The Cyclicity Question

Diksha Mukhija

A dissertation submitted for the partial fulfilment of BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali
2018

Certificate of Examination

This is to certify that the dissertation titled The Cyclicity Question submitted by Ms. Diksha Mukhija (Reg. No. MS13103) for the partial fulfilment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Tanusree Khandai

Dr. Varadharaj R. Srinivasan

Dr. Amit Kulshrestha
(Supervisor)

Dated: April 20, 2018

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Amit Kulshrestha at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of work done by me and all sources listed within have been detailed in the bibliography.

Diksha Mukhija
(Candidate)

Dated: April 20, 2018

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Amit Kulshrestha
(Supervisor)

ACKNOWLEDGEMENT

Firstly, I would like to thank my supervisor Dr. Amit Kulshrestha for his support and guidance throughout these five years I have known him. He has always motivated me to challenge myself and thrive beyond my comfort zone. His inputs on the presentation and on conceptual framework of my work have been immensely insightful and helpful. I am especially indebted to Dr. Abhay Soman for he has been an immense source of knowledge and guidance throughout the past year. While he has been a great mentor academically, he has been a greater friend non academically. His companionship through all my silliness and food cravings is something I will cherish for my life.

I would now like to express my gratitude to Kanika Singla who always spared time for me, from helping me prepare my presentation to proofreading my thesis. A special thanks to Yashpreet Kaur and Dr. Sushil Bhunia whose company made me sail through the hard times cheerfully.

I would also like to thank Dr. Varadharaj R. Srinivasan and Dr. Tanusree Khandai for reviewing my thesis and Dr. Aribam Chandrakant, for his happy to help smile and his immense confidence in me.

The list cannot end without mentioning the people who bear me on a daily basis. My parents who always like to see me stuffing food and sleeping peacefully at home. My brother, Nikhil Mukhija, for just being what he is, idiotic, loving, caring and full of enthusiasm, constantly bothering me with his extremely curious attitude. My friends Rimpy and Pragya for always being there and teasing me from the past five years and hopefully will be continuing to do so in coming five years as well. The best senior possible one can ask for, Lata di, who is there at any hour of the day. I feel blessed to know someone who is too good to be real.

And the biggest thank you to all those I forgot to mention, I am going to do that personally.

Dated: April 2018 **Diksha Mukhija**

Contents

Chapter 0

Introduction

In this thesis we study division algebras over fields. The main aim of the thesis is to investigate conditions under which a given division algebra is cyclic. This is called cyclicity problem. Division algebras and cyclic algebras are examples of, what are called, central simple algebras. The algebra of matrices of a given size over a field is an example of central simple algebra. By definition, associative algebras A over a field F with centre $Z(A) = F$ and having no proper non-trivial two sides ideal are *central simple algebras*. By a theorem of Wedderburn, central simple algebras are precisely the matrix algebras over division algebras.

The theory of central simple algberas has deep connections with number theory, K-theory and geometry. We will be mainly interested in studying cyclic algebras. For instance, the Hamiltonian algebra is an example of a cyclic algebra. More generally, quaternion algebras over a field are cyclic algebras. The structure of a cyclic algebra is easier to study and has an explicit connection to second Galois cohomology group. The 2-cocycle associated to a cyclic algebra has a very simple form. This is also helpful in deciding, when a cyclic algebra is isomorphic to a matrix algebra over a field.

We will see that division algebras of degree two and three are cyclic. As a consequence of primary decomposition theorem, degree six division algebras are also cyclic. So, one may ask following question.

Cyclicity Question *Is every division algebra over a field cyclic?*

The cyclicity question in its naive form has a negative answer. As we will see an explicit example of degree four noncyclic division algebra over a formally real pythagorean field. Infact, there also exists cyclic algebras which are not division.

The existence of a noncyclic division algebra confirms an intimate relationship between underlying field and the structure of a division algebra. Thus, the cyclicity of division algebras could also be questioned in the context of the base field. In many cases after putting conditions on the field, all division algebra become cyclic. For instance, any division algebra over a global field, i.e., a finite extension of rational numbers or a global function fields, is always cyclic. This was proved by Hasse, Brauer, Noether and Albert (§18.4 [Pie82]).

All the results and questions about cyclic algebras and cyclicity of division algebras are discussed elaborately in chapter four. First three chapters provide the mathematical background, which helps in understanding the problem and progress made so far.

We now give some important conditions under which a given central division algebra is cyclic.

- Let D be division algebra over a field F. Then D is cyclic if and only if there exists a cyclic splitting subfield of degree $\deg(D)$.
- Let D be a division algebra over F of prime degree p. Then D is cyclic if and only if there is a p-power central element.

In the first chapter, we define all our central tools of study, central simple algebras, division algebras and some theorems related to them. We also study in detail about quaternion algebras since they are centric to both, degree two cyclic and division algebras. Biquaternion algebras play an important role in our study since they help us construct a noncyclic division algebras.

Second chapter discusses the cohomological tools that are helpful to study many objects of interest. The abelian cohomology plays an important role in the study of crossed product algebra. The crossed product algebras and two cocycles are in one to one correspondence. Cyclic algebras are special type of crossed product algebras where the Galois group is cyclic. We also talk about one cocycles since they help defining twisted action useful in the construction of cyclic algebras.

Study of division algebras is incomplete without talking about the Brauer group. Third chapter defines and explains the Brauer group and its associated properties. Brauer group classifies the isomorphic division algebras.

In the final chapter, we define and give examples of cyclic alegbras. Some results are being discussed which give us condition, when a central simple algebra is cyclic. We finally talk about the cyclicity question and mention the progress on the results and the open questions.

Chapter 1

Central Simple Algebras

In this chapter we'll define the algebras we'll be dealing with throughout the upcoming chapters. We will also see some important results associated to them which will build our foundation for further study.

An algebra A is called simple if A has no nontrivial two sided ideals.

Definition 1.0.1 (Central simple algebra)**.** *An Algebra A is said to be a central simple algebra over F if and only if center of A is F and there are no nontrivial two sided ideals of A and A is finite dimensional as a vector space over F.*

We'll denote the center of an algebra A by $\mathbf{Z}(A)$. A trivial example of central simple algebra is the matrix algebra $M_n(F)$. Another class of examples is division algebra. We'll define them in the coming section.

1.1 Division algebras

Definition 1.1.1 (Division algebra)**.** *A Division Algebra is a non-commutative finite dimensional associative algebra over some field where every non zero element has a multiplicative inverse.*

Let A be a division algebra and I be a non-trivial ideal of A. Since A is a division algebra, so every non-zero element has an inverse, thus, $1 \in I$. Therefore, $I = A$. Since by definition A is non-commutative and it is a vector field over F, $\mathbf{Z}(A) = F$. Hence division algebras are central simple over F.

Example 1.1.2 (Hamilton's example)**.** The real algebra spanned by $1, i, j, k$ such that $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$. A general element of this algebra looks like $r_1 + r_2 i + r_3 j + r_4 k$ where $r_1, r_2, r_3, r_4 \in \mathbb{R}$. To show that it is a division algebra we need to find an inverse for every non zero element. We define a map $\phi : \mathbb{H} \to \mathbb{H}$ given by $\phi(r_1 + r_2 i + r_3 j + r_4 k) = r_1 - r_2 i - r_3 j - r_4 k$, known as *conjugation.* One can check that the map defined above is actually an automorphism. Now to see that $\mathbb{H}$

is a division algebra, $\alpha^{-1} = \phi(\alpha)/n(\alpha)$ is inverse of α where $n(\alpha) = r_1^2 + r_2^2 + r_3^2 + r_4^2$ and $\alpha = r_1 + r_2 i + r_3 j + r_4 k$.

One must observe that the quaternion algebra defined above is a non-commutative associative algebra. And we can embed $\mathbb{H}$ into the algebra $M_2(\mathbb{C})$ using the relations:

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

If we define the Hamilton's algebra over any other field. it would result in a *central simple algebra.*

Another example of central simple algebras are *Cyclic algebras.* They are central object of study here and we will study about them in greater detail in chapter 4.

Definition 1.1.3 (Cyclic Algebras)**.** *Let L/F be a cyclic Galois extension of fields with Galois group generated by σ. Choose $0 \neq b \in F^*$ and $n = degree(L/F)$, we define an algebra $A = \triangle(L, \sigma, b)$ as follows:*

$$A = \oplus_{i=0}^{n-1} L u^i$$

*where $u^n = b$ and the product structure is given by $ux = \sigma(x)u \ \forall x \in L$.Such an algebra $A = \triangle(L, \sigma, b)$ is called a **Cyclic algebra**.*

$\mathbb{H}$ is the cyclic algebra $\triangle(\mathbb{C}/\mathbb{R}, \sigma, -1)$, where σ is complex conjugation. It is both a divison as well as a cyclic algebra.

We'll see some results about Divison algebras now which will be useful in the coming chapters.

Lemma 1.1.4. *If D/F is a division algebra and F is algebraically closed then $D = F$.*

Proof. Suppose $\alpha \in D \setminus F$. Since D is finite dimensional, the ring $F[\alpha] \subset D$ is finite dimensional. $F[\alpha]$ is a domain because D is, So $F[\alpha] = F(\alpha)$ is a finite dimensional field over F, thus $F = F[\alpha]$ which is a contradiction. □

Theorem 1.1.5 (Wedderburn's little theorem)**.** *Every finite domain is a field.*

Proof. Let A be a finite domain. For each non-zero x in A, consider the two maps:

$$a \mapsto ax, \qquad a \mapsto xa$$

from $A \to A$, both are injective(by cancellation property) and Since A is finite, both are surjective as well. Thus using the two maps we can conclude A forms a group under multiplication. Now we need to show A forms a commutative group under multiplication. We will use induction on size of A to prove this. Since A is a division ring, we'll assume that all division rings that are a proper subset of A are fields. Since the center of A is a field, say $\mathbf{Z}(A)$, we can assume A to be a vector space over $\mathbf{Z}(A)$ of dimension n. Aim is to show $n = 1$. Let $|\mathbf{Z}(A)| = q$, then A has the order q^n. Now for $x \in A$ but $x \notin \mathbf{Z}(A)$, consider the centralizer of x in A, $\mathbf{Z}_x$ and as $\mathbf{Z}(A) \subset \mathbf{Z}_x \subset A$. We have $\mathbf{Z}_x$ a field by induction since $|\mathbf{Z}_x| = q^d$ where $d|n$ and $d < n$. Now consider $\mathbf{Z}(A)^*$, $\mathbf{Z}_x^*$, A^* as groups, and we can write the class equation as:

$$q^n - 1 = (q-1) + \sum \frac{q^n - 1}{q^d - 1}$$

where sum is taken over all the conjugacy classes not contained in $\mathbf{Z}(A)_*$. Now

$$x^n - 1 = \prod_{m|n} \phi_m(x) \quad and \quad x^d - 1 = \prod_{m|d} \phi_m(x)$$

for $x = q$, as $d|n$ but $d \neq n$. $\phi_n(q)$ divides both $q^n - 1$ and each $\frac{q^n-1}{q^d-1}$. So $\phi_n(q)$ must divide $q-1$. So $|\phi_n(q)| \leq q-1$. Now for $n > 1$, $\phi_n(x) = \prod(x-\zeta)$ where ζ is primitive nth root of unity. Now take $n = q$ and take absolute values. We get

$$|\phi_n(q)| = \prod |q - \zeta|$$

and we know $|q - \zeta| > |q - 1|$, Thus, we get $|\phi_n(a)| > q - 1$. So, $n = 1$. □

Theorem 1.1.6 (Frobenius theorem)**.** *It states that every finite dimensional associative division algebra over the real numbers is ismorphic to one of the following:*

- $\mathbb{R}$.
- $\mathbb{C}$.
- $\mathbb{H}$.

Proof. Let D be the division algebra over $\mathbb{R}$(associative and finite dimensional). D can be considered as finite dimensional vector space over $\mathbb{R}$ and so $d \in D$ defines and endomorphism of D by left multiplication and we can identify d with that endomorphism(so it makes sense to talk about its trace and characterstic polynomial). For $z \in \mathbb{C}$ define $Q(z : x) = x^2 - 2(Re(z))x + |z^2| = (x - z)(x - \bar{z}) \in \mathbb{R}[x]$, for $x \in \mathbb{C} \setminus \mathbb{R}$, $Q(z : x)$ is irreducible over $\mathbb{R}$. Let $V = \{a \in D \text{ such that } a^2 \leq 0\}$.

Claim: V is a vector subspace of D of co-dimension 1. Moreover, $D = \mathbb{R} \oplus V$ as $\mathbb{R}$ vector spaces.

Proof of claim: Let m be the dimension of D as an $\mathbb{R}$-vector space and pick $a \in D$ with characteristic polynomial $p(x)$. By the fundamental theorem of algebra, we can write

$$p(x) = (x-t_1)(x-t_2)\dots(x-t_r)(x-z_1)(x-\bar{z}_1)\dots(x-z_s)(x-\bar{z}_s) \quad t_i \in R, \;\; z_j \in \mathbb{C}/\mathbb{R}.$$

$$so, \qquad p(x) = (x - t_1)(x - t_2) \dots (x - t_r)Q(z_1 : x) \dots Q(z_s : x)$$

By Cayley-Hamilton theorem $p(a) = 0 \Rightarrow$ either $a - t_i = 0$ for some t_i or $Q(z_j : a) = 0$ for some j. The first case implies a is real(but $a^2 \leq 0 \Rightarrow a = 0$). So this case does not give us any information. From the second case, we get $Q(z_j : x)$ is minimal polynomial for a and characteristic polynomial and minimal polynomial have same roots, therefore, $p(x) = Q(z_j, x)^k = (x^2 - 2(Re(z))x + |z^2|)^k$. Now $tr(a)$ is the coefficient of the term x^{2k-1} upto sign and so $tr(a) = 0$ if and only if $2Re(z) = 0$ and so $Re(z) = 0 \Rightarrow a^2 = -|z_j|^2 \leq 0$. So V is the subset of all a with $tr(a)$. In particular, it is a vector subspace of co-dimension 1 and $D = \mathbb{R} \oplus V$, as a vector space. Hence, the claim is proved. Now for the last step let $a, b \in V$, define $B(a, b) = (-ab - ba)/2$ and we know that $(a+b)(a+b) = a^2 + b^2 + ab + ba \Rightarrow ab + ba = (a+b)^2 - a^2 - b^2$. This implies that $B(a, b) = 0$ is real and further $B(a, a) = -a^2 > 0$(because $a^2 < 0$ for $a \neq 0$). Thus, B is a positive definite bilinear form, in other words, an inner product on V. Suppose $W \subset V$ generates D as an algebra and is minimal with respect to this property. Let $e_1, e_2, \dots, e_n$ be an orthonormal basis of W with respect to the negative definite bilinear form $-B$, these elements satisfy $e_i^2 = -1$, $e_i e_j = -e_j e_i$ (because $B(e_i, e_i) = 1$ and $B(e_i, e_j) = 0$)

- If $n = 0$, then D is isomorphic to $\mathbb{R}$.

- If $n = 1$, then D is generated by 1 and e_1 subject to the relation $e_1^2 = -1$, so it isomorphic to $\mathbb{C}$.

- If $n = 2$, then D will be generated by $1, e_1, e_2$ subject to the relations $e_1^2 = e_2^2 = -1$ and $e_1 e_2 = -e_2 e_1$ and $(e_1 e_2)(e_2 e_1) = 1$. These are precisely the relations for $\mathbb{H}$(Hamiltonian quaternions). So then it will be isomorphic to $\mathbb{H}$.

- If $n > 2$ then D can not be a division algebra (for that assume $n > 2$, Let $u = e_1 e_2 e_u$, so $u^2 = e_1 e_2 e_u e_1 e_2 e_u = e_2 e_1 e_1 e_u e_2 e_u = e_2 e_u e_u e_2 = 1$ So if D is a division algebra, then $0 = u^2 - 1 = (u-1)(u+1) \Rightarrow u = \pm 1 \Rightarrow e_1 e_2 = \pm e_u$, so $e_1, e_2, \dots, e_{u-1}$ generates D, which is contradiction to the minimality of W. So D is not a division algebra).

□

1.2 Some results on central simple algebras

In this section we will discuss some essential theorems about central simple algebras. Main theorem discussed here is the Wedderburn's structure theorem for a simple algebra. In general theorem is given for semisimple algebras.

Theorem 1.2.1 (Wedderburn's Structure Theorem §3.5, [Pie82])**.** *Any central simple algebra A/F has the form $M_r(D)$ where D/F is a division algebra and $M_r(D)$ is the algebra of $r \times r$ matrices over D. Conversely, any algebra of the form $M_r(D)$ for a division algebra D/F is a central simple algebra over (i.e., with center F). Furthermore, if A is central simple then any A module is the direct sum of copies of a unique (up to isomorphism) irreducible module.*

As a consequence of this theorem and lemma 1.1.4:

Corollary 1.2.2. *If A/F is a central simple algebra, and F is an algebraically closed field then $A \simeq M_n(F)$.*

Proof. Since the only division algebra over an algebrically closed field is itself. Thus, by Wedderburn's structure theorem A is isomorphic to a matrix algebra over F. □

Now that we already know the structure of a central simple algebra in terms of a division algebra. Using their structure we further define an operation on the class of all central simple algebras over a given field.

Lemma 1.2.3. *Let A be a central simple algebra over F and B be a simple F-algebra. Then $A \otimes_F B$ is also a simple F-algebra.*

Proof. We have $A \simeq M_r(D)$(using Wedderburn's structure theorem) where D is a division ring over F, and $\mathbf{Z}(D) = \mathbf{Z}(M_r(D)) = \mathbf{Z}(A) = F$. Since A is a finite dimensional over F, so from now onwards we assume A to be a division algebra and note every two sided ideal of $M_r(A \otimes_F B)$ comes from a two sided ideal of $A \otimes_F B$. Let $\mathcal{A} \neq 0$ be a two-sided ideal of $A \otimes_F B$ and $\{e_i\}_{i \in I}$ be a F-basis of B. We can express any $a \in \mathcal{A}, a \neq 0$, as $a = \sum_{i \in J} a_i \otimes e_i, J \subset I, a_i \in A$. We call $l(a) = |J|$ and choose $a \in \mathcal{A}$ with $l(a)$ minimal. We can assume $a_{j_0} = 1$ by replacing a by $(a_{j_0}^{-1} \otimes 1)a$, for some $j_0 \in J$. For any $d \in A, a' = (d \otimes 1)a - a(d \otimes 1) = \sum (da_i - a_i d) \otimes e_i \in \mathcal{A}$ and $l(a') \subset l(a)$, a_{j_0} being 1. Since $l(a)$ is minimal, $a' = 0$ implies $da_i = a_i d$ for all $i \in J$, so we get $a_i \in F$ for all $i \in J$ Thus $a \in \mathcal{A} \cap 1 \otimes B$. Since B is simple, $\mathcal{A} \cap (1 \otimes B) = 1 \otimes B \Rightarrow 1 \otimes 1 \in \mathcal{A} \Rightarrow \mathcal{A} = A \otimes_F B$. □

Lemma 1.2.4. *Let A and B be F-algebras, then $\mathbf{Z}(A \otimes_F B) = \mathbf{Z}(A) \otimes_F \mathbf{Z}(B)$.*

Proof. Note that $\mathbf{Z}(A) \otimes_F \mathbf{Z}(B) \subset \mathbf{Z}(A \otimes_F B)$. Let $x \in \mathbf{Z}(A \otimes_F B)$, and express $x = \sum_i e_i \otimes b_i$, where $\{e_i\}_{i \in I}$ is a basis of A over F. By linear independence of $\{e_i\}$, the condition $(1 \otimes b)x = x(1 \otimes b)$ for all $b \in B$ implies that $bb_i = b_i b$ for all $b \in B$. Thus $\mathbf{Z}(A \otimes_F B) \subset A \otimes_F \mathbf{Z}(B)$. Similarly we have $\mathbf{Z}(A \otimes_F B) \subset \mathbf{Z}(A) \otimes_F B$. So that $\mathbf{Z}(A \otimes_F B) \subset A \otimes_F \mathbf{Z}(B) \cap \mathbf{Z}(A) \otimes_F B \subset \mathbf{Z}(A) \otimes_F \mathbf{Z}(B)$. □

As a consequence of lemma 1.2.3 and 1.2.4 we have the following theorem.

Theorem 1.2.5. *If A and B are central simple algebras over F then $A \otimes_F B$ is also a central simple algebra over F.*

Definition 1.2.6. *A is said to be a **form** or **descent** over F for the Matrix Algebra $M_n(F)$ if there exists a field extension L over F such that $L \otimes_F A \xrightarrow{\sim} M_n(L)$.*

Since $M_n(F) \otimes_F F \simeq M_n(F)$, the algebra $M_n(F)$ is a form over F. With the help of the following proposition, we will show that the dimension of a central simple algebra A/F is always of the form n^2. Consequently, using Wedderburn's structure theorem, dimension of a division algebra is also of the form n^2.

Proposition 1.2.7. *The following two statements are equivalent:*

1. *A is a central simple algebra over F.*

2. *A is a form over F for the matrix algebra.*

Proof. ($2 \Rightarrow 1$) Let A be a form over F for the matrix algebra and let L be a field extension of F such that $L \otimes_n \xrightarrow{\sim} M_n(L)$. Then $[A : F] = [M_n(L) : L] = n^2$. By proof of 1.2.5,

$$\mathbb{Z}(L \otimes_F A) = L \otimes_F \mathbb{Z}(A) = \mathbb{Z}(M_n(L)) = L.$$

Thus $[\mathbb{Z}(A) : F] = [L \otimes_F \mathbb{Z}(A) : L] = 1$ and $\mathbb{Z}(A) = F$. If $\mathcal{A} \neq 0$ is a two-sided ideal of A, then $L \otimes_F \mathcal{A} \neq 0$ is a two-sided ideal of $L \otimes_F A \xrightarrow{\sim} M_n(L)$. Since $M_n(L)$ is simple, we get $L \otimes_F \mathcal{A} = L \otimes_F A$; hence $\mathcal{A} = A$.
($1 \Rightarrow 2$) A is a central simple algebra over F and Let $\overline{F}$ denote the algebraic closure of F. Again, using the proof of Theorem 1.4, $\overline{F} \otimes_F A$ is central simple over $\overline{F}$. Since the only finite dimensional divison algebras over an algebraically closed field is itself, it follows, by *Wedderburn's theorem*, that $\overline{F} \otimes_F A \xrightarrow{\sim} M_n(\overline{F})$. □

$\overline{F} \otimes_F A \xrightarrow{\sim} M_n(\overline{F})$, Thus, $[A : F] = [M_n(\overline{F}) : \overline{F}] = n^2$. It follows from the proof:

Corollary 1.2.8. *The dimension of a central simple algebra A/F (over F) is always of the form n^2.*

Definition 1.2.9. *An extension L/F of fields is called a **splitting field** for A if $L \otimes_F A \xrightarrow{\sim} M_n(L)$.*

So we now know that for every central simple algebra there exists a splitting field, infact, a finite dimensional splitting field exists for every central simple algebra.

Proposition 1.2.10. *Every cenral simple algebra A over F admits a splitting field L which is a finite extension of F.*

Proof. Let $\overline{F}$ denote the algebraic closure of F and $\phi : \overline{F} \otimes_F A \xrightarrow{\sim} M_n(\overline{F})$ be an isomorphism of $\overline{F}$-algebras. If $\{e_i\}$, $1 \leq i \leq n^2$ is a F-basis of A and $\phi(1 \otimes e_i) = \sum_{j,k} \lambda_{ijk} e_{jk}$, $1 \leq j,k \leq n, e_{jk}$ denoting the standard basis of $M_n(\overline{F})$, we set $L = F(\lambda_{ijk})$, $1 \leq i \leq n^2, 1 \leq j,k \leq n$. Then ϕ induces an L-algebra homomorphism $\widetilde{\phi} : L \otimes_F A \to M_n(L)$. Since $L \otimes_F A$ is simple, $\widetilde{\phi}$ is injective. Since $n^2 = [A : F] = [M_n(L) : L]$, thus $\widetilde{\phi}$ is an isomorphism. □

1.3 Quaternion Algebra

We have already defined Hamilton's quaternions in Example 1.1.2, we will generalise them in this section. Unless stated we will assume F to be a field of characterstic not 2. We have referred to [GS06] for this section.

Definition 1.3.1. *Consider a field F and a cyclic Galois extension $L = F(\sqrt{a})$ of degree 2 with Galois group $G = \{1, \sigma\}$. Let $b \in F^*$, then the cyclic algebra over F is $A = L \oplus L\eta$ with $\eta^2 = b$ and $\eta x = \sigma(x)\eta$. Algebra A is a cyclic algebra denoted by $\left(\frac{a,b}{F}\right)$ and is called Quaternion algebra over F.*

Simplifying the above definition, $\left(\frac{a,b}{F}\right)$ is the 4-dimensional F-algebra with basis $1, i, j, ij$, multiplication determined by

$$i^2 = a, j^2 = b, ij = -ji.$$

We call the set $\{1, i, j, ij\}$ a quaternion basis of $\left(\frac{a,b}{F}\right)$. We call an element q of $\left(\frac{a,b}{F}\right)$ a *pure quaternion* if $q^2 \in F$ but $q \notin F$, which yields q is of the form $yi + zj + wij$.

Remark 1.3.2. The isomorphism class of the algebra $\left(\frac{a,b}{F}\right)$ depends only on the classes of a and b in F^*/F^{*2}, because we can substitute $i \mapsto ui$, $j \mapsto vj$ and induce an isomorphism

$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{u^2a, v^2b}{F}\right)$$

for all $u, v \in F^*$.

Using this remark we can note that any algebra $\left(\frac{a,b}{F}\right)$ is isomorphic to $\left(\frac{b,a}{F}\right)$ via the mapping $i \mapsto abj$, $j \mapsto abi$.

$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{a^2b^3, a^3b^2}{F}\right) \simeq \left(\frac{b,a}{F}\right)$$

We can define the conjugation map in a generalised quaternion algebra in the same manner as in 1.1.2. We define the norm of an element $q = x + yi + zj + wij$ by $N(q) = q\bar{q}$, that is,

$$N(q) = x^2 - ay^2 - bz^2 + abw^2$$

Lemma 1.3.3. *An element q of the quaternion algebra $\left(\frac{a,b}{F}\right)$ is invertible if and only if it has non-zero norm. Hence $\left(\frac{a,b}{F}\right)$ is a division algebra if and only if the norm $N : \left(\frac{a,b}{F}\right) \to F$ does not vanish outside 0.*

Apart from Hamilton's quaternions we will give another basic example of quaternion algebra.

Example 1.3.4 (The matrix algebra $M_2(F)$)**.** We take the algebra $M_2(F)$ of 2×2 matrices and consider the assignment:

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}.$$

It defines an isomorphism from $\left(\frac{1,b}{F}\right) \to M_2(F)$. Since the matrices

$$Id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \text{ and } IJ = \begin{bmatrix} 0 & b \\ -1 & 0 \end{bmatrix}$$

and satisfy the quaternion relations, that is,

$$I^2 = Id, \quad J^2 = b.Id, \quad IJ = -JI.$$

Definition 1.3.5. *A quaternion algebra over F is called split if it is isomorphic to $M_2(F)$ as an F-algebra.*

From the above example we can observe that $\left(\frac{1,b}{F}\right)$ is split.

Proposition 1.3.6. *For a quaternion algebra $\left(\frac{a,b}{F}\right)$ the following conditions are equivalent:*

1. *The algebra $\left(\frac{a,b}{F}\right)$ is split.*
2. *The algebra $\left(\frac{a,b}{F}\right)$ is not a division algebra.*
3. *The norm map $N : \left(\frac{a,b}{F}\right) \to F$ has a non-trivial zero.*
4. *The element b is a norm from the field extension $F(\sqrt{a})|F$.*

Alternatively in (4)*, we can also say the element a is a norm from the field extension $F(\sqrt{b})|F$.*

Proof. (1) $\Rightarrow$ (2) is clear from the fact that there exists many elements in $M_2(F)$ which do not have an inverse. (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (2) are clear from lemma 1.3. Now we will prove (3) $\Rightarrow$ (4), If $a \in F^{*2}$, then the norm of the element $q = (\sqrt{a}, 1, 0, 0)$ is a non-trivial zero and a is a norm from the field extension $F(\sqrt{b})|F$. So we will prove this for the non-trivial case, that is, when $a \notin F^{*2}$. Let $q = x + yi + zj + wk$ be the element with zero norm. Therefore $x^2 - ay^2 - bz^2 + abw^2 = 0$, $(z^2 - aw^2)b = x^2 - ay^2$, and so in particular $z^2 - aw^2 = (z + \sqrt{a}w)(z - \sqrt{a}w) \neq 0$, else a would be a square in F. Thus, b is a norm from the field extension $F(\sqrt{a})|F$. We will now assume (4) and show that $\left(\frac{a,b}{F}\right) \cong \left(\frac{1,4a^2}{F}\right)$ so that the algebra $\left(\frac{a,b}{F}\right)$ splits. Again we assume that a is not a square in F. Let $K = F(\sqrt{a})$. If b is a norm from K, then so is b^{-1}, so by using (4) we have $b^{-1} = r^2 - as^2$ for some $r, s \in F$. Take $u = rj + sij$, we get $u^2 = br^2 - abs^2 = 1$. We then verify $ui = -iu$, which implies that the element $v = (1 + a)i + (1 - a)ui$ satisfies $uv = (1 + a)ui + (1 - a)i = -vu$ and $v^2 = (1 + a)^2 a - (1 - a)^2 a = 4a^2$. So now change the basis for $\left(\frac{a,b}{F}\right)$ to $\{1, u, v, uv\}$. We get the isomorphism $\left(\frac{a,b}{F}\right) \cong \left(\frac{1,4a^2}{F}\right)$. From example 1.3.4 we get that $\left(\frac{a,b}{F}\right)$ splits. □

From this proposition we get the condition that $\left(\frac{a,b}{F}\right)$ is a matrix algebra if and only if there exists $r, s \in F$ such that $b = r^2 - as^2$. All these results obtained for quaternion algebras over field of characteristic 2 are analogous to this proposition. We just give the definition here.

Definition 1.3.7. *Let F be a field of characteristic 2, we define the generalised quaternion algebra $\left[\frac{a,b}{F}\right)$ via the F-basis $\{1, i, j, ij\}$ satisfying the relations*

$$i^2 + i = a, \quad j^2 = b, \quad ij = ji + j$$

where $a \in F$ and $b \in F^*$.

We will just state the result analogous to the previous proposition for charactersistic not 2.

Proposition 1.3.8. *Let F be a field of characteristic not 2. The quaternion algebra over F generated by i, j with the relations $i^2 + i = a$, $j^2 = b$, $ij = ji + j$, $a, b \in F^*$, is a matrix algebra if and only if there exists $r, s \in F$ such that $b = r^2 + rs - as^2$.*

1.3.1 Tensor product of quaternion algebras

In this section we consider the tensor product of quaternion algebras. Simplest of these are biquaternion algebras. Let F be a field of characteristic not 2. *Biquaternion algebras* are F-algebras that are isomorphic to a tensor product of two quaternion algebras over F. We state some results here which will be used in the next chapter in context of the Brauer group.

Lemma 1.3.9. *The tensor product of two matrix algebras $M_n(F)$ and $M_m(F)$ over F is isomorphic to the matrix algebra $M_{mn}(F)$.*

Proof. We already know $M_n(F) \simeq End_F(F^n)$ and $M_m(F) \simeq End_F(F^m)$. So given any $\phi \in End_F(F^n)$ and $\psi \in End_F(F^m)$, we map the pair (ϕ, ψ) to $\phi \otimes \psi$ of $End_F(F^n \otimes_F F^m)$. We have $M_{mn}(F) \simeq End_F(F^n \otimes_F F^m)$, and the resulting map from $End_F(F^n) \otimes End_F(F^m) \to End_F(F^n \otimes_F F^m)$ is injective as well as surjective(due to dimension equality). Thus, we get the required isomorphism $M_n(F) \otimes M_m(F) \cong M_{mn}(F)$. □

Lemma 1.3.10. *Given the elements $a, b, b' in F^*$, we have an isomorphism*

$$\left(\frac{a,b}{F}\right) \otimes_F \left(\frac{a,b'}{F}\right) \xrightarrow{\sim} \left(\frac{a,bb'}{F}\right) \otimes_F M_2(F).$$

Proof. Consider the standard F-basis $(1, i, j, ij)$ and $(1, i', j', i'j')$ for the quaternion algebras $Q_1 = \left(\frac{a,b}{F}\right)$ and $Q_2 = \left(\frac{a,b'}{F}\right)$ respectively. Consider the F-subspace of the algebra $Q_1 \otimes Q_2$

$$\begin{aligned} X &= F.(1 \otimes 1) + F.(i \otimes 1) + F.(j \otimes j') + F.(k \otimes j') \\ &= F.1 + F.I + F.J + F(I.J), \end{aligned}$$

where we have set $I = i \otimes 1$, $J = j \otimes j'$ (with $IJ = k \otimes j'$). It is a 4-dimensional subspace of $Q_1 \otimes Q_2$. In fact, X is a subalgebra since it satisfies the relations

$$\begin{aligned} I^2 = i^2 \otimes 1 = a, \qquad J^2 = j^2 \otimes j' = bb', \\ - I.J = -ij \otimes j' = ji \otimes j' = J.I. \end{aligned}$$

So the subalgebra X is isomorphic to the quaternion algebra $\left(\frac{a,bb'}{F}\right)$. Now we look at another F-subalgebra

$$\begin{aligned} Y &= F.(1 \otimes 1) + F.(1 \otimes j') + F.(i \otimes k') + F.(-b'i \otimes i') \\ &= F.1 + F.\widetilde{I} + F.\widetilde{J} + F.\widetilde{I}\widetilde{J}. \end{aligned}$$

where $\widetilde{I} = 1 \otimes j'$, $\widetilde{J} = i \otimes k'$ (with $\widetilde{I}\widetilde{J} = i \otimes j'k' = -b'i \otimes i'$) and they satisfy

$$\begin{aligned} \widetilde{I}^2 = 1 \otimes j'^2 = b', \qquad \widetilde{J}^2 = i^2 \otimes k'^2 = -a^2b', \\ - \widetilde{J}\widetilde{I} = -i \otimes k'j' = i \otimes j'k' = \widetilde{I}\widetilde{J}. \end{aligned}$$

Thus, Y is isomorphic to the quaternion algebra $\left(\frac{b', -a^2b'}{F}\right)$ which is isomorhpic to $M_2(F)$. The set $\{I, J\}$ commutes elementwise with the set $\{\widetilde{I}, \widetilde{J}\}$. Thus, elements of X commutes with elements of Y. The subalgebras X and Y generate the entire algebra $Q_1 \otimes Q_2$. Thus, we conclude

$$Q_1 \otimes Q_2 = X \otimes Y = \left(\frac{a,bb'}{F}\right) \otimes_F M_2(F).$$

□

Corollary 1.3.11. *For a quaternion algebra $\left(\frac{a,b}{F}\right)$ the tensor product algebra $\left(\frac{a,b}{F}\right)\otimes_F \left(\frac{a,b}{F}\right)$ is isomorphic to the matrix algebra $M_4(F)$.*

Proof. In the previous lemma we substitue $b' = b$ and using the example 1.3.4 and lemma we get

$$\left(\frac{a,b}{F}\right)\otimes_F\left(\frac{a,b}{F}\right) \cong \left(\frac{a,b^2}{F}\right)\otimes_F M_2(F) \cong \left(\frac{a,1}{F}\right)\otimes_F M_2(F) \cong M_2(F)\otimes_F M_2(F) \cong M_4(F).$$

□

Now we will define an *Albert form* associated to a biquaternion algebra which will help us determine when a biquaternion algebra is division. Let $A = \left(\frac{a,b}{F}\right)$ and $B = \left(\frac{a',b'}{F}\right)$ be given quaternion algebras over F. The respective spaces of pure quaternions, A_0 and B_0, carry the following ternary quadratic forms:

$$q_A := \langle -a, -b, ab\rangle, \quad \text{and} \;\; q_B := \langle -a', -b', a'b'\rangle.$$

We define an *Albert form* of $A \otimes_F B$ to be the 6-dimensional form

$$q := q_A \perp \langle -1\rangle q_B = \langle -a, -b, ab, a', b', -a'b'\rangle. \tag{1.1}$$

Theorem 1.3.12 (Albert)**.** *For a biquaternion algebra $A = Q_1 \otimes_F Q_2$ over F the following statements are equivalent:*

1. *The algebra A is not a division algebra.*
2. *There exists $a, b, b' \in F^*$ such that $Q_1 \xrightarrow{\sim} \left(\frac{a,b}{F}\right)$ and $Q_2 \xrightarrow{\sim} \left(\frac{a,b'}{F}\right)$.*
3. *The Albert form 1.1 has a nontrivial zero on A.*

Chapter 2

Galois Cohomology

We introduce in this chapter, some cohomological tools which will be useful in defining some concepts in upcoming chapters. We begin by defining some terms which are going to be used to define the cohomological tools. In this chapter we have mainly referred from the books [GS06] and [Ber10].

Let G be a group. By a *(left) G-module*, we talk about an abelian group A, equipped with a left action by G. We can also refer A as a module over the integral group ring $\mathbb{Z}[G]$ via the action

$$(\sum n_\sigma \sigma)a := \sum n_\sigma \sigma(a),$$

for elements $\sum n_\sigma \sigma \in \mathbb{Z}[G]$ and $a \in A$. We say that A is a *trivial* G-module if G acts trivially on A, that is, $\sigma a = a$ for all $a \in A$. We denote by A^G the subgroup of G-invariant elements in a G-module A. For the rest of chapter, we let F to be a field with a finite Galois extension L. Let the Galois group of L/F be G of order n. Let A be any discrete topological space.

Definition 2.0.1. *For any G-set A, we set*

$$H^0(G, A) = A^G$$

The set $H^0(G, A)$ is called the ***0th cohomology set*** *of G with values in A. If A is a G-group, then this is a subgroup of A. Hence we call $H^0(G, A)$ as zeroeth cohomology group of G with values in A.*

2.1 Abelian Galois cohomology

In general, only second cohomology group is abelian. Here we consider A to be a G-module.

Definition 2.1.1. A (normalized) 2-cocycle of G with values in A is a map $f : G \times G \to A$ satisfying $f(1,1) = 1$ and

$$\sigma_1 f(\sigma_2, \sigma_3) f(\sigma_1, \sigma_2\sigma_3) f(\sigma_1\sigma_2, \sigma_3)^{-1} f(\sigma_1, \sigma_2)^{-1} = 1 \qquad \text{for all } \ \sigma_1, \sigma_2, \sigma_3 \in G$$

The set of 2-cocycles of G with values in A is denoted by $Z^2(G, A)$. This set is an abelian group for the operation $(f + g)(s,t) = f(s,t)g(s,t)$.

Remark 2.1.2. Since f is a normalised 2-cocycle $f(\sigma, 1) = f(1, \sigma) = 1$ for all $\sigma \in G$.

$$\begin{aligned} &1.f(1,\sigma)f(1,1.\sigma)f(1,\sigma)^{-1}f(1,1) = 1 \\ &\Rightarrow f(1,\sigma) = 1. \end{aligned}$$

Similary substitue $\sigma_1 = \sigma_3 = 1$ and $\sigma_2 = \sigma$ to get $f(\sigma, 1) = 1$.

Definition 2.1.3. *Two 2-cocycles f, g are said to cohomologous or equivalent if there exists a continous map $h : G \to A$ such that*

$$g(s,t) = s(h(t))(h(st))^{-1}h(s)f(s,t) \textit{ for all } s,t \in G$$

It is denoted by $f \sim g$.

Definition 2.1.4. *The equivalence classes of 2-cocycles form an abelian group, denoted by $H^2(G, A)$, called the* ***second cohomology group*** *of G with values in A.*

We can also define the second cohomology group using coboundaries.

Definition 2.1.5. *A (normalised) 2-coboundary is a map $\delta h : G \times G \to A$ of the form $(s,t) \mapsto s(h(t))(h(st))^{-1}h(s)$ where $h : G \to A$ is a map with $h(1) = 1$.*

We first verify that δh is a 2-cocycle.

$$\begin{aligned} &s\,\delta h(t,r)\,\delta h(s,tr)\,(\delta h(st,r))^{-1}(\delta h(s,t))^{-1} \\ &= st(h(r))s(h(tr)^{-1})s(h(t))s(h(tr))h(str)^{-1}h(s)(st(h(r))h(str)^{-1}h(st))^{-1}(s(h(t))h(st)^{-1}h(s))^{-1} \\ &= 1 \end{aligned}$$

The set of 2-coboundaries form a subgroup of $Z^2(G, A)$, denoted by $B^2(G, A)$ and we have the second cohomology group $H^2(G, A) = Z^2(G, A)/B^2(G, A)$.

2.2 Non-abelian Galois cohomology

Definition 2.2.1. *Let A be a G-group. A 1-cocycle of G with values in A is a continuous map $\alpha : G \to A$ such that*

$$\alpha(\sigma\tau) = \alpha(\sigma)\sigma\alpha(\tau) \textit{ for all } \sigma, \tau \in G.$$

We denote by $Z^1(G, A)$ the set of all 1-cocycles of G with values in A. The constant map

$$\begin{aligned} G &\to A \\ \sigma &\mapsto 1 \end{aligned}$$

is an element of $Z^1(G, A)$, which is called the trivial 1-cocycle. Notice also that for any 1-cocycle α, we have $\alpha(1) = 1$.

Remark 2.2.2. If G acts trivially on A, a 1-cocycle is just a continuous homomorphism $\alpha : G \to A$.

We will now define the first cohomology set $H^1(G, A)$. In order to define it, we need the notion of cohomologous cocycles.

Definition 2.2.3. *Two 1-cocycles α, α' are said to be cohomologous if there exists $a \in A$ satisfying*

$$\alpha'_\sigma = a^{-1}.a_\sigma.\sigma(a) \text{ for all } \sigma \in G.$$

It is denoted by $\alpha \sim \alpha'$.

The relation $\sim$ obtained above is an equivalence relation on $Z^1(G, A)$.

Definition 2.2.4. *We denote by $H^1(G, A)$ the quotient set*

$$H^1(G, A) = Z^1(G, A)/\sim .$$

It is called the ***first cohomology set*** *of G with coefficients in A.*

The set $H^1(G, A)$ is not a group in general. If A is a G-module, the set $Z^1(G, A)$ is an abelian group for the pointwise multiplication of functions. This operation is compatible with the equivalence relation, hence it induces an abelian group structure on $H^1(G, A)$.

2.3 Twisting

In this section, we alter the given action of group G on a set. This change in action will be termed as twisting and will be used in construction of a cyclic algebra.

2.3.1 Construction

Let A be a group equipped with a left action by another group G. Suppose further that X is a set on which both G and A act in a compatible way, that is, we have

$$\sigma(a(x)) = (\sigma(a))(\sigma(x)) \text{ for all } x \in X, a \in A \text{ and } \sigma \in G$$

Given a 1-cocycle, $\sigma \mapsto a_\sigma$ of G with values in A we define the *twisted action* of G on X by the cocycle a_σ, via the rule:

$$(\sigma, x) \mapsto a_\sigma(\sigma(x)).$$

We first verify that it is a G-action on X. If $\sigma = 1$, a_1 is also trivial. Thus, $1 \in G$ acts trivially on X. Now for any $\sigma, \tau \in G$ we have:

$$\begin{aligned}(\sigma\tau, x) &= a_{\sigma\tau}(\sigma\tau(x)) \\ &= a_\sigma \sigma_\tau(\sigma\tau(x)) \\ &= a_\sigma \sigma(a_\tau(\tau(x))) \\ &= a_\sigma \sigma(\tau, x) \\ &= (\sigma, (\tau, x))\end{aligned}$$

Thus, it is indeed a G-action. In the above construction, we took X be a set. Similar construction can be done when X has some algebraic structure, that is, it is a group or a vector space. When X has algebraic structure G and A act on it by automorphisms, and the twisted action is also by automorphisms.

We denote X equipped with the twisted G-action by the cocycle a_σ, by ${}_{a_\sigma}X$. The above construction can only be carried out on the level of cocycles and not on that of cohomology classes. Equivalent cohomology classes give rise to different twisted actions.

Consider a field F with Galois extension L with Galois group G. We let $A = PGL_n(F)$ and $X = M_n(F)$, a central simple F-algebra. We take a 1-cocycle a_σ from G to $PGL_n(F)$. Claim is that the G-invariants ${}_{a_\sigma}X^G$ under the twisted action form a central simple algebra over F that is split by L.

2.3.2 Galois descent

In this subsection, we describe Galois descent for central simple algebra. We mainly follow an article by Jahnel [Jah].

Proposition 2.3.1 (Galois descent). *Let L/F be a finite Galois extension of fields and $G := Gal(L/F)$ be its Galois group. Further, let $X = M_n(L)$ be a central simple algebra over L together with a (left) G-action on X, that is, G acting on $M_n(L)$ entry wise. Thus for each $\sigma \in G$, the action is a σ-linear map $T_\sigma : X \to X$.*

Then there is a central simple algebra Y over F such that there is an isomorphism $Y \otimes_F L \simeq M_n(L)$. This isomorphism respects the algebraic structure as well as the G-action. The G-action on $Y \otimes_F L$ is the canonical action of G on L.

Proof. Define $Y := X^G$. We need to show if X is a central simple algebra over L then Y is a central simple algebra over F. This can be directly concluded if we are able to prove $X^G \otimes_F L = M_n(L)$. To prove this, we let $\{l_1, ..., l_n\}$ be a F-basis of L and show the following claim.

Claim: *There exist an index set J and a subset $\{x_j | j \in J\} \subset X^G$ such that $\{l_i x_j | i \in \{1, ..., n\}, j \in J\}$ is an F-basis of X.*

By Zorn's Lemma, there exists a maximal subset $\{x_j | j \in J\} \subset X^G$ such that $\{l_i x_j | i \in \{1, ..., n\}, j \in J\} \subset X$ is a system of F-linearly independent vectors. Assume that, system is not a basis of X. Then $\langle l_i x_j | i \in \{1, ..., n\}, j \in J\rangle_F$ is a proper G-invariant L-sub-vector space of X and one can choose an element $x \in X/\langle l_i x_j | i \in \{1, ..., n\}, j \in J\rangle_F$. For every $l \in L$, the sum

$$\sum_{\sigma \in G} T_\sigma(lx) = \sum_{\sigma \in G} \sigma(l) T_\sigma(x)$$

is G-invariant. Now, by linear independence of vectors, the matrix

$$\begin{pmatrix} \sigma_1(l_1) & \dots & \sigma_1(l_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(l_1) & \dots & \sigma_n(l_n) \end{pmatrix}$$

is of maximal rank. This implies, there exists an $l \in L$ such that

$$x_\beta := \sum_{\sigma \in G} \sigma(x) \sigma(l)$$

has a non-zero image in $X/\langle l_i x_j | i \in \{1, ..., n\}, j \in J\rangle_F$. Therefore,

$$\{l_i x_j | i \in \{1, ..., n\}, j \in J\} \ \cup \ \{l_i x_\beta | i \in \{1, \dots, n\}\}$$

is a F-linearly independent system of vectors contradicting the maximality of $\{x_j | j \in J\}$. □

In the above proposition, instead of entry wise action, we will consider the twisted G-action. Since $M_n(L)$ is split by L, the algebra obtained by the above proposition is central simple algebra over F split by L. Infact we will state a stronger result. We denote by $[A]$, the set of all isomorphic classes of central simple algebra A of dimension n^2 over F and split by L.

Theorem 2.3.2. *Let L/F be finite extension of fields, $G := Gal(L/F)$ its Galois group. Then there exists a bijection between the set of all which are of dimension n^2*

over F and split by L and the first cohomology set of G with values in $PGL_n(L)$

$$\begin{aligned} \alpha : [A] &\overset{\cong}{\to} H^1(G, PGL_n(L)) \\ A &\mapsto a_A \end{aligned}$$

Proof. Let A be a central simple algebra over F split by L, then

$$A \otimes_F L \underset{f}{\overset{\cong}{\to}} M_n(L).$$

The following diagram:

$$\begin{tikzcd} A \otimes_F L \arrow[r, "f"] \arrow[d, "\sigma"] & M_n(L) \arrow[d, "\sigma"] \\ A \otimes_F L \arrow[r, "f"] & M_n(L) \end{tikzcd}$$

for $\sigma \in G$ does not commute in general. Thus, we put $f \circ \sigma = a_\sigma \circ (\sigma \circ f)$ where $a_\sigma \in PGL_n(L)$ for each σ. Now, we have:

$$\begin{aligned} f \circ \sigma\tau &= (f \circ \sigma) \circ \tau \\ &= a_\sigma \circ (\sigma \circ f) \circ \tau \\ &= a_\sigma \circ \sigma \circ (f \circ \tau) \\ &= a_\sigma \circ \sigma \circ (a_\tau \circ (\tau \circ f)) \\ &= a_\sigma \circ \sigma a_\tau \circ (\sigma\tau \circ f) \\ &= a_{\sigma\tau} \circ (\sigma\tau \circ f). \end{aligned}$$

That is, $a_\sigma \circ \sigma a_\tau = a_{\sigma\tau}$. Thus, a_σ for $\sigma \in G$ is a cocycle. If $f' : A \otimes_F L \to M_n(L)$ is another isomorphism, then cocycle obtained using f' is cohomologous to the cocycle obtained by f. Indeed, there exists some $b \in PGL_n(L)$ such that $f = b \circ f'$. The equality $f \circ \sigma = a_\sigma \circ (\sigma \circ f)$ yields

$$f' \circ \sigma = b^{-1} \circ f \circ \sigma = b^{-1} \cdot a_\sigma \circ (\sigma \circ (b \circ f')) = b^{-1} \cdot a_\sigma \cdot^\sigma b(\sigma \circ f')$$

Thus f' yields a cocycle that is cohomologous to a_σ. Thus, the mapping α is well defined.

Injectivity of α: Suppose α is not injective, then there exist A and A' in $[A]$ that yield the same cohomology class a_σ in $H^1(G, PGL_n(L))$ for a suitable choices of f and f'. Thus, we have $f \circ \sigma = a_\sigma \circ (\sigma \circ f)$ and $f' \circ \sigma = a_\sigma \circ (\sigma \circ f')$ satisfying the following diagram

$$\begin{tikzcd}
A \otimes_F L \arrow[r, "f"] \arrow[d, "\sigma"'] & M_n(L) \arrow[r, "f'"] \arrow[d, "\sigma"'] & A' \otimes_F L \arrow[d, "\sigma"] \\
A \otimes_F L \arrow[r, "f"] & M_n(L) \arrow[r, "f'"] & A' \otimes_F L
\end{tikzcd}$$

Consequently, $f' \circ \sigma \circ f'^{-1} \circ \sigma^{-1} = f \circ \sigma \circ f^{-1} \circ \sigma^{-1}$ and therefore,

$$f \circ \sigma \circ f^{-1} \circ f' \circ \sigma \circ f'^{-1} = Id$$

Since, the outer part commutes, taking G-invariants on both sides, we get $A \cong A'$.

Surjectivity of α: Let $(a_\sigma)_{\sigma \in G} \in H^1(G, PGLn(L))$ be a cocycle. We define a new G-operation on $M_n(L)$, by letting $\sigma \in G$ operate as

$$a_\sigma \circ \sigma : M_n(L) \xrightarrow{\sigma} M_n(L) \xrightarrow{a_\sigma} M_n(L).$$

This is a σ linear mapping, also satisfying the relation

$$(a_\sigma \circ \sigma) \circ (a_\tau \circ \tau) = a_\sigma \circ \sigma \cdot a_\tau \circ \sigma\tau = a_{\sigma\tau} \circ \sigma\tau.$$

So, we have a new (left) G-action on $M_n(L)$. Using *Galois descent* 2.3.1, we get a desired algebra that is central simple over F and is split by L. □

Chapter 3

Brauer Group

In this chapter, we characterize the set of isomorphism classes of division algebras. We will first define *Brauer group* to classify division algebras. For this exposition we follow notes by Sridharan and Parimala (Chapter I, [SR]).

3.1 Brauer Group

We form a set S consisting of isomorphism classes of central simple algebras over F. S is a commutative monoid with tensor product over F as the operation. We have already seen in 1.2.1 that if A is a central simple algebra over F, then $A \xrightarrow{\sim} M_r(D_A)$ where D_A is a central divison algebra over F (*Wedderburn's Theorem*). Using this, we define an equivalence relation on S:

Definition 3.1.1. *Two central simple algebras, A and B over F are said to be* ***Brauer equivalent*** *if D_A and D_B are isomorphic.*

Equivalently, two algebras A and B are Brauer equiavlent if and only if $M_R(A) \xrightarrow{\sim} M_s(B)$. A and B are isomorphic if they are Brauer equivalent and $[A : F]$ is equal to $[B : F]$. The equivalence relation on S is compatible with the monoid structure on S. Thus, the set $S/\sim$ is again a commutative monoid under the operation induced by tensor product over F. We denote class of Brauer equivalent algebras of A by $[A]$. The identity element is the class of all matrix algebras over F i.e. $[M_n(F)]$.

We further realize that it is not just a commutative monoid but a group with $[A^{op}]$, inverse of $[A]$.

Proposition 3.1.2. *For a central simple algebra A over F, if A^{op} denotes the opposite algebra. Then A^{op} is central simple and $[A][A^{op}] = [F]$ in $S/\sim$.*

Proof. If A is central simple then so is A^{op}. We take the help of the maps $A \to End_F A, a \mapsto L_a$ and $A^{op} \to End_F A, a \mapsto R_a; L_a, R_a$ denoting the left and right multiplication, to induce a homomorphism $\phi : A \otimes_F A^{op} \to End_F A$, since $L_a \circ R_b =$

$R_b \circ L_a; a, b \in A$. And $A \otimes_F A^{op}$ is simple, ϕ is injective. Now, we check the dimension $[A \otimes_F A^{op} : F] = [A : F]^2 = [End_F A : F]$, which implies ϕ is surjective and hence an isomorphism. For a suitable choice of basis of A over F, $End_F A$ is isomorphic to a matrix algebra over F. □

The group $S/\sim$ is called the *Brauer Group* of F, denoted by Br(F). Thus, Brauer group classifies finite dimensional central division algebras over F.

Example 3.1.3. *If F is an algebraically closed field, the only finite dimensional division algebra over F is itself 1.1.4. Thus, Br(F) is trivial.*

Example 3.1.4 (Wedderburn's little theorem 1.1.5)**.** *If F is a finite field then Br(F) is trivial.*

Example 3.1.5 (Frobenius theorem 1.1.6)**.** $Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$

Further, if $F \subset L$ then $Br(F) \subset Br(L)$.

3.2 Existence of Galois Splitting Field

Following two theorems help us in giving some insight about the structure of a simple sub algebra sitting in a central simple algebra.
If B is a simple subalgebra of a central simple algebra A over F:

Theorem 3.2.1. *The commutant $B^{'}$ of B is equal to $\{a \in A | \ ab = ba \ \forall \ b \in B\}$. Also $[B : F][B^{'} : F] = [A : F]$.*

Theorem 3.2.2. *IF $\phi : B \to A$ is a F-algebra homomorphism. Then there exists a $u \in A$ which is a unit such that, $\phi(x) = uxu^{-1} \ \forall \ x \ \in B$. In other words, ϕ extends to an inner automorphism of A.*

A commutative subring B of A is said to be *maximal commutative subring* if it is not contained in any other commutative subring of A.

Corollary 3.2.3. *If L is a subfield of a central simple algebra A over F. Then L is a maximal commutative subring of F if and only if $[L : F]^2 = [A : F]$.*

The above corollary is also valid for a central division algebras over F.

Proposition 3.2.4. *If L is a maximal commutative subring of a central simple F-algebra A, then L is a splitting field of A.*

Proof. One can see A as the bimodule ${}_A A_L$. The mapping $A \to End_L A$, $a \mapsto L_a$ and $L \to End_L A$, $x \mapsto R_x$ commute to yield an induced homomorphism $\phi : L \otimes_F A \to End_L A$. Since the field L is a maximal commutative subring of A, $[L : F]^2 = [A :$

$F] = [A : L][L : F] = n^2$ so that $[L \otimes_F A : L] = n^2 = [End_L A : L]$. Since $L \otimes_F A$ is central simple over L, ϕ is an isomorphism. The algebra $End_L A$ can be identified as $M_n(L)$ through a choice of an L-basis for A. □

Lemma 3.2.5. *If L is a splitting field for A, then L is also a splitting field for A^{op}. In fact, L is a splitting field for all central simple F-algebras, B which are Brauer equivalent to A.*

Thus, using the above lemma, it makes sense to talk about splitting field of an element of $Br(F)$.

Proposition 3.2.6. *Let A be a central simple algebra over F and L, a finite extension of F. Then L is a splitting field for A if and only if there exists a central simple algebra B, Brauer equivalent to A, which contains L as a maximal commutative subring. The algebra B is unique up to isomorphism.*

Proof. If B, B' are two central simple algebras Brauer equivalent to A and both of which contain the field L as a maximal commutative subring, then $[B : F] = [L : F]^2 = [B' : F]$. Thus B and B' are Brauer equivalent central simple F-algebras of the same rank and hence isomorphic. This proves the uniqueness of B up to isomorphism. $B \sim A$ contains L as a maximal commutative subring. Then L splits B and hence L splits A. Conversely, A is a central simple algebra over F, split by a finite extension L over F. Without loss of generality, we take $A = D$ is a division algebra over F. Since L also splits D^{op}, we have an isomorphism $\phi : L \otimes_F D^{op} \xrightarrow{\sim} M_n(L)$. We regard L^n as a bimodule ${}_L L^n_D$ through ϕ. Let m be the dimension of L^n regarded as a right vector space over D. Then we have an injection $L \hookrightarrow End_D L^n \xrightarrow{\sim} M_m(D)$. Thus $B = M_m(D)$ is a central simple algebra over F, Brauer equivalent to D, containing L as a subfield. We have $mn^2 = [L^n : D][D : F] = [L^n : F] = n[L : F]$ so that $[L : F] = mn$. Further, $[M_m(D) : F] = m^2n^2$. Thus, L is a maximal commutative subring of $M_m(D)$. □

We define degree of an algebra to be the squareroot of its dimension which is a natural number (Since dimension of an algebra over a field is always an integral square 1.2.8).

Index of A is *defined to be* degree of D_A.

Corollary 3.2.7. *Index of a central simple algebra A always divides $[L : F]$ where L splits A.*

Proof. Since L splits A, using the previous proposition, there exists a central simple algebra B, Brauer equivalent to A, such that L is a maximal commutative subring of B. Index of A is same as that of B and we have $B = M_r(D_A)$ for some $r \in \mathbb{N}$. By dimension equality $[B : F] = r^2[D_A : F]$, then, $[L : F]^2 = r^2 deg(D_A)^2$. Therefore, $deg(D_A) | [L : F]$. □

Theorem 3.2.8. *If D is a central division algebra over F, then there exists a maximal commutative subring L of D which is separable over F.*

Corollary 3.2.9. *If A is a central simple algebra over F, then there exists a finite Galois extension L of F which splits A.*

Proof. We can assume, A is a central division algebra over F. Let L_1 be a maximal commutative subfield of A, separable over F, existence of such a subfield is guaranteed by previous theorem. Using 3.2.4, L_1 splits A. Any field containing L_1 again splits A, so we chose Galois closure of L_1 over F to be the finite Galois extension L. □

3.3 Crossed product algebra

Let L be a finite Galois extension of F with Galois group $G(L/F) = G$. We have already defined the 2nd cohomology group in section 2.1. We fix a 2-cocycle f in $Z^2(G, L^*)$. Recall that a (normalised) 2-cocycle is a map from $G \times G \to L^*$ such that $f(1,1) = 1$ and it satisfies the following condition

$$\sigma_1 f(\sigma_2, \sigma_3) f(\sigma_1, \sigma_2\sigma_3) f(\sigma_1\sigma_2, \sigma_3)^{-1} f(\sigma_1, \sigma_2)^{-1} = 1 \qquad \text{for all} \ \ \sigma_1, \sigma_2, \sigma_3 \in G.$$

Now, for each $\sigma \in G$, we consider a symbol $\{e_\sigma\}$ and define (L, G, f) to be a vector space over L with basis $\{e_\sigma\}_{\sigma\in G}$, that is,

$$(L, G, f) = \oplus_{\sigma \in G} L e_\sigma.$$

The vector space (L, G, f) acts as an algebra over F with the following multiplication:

$$(\lambda e_\sigma)(\mu e_\tau) = \lambda \sigma(\mu) f(\sigma, \tau) e_{\sigma\tau}.$$

This multiplication will be helpful in giving algebra structure to (L, G, f). The vector space (L, G, f) is known as a *crossed product* over L.

Proposition 3.3.1. *The multiplication (L, G, f) mentioned above makes it a central simple algebra over F with L as a maximal commutative subring of (L, G, f) via the injection $x \mapsto xe_1$, that is, $[(L, G, f) : F] = [L : F]^2$.*

Proof. Since f is a 2-cocycle, we get

$$\begin{aligned}
(e_{\sigma_1} e_{\sigma_2}) e_{\sigma_3} &= f(\sigma_1, \sigma_2) e_{\sigma_1\sigma_2} e_{\sigma_3} \\
&= f(\sigma_1, \sigma_2) f(\sigma_1\sigma_2, \sigma_3) e_{\sigma_1\sigma_2\sigma_3} \\
&= \sigma_1 f(\sigma_2, \sigma_3) f(\sigma_1, \sigma_2\sigma_3) e_{\sigma_1\sigma_2\sigma_3} \\
&= e_{\sigma_1}(f(\sigma_2, \sigma_3) e_{\sigma_2\sigma_3}) \\
&= e_{\sigma_1}(e_{\sigma_2} e_{\sigma_3}).
\end{aligned}$$

Thus, (L, G, f) follows associativity. Further, because f is a normalized cocycle, it implies that e_1 is the identity element of (L, G, f). Since, (L, G, f) is a (left) vector space over L of dimension $|G| = [L : F]$, it follows

$$[(L, G, f) : F] = [(L, G, f) : L][L : F] = [L : F]^2.$$

Thus, L is a maximal commutative subring of (L, G, f). Now, if (L, G, f) is not central over F, then there exists a central element $x = \sum_{\sigma \in G} x_\sigma e_\sigma, x_\sigma \in L$ of (L, G, f). Then, for every $a \in L^*$, the condition $ax = xa$ implies $x_\sigma = 0$ for $\sigma \neq 1$. Thus, we get $x = x_1 e_1$. Further, the condition $xe_\sigma = e_\sigma x$ for all $\sigma \in G$ implies that $\sigma(x_1) = x_1$, so $x_1 \in F$. Now, we are left to prove that (L, G, f) is simple. Let $\mathcal{A}$ be a non-zero two-sided ideal of (L, G, f). For $x \in \mathcal{A}$, $x \neq 0$, if $x = \sum_{\sigma \in G} x_\sigma e_\sigma$, we define $l(x) =$ the number of $x_\sigma \neq 0$ in this expression. Let $x \in \mathcal{A}$ be an element with $l(x)$ minimal. Let σ_o be such that $x_{\sigma_o} \neq 0$. We multiply x on the left by $x_{\sigma_o}^{-1}$ and on the right by $e_{\sigma_o}^{-1}$. Thus, we can assume $x = 1.e_1 + \sum_{\sigma \neq 1} x_\sigma e_\sigma$. For every $d \in L$, $l(dx - xd) < l(x)$, unless $(dx - xd) = 0$. Since $(dx - xd) \in \mathcal{A}$, it follows that $dx - xd = 0$ for every $d \in L$, that is, $x_\sigma = 0$ for all $\sigma \neq 1$. Thus $x = e_1 \in \mathcal{A}$ so that $\mathcal{A} = (L, G, f)$. Hence (L, G, f) is a central simple algebra over F. □

Corollary 3.3.2. *If $\{e'_\sigma\}_{\sigma \in G}$ are non-zero elements of (L, G, f) satisfying $e'_\sigma x = \sigma(x) e'_\sigma$, for all $x \in (L, G, f)$, then there exist non-zero elements $u_\sigma \in L^*$, for each $\sigma \in G$, such that $e'_\sigma = u_\sigma e_\sigma$.*

Proof. Let $x = e_\sigma^{-1} \lambda$, where $\lambda \in L$. We have

$$\begin{aligned} e'_\sigma e_\sigma^{-1} \lambda &= \sigma(e_\sigma^{-1} \lambda) e'_\sigma \\ &= \sigma(\sigma^{-1}(\lambda) e_\sigma^{-1}) e'_\sigma \\ &= \lambda \sigma(e_\sigma^{-1}) e'_\sigma \\ &= \lambda e'_\sigma e_\sigma^{-1} \end{aligned}.$$

Thus, $e'_\sigma e_\sigma^{-1}$ commutes with every element of L. Since L is a maximal commutative subring of (L, G, f), we get $e'_\sigma e_\sigma^{-1} = u_\sigma \in L^*$. □

Infact, the following proposition shows that the isomorphism class of (L, G, f) is uniquely determined by the cohomology class $[f]$ of f in $H^2(G, L^*)$.

Proposition 3.3.3. *Let f and $g \in Z^2(G, L^*)$, then (L, G, f) and (L, G, g) are isomorphic if and only if $f - g \in B^2(G, L^*)$.*

Proof. ($\Leftarrow$) Suppose $f - g = \delta h$ where $h : G \to L^*$ is a map with $h(1) = 1$. Let $\{e_\sigma\}, \{e'_\sigma\}\sigma \in G$ be basis of (L, G, f) and (L, G, g) respectively satisfying the algebra structure. With the help of the map $e_\sigma \mapsto h(\sigma)e'_\sigma, x \mapsto x; x \in L$ we induce an isomorphism of the F-algebras (L, G, f) onto (L, G, g).

($\Rightarrow$) Conversely, suppose we have an isomorphism of F-algebras, $\phi : (L, G, f) \to (L, G, g)$. Since Le'_1 and $\phi(Le_1)$ are simple subalgebras of (L, G, g), both are isomorphic to L. With the help of previous corollary, there exists a unit $u \in (L, G, g)$ such that $\phi(xe_1) = u(xe'_\sigma)u^{-1}$ for all $x \in L$. Now by replacing ϕ by $Intu^{-1} \circ \phi$, we can assume that $\phi(xe_1) = xe'_1$. Then, since $\{\phi(e_\sigma)\}, \sigma \in G$, satisfy the algebra structure of the crossed algebra, there exists $u_\sigma \in L^*$ such that $phi(e_\sigma) = u_\sigma e'_\sigma$ with $u_1 = 1$ again by previous corollary. Let $h : G \to L^*$ be defined by $h(\sigma) = u_\sigma$. From here we get $f = g + \delta h$. □

Proposition 3.3.4. *For $f \in Z^2(G, L^*)$, the algebra (L, G, f) is isomorphic to matrix algebra if and only if $f \in B^2(G, L^*)$.*

Proof. ($\Leftarrow$) Let $f \in B^2(G, L^*)$. With the help of 3.3.3, it will suffice our purpose if (L, G, f) is a matrix algebra for $f = 1$, the trivial cocycle. Consider the assignment $\phi(e_\sigma) = \sigma$, $\phi(x) = R_x, x \in L, R_x$ denoting multiplication by x. This assignment extends to a F-algebra homomorphism $\phi : (L, G, f) \to End_F L$, which is indeed an isomorphism.

($\Rightarrow$) If $(L, G, f) \xrightarrow{\sim} M_n(F)$, $n = [L : F]$ and since $(L, G, 1) \xrightarrow{\sim} M_n(F)$, it follows from 3.3.3 that $f \in B^2(G, L^*)$. □

Proposition 3.3.5. *Let $f, g \in Z^2(G, L^*)$, then the algebra $(L, G, f + g)$ is Brauer equivalent to $(L, G, f) \otimes_F (L, G, g)$.*

3.4 The Brauer Group is Torsion

In this section, we aim to prove that the Brauer group of a field is *torsion*, that is, every element has a finite order. We denote the subset of $\mathrm{Br}(F)$, consisting of those Brauer classes which are split by L, by $\mathrm{Br}(L/F)$. By the last proposition of previous section, $\mathrm{Br}(L/F)$ forms a subgroup of $\mathrm{Br}(F)$.

We define a map $c : H^2(G, L^*) \to Br(L/F)$ as $[f] \mapsto [(L, G, f)]$. Using the previous section, this map is an injective homomorphism. Infact, we will prove it is an isomorphism using the next proposition.

Proposition 3.4.1. *Every Central simple algebra F, split by a finite Galois extension L/F is Brauer equivalent to a crossed product over L.*

Proof. Let A be a central simple algebra over F, split by a finite Galois extension L of F. With the help of 3.2.6, $A \sim B$ where B contains L as a maximal commutative subring. Since every $\sigma \in G = Gal(L/F)$ can be extended to an inner automorphism

Intu_σ of B, u_σ being a unit of B. We choose $u_1 = 1$. Since, Int$(u_\sigma u_\tau)$ and Int$(u_{\sigma\tau})$ both extend $\sigma\tau \in G$, it follows that $u_\sigma u_\tau u_{\sigma\tau}^{-1}$ commutes with every element of L and hence belong to L^*. Let $f(\sigma, \tau) = u_\sigma u_\tau u_{\sigma\tau}^{-1}; \sigma, \tau \in G$. Then $f(1, 1) = 1$ and the condition $(u_{\sigma_1} u_{\sigma_2})u_{\sigma_3} = u_{\sigma_1}(u_{\sigma_2} u_{\sigma_3})$ implies that f is a 2-cocycle. The map $e_\sigma \mapsto u_\sigma, x \mapsto x, x \in L, \sigma \in G$ defines a homomorphism ϕ of (L, G, f) onto B. Since, (L, G, f) is simple and $[(L, G, f) : F] = [B : F] = n^2$, ϕ is indeed an isomorphism. □

Corollary 3.4.2. *Every central simple algebra over F is Brauer equivalent to a crossed product over some finite Galois extension of F.*

Proof. For any central simple algebra A, there exists a finite Galois extension that splits it. Thus, by previous proposition there exists a crossed product algebra B over some finite Galois extension of F that is Brauer equivalent to A.content... □

Therefore, we have the following result:

Theorem 3.4.3. *We have an isomorphism $c : H^2(G, L^*) \xrightarrow{\sim} Br(L/F)$ given by $[f] \mapsto [(F, G, f)]$, where L is a finite Galois extension of F with Galois group G.*

One must note that we are talking about Brauer equivalence, not isomorphism, since every central division algebra will not necessarily contain a maximal commutative subfield which is Galois over F.

For a central simple algebra A over F, we define the *exponent* of A to be order of $[A]$ in $Br(F)$, denoted by $\exp(A)$. We will show that $\exp(A)$ is finite for every central simple algebra A in $\mathrm{Br}(F)$.

Theorem 3.4.4. *For any central simple algebra A over F, exp(A) divides index(A), i.e, Brauer Group is torsion.*

Proof. By definition, the exponent and index are Brauer class invariants, thus, it suffices the purpose to prove the theorem for division algebra D. Let $[D : F] = n^2$, so that index$D$ = n. We already know D is Brauer-equivalent to a crossed product over some finite Galois extension L of F. Let $\phi : (L, G, f) \to M_m(D)$ be an isomorphism of F-algebras, $G = Gal(L/F)$, $m \geq 1$. Since L is a maximal commutative subring of (L, G, f), $[L : F]^2 = [(L, G, f) : F] = [M_m(D) : F] = m^2n^2$. So, we have $[L : F] = mn$. We can also see L as a maximal commutative subring of $M_m(D)$ through ϕ. We regard left $M_m(D)$-module D^m as a left vector space over L with dimension p. Then $[D^m : F] = [D^m : L][L : F]$ so that $mn^2 = pmn \Rightarrow p = n$.

Now for any $\sigma \in G$, $\phi(e_\sigma) \in M_m(D)$ operates on D^m and $\phi(e_\sigma)(\lambda x) = \sigma(\lambda)\phi(e_\sigma)(x)$, for $\lambda \in L, x \in D^m$, that is, $\phi(e_\sigma)$ is σ-semilinear. For a choice of basis $\{e_i\}1 \leq i \leq n$ of D^m over L, $\{\phi(e_\sigma)\}_{\sigma\in G}$ can be represented by matrices $T_\sigma \in M_n(L)$. The condition $e_\sigma e_\tau = f(\sigma, \tau) \cdot e_{\sigma\tau}$ translates into the condition $T_\sigma \sigma(T_\tau) = f(\sigma, \tau)T_{\sigma\tau}$, where the action of G on $M_n(L)$ is entry-wise. Let $h(\sigma) = \det T_\sigma, \sigma \in G$. Then $h : G \to L^*$ is a map with $h(1) = 1$. We have $\sigma(h(\tau))h(\sigma) = f(\sigma,\tau)^n h(\sigma\tau)$; that is, $nf \in B^2(G, L^*)$. Thus, $[(L, G, f)]^n$ is trivial in $\mathrm{Br}(F)$. Thus, $\exp D = \exp(L, G, f)$ divides $n = \mathrm{degree}D$. □

3.5 Quaternion Algebras

We have already discussed about quaternion algebras in chapter one. In this section, we will talk about quaternion algebras in context of Brauer group. We will show that the 2-torsion elements in the Brauer Group are precisely Quaternion Algebras. We will begin by proving the following lemma.

Lemma 3.5.1. *Let A be a central simple algebra over F. If p is a prime which divides index A, then p divides exp A.*

Proof. Since index and exponent are Brauer class invariants, we let A to be a crossed product algebra over a finite Galois extension L of F. Let $G = \mathrm{Gal}(L/F)$. Since L splits A, index A divides $[L : K]$. Thus, p divides $[L : F]$ = order of G. Let H be a p-sylow subgroup of G and let L_1 be the fixed field of H, so that $[L_1 : F] = [G : H]$ is coprime to p.
Claim: $L_1 \otimes_F A$ is not a matrix algebra oevr L_1.
Otherwise, index A would divide $[L_1 : F]$, and $p|[L_1 : F]$ is a contradiction. Further, $L \otimes_{L_1} (L_1 \otimes_F A) \simeq L \otimes_F A \xrightarrow{\sim} M_n(L)$, so that index $L_1 \otimes_F A$ divides $[L : L_1] = p^k, k \geq 1$. Let index $L_1 \otimes_F A = p^r, r \geq 0$. In fact $r \geq 1$ since $L_1 \otimes_F A$ is not a matrix algebra. Since exp $L_1 \otimes_F A$ divides index $L_1 \otimes_F A$, exp $L_1 \otimes_F A = p^r$, with $r \geq 1$. Since $\mathrm{Br}(F)$ $\to \mathrm{Br}(L)$, induced by $[A] \to [L \otimes_F A]$ is a homomorphism, $\exp_{L_1}(L_1 \otimes_F A)$ divides exp A so that p divides exp A. □

Let ${}_2\mathrm{Br}(F)$ denote the 2-torsion subgroup of $\mathrm{Br}(F)$, that is, the subgroup of elements of order ≤ 2. Let $[A] \in {}_2\mathrm{Br}(F)$. From the previous lemma, we can conclude that index A is a power of 2.

Definition 3.5.2. *An involution (of the first kind) of a central simple algebra A over F is an antiautomorphism $\sigma : A \to A$ such that σ^2 = identity and σ is identity on F.*

An algebra A is *involutorial* if it admits an involution. If A is involutorial, then $A \xrightarrow{\sim} A^{op}$ so that $[A] \in_2 \mathrm{Br}(F)$.

Lemma 3.5.3. *Let A and B be central simple algebras over F which are Brauer equivalent. If A has an involution, then B has an involution.*

Proof. We can prove this by proving if D is central division algebra over F, D has an involution if and only if $M_r(D)$ has an involution.
If D has an involution σ, $x \mapsto \sigma(x^t)$ defines an involution of $M_r(D)$, the action of σ on $M_r(D)$ being entry-wise.

Suppose $M_r(D)$ has an involution σ. Let $\sigma(e_{ij}) = f_{ji}$, where $\{e_{ij}\}, 1 \leq i,j \leq r$ are the matrix units of $M_r(D)$. Since σ is an anti-automorphism, it follows that $\{f_{ij}\}, 1 \leq i,j \leq r$ are again metric units of $M_r(D)$ so that they generate an F-subalgebra of $M_r(D)$, isomorphic to $M_r(F)$. Thus, there exists a unit $u \in M_r(D)$ such that $f_{ij} = ue_{ij}u^{-1}$, for all i,j. We have $f_{ij} = \sigma(e_{ji}) = ue_{ij}u^{-1}$ and $e_{ji} = \sigma(ue_{ij}u^{-1}) = \sigma u^{-1}ue_{ji}u^{-1}\sigma u$. Thus $v = u^{-1}\sigma u$ commutes with $M_r(F)$ so that v belongs to the commutant of $M_r(F)$ in $M_r(D)$, that is, D.

Case 1. Let $u + \sigma u = 0$. Then $v = -1$ and $\sigma' = \text{Int}u^{-1} \circ \sigma$ is an involution of $M_r(D)$. Since $\sigma'(e_{ij}) = e_{ji}$, σ' maps $M_r(F)$ onto itself and hence maps the commutant of $M_r(F)$, that is, D onto itself, thus giving an involution on D.

Case 2. Let $u + \sigma u \neq 0$. Then $v \neq 0$ and $1 + v \in D$ is a unit. Thus $u' = u + \sigma u = u(1+v)$ is a unit of $M_r(D)$ and $\sigma^{prime} = \text{Int}(u'^{-1}) \circ \sigma$ defines an involution of $M_r(D)$ which restricts again to an involution of D. □

Lemma 3.5.4. *Let A be an algebra of exponent 2 which is a crossed product over some $L \supset F$. Then A has an involution.*

Proof. Let $A \overset{\sim}{\rightarrow} (L, G, f)$ with $G = \text{Gal}(L/K)$, $2f \in B^2(G, L^*)$. Let $h : G \rightarrow L^*$ be a map with $h(1) = 1$ and such that for all $\sigma, \tau \in G$, $f(\sigma,\tau)^2 = \sigma(h(\tau))h(\sigma\tau)^{-1}h(\sigma)$. Thus, the assignment $e_\sigma \mapsto e_\sigma^{-1}h(\sigma), l \mapsto l, l \in L, \sigma \in G$ induces an involution of (L, G, f). □

From the above lemma we get the following theorem:

Theorem 3.5.5. *For a central simple algebra A over F, the following statements are equivalent:*

1. *$[A] \in_2 Br(F)$*

2. *A admits of an involution over F.*

We have already seen in chapter one that there exists a canonical involution in quaternion algebras, that is, conjugation. In fact we have a much stronger result mentioned below.

Lemma 3.5.6. *Central simple algebras over F of rank 4 are quaternion algebras over F.*

Chapter 4

Cyclic Algebras

In this chapter, we will first discuss about cyclic algebras. After getting acquainted with the basics we will discuss the central question of the cyclicity of a division algebra.

4.1 Cyclic algebras

Definition 4.1.1 (Cyclic algebras)**.** *Let F be a field and L/F be a cyclic Galois extension of degree n with Galois group G generated by σ. We define $A = \oplus_{i=0}^{i=n-1} Lu^i$ where $u^n = b$ and the product structure is given by $uy = \sigma(y)u$ for all $y \in L$. The algebra A is called a Cyclic Algebra over F and is denoted by $\triangle(L/F, \sigma, b)$.*

The central simple algebra A over F defined above is split by L.

Example 4.1.2 (Hamilton's quaternions)**.** Consider the field of real numbers $\mathbb{R}$ and its cyclic Galois extension $\mathbb{C}$ of degree 2 with Galois group $G = \{1, \sigma\}$. Let $b = -1$, then the cyclic algebra over $\mathbb{R}$ is $A = \mathbb{C} \oplus \mathbb{C}j$ with $j^2 = -1$ and $jx = \bar{x}j$ (σ being the conjugation map). Thus $A = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij$.

Hamilton's quaternions could be generalised over any field.

Example 4.1.3 (Quaternion algebra)**.** Consider a field F and a cyclic Galois extension $L = F(\sqrt{a})$ of degree 2 with Galois group $G = \{1, \sigma\}$. Let $b \in F^*$, then the cyclic algebra over F is $A = L \oplus L\eta$ with $\eta^2 = b$ and $\eta x = \sigma(x)\eta$. Algebra A is a cyclic algebra denoted by $(\frac{a,b}{F})$ and is called *Quaternion algebra* over F.

Quaternion algebra is the degree two case of symbol algebra.

Example 4.1.4 (Symbol algebra)**.** Consider a field F containing a primitive n^{th} root of unity ρ and a cyclic Galois extension $L = F(a^{1/n})$ of degree n with Galois group G generated by σ where $\sigma(a^{1/n}) = \rho(a^{1/n})$. Let $b \in F^*$, consider the algebra $A = \oplus_{i=0}^{i=n-1} L\eta^i$ with $\eta^n = b$ and $\eta x = \sigma(x)\eta$. The algebra A is a cyclic algebra denoted by $(a, b)_{F,n}$ and is called a *Symbol algebra* over F.

4.1.1 Construction of a Cyclic algebra

In this section we construct a cyclic algebra over F as a twisted form of a matrix algebra over F. Main reference of this section is (§2.3, [GS06]). We keep notations as in the definition (4.1) above. Recall that a 1-*cocyle* is a map $f : G \to L^*$ satisfying $f(st) = f(s)sf(t)$ for all $s, t \in G$.

We fix a character of G, $\chi : G \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ and consider the matrix

$$\widetilde{F}(b) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \in GL_n(F)$$

Let $F(b)$ denote image of $\widetilde{F}(b)$ in $PGL_n(F)$. We note that $\widetilde{F}(b)^n = b.I_n$ since

$$\widetilde{F}(b) = \begin{bmatrix} 0 & I_{n-i} \\ b.I_i & 0 \end{bmatrix}.$$

Hence $F(b)^n = I$. Thus the element $F(b)$ has exact order n in $PGL_n(F)$ and we can consider the homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $PGL_n(F)$ sending 1 to $F(b)$. Composing this homomorphism and injection of $PGL_n(F)$ in $PGL_n(L)$ we get a homomorphism $z(b)$ from G to $PGL_n(L)$.

$$z(b) : G \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \to PGL_n(F) \hookrightarrow PGL_n(L)$$

Since the action of G on $PGL_n(F)$ (acting element wise) is trivial, $z(b)$ is infact a 1-cocycle from G to $PGL_n(L)$. Now using the twisted G-action ${}_{z(b)}M_n(L)$ on the matrix algebra $M_n(L)$ coming from $z(b)$ and taking G-invariants, we get a F-algebra which is central simple and is split by L as proved 2.3. We denote this algebra by (χ, b). We will show that this construction yields a cyclic algebra which is in accordance with our definition (4.1).

Before that let us first look at example 4.1.2 again using above construction. We keep the same notations.

Example 4.1.5. Consider the automorphism $\chi : G \to \mathbb{Z}/2\mathbb{Z}$, which maps $1 \mapsto 0$ and $\sigma \mapsto 1$. Fix $b = -1$, then $\widetilde{F}(b) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $z(b) : G \to PGL_2(\mathbb{C})$ maps

$\sigma \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. The twisted G-action on $M_2(\mathbb{C})$ is as follows:

$$\left(\sigma, \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} \\ \bar{x}_{21} & \bar{x}_{22} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \bar{x}_{22} & -\bar{x}_{21} \\ -\bar{x}_{12} & \bar{x}_{11} \end{pmatrix}.$$

Taking G-invariants of the twisted G-action on $M_2(\mathbb{C})$ we get the algebra

$$A' = \left\{ \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} \right\} \subset M_2(\mathbb{C}).$$

There is an isomorphism between A in the example 1.1.2 and A' given by $i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

One can follow the same process for quaternion algebra and symbol algebra but the calculation of G-invariants would become extremely difficult in case of symbol algebra. We will now prove this in general.

Proposition 4.1.6 (Proposition 2.5.2, [GS06]). *There is an element $y \in (\chi, b)$ constructed above such that (χ, b) is generated as a F-algebra by L and y, with the relations*

$$y^m = b, \qquad y\lambda = \sigma(\lambda)y$$

for all $\lambda \in L$, where σ is the generator of G mapped to 1 by χ.

Proof. Let us denote by A the algebra generated by y and L i.e. $A = \oplus_{i=0}^{i=n-1} Ly^i$, equipped with the given relations. We aim to prove that $(\chi, b) \simeq A$. Thus we define a F-algebra homomorphism $j : A \to M_n(L)$ and then verify that j maps A bijectively to (χ, b).

$$j(y) = \tilde{F}(b) \quad and \quad j(\lambda) = diag(\lambda, \sigma(\lambda), \ldots, \sigma^{n-1}(\lambda)) \; for \; \lambda \in L$$

We have already chosen $\tilde{F}(b)$ in such a way that $\tilde{F}^n = b.I_n$ and by matrix multiplication we can easily verify that j is indeed a homomorphism since

$$\tilde{F}(b)j(\lambda) = j(\sigma(\lambda))\tilde{F}(b). \tag{4.1}$$

Now we will verify that $j(A)$ comprises of elements which are G-invariant under the twisted action i.e $j(A)$ comprises of all those M such that $\tilde{F}(b)^{-1}\sigma(M)\tilde{F}(b) = M$. We check this on the generators of A, $\tilde{F}(b)$ satisfies the above relation. Also for $j(\lambda)$ since it satisfies the relation (4.1) above. Thus the image of $j(A)$ lands in (χ, b). Now all we need to verify is that $j : A \to (\chi, b)$ is an isomorphism. Since the dimension after tensoring with L is equal, verifying surjectivity will serve our purpose. The image of $j \otimes_L id_K$ in $(\chi, b) \otimes_F L \cong M_m(L)$ is the L- subalgebra generated by $\widetilde{F}(b)$ and the diagonal subalgebra $L \oplus \ldots \oplus L$. If $E_{i,j}$ is the usual basis of $M_m(L)$, we just need to check that $E_{i,j}s$ belong to this subalgebra for $i \neq j$. This is achieved by computing $E_{i,j} = \widetilde{F}(b)^{i-j} E_{j,i}$ for $i \neq j$.

□

4.1.2 Some Results

We will now see some results on when a given algebra is cyclic. First we will first mention some standard results which will be useful.

Proposition 4.1.7 (Proposition 2.2.8, [GS06]). *A central simple algebra A of degree n over a field F is split if and only if it contains a F-subalgebra isomorphic to the direct product $F \times \ldots \times F$.*

Lemma 4.1.8 (Speiser, Lemma 2.3.8, [GS06]). *Let $L|F$ be a finite Galois extension with group G, and V a F-vector space equipped with a semi-linear G-action, i.e. a G-action satisfying*

$$\sigma(\lambda\nu) = \sigma(\lambda)\sigma(\nu) \text{ for all } \sigma \in G, \nu \in V \text{ and } \lambda \in F.$$

Then the natural map

$$\lambda : V^G \otimes_F L \to V$$

is an isomorphism, where the superscript G denoted the invariants under G.

Theorem 4.1.9 (Skolem-Noether theorem, Lemma 2.5.4, [GS06]). *Let A be a central simple F-algebra of degree n containing a F-subalgebra L which is a cyclic Galois field extension of degree n. Then there exists $y \in A^*$ such that*

$$y^{-1}xy = \sigma(x) \tag{4.2}$$

for all $x \in L$, where σ is a generator of $G = Gal(L/F)$.

We use these results to prove the following proposition:

Proposition 4.1.10. *Let A be a central simple F-algebra of degree n containing a F-subalgebra L which is a cyclic Galois extension of degree n. Then A is isomorphic to a cyclic algebra given by*

$$A \simeq \oplus_{i=0}^{i=n-1} Ly^i$$

satisfying the relations

$$y^n = b, \qquad yl = \sigma(l)y$$

for all $\in L$, where σ is the generator of G and $b \in F$.

Proof. We are given a central simple algebra A of degree n containing a subfield L of dimension n over F. Consider the y in 4.1.9, we first verify that $y^m \in F$. We substitute $\sigma(x)$ in place of x for $x \in L$, in $\sigma(x) = y^{-1}xy$, and get $\sigma^2(x) = y^{-2}xy^2$. Iterating it $n-1$ times we get

$$x = \sigma^n(x) = y^{-n}xy^n$$

Thus y^n commutes with all $x \in L$ and hence it lies in L because $Z_A(L) = L$, L being the maximal commutative subring of A. Now again in 4.2 we put $x = y^n$, so we get $\sigma(y^n) = y^n$, that is, $y^n \in F$.

We set $b := y^n$. Now we just need to show that L and powers of y generate A. If $1, y, \ldots, y^{n-1}$ are L-linearly independent in A, where L acts by left multiplication. If this is not the case then there exists a non-trivial L-linear relation $\sum \lambda_i y^i = 0$ with least number of nonzero coefficients. We multiply by a power of y and assume that λ_o and λ_j for some $j \neq 0$ are not 0. Now we chose $l \in L^*$ with $l \neq \sigma(l)$. Again after iteration of 4.2 we get

$$\sum y^i \sigma^i(l)\lambda_i = l(\sum y^i \lambda_i) = 0.$$

Then $\sum y^i(l\lambda_i - \sigma^i(l)\lambda_i) = 0$ is a non-trivial L-linear relation with lesser nonzero coefficients, which is a contradiction. □

Now that we have proved the proposition, we can consider following as the definition of cyclic algebra.

Definition 4.1.11. *A central simple algebra A is cyclic if and only if there exists a strictly maximal subfield L of A such that E/F is a cyclic extension.*

Thus a cyclic algebra will always contain a maximal cyclic subfield but it can also contain other maximal subfields which are not cyclic. Here is an example.

Example 4.1.12. Consider a field extension $L = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$ where α is a root of the polynomial $x^4 - 4x^2 + 2$ over $\mathbb{Q}$. Roots of the polynomial are $\pm\sqrt{2+\sqrt{2}}$, and $\pm\sqrt{2-\sqrt{2}}$ all of which lie in $\mathbb{Q}(\alpha)$. The automorphism $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ over $\mathbb{Q}$ given by $\sigma(\sqrt{2+\sqrt{2}}) = -\sqrt{2-\sqrt{2}}$, and $\sigma(\sqrt{2-\sqrt{2}}) = \sqrt{2+\sqrt{2}}$ is of order 4. Therefore, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a cyclic Galois extension of degree 4.

Consider the cyclic algebra $A = (\mathbb{Q}(\alpha), \langle\sigma\rangle, 3)$ over $\mathbb{Q}$. By *Skolem-Noether theorem* let $z \in A^*$ be such that $\sigma(x) = z^{-1}xz$ for all $x \in L$ and $z^4 = 3$. Since $\mathbb{Q}(\alpha)^{\sigma^2} = \mathbb{Q}(\sqrt{2})$, we have $z^2 \in C_A(\mathbb{Q}(\sqrt{2}))$. Thus, $\mathbb{Q}(\sqrt{2}, z^2) \subset A$. As $(z^2)^2 = 3$, we have $\mathbb{Q}(\sqrt{2}, z^2) \cong \mathbb{Q}(\sqrt{2}, \sqrt{3}) \hookrightarrow A$.

Hence, A is a cyclic algebra of degree 4 containing both maximal 4-degree cyclic subfield as well as a maximal subfield that is biquadratic.

4.1.3 Cohomological Equivalence

We saw that cyclic algebra are particular case of a crossed product algebra. Cyclic algebra is a crossed product algebra with a finite cyclic Galois extension. The crossed product algebra is given with the help of a 2-cocycle. In this section we give an explicit mapping between a cyclic algebra and 2-cocycle corresponding to it.

Proposition 4.1.13 (§15.1, Proposition a, [Pie82])**.** *Let L/F be a cyclic extension such that $G =$ Gal(L/F) is cyclic of order n with the generator σ. If a central simple algebra A contains L as a maximal subfield, then there is an element u in A that satisfies*

1. $A = \oplus_{0 \leq j < n} Lu^j$.
2. $ul = \sigma(l)u$ *for all* $l \in L$, *and*
3. $u^n = b$ *where* $b \in F^*$.

Conversely, if A is the F-algebra that is defined by the conditions $1, 2$ *and* 3, *then* $A \cong (L, G, \phi_b)$, *where ϕ_b is a 2-cocycle from $G \times G \to L^*$ given by*

$$\phi_b(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } \ 0 \leq i, j, i+j < n, \\ b & \text{if } \ 0 \leq i, j < n \leq i+j. \end{cases}$$

Proof. ($\Rightarrow$) We have already proved the first part of the proposition in proposition 4.1.10.

($\Leftarrow$) For converse we first verify that ϕ_b is a 2-cocycle.

Now we give an isomorphism between (L, G, ϕ_b) and A

$$e_1 \mapsto 1_A$$
$$e_\sigma \mapsto u.$$

The map is well defined since ϕ_b is normalized. If $1 < j < n$, then $e_\sigma e_{\sigma^{j-1}} = \phi_b(\sigma, \sigma^{j-1}) e_{\sigma^j} = e_{\sigma^j}$. Therefore, $e_{\sigma^j} = u^j$ for all $1 \leq j < n$ by induction. Also, $u^n = e_\sigma e_{\sigma^{n-1}} = \phi_b(\sigma, \sigma^{n-1}) e_1 = b$. Thus, A is the algebra that satisfies $1, 2$ and 3. □

From now onwards we denote (L, G, ϕ_b) by (L, σ, b). As a consequence of the previous proposition we have the following corollaries:

Corollary 4.1.14. *We have* $(L, \sigma, a) \otimes_F (L, \sigma, b) \sim (L, \sigma, ab)$.

Proof. We have the 2-cocycles ϕ_a and ϕ_b satisfying $(\phi_a \phi_b)(x, y) = (\phi_a(x, y))(\phi_b(x, y))$. Thus, $\phi_a \phi_b = \phi_{ab}$. Hence, it follows that $(L, \sigma, a) \otimes_F (L, \sigma, b) \sim (L, \sigma, ab)$. □

Example 4.1.15. Let F be a field containing primitive nth root of unity, ξ. Let $(a,b)_{F,n}$ and $(a,c)_{F,n}$ be symbol algebras over F of degree n. By the above corollary $(a,b)_{F,n} \otimes_F (a,c)_{F,n} \sim (a,bc)_{F,n}$.

Corollary 4.1.16. *If $k \in \mathbb{Z}$ is co-prime to n, then $(L, \sigma^k, a^k) \cong (L, \sigma, a)$.*

Proof. Since k is co-prime to n, $G = \langle \sigma \rangle = \langle \sigma^k \rangle$. By, *Skolem-Noether theorem* $\sigma^k(x) = u^{-k}xu^k$ and $(\sigma^k)^n = 1$. Thus, $(u^k)^n = a^k$. □

Remark 4.1.17. *The cyclic algebra $(L, \sigma, 1)$ is split for any cyclic Galois extension L of F.*

Indeed, we have an explicit isomorphism from $(L, \sigma, 1) \to \text{End}_F(L)$ which suffices our purpose since $M_n(F) \simeq \text{End}_F(L)$. Consider the map $\phi : (L, \sigma, 1) \to \text{End}_F(L)$ given by

$$e_\sigma \mapsto \sigma$$
$$\lambda \mapsto l_\lambda$$

where both σ and l_λ are L-isomorphisms given by

$$\sigma(x) = \sigma \cdot x$$
$$l_\lambda(x) = \lambda x,$$

that is, σ has the usual G-action since σ lies in the Galois group of L/F. To verify that the given map is well defined we need to verify the cocycle condition.

$$\begin{aligned}
\phi(e_\sigma y)(x) &= \phi(\sigma(y)e_\sigma)(x) \\
&= \phi(\sigma(y))\phi(e_\sigma)(x) \\
&= l_{\sigma y} \circ \sigma(x) \\
&= \sigma(y)\sigma(x) \\
&= \sigma(yx) \\
&= \sigma(l_y(x)) \\
&= \phi(e_\sigma)\phi(y)(x).
\end{aligned}$$

Thus, the given map respects the algebra structure also note that map is injective. By dimension count, it is surjective as well.

Hence, we can say whenever there exists a cyclic Galois extension of degree n over F, there always exists a cyclic algebra over it, that is, $M_n(F)$.

4.1.4 The Primary Decomposition of Cyclic Algebras

In this section we will prove that A is cyclic if and only if its primary components are cyclic. Before proving we will state two lemmas which will be useful in proving the result.

Lemma 4.1.18. *Let L_1/F and L_2/F be finite field extensions where L_1 and L_2 are subfields of the algebraic closure of F.*

1. *If $[L_1 : F]$ and $[L_2 : F]$ are relatively prime, then L_1 and L_2 are linearly disjoint over F.*

2. *If L_1/F and L_2/F are Galois, and L_1 and L_2 are linearly disjoint over F, then $(L_1 \otimes L_2)/F$ is Galois and $G((L_1 \otimes L_2)/F) \cong G(L_1/F) \times G(L_2/F)$.*

3. *If L/F is Galois, Gal$(L/F) = H_1 \times H_2$, L_1 is the fixed field of H_1 and L_2 is the fixed field of H_2. Then, L_1 and L_2 are linearly disjoint over F. $L = L_1 \otimes L_2$, L_1/F and L_2/F are Galois and $G(L_1/F) = H_1$ and $G(L_2/F) = H_2$.*

Lemma 4.1.19. *Let L_1/F and L_2/F be cyclic extensions with $G(L_1/F) = \langle\sigma_1\rangle$ and $G(L_2/F) = \langle\sigma_2\rangle$. Assume that $n_1 = [L_1 : F]$ is relatively prime to $n_2 = [L_2 : F]$, say $n_1a + n_2b = 1$ where $a, b \in \mathbb{Z}$. If $y \in F^*$, then $(L_1, \sigma_1, y^a) \otimes_F (L_2, \sigma_2, y^b) \simeq ((L_1 \otimes L_2), (\sigma_1, \sigma_2), y)$.*

Now we will prove the main result which will be useful in the coming section in proving cyclicity of degree 6 algebra.

Proposition 4.1.20. *If A and B are central simple algebras over F of relatively prime degrees. Then, $A \otimes_F B$ is cyclic if and only if A and B both are cyclic.*

Proof. Let degree$(A) = n_1$ and degree$(B) = n_2$ where $n_1a + n_2b = 1, a, b \in \mathbb{Z}$. $(\Rightarrow)$ Let $A \otimes B = (L, \sigma, y)$, where $y^{mn} \in F^*$ and $G(L/F) = \langle\sigma\rangle$. Under the correspondence $\sigma \mapsto (\sigma^{n_2b}, \sigma^{n_1a})$, we get $\langle\sigma\rangle \cong \langle\sigma^{n_2b}\rangle \times \langle\sigma^{n_1a}\rangle$. Let L_1 be the fixed field of σ^{n_2b} and L_2 be the fixed field of σ^{n_1a}. By lemma 4.1.18 $L = L_1 \otimes L_2$, and $G(L_1/F) = \langle\sigma^{n_2b}\rangle$, and $G(L_2/F) = \langle\sigma^{n_1a}\rangle$. Using corollary 4.1.14 we have $A_1 = (L_1, \sigma^{n_2}, y) \cong (L_1, \sigma^{n_2b}, y^b)$ and $B_1 = (L_2, \sigma^{n_1}, y) \cong (L_2, \sigma^{n_1a}, y^a)$. By lemma 4.1.19, $A_1 \otimes B_1 \cong (L_1 \otimes L_2, (\sigma^{n_2b}, \sigma^{n_1a}), y) = (L, \sigma, y) = A \otimes B$. Since Deg$(A_1) =$ Deg$(A) = n_1$ and Deg$(B_1) =$ Deg$(B) = n_2$, it follows that in the Brauer group, $[A] = [A][A]^{-an_1}[B]^{bn_2} = ([A][B])^{bn_2} = [A \otimes B]^{n_2b} = [A_1 \otimes B_1]^{bn_2} = [A_1]$. Similary we get $[B] = [B_1]$. Since the dimension of A is same as of A_1 and dimension of B is same as of B_1. So, A and B are cyclic.

$(\Leftarrow)$ If A and B are cyclic, then using lemmas 4.1.18 and 4.1.19 $A \otimes B$ is also cyclic. □

Corollary 4.1.21. *A central division algebra is cyclic if and only if its primary components are cyclic.*

4.2 The Cyclicity Question

Now we will address the central question for which the basics have been build so far. This section mostly discusses a survey article by Saltman in detail (cf. [Sal05]). The main question in the article is following.

Question 4.2.1. *Whether every division algebra is cyclic?*

This question has a negative answer. We will give an explicit example of a non-cyclic division algebra. Let us first see a result on the condition when a division algebra is cyclic.

Theorem 4.2.2. *A division algebra D/F is cyclic if and only if there is a subfield $L \subset D$ of degree $\deg(D)$ over F which is cyclic over F.*

Proof. Since we have already proved proposition 4.1.10, this theorem is a corollary of it as division algebras are special type of central simple algebras. □

4.2.1 Non-cyclic division algebra

In this section we give an explicit example of a non-cyclic division algebra. We use some results from the theory formally real fields and valued fields. All the results mentioned here are referred from (Chapter VI and Chapter VIII, [Lam05]).

Definition 4.2.3 (Pythagorean field)**.** *A field F pythagorean if sum of squares is again a square, i.e., $F^2 + F^2 \subseteq F^2$.*

If $\text{char}(F) = 2$, we have $a^2 + b^2 = (a + b)^2$, so F is always pythagorean. We will use a field that is *formally real pythagorean field*, i.e., pythagorean field where -1 can not be written as a sum of squares. For example, the field of real numbers $\mathbb{R}$ is a formally real pythagorean field whereas complex numbers $\mathbb{C}$ is pythagorean but not formally real. We denote the Laurent series field of F by $F((t))$. It consists of all formal Laurent series of the form

$$f = a_n t^n + a_{n+1} t^{n+1} + \dots \quad (n \in \mathbb{Z}, a_i \in F)$$

Proposition 4.2.4. *Let F be a formally real pythagorean field and $F_1 = F((t))$. Then, F is a pythagorean field if and only if F_1 is.*

Proof. ($\Leftarrow$) Let F_1 be a formally real pythagorean. Then F is also formally real. Moreover F_1 follows the pythagorean property for all values of t. In particular for $t = 0$. Thus, F is also pythagorean.

($\Rightarrow$) Assume F is formally real pythagorean. Consider $f^2+g^2 \in F_1$, where

$$f = a_n t^n + a_{n+1}t^{n+1} + \dots, \quad g = b_m t^m + b_{m+1}t^{m+1} + \dots, \quad a_n \neq 0 \neq b_m.$$

Assume $n < m$, then $f^2+g^2 = (a_n t^n)^2(1+\dots)$ which is a square in F_1. Now assume $m = n$, and write

$$a_n^2 + b_n^2 = c_n^2 (c_n \in F^*).$$

Thus, we have $f^2+g^2 = (c_n t^n)^2(1+\dots)$, which is again a square in F_1. □

Lemma 4.2.5. *Let L/F be a cyclic Galois extension of degree 4. Then there is a unique intermediate field $F \subseteq K \subseteq L$ such that $K = F\sqrt{a}$ with $a \in F^*$, and a is a sum of squares.*

We will state *Springer's theorem*, but we will first define what a valuation on a field is.

Definition 4.2.6 (Valuation)**.** *Let F be a field and let Γ be a totally ordered abelian group. A valuation on F is any map*

$$v : F \to \Gamma \cup \{\infty\}$$

which satisfies the following properties for all $a, b \in F$:

1. *$v(a) = \infty$ if and only $a = 0$.*

2. *$v(ab) = v(a) + v(b)$*

3. *$v(a+b) \geq min(v(a), v(b))$ with equality if $v(a) \neq v(b)$.*

We associate with a valuation following rings:

- A valuation ring, $\mathcal{O}_v = \{x \in F : v(x) \geq 0\}$

- A unique maximal ideal, $\mathfrak{m}_v = \{x \in F : v(x) > 0\} \subset \mathcal{O}_v$

- A residue class field, $\overline{F} = \mathcal{O}_v/\mathfrak{m}_v$.

- The group of units of $\mathcal{O}_v$, $U = \{x \in F^* : v(x) = 0\}$.

The image of $x \in \mathcal{O}_v$ in the residue field is denoted by $\overline{x}$. We are interested in valuation with the value group, $\Gamma = \mathbb{Z}^r$ for some natural number r. A valuation is called *discrete* if the value group is $\mathbb{Z}$. For a discrete valuation v, an element $\pi \in \mathfrak{m}_v$ with $v(\pi) = 1$ is called a *uniformizer* of F.

Theorem 4.2.7 (Springer's theorem). *Let F be a complete discrete valued field such that char($\overline{F}$) $\neq 2$. Suppose that $\phi = q_1 \perp \langle \pi \rangle q_2$, where $q_1 = \langle u_1, \ldots, u_r \rangle$ and $q_2 = \langle u_{r+1}, \ldots, u_n \rangle$ ($u_i \in U$). Then q is anisotropic over F if and only if $\overline{q_1}$ and $\overline{q_2}$ are anisotropic over $\overline{F}$.*

Example 4.2.8 (Non-cyclic division algebra). Let $F = \mathbb{R}((x))((y))$, and $B = \left(\frac{-1,-1}{F}\right)$, $C = \left(\frac{x,y}{F}\right)$. Consider the biquaternion algebra $A = B \otimes_F C$. By using theorem 1.3.12 we can show that the algebra A is a division algebra. Thus, we need to verify that the Albert form q of $B \otimes_F C$ is anisotropic over $\mathbb{R}((x))((y))$. Viewing $\mathbb{R}((x))((y))$ as $L((y))$, where $L = \mathbb{R}((x))$, the Albert form

$$\begin{aligned} q &\cong \langle 1, 1, 1, x, y, -xy \rangle \\ &\cong \langle 1, 1, 1, x \rangle \perp \langle 1, -x \rangle \langle y \rangle \end{aligned}$$

By (theorem 4.2.7, applied to y-adic valuation on $L((y))$), q is anisotropic if and only if $\langle 1, 1, 1, x \rangle$ and $\langle 1, -x \rangle$ are anisotropic over $\mathbb{R}((x))$. Again by (theorem 4.2.7, applied to x-adic valuation on L), $\langle 1, 1, 1, x \rangle$ (respectively $\langle 1, -x \rangle$) is anisotropic if and only if $\langle 1, 1, 1 \rangle$ and $\langle 1 \rangle$ (respectively $\langle 1 \rangle$ and $\langle -1 \rangle$) are anisotropic over $\mathbb{R}$. Since $\mathbb{R}$ is a formally real, the quadratic forms $\langle 1, 1, 1 \rangle$, $\langle 1 \rangle$ and $\langle -1 \rangle$ are indeed anisotropic. Hence, by Albert's theorem(1.3.12) A is a division algebra.

If A is a cyclic algebra, then it contains a degree 4 cyclic Galois extension L over F. By (lemma 4.2.5) L will have a unique proper subfield of the form $K = F\sqrt{r^2 + s^2}$ over F. Since F is a formally real pythagorean field (cf. proposition 4.2.4), $K = F$ which is a contradiction. Hence, A must be a non-cyclic division algebra.

4.3 Prime Degree Division Algebras

In this section we first prove that degree 2 and 3 division algebras are cyclic.

Division algebras of degree 2 are cyclic We have already seen in chapter 1 §3.5, that degree 2 division algebras over any field are precisely quaternion algebras which are cyclic.
Thus, *degree 2 division algebras over any field are always cyclic.*

4.3.1 Factorization theorem

In this section we follow Chapter 5, [Lam91]. Let R be any ring with identity, and $R[t]$ denote the polynomial ring in one variable t over R, where t commutes elementwise with R. For a polynomial

$$f(t) = \sum_{i=0}^{n} a_i t^i$$

and an element $r \in R$, we define $f(r) := \sum_{i=0}^{n} a_i r^i \in R$. Note that to evaluate $f = gh \in R[t]$ at $r \in R$ we first write f in the form $\sum a_i t^i$, and then substitute r for t.

Definition 4.3.1. *An element $r \in R$ is said to be a right root of $f \in R[t]$ if $f(r) = 0$.*

- In general, if $f = gh$ it does not follow that $f(r) = g(r)h(r)$. Indeed, consider a division algebra D with center F, and $d, d_1 \in D \setminus \{0\}$ are such that $dd_1 \neq d_1 d$. Put $g(t) = (t - d)$, and $h(t) = (t - d_1)$. Then $g(D)h(D) = 0$, while

$$\begin{aligned} gh(d) &= (t^2 - (d + d_1)t + dd_1)|_{t=d} \\ &= d^2 - d^2 - d_1 d + dd_1 \\ &= dd_1 - d_1 d \\ &\neq 0. \end{aligned}$$

- Over a field, a polynomial of degree n has at most n distinct roots. Over a division algebra, this is no longer true. For instance, in the Hamiltonian division algebra $\mathbb{H}$ over $\mathbb{R}$, any conjugate of i is a root of $t^2 + 1$, since i has infinitely ,any conjugates, $t^2 + 1$ has infinitely many roots.

- If $f = \sum a_i t^i \in F[t]$, and $d \in D$ is a root of f, then any comjugate zdz^{-1} is also a root. Indeed, $zf(t)z^{-1} = \sum z a_i t^i z^{-1} = \sum a_i (ztz^{-1})^i$ (since $za_i = a_i z$). Also, $zf(t)z^{-1} = f(t)$.

Definition 4.3.2. *We say that a conjugacy class A is algebraic over F if one (and hence all) of its elements is algebraic over F.*

Lemma 4.3.3. *Let D be a division ring and let $f = gh \in D[t]$. Let $d \in D$ be such that $a := h(d) \neq 0$. Then*

$$f(d) = g(ada^{-1})h(d).$$

In particular, if d is a root of f but not of h, then ada^{-1} is a root of g.

Proof. Let $g = \sum b_i t^i$. Then $f = \sum b_i h(t) t^i$, so

$$\begin{aligned} f(d) &= \sum b_i h(d) d^i = \sum b_i a d^i \\ &= \sum b_i a d^i a^{-1} a \\ &= \sum b_i (ada^{-1})^i a \\ &= g(ada^{-1})h(d). \end{aligned}$$

Since D is a division algebra, if d is a root of f but not of h, then ada^{-1} is a root of g. □

Lemma 4.3.4. *For $f(t) \in D[t]$ and $d \in D$, we have*

$$f(t) = q(t)(t-d) + f(d).$$

In particular, d is a root of f if and only if $t-d$ divides f.

Proof. We proceed by induction on deg $f(t)$. If deg $(f(t)) = 1$, $f(t) = at + b$, then $f(t) = a(t-d) + ad + b$, i.e., we can take $q(t) = a$. Suppose $degf = n > 1$ and $d_n \in D$ be the leading coefficient of $f(t)$. Put $g(t) = f - d_n t^{n-1}(t-d)$, then $deg\ g < degf$, and $f(d) = g(d)$. Thus, by the induction there exists $q_1 \in D[t]$ such that $g(t) = f(t) - d_n t^{n-1}(t-d) = q_1(t-d) + g(d)$. Hence, $f(t) = (q_1 + d_n t^{n-1})(t-d) + f(d)$. □

Proposition 4.3.5. *Let D be a division ring and let f be a polynomial of degree n in $D[t]$. Then the roots of f lie in at most n conjugacy classes of D. If $f = \prod_{i=1}^{i=n}(t-a_i)$, where $a_i \in D$, then any root of f is some conjugate of a_i.*

Proof. We induct on n, the degree of polynomial f. If $n = 1$, then $f = t - a$, and proposition is clear. For $n \geq 2$, let $d \in D$ be a root of f, and write $f = g(t)(t-d)$. Suppose $d' \neq d$ is another root of f. Then by lemma 4.3.3, d' is conjugate root of g. By induction hypothesis, d' lies in at most $n-1$ conjugacy classes of D. Hence, roots of f lie in at most n conjugacy classes of D. □

Proposition 4.3.6. *Let D be a central division algebra over F and A be a conjugacy class of D which is algebraic over F with minimal polynomial $f \in F[t]$. If a polynomial $h \in D[t] \setminus \{0\}$ vanishes identically on A, then $degh \geq degf$.*

Proof. Let $h = t^m + d_1 t^{m-1} + \ldots + d_m \in D[t]$ be such that $h(A) = 0$ and $m = degh < degf$ is as small as possible. Since $h \notin F[t]$ there exists some $d_i \notin F$, and $s \in D$ such that $d_i s \neq s d_i$. For any $a \in A$, $h(a) = a^m + d_1 a^{m-1} + \ldots + d_m = 0$. Hence

$$0 = (sas^{-1})^m + d_1(sas^{-1})^{m-1} + \ldots + d_m.$$

On the other hand, using $sd_j a^{m-j} s^{-1} = sd_j s^{-1} s a^{m-j} s^{-1} = (sd_j s^{-1})(sas^{-1})^{m-j}$ we also have

$$0 = (sas^{-1})^m + (sd_1 s^{-1})(sas^{-1})^{m-1} + \ldots + (sd_m s^{-1}).$$

Hence the polynomial

$$\sum_{j=1}^{m} (d_j - sd_j s^{-1}) t^{m-j}$$

vanishes on $sAs^{-1} = A$. Since $d_i s \neq s d_i$, the above polynomial is nonzero, and its degree $< m$. This contradicts the choice of m. □

Theorem 4.3.7 (Wedderburn's factorization theorem)**.** *Let D be a central division algebra over F, let A be a conjugacy class of D which is algebraic over F with minimal* *polynomial $f \in F[t]$ of degree n. Then there exists $a_1, \dots, a_n \in A$ such that $f = \prod_{i=1}^{n}(t - a_i) \in D[t]$. Also, f is product of the same linear factors, permuted cyclically. The element $a_1 \in A$ can be arbitarily prescribed.*

Proof. Fix $a_1 \in A$, and consider a factorization of f

$$f = g(t)(t - a_r) \dots (t - a_1)$$

with $g \in D[t]$, $a_i \in A$, where r is chosen as large as possible. We claim that $h = (t - a_r) \dots (t - a_1)$ vanishes identically on A. Indeed, for $a \in A$ we have $f(a) = 0$. If $h(a) \neq 0$ then by lemma 4.3.3, $g(a_{r+1}) = 0$ for a conjugate a_{r+1} of a. Then we can write $g = g_1(t)(t - a_{r+1})$ for some $g_1 \in D[t]$, and thus f has a right factor $(t - a_{r+1})(t - a_r) \dots (t - a1)$, which contradicts with choice of r. Hence $h(a) = 0$ for every $a \in A$. Hence by proposition 4.3.6, $degf \geq degh \geq degf$, i.e., $f(t) = \prod_{i=0}^{n}(t - a_i)$.

To prove the last assertion, we show that for $f \in F[t]$ if $f = gh \in D[t]$, then $f = hg \in D[t]$. Indeed, for $g \in D[t]$, we have $gf = fg$ since coefficients of f are in F. Thus, $gf = fg = ghg$, i.e., $g(f - hg) = 0 \in D[t]$. Hence, $f = hg$. □

4.3.2 Division algebras of degree 3 are cyclic

This section is followed from the exercises based on Chapter 24, [Row08].

Lemma 4.3.8. *Let $a, b \in D$ with $v = ab - ba \neq 0$. Then $vav^{-1} = b$ if and only if $(a + b)ba = ba(a + b)$.*

Proof. We have

$$\begin{aligned} vav^{-1} &\Leftrightarrow va = bv \\ &\Leftrightarrow (ab - ba)a = b(ab - ba) \\ &\Leftrightarrow ab - ba^2 = bab - b^2a \\ &\Leftrightarrow aba + b^2a = bab + ba^2 \\ &\Leftrightarrow (a + b)ba = ba(b + a) \\ &\Leftrightarrow (a + b)ba = ba(a + b). \end{aligned}$$

□

Lemma 4.3.9. *Let d_1 be a root of $f(t) = (t - d_3)(t - d_2)(t - d_1) \in F[t]$, and $d_1d_2 \neq d_2d_1$. Then*

$$d_3 = (d_1d_2 - d_2d_1)d_2(d_1d_2 - d_2d_1)^{-1}.$$

Moreover, for $i, j \in \mathbb{Z}/3$ we have

$$d_id_j - d_jd_i \in \{(d_1d_2 - d_2d_1), -(d_1d_2 - d_2d_1)\}.$$

Proof. Let $g(t) = (t - d_2)(t - d_1) = t^2 - (d_1 + d_2)t + d_2 d_1$. Thus, $f(t) = (t - d_3)g(t)$. Consider $g(d_2) = d_2^2 - (d_1 + d_2)d_2 + d_2 d_1 \neq 0$, i.e. d_2 is not a root of $g(t)$. By lemma 4.3.3, $(-d_1 d_2 + d_2 d_1)d_2(-d_1 d_2 + d_2 d_1)^{-1}$ must be a root of $(t - d_3)$, so $d_3 = (-d_1 d_2 + d_2 d_1)d_2(-d_1 d_2 + d_2 d_1)^{-1}$.

For the second part, we put $b = d_1 d_2 - d_2 d_1$. We have $d_1 + d_2 + d_3 = \alpha \in F$. Consider $i, i+1, i+2 \in \mathbb{Z}/3$, and

$$\begin{aligned} d_i d_{i+1} - d_{i+1} d_i &= d_i(\alpha - d_i - d_{i+2}) - (\alpha - d_i - d_{i+2})d_i \\ &= d_i \alpha - d_i^2 - d_i d_{i+2} - \alpha d_i + d_i^2 + d_{i+2} d_i \\ &= d_{i+2} d_i - d_i d_{i+2} \end{aligned}$$

Therefore, we get

$$d_2 d_3 - d_3 d_2 = d_1 d_2 - d_2 d_1 = d_3 d_1 - d_1 d_3 = b.$$

While,

$$d_1 d_3 - d_3 d_1 = d_1(\alpha - d_1 - d_2) - (\alpha - d_1 - d_2)d_1 = d_2 d_1 - d_1 d_2 = -b.$$

□

Lemma 4.3.10. *Let A be a central division algebra over F. There exists $0 \neq a \in A$ such that $\mathrm{Trd}_A(a) = 0$.*

Proof. By (theorem 3.2.8), there exists $a \in A$ such that $[F(a) : F] = n$. Since D is non-commutative there exists $b \in A \setminus F(a)$ such that $ab \neq ba$. We have

$$\phi : F(a) \to F, \quad x \mapsto \mathrm{Trd}_A(x(ab - ba)).$$

Thus, $\ker \phi \neq \{0\}$. □

Proposition 4.3.11. *A central division algebra of degree 3 is cyclic.*

Proof. Let D be a central division algebra of degree 3. By previous lemma, we get an element $d_1 \in A \setminus F$ such that $\mathrm{Trd}_D(d_1) = 0$. Let $f(t) \in F[t]$ be the minimal polynomial of d_1 over F. By Wedderburn's Factorization theorem, we can write $f = (t - d_3)(t - d_2)(t - d_1)$. Put $b = d_1 d_2 - d_2 d_1$, and $d_3 = b d_2 b^{-1}$ and $d_3 d_2 - d_2 d_3 = -(d_1 d_2 - d_2 d_1) = -b$. Also,

$$f = (t - d_1)(t - d_3)(t - d_2),$$

consequently $d_1 = bd_3b^{-1}$. Since $d_1 + d_2 + d_3 = 0$ we have

$$\begin{aligned} b(d_3d_2^{-1})b^{-1} &= bd_3b^{-1}bd_2^{-1}b^{-1} \\ &= d_1d_3^{-1} \\ &= (-d_2 - d_3)d_3^{-1} \\ &= -1 - d_2d_3^{-1}. \end{aligned}$$

Hence, $K = F[d_3d_2^{-1}]$ has a nontrivial automorphism over F given by conjugation by b, and thus cyclic. Therefore, $D \cong (K/F, Int(b), b^3)$, and hence D is a cyclic algebra. □

Corollary 4.3.12. *Division alegbra of degree* 6 *over any field F is always cyclic.*

Proof. We have already seen that division algebras of degree 2 and 3 are cyclic. With help of proposition 4.1.20, degree 6 division algebras are also cyclic. □

4.3.3 Cyclicity of higher degree division algebras and open questions

We have already seen degree two and three algebras are cyclic. The question now arises for higher prime degree division algebras. We first state some results regarding their cyclicity.

Theorem 4.3.13 (Albert). *Let D be a prime degree p division algebra over F. Then D/F is cyclic if and only if there is a $d \in D \setminus F$ such that $d^p \in F$.*

A division algebra over a field of characteristic p is called *p-algebra* if its degree is p-primary. We now state a characterization of p-algebra in terms of existence of a purely inseparable maximal field extension. More precisely, we have the following result.

Theorem 4.3.14 (Hood, [Hoo71]). *Suppose that D is a central division p-algebra over F. Then D is cyclic if and only if there is a subfield $L \subset D$ such that L/F is purely inseparable and has degree equal to* $\deg(D)$.

In the other direction, we consider a division algebra of prime degree p over a field of characteristic different from p. We have the following criterion for cyclicity in terms of multiplicative group structure of D^*.

Theorem 4.3.15 (Mahdavi-Hezavehi, Tignol, [MHT03]). *Suppose D has prime degree p not equal to the characteristic of F. Then D is cyclic if and only if the multiplicative group D^* contains a metabelian, nonabelian subgroup.*

We have already seen that degree 2 and 3 division algebras are cyclic. For degree 5 division algebras, all dihedral division algebras are cyclic [RS82]. But in general, and for higher prime degree algebras cyclicity is now known.

The study of a cyclic algebra is an intense area of research. We now state some open problems as stated in [Sal05] related to cyclicity question.

Question 4.3.16. *Suppose D is a division algebra over F of prime degree p. Is D cyclic?*

The above problem is elaborated in [ABGV11].

Question 4.3.17. *Suppose D/F is a division algebra of degree n, and K/F is a finite extension of degree prime to n. Assume $D \otimes_F K$ is cyclic. Does this imply D is cyclic?*

Bibliography

[ABGV11] Asher Auel, Eric Brussel, Skip Garibaldi, and Uzi Vishne, *Open problems on central simple algebras*, Transform. Groups **16** (2011), no. 1, 219–264. MR 2785502

[Ber10] Grégory Berhuy, *An introduction to Galois cohomology and its applications*, London Mathematical Society Lecture Note Series, vol. 377, Cambridge University Press, Cambridge, 2010, With a foreword by Jean-Pierre Tignol. MR 2723693

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR 2266528 (2007k:16033)

[Hoo71] J. Myron Hood, *Central simple p-algebras with purely inseparable subfields*, J. Algebra **17** (1971), 299–301. MR 0269690

[Jah] Jörg Jahnel, *The Brauer-Severi variety associated with a central simple algebra: a survey*, `https://www.math.uni-bielefeld.de/lag/man/052.pdf`.

[Lam91] T. Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 1991. MR 1125071

[Lam05] ———, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005. MR 2104929

[MHT03] M. Mahdavi-Hezavehi and J.-P. Tignol, *Cyclicity conditions for division algebras of prime degree*, Proc. Amer. Math. Soc. **131** (2003), no. 12, 3673–3676. MR 1998187

[Pie82] Richard S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York-Berlin, 1982, Studies in the History of Modern Science, 9. MR 674652

[Row08] Louis Halle Rowen, *Graduate algebra: noncommutative view*, Graduate Studies in Mathematics, vol. 91, American Mathematical Society, Providence, RI, 2008. MR 2462400

[RS82] Louis H. Rowen and David J. Saltman, *Dihedral algebras are cyclic*, Proc. Amer. Math. Soc. **84** (1982), no. 2, 162–164. MR 637160

[Sal05] David J. Saltman, *The cyclicity question*, Algebra and number theory, Hindustan Book Agency, Delhi, 2005, pp. 116–125. MR 2193348

[SR] Parimala R. Sridharan R., 2- *torsion in Brauer groups: a theorem of Merkurjev*, `www.math.ethz.ch/~knus/sridharan/merkurjev84.pdf`.