h(z, z)b \in A_0$. Thus the restriction of h to V_0 induces an ε-hermitian form (V_0, h_0). Since h is anisotropic, the form (V_0, h_0) is anisotropic and hence non-degenerate. Since V is an A-module, we have $V_0 \oplus V_0\sqrt{d} \subset V$ and $\rho(h_0)$ is the restriction of h to $V_0 \oplus V_0\sqrt{d}$. Once again using the fact that h is isotropic we have $h = h'_1 \perp \rho(h_0)$. Since $\pi_2(\rho(h_0))$ is hyperbolic (by 3.1), by the Witt's cancellation, we have $\pi_2(h'_1) = h' \perp \mathbf{h}'$ for some hyperbolic space $\mathbf{h}'$. Since dim(h_1) <dim(h), we have dim$(\mathbf{h}')$ <dim$(\mathbf{h}$. Hence by induction, we have $h'_1 = h_1 \perp \rho(h'_2)$ with $\pi_2(h_1) = h'$. We have

$$h = h'_1 + \rho(h_0) = h_1 + \rho(h'_2) + \rho(h_0).$$

Let $h_2 = h'_2 + h_0$. Then h_1 and h_2 have the required properties. □

Corollary 3.3 Let K/k, A_0, A, σ, τ as above. With the notation as above we have the following exact sequence:

$$W^{\varepsilon}(A_0,\tau) \xrightarrow{\rho} W^{\varepsilon}(A,\sigma) \xrightarrow{\pi_2} W^{-\varepsilon}(A_0,\tau).$$

Proof: Follows from (3.1) and (3.2). □

Theorem 3.4 Let k be a field of characteristic not equal to 2 and $K = k(\sqrt{d})$ a quadratic extension of k. Let A_0 be a central simple algebra over k with an involution τ. Let $A = A_0 \otimes_k K$ and $\sigma = \tau \otimes \theta$, where θ is an automorphism of K. Let $\eta \in \{\pm 1\}$ be such that $\theta(\sqrt{d}) = \eta(\sqrt{d})$. Then we have

$$u(A,\sigma,\varepsilon) \leq \tfrac{1}{2}u(A_0,\tau,\eta\varepsilon) + u(A_0,\tau,\varepsilon).$$

Proof: If $u(A_0,\tau,\epsilon)$ is not finite, then there is nothing to prove. Assume that $u(A_0,\tau,\epsilon)$ is finite.

Let h be an anisotropic ε-hermitian form over (A,σ). Suppose that the dimension of $h \geq \frac{1}{2}u(A_0,\tau,\eta\varepsilon)+u(A_0,\tau,\varepsilon)+1$. We know that $\dim\pi_2(h) = 2\dim(h)$. Thus $\dim\pi_2(h) \geq u(A_0,\tau,\eta\varepsilon) + 2u(A_0,\tau,\varepsilon) + 2$. Since any $\eta\varepsilon$-hermitian space of dimension bigger that $u(A_0,\tau,\eta\varepsilon)$ is isotropic, we have $\pi_2(h) = h' + \mathbf{h}$ with $\dim h' \leq u(A_0,\tau,\eta\varepsilon)$. In particular, then $\dim(\mathbf{h}) \geq 2u(A_0,\tau,\varepsilon) + 2$. By (3.2), there exist an ε-hermitian space h_1 over (A,σ) and an ε-hermitian space h_2 over (A_0,τ) such that

$$h = h_1 \perp \rho(h_2) \quad \text{and} \quad \pi_2(h_1) = h'.$$

Since $\dim(\rho(h_2))$ $=\dim(h_2)$, we have $\dim h_2 \geq u(A_0,\tau,\varepsilon) + 1$. Hence h_2 is isotropic. Therefore $\rho(h_2)$, in particular h, is isotropic. Which is a contradiction. Hence $\dim(h) \leq \frac{1}{2}u(A_0,\tau,\eta\varepsilon) + u(A_0,\tau,\varepsilon)$. This proves the theorem. □

Theorem 3.5 Let k be a field of characteristic not equal to 2 and $K = k(\sqrt{d})$ a quadratic extension of k. Let A_0 be a central simple algebra over k with an involution τ. Let $A = A_0 \otimes_k K$ and $\sigma = \tau \otimes id$, where is is the identity map of K. Then

$$u(A, \sigma, \varepsilon) \leq \frac{3}{2} u(A_0, \tau, \varepsilon).$$

Proof. By (3.4), we have $u(A, \sigma, \varepsilon) \leq \frac{1}{2} u(A_0, \tau, \eta\varepsilon) + u(A_0, \tau + \varepsilon)$. Since $\sigma = \tau \otimes id$, we have $\eta = 1$. Therefore $u(A, \sigma, \varepsilon) \leq \frac{3}{2} u(A_0, \tau, \varepsilon)$. □

Theorem 3.6 Let k be a field of characteristic not equal to 2 and K/k a quadratic extension. Let A_0 be a central simple algebra over k with an involution τ. Let $A = A_0 \otimes_k K$ and $\sigma = \tau \otimes -$, where $-$ is the non-trivial automorphism of K/k. Then

$$u(A, \sigma, \varepsilon) \leq \text{minimum}\{u(A_0, \tau, \varepsilon) + \tfrac{1}{2} u(A_0, \tau, -\varepsilon), u(A_0, \tau, -\varepsilon) + \tfrac{1}{2} u(A_0, \tau, \varepsilon)\}.$$

Proof: By (3.4), we have $u(A, \sigma, \varepsilon) \leq \frac{1}{2} u(A_0, \tau, \eta\varepsilon) + u(A_0, \tau + \varepsilon)$. Since $\sigma = \tau \otimes -$, we have $\eta = -1$. Therefore $u(A, \sigma, \varepsilon) \leq \frac{1}{2} u(A_0, \tau, -\varepsilon) + u(A_0, \tau + \varepsilon)$. Since, σ is an involution of second kind we have, $u(A, \sigma, \varepsilon) = u(A, \sigma, -\varepsilon)$ (see chapter 1). Thus $u(A, \sigma, \varepsilon) \leq minimum\{u(A_0, \tau, \varepsilon) + \frac{1}{2} u(A_0, \tau, -\varepsilon), u(A_0, \tau, -\varepsilon) + \frac{1}{2} u(A_0, \tau, \varepsilon)\}$. □

Corollary 3.7 Let k be a field of characteristic not equal to 2 and K/k a quadratic extension. Let H be a quaternion algebra over K with an involution σ of second kind. Then $u(H, \sigma, \varepsilon) \leq \frac{7}{8} u(k)$.

Proof: Let H be a quaternion algebra over K with an involution σ of second kind. By a theorem of Albert (see [10]), there exists a quaternion subalgebra H_0 over k such that $H = H_0 \otimes_k K$ and $\sigma = \tau \otimes -$, τ is the canonical involution on H_0 and $-$ the non-trivial automorphism of K/k. By (3.6), we have $u(H, \sigma, \varepsilon) \leq u(H_0, \tau, 1) + \frac{1}{2}u(H_0, \tau, -1)$. By (1.9), we have $u(H_0, \tau, 1) \leq \frac{1}{4}u(k)$ and $u(H_0, \tau, -1) \leq \frac{5}{4}u(k)$. Hence $u(H, \sigma, \varepsilon) \leq \frac{1}{4}u(k) + \frac{1}{2} \times \frac{5}{4}u(k) = \frac{7}{8}u(k)$. □

Corollary 3.8 Let k be a field of characteristic not equal to 2. Let H_1 and H_2 be two quaternion algebras over k and τ the involution given by the tensor product of canonical involutions on H_1 and H_2. Then $u(H_1 \otimes H_2, \tau, 1) \leq \frac{29}{16}u(k)$.

Proof: Since H_2 is a quaternion algebra, there exist λ and μ as in the paragraph before (1.5.1). Thus by (1.5.3), we have $u(H_1 \otimes H_2, \tau, 1) \leq \frac{1}{2}u(H_1 \otimes k(\lambda), \tau_2, -1) + u(H_1 \otimes k(\lambda), \tau_1, 1)$. Since τ_1 is an involution of second kind, by (3.7), we have $u(H_1 \otimes k(\lambda), \tau_1, \varepsilon) \leq \frac{7}{8}u(k)$. Since τ_2 is an involution of first kind, by (3.5), we have $u(H_1 \otimes k(\lambda), \tau_2, -1) \leq \frac{3}{2}u(H_1, \bar{\ }, -1)$. By (1.5.4), we have $u(H_1, \bar{\ }, -1) \leq \frac{5}{4}$. Hence $u(H_1 \otimes k(\lambda)) \leq \frac{15}{4}$. Therefore, we have

$$u(H_1 \otimes H_2, \tau, 1) \leq \frac{1}{2} \times \frac{15}{8}u(k) + \frac{7}{8}u(k) = \frac{29}{16}u(k).$$

□

Corollary 3.9 Let k be a field of characteristic not equal to 2. Let H_1 and H_2 be two quaternion algebras over k and τ the involution given by the tensor product of canonical involutions on H_1 and H_2. Then $u(H_1 \otimes H_2, \tau, -1) \leq \frac{17}{16}u(k)$.

Proof: As in the proof of (3.8), we have

$$\begin{array}{rcl} u(H_1 \otimes H_2, \tau, -1) & \leq & \frac{1}{2}u(H_1 \otimes k(\lambda), \tau_2, 1) + u(H_1 \otimes k(\lambda), \tau_1, 1) \\ & \leq & \frac{1}{2} \times \frac{1}{4}u(k(\lambda)) + \frac{7}{8}u(k) \\ & \leq & \frac{1}{8} \times \frac{3}{2}u(k) + \frac{7}{8}u(k) \\ & = & \frac{17}{16}u(k). \end{array}$$

□

Corollary 3.10 Let k be a field of characteristic not equal to 2. Let A be a central simple k-algebra of degree 4 with an orthogonal involution τ. Then $u(A, \tau, +1) \leq \frac{29}{16}u(k)$ and $u(A, \tau, -1) \leq \frac{17}{16}u(k)$.

Proof. Since A is a central simple k-algebra of degree 4 with an involution of first kind, we have $A \simeq H_1 \otimes H_2$. Let σ be the tensor product of the canonical involutions on H_1 and H_2. Then σ is an orthogonal involution on $H_1 \otimes H_2$ (cf. [7], 8.1.3). Hence we have $u(A, \tau, \varepsilon) = u(A, \sigma, \varepsilon)$ (cf. §1.5). The corollary follows from (3.8) and (3.9).

Remark 3.11 . Let H be a quaternion algebra over K and σ an involution of second kind with fixed field k. Then by ([8]), we have $u(H, \sigma, \epsilon) \leq \frac{5}{4}u(k)$. Let A be a central simple k-algebra of degree 4, with an orthogonal involution τ. Then, by ([8]), we have $u(A, \tau, 1) \leq \frac{55}{16}u(k)$ and $u(A, \tau, -1) \leq \frac{21}{16}u(k)$. Hence our bounds are sharper.

References

[1] A. Adrian Albert. *Structure of algebras*. Revised printing. American Mathematical Society Colloquium Publications, Vol. XXIV. American Mathematical Society, Providence, R.I., 1961.

[2] Reinhold Baer. *Linear algebra and projective geometry*. Academic Press Inc., New York, N. Y., 1952.

[3] E. Bayer-Fluckiger and R. Parimala. Galois cohomology of the classical groups over fields of cohomological dimension ≤ 2. *Invent. Math.*, 122(2):195–229, 1995.

[4] P. K. Draxl. *Skew fields*, volume 81 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[5] D. K. Faddeev. Simple algebras over a field of algebraic functions of one variable. *Amer. Math. Soc. Transl. (2)*, 3:15–38, 1956.

[6] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[7] Max-Albert Knus. *Quadratic and Hermitian forms over rings*, volume 294 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles*

of Mathematical Sciences]. Springer-Verlag, Berlin, 1991. With a foreword by I. Bertuccioni.

[8] M. G. Mahmoudi. Hermitian forms and the u-invariant. *Manuscripta Math.*, 116(4):493–516, 2005.

[9] L. H. Rowen, A. S. Sivatski, and J.-P. Tignol. Division algebras over rational function fields in one variable. In *Algebra and number theory*, pages 158–180. Hindustan Book Agency, Delhi, 2005.

[10] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1985.