INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH, MOHALI

A study on central simple algebras

by

Jayanth Guhan

A dissertation submitted for the partial fulfilment of
BS-MS dual degree in Mathematics
under the guidance of
Prof. Varadharaj Srinivasan
Department of Mathematics

April 2017

Certificate of Examination

This is to certify that the dissertation titled **"A study on central simple algebras"** submitted by **Jayanth Guhan** (Reg. No. MS12104) for the partial fulfillment 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. Chetan Balwe Dr. Chandrakant Aribam Dr. Varadharaj Srinivasan

(Supervisor)

Dated: April 2017

Declaration of Authorship

The work presented in this dissertation has been carried out by me under the guidance of Dr. Varadharaj Srinivasan 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. This work is based on the research article on "Division Algebras Of Degree 4 And 8 With Involution", *Israel Journal Of Mathematics, Vol.33, No.2, 1979*, by S.A. Amitsur, L.H. Rowen, J.P. Tignol. 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.

Jayanth Guhan

(Candidate)

Dated: April 2017

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

Dr. Varadharaj Srinivasan

(Supervisor)

Abstract

The main goal of this thesis is to understand the paper [1] on "Division Algebras of Degree 8 with Involutions" by S. A. Amitsur, J.P. Tignol and L.H. Rowen. To this end we set up the foundations of central simple algebras and explore their properties. We shall discuss the Artin-Wedderburn Theorem, the Skolem-Noether Theorem, and some consequences of the same. Further in, we shall define the Brauer group of a field, and what it means to split a central simple algebra. We shall discuss the existence of Galois splitting fields, and then move on to discuss Brauer Groups of certain fields, concluding with Chevalley's Theorem.

For a central simple F-algebra A, the dimension $[A : F]$ is a perfect square, say n^2. The number n is called the degree of the central simple F-algebra. A central simple F-algebra is defined to be a quaternion algebra, if $n = 2$. An involution (of the first kind) of A is an antiautomorphism of degree 2 fixing F. It can be shown that, any central simple algebra with involution has degree 2^m for some m. A tensor product of quaternion sublagebras with involutions results in a central simple algebra of degree 2^m, with the natural involution. Conversely, if a central simple F-algebra with an involution has degree 2^m for some m, can it always be written as a tensor product of quaternion F-algebras? We set up the necessary and sufficient conditions for a central simple F-algebra to have involutions, and to be tensor products of quaternion algebras. We use these conditions on "generic abelian crossed products" to construct a counterexample; a division algebra of degree 8 with involution, which cannot be expressed as the tensor product of quaternion subalgebras.

[1] *S.A. Amitsur, L.H. Rowen, J.P. Tignol, Division Algebras Of Degree* 4 *And* 8 *With Involution, Israel Journal Of Mathematics, Vol.33, No.2, 1979.*

Acknowledgements

I'd like to express my gratitude to my supervisor, Prof. Varadharaj Srinivasan, for giving me a well-thought out problem in an area of my preference, and have me prepare and present the topic until I was deeply familiar with it. In addition, I'd like to thank Prof. Amit Kulshrestha and Abhay Soman for their engaging discussions and their general feedback.

I'd like to mention my friends, Ketika Garg, Mishty Ray, and Satya Spandana for their constant moral support. I am deeply thankful for Sri Pujha's never ending encouragement and for being a constant source of inspiration. Lastly, I am grateful for my parents' unwavering faith in my abilities throughout the course of this year.

Contents

Chapter 1

Preliminaries

In this chapter, we open up with some preliminaries, discussing the basic structure of semisimple and simple rings. Using the Artin-Wedderburn theorem, one can lay out a definitive structure for all finite dimensional central simple algebras. We shall briefly discuss the lemmas and propositions necessary to prove the Artin-Wedderburn theorem and its consequences. The proofs which are omitted in this chapter can be found in [1].

1.1 Semi-Simple Modules

Definition 1.1. Let A be a ring. An A-module M is said to be simple if it has no non-trivial submodules. An A-module M is semi-simple if it can be written as a sum of a family of simple A-submodules.

Lemma 1.2 (Schur)**.** *Let A be a ring and $f : M \to N$ be an A-linear map, where M and N are A-modules.*

a) If M is simple, then either $f = 0$ or f is injective.

b) If N is simple, then either $f = 0$ or f is surjective.

Corollary 1.3. *The endomorphism ring of a simple module is a division ring.*

Remark. The homomorphic image of a semi-simple module will also be a semi-simple module. This is a simple consequence of Schur's Lemma; any map between two simple modules is either an isomorphism or trivial. Thus, the image of a semi-simple module M can be written as a sum of simple modules, which are isomorphic images of simple submodules of M.

We state the following theorem without proof;

Theorem 1.4. *Let A be a ring, and M an A-module. Then, the following conditions are equivalent:*

a) M is a semi-simple A-module.

b) M is a direct sum of simple modules.

c) Every submodule of M is direct summand of M.

Corollary 1.5. *Every submodule of a semi-simple module is semi-simple.*

Remark. a) If $M = \sum_{i \in I} S_i$ with S_i simple and S is a simple submodule of M, then S is isomorphic to S_i for some $i \in I$.

b) If $M = S_1 \oplus S_2 \oplus \cdots S_n = T_1 \oplus T_2 \oplus \cdots T_m$, then $n = m$ and there exists a permutation σ of $\{1, 2, 3 \cdots n\}$ such that $S_i = T_{\sigma(i)}$, for all $i \in \{1, 2, 3 \cdots n\}$.

Definition 1.6. Let S be a simple A-module. An A-module M is said to be isotypical of type S, if M is the sum of a family of simple submodules each of which is isomorphic to S.

Let $M = \bigoplus_{i \in I} S_i$, where S_i is simple for all $i \in I$. By collecting all isomorphic S_i's together, we can write $M = \bigoplus_{\gamma \in \Gamma} M_\gamma$, where each M_γ is the direct sum of submodules isomorphic to S_γ, where $S_\gamma \neq S_{\gamma'}$ for $\gamma \neq \gamma'$. The submodules M_γ are called the isotypic components of M. It can be further shown that every M_γ is the sum of all submodules of M which are isomorphic to S_γ.

We state the following without proof;

Theorem 1.7. *Let M be a semi-simple A-module with isotypical components $\{M_\gamma\}_{\gamma\in\Gamma}$. Then, $End_A(M) \cong \prod_{\gamma\in\Gamma} End_A(M_\gamma)$.*

Theorem 1.8. *Let M be an A-module and $M = M_1 \oplus M_2 \oplus \cdots M_n$, where each M_i is isomorphic to an A-module N. Then $End_A(M) \cong \mathbb{M}_n(End_A(N))$.*

Corollary 1.9. *Let M be semi-simple A-module of length n, isotypical of type S. Then $End_A(M) \cong \mathbb{M}_n(D)$, where D denotes the (division) ring of endomorphisms of S.*

1.2 The Artin-Wedderburn Theorem

Definition 1.10. A ring A is semi-simple if it semi-simple as a left module over itself.

Remark. a) It can be shown that a ring A is semi-simple if and only if every A-module is semi-simple.

b) Every semi-simple ring can be written as a direct sum of a finite number of simple left ideals.

Theorem 1.11. *A semi-simple ring is a finite direct product of matrix rings over division rings.*

Proof. Let A be a semi-simple ring. Then, we can write A as a finite direct sum of simple ideals, say; $A = S_1 \oplus S_2 \oplus S_3 \oplus \cdots S_n$. We observe that A as an A-module will have finite length as a result. Let $M_1, M_2, \cdots M_r$ be the isotypical components of A. Then, as we have seen before, $End_A(A) \cong \prod_{i=1}^{r} End_A(M_i)$. Since $End_A(A) \cong A^\circ$, (where A° is the opposite ring of A), and $End_A(M_i)$ is isomorphic to a matrix ring over a division ring, it follows that A° is isomorphic to a finite product of matrix rings over division rings. Therefore, A must be isomorphic to a finite product of matrix rings over division rings. □

Definition 1.12. A ring A is said to simple if it is semi-simple and has no non-trivial two-sided ideals.

Theorem 1.13 (Wedderburn)**.** *A ring is simple if and only if it isomorphic to* $\mathbb{M}_n(D)$*, for some division ring* D*. The integer* n *and (upto isomorphism) the division ring* D *are uniquely determined.*

Proof. For the sake of brevity, we shall omit the proof of uniqueness from the theorem. Let A be a simple ring. By the Artin-Wedderburn Theorem, it must be isomorphic to a finite product of matrix rings over division rings. But, since A has no non-trivial two-sided ideals, the number of factors is such a decomposition must be one. Therefore $A \cong \mathbb{M}_n(D)$, for some integer n and division ring D.

Conversely, we need to show that $A = \mathbb{M}_n(D)$ is simple, for an arbitrary division ring D and any integer n. Let $S_j = \sum_{i=1}^{n} DE_{ij}$. Clearly, every S_j is a left ideal of A, and $A = S_1 \oplus S_2 \oplus \cdots S_n$. It can be shown that each S_j is simple as well. Furthermore, all S_j are clearly isomorphic to each other, so A is a simple ring of length n, and we are done.

□

Chapter 2

Central Simple Algebras

In this chapter, we shall explore the basic properties of central simple algebras in depth. Again, we closely follow the notes written by R. Sridharan [1]. We shall evaluate the tensor product of two central simple algebras and discover that it too, is a central simple algebra. We shall find ways to create new central simple algebras over extended fields, and then prove the well known result; the dimension of the central simple algebra over its base field is a perfect square. We shall prove the famous Skolem-Noether theorem, and discuss some of its consequences. Further on, we define the Brauer Group of a field, and show how the structure is formulated. We use this concept to define what it means to split a central simple algebra, and then discuss the existence of Galois splitting fields.

Throughout this chapter, K will denote a (commutative) field and all tensor products are taken over K unless mentioned otherwise. By a K-algebra, we shall mean an associative algebra over K. Unless otherwise stated, the K-vector space dimension of every K-algebra A, denoted by $[A : K]$, will be assumed to be finite.

Let A be a K-algebra. The natural homomorphism $K \to A$ (given by $k \to k1$) is a K-algebra monomorphism and we shall often identify K with its image in A under this monomorphism.

2.1 Properties of Central Simple Algebras

Definition 2.1. Let A be a K-algebra. A is central if the center of A coincides with K. Furthermore, A is central simple if A is central and simple as well.

We shall call a ring A quasi-simple if it has no non-trivial two-sided ideals. Notice that, any finite dimensional quasi-simple algebra is simple.

Lemma 2.2. *Let B be a quasi- simple ring. Then, the matrix ring $\mathbb{M}_n(B)$ is quasi-simple for any integer $n \geq 1$.*

Proof. Let $\Delta \in \mathbb{M}_n(B)$ be a non-zero two-sided ideal. Let Δ' be the subset of all elements in B such that an element of Δ' is an entry in some element of Δ. It is a simple matter of computation to show that Δ' is a two-sided ideal as well. Therefore, $\Delta' = B$, and $E_{ij} \in \Delta$ for all $i, j \in \{1, 2, 3, \cdots n\}$ (since $E_{kl} = E_{kk'}E_{k'l'}E_{l'l}$, for all $1 \leq k, k', l, l' \leq n$). Therefore, $\mathbb{M}_n(B)$ is quasi-simple as well.

□

Theorem 2.3. *Let A be a central simple K-algebra. Then if B is a (not necessarily finite dimensional) quasi-simple K-algebra, then $A \otimes B$ is quasi-simple as well.*

Proof. Since A is simple, by Wedderburn's Theorem, there exists a division ring D such that $A \cong \mathbb{M}_n(D)$. Notice that D is a central division algebra over K. We have;

$$A \otimes B \cong \mathbb{M}_n(D) \otimes B \cong \mathbb{M}_n(D \otimes B)$$

If $D \otimes B$ is quasi-simple, the above lemma would imply that the same is true of $A \otimes B$, and the theorem would be proved. So, it is enough to prove the theorem in the case when A is a central division algebra.

Let then D be a central division algebra and let Δ be any non-zero two-sided ideal of $D \otimes B$. Let $(e_\alpha)_{\alpha \in I}$ be a basis of B over K. Clearly, any element $a \in \Delta$ can be

written uniquely in the form $a = \sum_{\alpha \in I} a_\alpha \otimes e_\alpha$, with $a_\alpha \in D$, $a_\alpha = 0$ for almost all α.

Let us write $J(a) = \{\alpha \in I : a_\alpha \neq 0\}$. Then for each $a \in \Delta$, $J(a)$ is a finite subset of I.

Let $c = \sum_{\alpha \in I} c_\alpha \otimes e_\alpha$ be a non-zero element of Δ such that $J(c)$ is minimal in the set $\{J(a) : a \in \Delta, a \neq 0\}$.

Multiplying c by an element of D, we can clearly assume that at least one c_α, say c_β, is equal to 1. Since Δ is a two-sided ideal, we have, for any $d \in D$,

$$c' = (d \otimes 1)c - c(d \otimes 1) = \sum_{\alpha \in I} (dc_\alpha - c_\alpha d) \otimes e_\alpha \in \Delta$$

Since $c_\beta = 1$, $dc_\alpha = c_\alpha d$ and thus $J(c') \subset J(c)$. Hence, by the minimality of $J(c)$, it follows that $c' = 0$, or, $dc_\alpha = c_\alpha d$ for all α. Since d is arbitrary and D is central, it follows that $c_\alpha \in K$. In other words $c \in \Delta \cap (1 \otimes B)$.

Thus $\Delta \cap (1 \otimes B)$ is a non-zero two-sided ideal of $1 \otimes B$. Since B is quasi-simple, it follows that $\Delta \cap (1 \otimes B) = 1 \otimes B$. In particular, $1 \otimes 1 \in \Delta$, or, $\Delta = A \otimes B$, and the theorem is proved.

□

Definition 2.4. If A is any ring and E is a non-zero subset of A, then we define the commutant E' of E as the set $\{a \in A : ae = ea, \forall e \in E\}$.

The following lemma is stated (using the notation given in the above definition) without proof;

Lemma 2.5. *Let A and B be two K-algebras. If $C \subset A$ and $D \subset B$ are K-subalgebras, then $(C \otimes D)' = C' \otimes D'$.*

Corollary 2.6. *a) If A and B are K-algebras, then $Z(A \otimes B) = Z(A) \otimes Z(B)$, where $Z(C)$ denotes the center of any K-algebra C.*

b) If A and B are central simple K-algebras, then $A \otimes B$ is a central simple K-algebra as well.

c) Let L be a finite field extension of K, and A be any central simple K-algebra, then $L \otimes A$ is a central simple K-algebra as well.

d) If A is a central simple K-algebra, then $[A : K]$ is always a perfect square.

Let A be a central simple K-algebra and A° be the opposite ring of A. Clearly, A° is again a central simple K-algebra. For any $a \in A$, let L_a denote the K-linear endomorphism of A given by left multiplication by a. Similarly, let R_a denote right multiplication by a. The mappings $\Phi : A \to End_K(A)$ and $\Psi : A^\circ \to End_K(A)$ given respectively by $\Phi(a) = L_a$ and $\Psi(a^\circ) = R_a$ are K-algebra homomorphisms. Since every element of $\Phi(A)$ commutes with every element of $\Psi(A^\circ)$, we have an induced K-algebra homomorphism $\theta : A \otimes A^\circ \to End_K(A)$ defined by $\theta(a \otimes b^\circ) = \Phi(a)\Psi(b^\circ) = L_a R_b$. $A \otimes A^\circ$ is called the enveloping algebra of A, and it is isomorphic to $End_K(A)$ under the above induced homomorphism. Notice that if $[A : K] = m$, then $A \otimes A^\circ \cong \mathbb{M}_m(K)$ as a corollary.

2.2 The Skolem-Noether Theorem

First, we state without proof, a small corollary of the Artin-Wedderburn Theorem;

Corollary 2.7 (Artin-Wedderburn)**.** *Let D be a division ring. Suppose M and N are two $\mathbb{M}_n(D)$-modules which have the same dimension as vector spaces over D. Then M and N are isomorphic as $\mathbb{M}_n(D)$-modules.*

Theorem 2.8. *Let A be a central simple K-algebra, and let B be a simple K-algebra. If $f, g : B \to A$ are K-algebra monomorphisms, then there exists an invertible element $u \in A$ such that, for any $b \in B$, $g(b) = uf(b)u^{-1}$.*

Proof. Suppose, A is a matrix algebra $\mathbb{M}_n(K)$ over K. Then, to say that we are given two K-algebra monomorphisms $f, g : B \to \mathbb{M}_n(K)$ is the same as saying

we are given two B-module structures on K^n. Call them V_f and V_g, given by the actions; $b \diamond v = f(b)v$, if $v \in V_f$ or $b \circ v = g(b)v$, if $v \in V_g$, for all $b \in B$. By the above corollary, these two B-modules will be isomorphic. However, they are isomorphic as K-modules as well. Therefore, we must have an invertible element $u \in \mathbb{M}_n(K)$, such that, for any $b \in B$ and $v \in K^n$,

$$u(f(b)v) = u(b \diamond v) = b \circ u(v) = g(b)u(v)$$

Since this holds for all $v \in K^n$, $uf(b) = g(b)u$, for all $b \in B$.

We shall use the above case to finish the proof. Since we know that $A \otimes A^\circ$ is a matrix algebra over K, we shall obtain the induced K-algebra monomorphisms $f \otimes 1^\circ, g \otimes 1^\circ :\to A \otimes A^\circ$, (where 1° is the identity map of A°). Since we have an invertible element in $A \otimes A^\circ$, say u, we have;

$$(g \otimes 1^\circ)(b \otimes a^\circ) = u(f \otimes 1^\circ)(b \otimes a^\circ)u^{-1}$$

for every $b \in B$ and $a^\circ \in A^\circ$.
First, substitute $b = 1$, and we notice that u commutes with every element in $1 \otimes A^\circ$, so $u \in (1 \otimes A^\circ)' = A \otimes 1$. So, we have an invertible element $t \in A$ such that $u = t \otimes 1$.
Next, substituting $a^\circ = 1$ and $u = t \otimes 1$, we get;

$$(g \otimes 1^\circ)(b \otimes 1) = (t \otimes 1)(f \otimes 1^\circ)(b \otimes 1)(t^{-1} \otimes 1)$$

and so, pulling back the map from the induced tensor, we get $g(b) = tf(b)t^{-1}$ for all $b \in B$, as required. □

Corollary 2.9. *Every K-algebra automorphism of a central simple K-algebra is an inner automorphism.*

Theorem 2.10. *Let A be a central simple K-algebra and B be a simple K-subalgebra of A. Let B' be the commutant of B in A. Then B' is simple, $B'' = B$, and $[B : K][B' : K] = [A : K]$.*

Proof. Consider $End_K(B)$, the K-vector space endomorphisms of B, as a K-algebra. Notice that, it is a matrix algebra over K, so it is a central simple K-algebra. Therefore, $A \otimes End_K(B)$ must be a central simple K-algebra as well. The inclusion of B in A induces a K-algebra monomorphism $f : B \to A \otimes End_K(B)$.

On the other hand, B can be embedded in $End_K(B)$ under the map $b \to L_b$ where L_b is the left multiplication by b. This induces a K-algebra monomorphism $g : B \to A \otimes End_K(B)$ such that $g = (I(u)) \circ f$ (where $I(u)$ is the inner automorphism of $A \otimes End_K(B)$ given by u). Thus $I(u)$ maps $f(B)$ isomorphically onto $g(B)$ and hence the commutant $f(B)'$ onto $g(B)'$. But, it is clear that $f(B)' = B' \otimes End_K(B)$ and $g(B)' = A \otimes B^\circ$. Thus $B' \otimes End_K(B) \cong A \otimes B^\circ$. Since B° is simple, it follows that $A \otimes B^\circ$ is simple and hence $B' \otimes End_K(B)$ is also simple, which implies that B' is simple.

Equating dimensions of $B' \otimes End_K(B)$ and $A \otimes B^\circ$, we get

$$[B' : K][B : K]^2 = [A : K][B : K]$$

which gives

$$[B' : K][B : K] = [A : K]$$

. Applying this formula to the simple subalgebra B', we get $[B'' : K][B' : K] = [A : K]$ so that we get $[B'' : K] = [B : K]$. Since $B \subseteq B''$, it follows that $B = B''$, and this completes the proof of the theorem. □

Corollary 2.11. *a) If B is a central simple K-subalgebra of a central simple K-algebra A, then B' is also central simple over K and the inclusions $B \hookrightarrow A$,and $B' \hookrightarrow A$, induce an isomorphism $B \otimes B' \leftrightarrow A$.*

b) Let A be a central simple K-algebra and let L be a commutative subfield of A containing K. Then the following conditions are equivalent:

i) L is a maximal commutative subring of A.

ii) L coincides with its commutant.

iii) $[A : K] = [L : K]^2$.

c) Let D be a central division algebra over K. If L is a maximal commutative subfield of D containing K, then $[D : K] = [L : K]^2$.

2.3 Brauer Groups And Splitting Fields

Definition 2.12. We say that two central simple K-algebras are equivalent (or Brauer equivalent), and write $A \sim B$, if there exist matrix algebras $\mathbb{M}_m(K)$ and $\mathbb{M}_n(K)$ such that $A \otimes \mathbb{M}_m(K) \cong B \otimes \mathbb{M}_n(K)$, or, $\mathbb{M}_m(A) \cong \mathbb{M}_n(B)$. It can be checked that this is an equivalence relation on the set of central simple K-algebras.

Remark. Let A, B be central simple K-algebras and let D_A and D_B denote the division algebra of A and B respectively. Then $A \sim B$ if and only if $D_A \cong D_B$. This reduces the study of central simple algebras to their respective division algebras.

The set of equivalence classes of central simple K-algebras is denoted by $Br(K)$. For any central simple K-algebra A, we shall denote its equivalence class by $[A]$. If A and B are central simple K-algebras, then it follows that $A \otimes B$ is again central simple over K. We define a binary composition in $Br(K)$ by setting $[A] \circ [B] = [A \otimes B]$. It is a simple task to check that this operation is well-defined.

With the above composition $Br(K)$ is an abelian group. The identity of this group is $[K]$, the class of K and consists of all matrix algebras over K. The inverse of $[A]$ is $[A^\circ]$.

Definition 2.13. Let L be a field extension of K and A be a central simple K-algebra. We say that L is a splitting field for A or that L splits A if $L \otimes A$ is L-isomorphic to $\mathbb{M}_n(L)$ for some n. (For example, if $L \supset K$ is an algebraically closed field, then L splits any central simple K-algebra A).

Theorem 2.14. *Let $L|K$ be a finite field extension. For any central simple K-algebra A, the following conditions are equivalent :*

a) L is a splitting field for A.

b) L is a maximal commutative subring of some central simple K-algebra equivalent to A.

Proof. Let $\Phi : L \otimes A \leftrightarrow End_L(V)$ be an L-isomorphism, where V is a finite dimensional L-vector space. Since L is finite dimensional over K, V is finite dimensional over K and $End_K(V)$ is a central simple K-algebra containing $End_L(V)$. Let C be the commutant of $\Phi(1 \otimes A)$ in $End_K(V)$. Since the commutant of $\Phi(L \otimes A)$ in $End_K(V)$ is clearly L ($L1$) and $1 \otimes A \subset L \otimes A$, it follows that $C \supset L$. Since $\Phi(1 \otimes A)$ is central simple it follows that C is central simple and that $A \otimes C \cong End_K(V)$,or, $A \sim C^\circ$. If we set $B = C^\circ$, then clearly $B \supset L$ and we would be through provided we show that L is a maximal commutative subring of B. It is enough to show that $[B : K] = [L : K]^2$. But we have $[B : K] = [C : K]$ and

$$\begin{aligned}[A : K][C : K] = [End_K(V) : K] &= [End_L(V) : K][L : K] \\ &= [L \otimes A : K][L : K] \\ &= [L : K]^2[A : K]\end{aligned}$$

which shows that $[C : K] = [L : K]^2$.

Conversely, let L be a maximal commutative subring of some central simple K-algebra equivalent to A. It is enough to show that if L is a maximal commutative subring of A, then L splits A. We know that $A \otimes A^\circ \cong End_K(A)$. Since $L \subset A$ and L is commutative, it follows that $L \subset A^\circ$. The commutant of $1 \otimes L$ in $A \otimes A^\circ$ is $A \otimes L$. On the other hand, the commutant of L in $End_K(A)$ is $End_L(A)$. Thus $A \otimes L \cong End_L(A) = \mathbb{M}_n(L)$ with $n = [A : L]$, and this finishes the proof. □

Corollary 2.15. *Any maximal commutative subfield of a central division algebra D is the splitting field for D.*

We state the following lemma without proof, for the sake of brevity;

Lemma 2.16. *Let $D \neq K$ be a central division algebra over K. Then D contains a separable algebraic extension of K containing K properly.*

Theorem 2.17. *Every central division algebra D over a field K contains a maximal commutative subfield which is separable over K.*

Proof. Let L be a subfield of D which is a maximal separable extension of K. We assert that L is a maximal commutative subfield of D. For, if not, let $L' \neq L$ be the commutant of L. Then L' can be thought of as a division algebra of center L. By the above lemma there exists a proper separable extension of L contained in L'. But this is a contradiction to our assumption on L. This shows that L is maximal commutative subfield, and the theorem is proved. □

Corollary 2.18. *a) Let K be a field and $L \supset K$ be a separably algebraically closed field (a field which has no proper separable algebraic extensions). Then L splits any central simple algebra over K.*

b) Every central simple algebra A over a field K admits a splitting field which is a (finite) Galois extension of K.

Proof. a) Let A be any central simple algebra over K. Then $L \otimes A \cong \mathbb{M}_n(D)$ where D is a (finite) central division algebra over L. If $D \neq L$, D must contain, by the above theorem, a proper finite separable extension of L. This is however impossible, since L is, by our assumption, separably algebraically closed. Thus $D = L$ and L splits A.

b) Let D be the division algebra of A. By the above theorem, D contains a maximal commutative subfield L which is separable over K. The field L splits D, and hence splits A also. Now, let L^* be the normal closure of L. Clearly L^* is finite and a Galois extension of K which splits A.

□

Chapter 3

Central simple algebras with involutions

Let R be a central simple algebra over a field F. If $deg(R) = 2$, R is called a quaternion F-algebra. We can find elements a_l, a_2, in R such that $0 \neq a_1^2 \in F, 0 \neq a_2^2 \in F$, $a_1 a_2 = -a_2 a_1$ and $R = F + Fa_l + Fa_2 + Fa_l a_2$. R has an involution $(*)$, given by;

$$(\gamma_1 + \gamma_2 a_1 + \gamma_3 a_2 + \gamma_4 a_1 a_2)^* = \gamma_1 - \gamma_2 a_1 - \gamma_3 a_2 - \gamma_4 a_1 a_2$$

A tensor product (over F) of m quaternion F-algebras is of degree 2^m and has the natural involution. On the other hand, any central division algebra D with involution has degree 2^m for some m, and it is possible to show that D is a tensor product of quaternion sublagebras when $m = 2$. Conversely, we would like to answer;

If a central simple F-algebra with an involution has degree 2^m for some m, is it isomorphic to a tensor product of quaternion subalgebras?

3.1 Tensor product of quaternions

Let R be a central simple F-algebra. A set $S = \{r_i\}$ is called a quaternion generating set, or a q-generating set if;

a) $0 \neq r_i^2 \in F$

b) $r_i r_j = \pm r_j r_i$

c) If $i \neq j$, there exists $r_k \in S$ commuting with either one of r_i or r_j, and anticommuting with the other.

It is easy to check that a q-generating set S of a central simple algebra R is F-independent. Furthermore, if $\{r_1, r_2\}$ is a q-generating set, then $\{1, r_1, r_2, r_1 r_2\}$ is also a q-generating set and the induced structure $Q = F + Fr_1 + Fr_2 + Fr_1 r_2$ is a quaternion F-algebra.

Theorem 3.1. *Suppose $deg(R) = 2^t$. R is a tensor product of quaternion F-algebras, iff R has a q-generating set S containing 4^t elements (in which case, S is a base of R).*

Proof. Let R be a tensor product of quaternions $Q_1 \otimes \cdots \otimes Q_r$, where each Q_i is of the form $Fr_{0i} + Fr_{1i} + Fr_{2i} + Fr_{3i}$, where $r_{0i} = 1$ and $r_{0i} = r_{1i} r_{2i}$. Then, $S = \{r_{i_1 1} r_{i_2 2} \cdots r_{i_t t} | i_u = 0, 1, 2, 3\}$ forms a base for R. Conversely, suppose R has a q-generating set S satisfying the hypothesis. Take $r_1, r_2 \in S$ such that they anticommute, and let Q_1 be the quaternion subalgebra generated by these two elements. Then, $R \cong Q_1 \otimes R_1$, R_1 being the centralizer of Q_1 in R. If we show that $S \cap R_1$ is a q-generating set for R_1, having 4^{t-1} elements, induction will finish the proof, since $deg(R_1) = 2^{t-1}$. For any $r_u \in S$, either $r_u \in R_1$, or $r_u \notin R_1$. Suppose, $r_u \notin R_1$. Either $r_1 r_u = -r_u r_1$ or $r_2 r_u = -r_u r_2$. Let $r_u = f_0 + f_1 r_1 + f_2 r_2 + f_3 r_1 r_2$, where each $f_i \in R_1$. We see that exactly one of the f_i's must be non-zero, and so $S = T_0 \cup T_1 r_1 \cup T_2 r_2 \cup T_3 r_1 r_2$, with each $T_i \subseteq R_1$. The number of elements in each T_i will be at most 4^{t-1}, since the elements are F-independent. Since the total

number of elements is 4^t, $T_0 = S \cap R_1$ will have 4^{t-1} elements, and is a q-generating set for R_1. □

3.2 Abelian Crossed Products

Suppose R is a crossed product having a maximal subfield K which is Galois over F, with an abelian Galois group $G = \langle\sigma_1\rangle \oplus \langle\sigma_2\rangle \oplus \cdots \langle\sigma_q\rangle$, where each σ_i has order 2 in G. We shall define $N_i(x) = x\sigma_i(x)$, as the norm with respect to σ_i. Notice that N_i is multiplicative and commutes with all σ_j and N_j.
From the Skolem-Noether theorem, we can find $z_i \in R$ such that $\sigma_i(x) = z_i x z_i^{-1}$, for all $x \in K$. Define $u_{ij} = z_i z_j z_i^{-1} z_j^{-1}$, and $b_i = z_i^2$. Notice that all u_{ij} and b_i are in K since they are in the centralizer of K. Write $U = \{u_{ij} | 1 \leq i, j \leq q\}$, $B = \{b_i | 1 \leq i \leq q\}$. It is possible to show that the following conditions are satisfied;

(A) $u_{ii} = 1, u_{ij} = u_{ji}^{-1}$

(B) $\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij}) = u_{jk}u_{ki}u_{ij}$

(C) $N_i(N_j(u_{ij})) = 1$

(D) $\sigma_j(b_i)b_i^{-1} = N_i(u_{ji})$

On the other hand, suppose K is an abelian extension of F with Galois group $G = \langle\sigma_1\rangle \oplus \langle\sigma_2\rangle \oplus \cdots \langle\sigma_q\rangle$, where each σ_i has order 2 in G, and the sets $U, B \subseteq K$ satisfy conditions (A) - (D), then it is possible to determine a unique central simple F-algebra R with K as its maximal subfield, and $\{z_i\} \subseteq R$ satisfying all the above properties. Since (K, G, U, B) are enough to completely understand R, we denote R by (K, G, U, B).

Remark. a) If U, B satisfy conditions (A), (B), (D), then U satisfies (C).

b) If U satisfies conditions (A) - (C), then there exists a set B whose elements are determined uniquely upto multiplication by elements in F, satisfying (D). This

is obtained from a generalization of Hilbert's Theorem 90, and in particular, we have elements a_k such that $a_k\sigma_i(a_k^{-1}) = N_k(u_{ik})$, and we choose $b_k = a_k^{-1}$.

We need to determine the conditions for a central simple algebra to possess involutions. The following theorem is stated without its proof, but for a detailed proof, refer [2] and [3].

Theorem 3.2. *Let $\tau \in G$ and $R = (K, G, U, B)$. Then the following conditions are equivalent;*

i) R has an involution of the first kind.

ii) R has an involution whose restriction to K is τ.

iii) If we adjust the conditions of $\{U, B\}$, we can write $R = (K, G, U, B)$ satisfying;

(E) $\tau(u_{ij})\sigma_i\sigma_j(u_{ij}) = 1$, for all i, j

(F) $\tau(b_i) = b_i$, for all i

Therefore, the six conditions that determine our central simple F-algebra R with involution, denoted by (K,G,U,B,τ), are given by;

(A) $u_{ii} = 1, u_{ij} = u_{ji}^{-1}$

(B) $\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij}) = u_{jk}u_{ki}u_{ij}$

(C) $N_i(N_j(u_{ij})) = 1$

(D) $\sigma_j(b_i)b_i^{-1} = N_i(u_{ji})$

(E) $\tau(u_{ij})\sigma_i\sigma_j(u_{ij}) = 1$, for all i, j

(F) $\tau(b_i) = b_i$, for all i

Denote the central simple F-algebra R with involution henceforth as (K, G, U, B, τ) with the restriction of involution to K being τ. For the reminder of the section, $q = 3$, $K = F(\xi_1, \xi_2, \xi_3)$, with $\xi_i^2 \in F$ and $\sigma_i(\xi_i) = -\xi_i, \sigma_j(\xi_i) = \xi_i$, for $i \neq j$. Let S_3 denote the permutation group of three elements, and for any $\pi \in S_3$, $sgn(\pi)$, the sign of π.

Theorem 3.3. *Suppose $U \subseteq K$ satisfies* (A), (B) *and* (E) *for $\tau = \sigma_1\sigma_2\sigma_3$. Define $v_{\pi(3)} = u_{\pi(1)\pi(2)}^{sgn(\pi)}$, for all $\pi \in S_3$. Then, the following hold;*

1) The v_i's satisfy the following relations;

i) $v_1v_2v_3 = \pm 1$

ii) $N_i(v_i) = 1$, *for all* i

2) The exists a set $B = \{b_1, b_2, b_3\}$, uniquely determined upto multiples of F, satisfying;

i) $\sigma_{\pi(1)}(b_{\pi(2)})b_{\pi(2)}^{-1} = N_{\pi(2)}(v_{\pi(3)})^{sgn(\pi)}$

ii) $\sigma_i(b_i) = b_i$

3) The set $\{U, B\}$ satisfies (A) - (F).

Proof. Notice that $\tau = \sigma_1\sigma_2\sigma_3 = \sigma_{\pi(1)}\sigma_{\pi(2)}\sigma_{\pi(3)}$, so by (E), we have;

$$1 = \sigma_{\pi(1)}\sigma_{\pi(2)}\sigma_{\pi(3)}(u_{\pi(1)\pi(2)})\sigma_{\pi(1)}\sigma_{\pi(2)}(u_{\pi(1)\pi(2)}) = \sigma_{\pi(1)}\sigma_{\pi(2)}(N_{\pi(3)}(v_{\pi(3)}^{sgn(\pi)}))$$

Thus, (1ii) is satisfied. Furthermore, $\sigma_i(v_i) = v_i^{-1}$ for all i, and (B) implies that;

$$v_1^{-1}v_2^{-1}v_3^{-1} = \sigma_1(v_1)\sigma_2(v_2)\sigma_3(v_3) = \sigma_1(u_{23})\sigma_2(u_{31})\sigma_3(u_{12}) = u_{23}u_{31}u_{12} = v_1v_2v_3$$

Therefore, $v_1^2v_2^2v_3^2 = 1$, and we are done.

Observe that U satisfies (C) as well, since;

$$N_{\pi(1)}N_{\pi(2)}(u_{\pi(1)\pi(2)}) = N_{\pi(1)}N_{\pi(2)}(v_{\pi(3)})^{sgn(\pi)} = N_{\pi(1)}N_{\pi(2)}((v_{\pi(1)}^{-1}v_{\pi(2)}^{-1}))^{sgn(\pi)}$$
$$= N_{\pi(2)}N_{\pi(1)}(v_{\pi(1)})^{-sgn(\pi)}N_{\pi(1)}N_{\pi(2)}(v_{\pi(2)})^{-sgn(\pi)} = 1$$

Therefore, by an earlier remark, it is possible to determine a set B which satisfies (D). Trivially, we get $\sigma_i(b_i) = b_i$ from (D), and the other condition is clear by definition of the v_i's.

It remains to show that B satisfies (F) as well. This is achieved by seeing that;

$$\sigma_{\pi(2)}(b_{\pi(1)})b_{\pi(1)}^{-1} = N_{\pi(1)}(v_{\pi(3)})^{-sgn(\pi)} = N_{\pi(1)}((v_{\pi(1)}v_{\pi(2)}))^{sgn(\pi)}$$
$$= N_{\pi(1)}((v_{\pi(2)}))^{sgn(\pi)}$$
$$= \sigma_{\pi(3)}(b_{\pi(1)})b_{\pi(1)}^{-1}$$

So, $\sigma_{\pi(2)}(b_{\pi(1)})b_{\pi(1)}^{-1} = \sigma_{\pi(3)}(b_{\pi(1)})b_{\pi(1)}^{-1}$. Therefore, since $\sigma_i(b_i) = b_i$, we have;

$$\tau(b_{\pi(1)}) = \sigma_{\pi(1)}\sigma_{\pi(2)}\sigma_{\pi(3)}(b_{\pi(1)}) = \sigma_{\pi(2)}\sigma_{\pi(3)}(b_{\pi(1)}) = b_{\pi(1)}$$

and B satisfies (F) as well. □

The converse of this theorem holds as well;

Theorem 3.4. *Given v_1, v_2, v_3 satisfying conditions* (1i) *and* (1ii) *in Theorem 3.3, we can define $u_{\pi(1)\pi(2)}^{sgn(\pi)} = v_{\pi(3)}$ and $u_{ii} = 1$. Then, $U = \{u_{ij}\}$ is well defined, and for $\tau = \sigma_1\sigma_2\sigma_3$, U satisfies* (A), (B) *and* (E), *and hence all conditions of Theorem 3.3.*

Proof. Clearly, U is well defined and satisfies (A). Notice that, by the proof used in (1ii) of Theorem 3.3, we get,

$$\sigma_{\pi(1)}\sigma_{\pi(2)}(N_{\pi(3)}(v_{\pi(3)}^{sgn(\pi)})) = \sigma_{\pi(1)}\sigma_{\pi(2)}\sigma_{\pi(3)}(u_{\pi(1)\pi(2)})\sigma_{\pi(1)}\sigma_{\pi(2)}(u_{\pi(1)\pi(2)}) = 1$$

so, U satisfies (E). Also, $\sigma_1(v_1)\sigma_2(v_2)\sigma_3(v_3) = v_1^{-1}v_2^{-1}v_3^{-1} = v_1v_2v_3$, and we are done, since U satisfies (B) as well. □

The above two theorems present interesting consequences on the elements of B, as we shall see.

Corollary 3.5. *Let $B = \{b_1, b_2, b_3\}$ be determined in the nature of Theorem 3.3. Then, $b_{\pi(1)} \in F(\xi_{\pi(2)}\xi_{\pi(3)}) \cap F(\xi_{\pi(2)})N_{\pi(1)}(K)$.*

Proof. We have that $\sigma_{\pi(1)}(b_{\pi(1)}) = b_{\pi(1)}$, by the conditions of the hypothesis. We had seen earlier that $\sigma_{\pi(2)}(b_{\pi(1)}) = \sigma_{\pi(3)}(b_{\pi(1)})$. Therefore, $b_{\pi(1)}$ is invariant under $\sigma_{\pi(1)}$ and $\sigma_{\pi(2)}\sigma_{\pi(3)}$, so $b_{\pi(1)} \in F(\xi_{\pi(2)}\xi_{\pi(3)})$.

By Hilbert's Theorem 90, we can obtain $y \in K$ such that $v_{\pi(3)} = \sigma_{\pi(3)}(y)y^{-1}$. Since $\sigma_{\pi(2)}(b_{\pi(1)}) = \sigma_{\pi(3)}(b_{\pi(1)})$, we have;

$$\sigma_{\pi(2)}(b_{\pi(1)})b_{\pi(1)}^{-1} = \sigma_{\pi(3)}(b_{\pi(1)})b_{\pi(1)}^{-1} = N_{\pi(1)}(v_{\pi(3)})^{-sgn(\pi)} = N_{\pi(1)}(\sigma_{\pi(3)}(y)y^{-1})^{-sgn(\pi)}$$

proving that $w = b_{\pi(1)}N_{\pi(1)}(y)^{sgn(\pi)}$ is invariant under $\sigma_{\pi(3)}$. But both $b_{\pi(1)}$ and $N_{\pi(1)}(y)$ are invariant under $\sigma_{\pi(1)}$, proving that $b_{\pi(1)} \in F(\xi_{\pi(2)})N_{\pi(1)}(K)$, since $w \in F(\xi_{\pi(2)})$. □

By varying π, we can see that;

(G) $b_1 \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$.

The converse for the above holds as well.

Theorem 3.6. *Suppose b exists in K satisfying* (G)*. Then, there exists a set $V = \{v_1, v_2, v_3\}$ satisfying* (1i) *and* (1ii) *and a corresponding set $B = \{b_1, b_2, b_3\}$ satisfying* (2i) *and* (2ii) *of Theorem 3.3. Furthermore, $b_1 = b$.*

Proof. Let $b = a_2N_1(y_2) = a_3N_1(y_3^{-1})$, where $a_i \in F(\xi_i)$ and $y_i \in K$. Define $v_2 = \sigma_2(y_3)^{-1}y_3$, $v_3 = \sigma_3(y_2)^{-1}y_2$ and $v_1 = (v_2v_3)^{-1}$. By definition, $v_1v_2v_3 = \pm 1$.

We see that $N_i(v_i) = 1$ for $i = 2, 3$. For, $i = 1$, we have;

$$N_1(v_3)^{-1} = N_1(y_2)^{-1}\sigma_3(N_1(y_2)) = b^{-1}\sigma_3(b) = b^{-1}\sigma_2(b)$$
$$N_1(v_2) = N_1(y_3)^{-1}\sigma_2(N_1(y_3))^{-1} = b^{-1}\sigma_3(b) = b^{-1}\sigma_2(b)$$

Therefore, $N_1(v_1) = N_1(v_2)^{-1}N_1(v_3)^{-1} = 1$, so $N_i(v_i) = 1$ for all i. B satisfies (2i) and (2ii) by the conditions of the hypothesis. If we show that b and b_1 differ by a multiple of an element in F, we can replace b by b_1 as desired. To do this, we see that;

$$\sigma_2(bb_1^{-1})(bb_1^{-1}) = N_1(v_3)^{-1}N_1(v_3) = 1$$
$$\sigma_3(bb_1^{-1})(bb_1^{-1}) = N_1(v_2)^{-1}N_1(v_2) = 1$$

Therefore, $bb_1^{-1} \in F$, and we are done. □

3.3 Generic abelian crossed products with involutions

Let K be an abelian extension of a field F with Galois group
$G = \langle\sigma_1\rangle \oplus \langle\sigma_2\rangle \oplus \cdots \langle\sigma_q\rangle$, where each σ_i has order 2 in G, and $U \subseteq K$ satisfies conditions (A) - (C). The "generic ableian crossed product" is constructed as follows [4]:
Consider the ring of polynomials $K[x_1, x_2 \cdots x_q]$ with non-commutative variables satisfying $x_i k = \sigma_i(k)x_i$, for all $k \in K$ and $x_i x_j = u_{ij}x_j x_i$, for all i, j. It can be shown that $K[x_1, x_2 \cdots x_q]$ is an Ore domain whose quotient division ring, written as $K(x_1, x_2 \cdots x_q)$, has the following structure:

From an earlier remark, it is possible to determine $B = \{b_l, \cdots, b_q\}$, which satisfy (D). Define $y_i = b_i^{-1}x_i^2$. We have $Cent(K(x_1, x_2 \cdots x_q)) = F(y_1, \cdots, y_q)$ which will be denoted by F'. The algebra $K(x_1, x_2 \cdots x_q)$ turns out to be a crossed product by the earlier notation, given by (K', G, U, B'), where $B' = \{x_i^2 | 1 \leq i \leq q\}$ and

$K' = K(y_1, \cdots y_q)$, with the automorphisms $\sigma \in G$ extended to K', given by $\sigma(y_i) = y_i$ for all i. Clearly, the invariant field of K' will be $F(y_1, \cdots, y_q)$. Since B' is equivalent to B in our case, the set $\{U, B\}$ satisfies (A) - (D). Furthermore, if we allow U to satisfy (E) for some $\tau \in G$, the algebra $K(x_1, x_2 \cdots x_q)$ has an involution as well, if B satisfies (F). However, the last requirement is superfluous if we take $q = 3$ and $\tau = \sigma_1\sigma_2\sigma_3$. We shall now denote the generic crossed product (K', G, U, B', τ) by (K, U, τ) from this point forwards.

Denote $K[x_1, x_2 \cdots x_q]$ by $K[x]$. For any element $f \in K[x]$, f can be written uniquely as $\sum k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q}$. Let $v(f)$ denote the element $k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q}$ with the largest $(\mu_1 \cdots \mu_q)$, ordered lexicographically. The involution $(*)$ now acts on $K[x]$ by $(\sum k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q})^* = \sum x_q^{\mu_q} \cdots x_1^{\mu_1} \tau(k_\mu)$.

Theorem 3.7. *If the algebra $A = (K, U, \tau)$ can be written as a tensor product of quaternions, then A has a q-generating set S containing 4^q elements of the following form: Each element of S has the form $k_i x_1^{\mu_1} \cdots x_q^{\mu_q}$, where $k_i, \in K$ and $\mu_1, \mu_2 \cdots \mu_q \in \{0, 1\}$.*

Proof. Since A has degree 2^q, A must have a q-generating set, say, $\{a_1, a_2, \cdots a_{4^q}\}$. Let $a_i = f_i g_i^{-1}$, where g_i's are in the centre, for all i. Then $\{f_1, f_2, \cdots f_{4^q}\}$ is a q-generating set, therefore, $\{v(f_1), v(f_2), \cdots v(f_{4^q})\}$ is as well. We know that each $v(f_i)$ can be uniquely written in the form $a_i x_1^{i_1} \cdots x_q^{i_q}$, where $a_i \in K$. Let $c_i = y_1^{j_1} \cdots y_q^{j_q}$, where $j_n = [i_n/2]$, for all n. Now, $v(f_i)c_i^{-1}$ is in the desired form, $k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q}$. Since each c_i is in F', $\{v(f_1)c_1^{-1}, v(f_2), \cdots v(f_{4^q}c_{4^q}^{-1})\}$ is a q-generating set as well.

□

We are now in a position to determine when the algebra $A = (K, U, \tau)$, can be written as a tensor product of quaternions.

Theorem 3.8. *Suppose $\tau = \sigma_1\sigma_2\sigma_3$, U satisfies* (A), (B), (C), *and B is chosen to satisfy* (D). *Then the generic abelian crossed product $A = (K, U, \tau)$ is a product of quaternions iff $b_1 \in FN_1(K)$.*

Proof. If A is a tensor product of quaternion subalgebras, then A has some set of square-central elements $a_1, \cdots a_{64}$, independent over $Cent(A)$ with $a_i a_j = \pm a_j a_i$ for all i, j. Consider the q-generating set of A, which would contain some element kx_1, and so $(kx_1)^2 \in F'$, which is $Cent(A)$. But, $(kx_1)^2 = k\sigma_1(k)x_1^2 = k\sigma_1(k)b_1y_1$. Therefore, $k\sigma_1(k)b_1 \in F' \cap K = F$, and $b_1 \in FN_1(K)$.

Conversely, if $k\sigma_1(k)b_1 \in F$ for some k in K, then (ξ_1, kx_1) is a q-generating set of A. A has an F'-quaternion subalgebra Q_1, thus $A \cong Q_1 \otimes_{F'} A'$, where A' is the centralizer of Q_1 in A. A has exponent 2 in the Brauer group, so A' has exponent 2. Therefore, A' is a product of quaternions, so A is a product of quaternions.

□

Therefore, for our purposes, we need to find b which satisfies (G), but $b \notin FN_1(K)$. Then there is a generic abelian crossed product $A = (K, U, \tau)$ for some U, such that A is a division algebra of degree 8, with involution, which is not isomorphic to a tensor product of quaternion algebras.

3.4 Equivalent conditions

To simplify the proofs necessary to show the existence of such a b and a field K that satisfy our propositions, we weaken them with some equivalent conditions. We introduce some notation here that will be used throughout this section.

Suppose H is a finite field extension of L, and T is a subset of H. Write $N(T; H/L) = \{norm(x) | x \in T\}$, where the norm is taken from H to L and denote $N(H; H/L)$ by $N(H/L)$. Take $K = F(\xi_1, \xi_2, \xi_3)$, and $F_1 = F(\xi_2\xi_3)$.

Lemma 3.9. $N_1(K) \cap F_1 = N(F(\xi_1)/F_1)N(F_1(\xi_1\xi_2)/F_1)$.

Proof. Suppose $a = N_1(u) \in F_1$, where $u \in K$. If $u \in F_1(\xi_1)$, then we are done. Suppose not, then $u = u_1(u_2 + \xi_2)$, for some $u_1, u_2 \in F_1(\xi_1)$, since 1 and ξ_2 form a base of K over $F_1(\xi_1)$. Now, we can write $a = N_1(u) = N_1(u_1(u_2 + \xi_2))$, which

is in F_1. Therefore, $N_1(u_2 + \xi_2) \in F_1$, since the norm is multiplicative. Now, $N_1(u_2+\xi_2) = N_1(u_2)+\xi_2(u_2+\sigma_1(u_2))+\xi_2^2$, and so, $u_2+\sigma_1(u_2) = 0$. We can now say that $u_2 = w\xi_2$ for some w in F_1. Finally;

$$a = N_1(u) = N_1(u_1)(-N_1(w)\xi_1^2 + \xi_2^2) = N_1(u_1\xi_1)N_1(w + \xi_1^{-1}\xi_2)$$

which is in $N(F_1(\xi_1\xi_2)/F_1)$. □

Corollary 3.10. *If $b \in FN_1(K) \cap F(\xi_2\xi_3)$, then;*

$$N(b; F_1/F) \in N(F(\xi_1)/F)[N(F(\xi_1\xi_2)/F) \cap N(F(\xi_2\xi_3)/F)].$$

Proof. Let $b = da$, where $d \in F$ and $a \in N_1(K) \cap F_1$. By the above lemma, $a \in N(F(\xi_1)/F)N(F_1(\xi_1\xi_2)/F_1)$. Notice that;

$$\begin{aligned} N(N(F(\xi_1)/F_1); F_1/F) &= N(F_1(\xi_1)/F) \\ &= N[N(F_1(\xi_1)/F(\xi_1)); F(\xi_1)/F] \\ &\subseteq N(F(\xi_1)/F) \\ N(N(F(\xi_1\xi_2)/F_1); F_1/F) &= N(F_1(\xi_1\xi_2)/F) \\ &= N[N(F_1(\xi_1\xi_2)/F(\xi_1\xi_2)); F(\xi_1\xi_2)/F] \\ &\subseteq N(F(\xi_1\xi_2)/F) \\ N(F_1(\xi_1\xi_2)/F) &= N(N(F_1(\xi_1\xi_2)/F_1); F_1/F) \\ &\subseteq N(F_1/F) \end{aligned}$$

Therefore, we must have;

$$\begin{aligned} N(b; F_1/F) &\in d^2N(F(\xi_1)/F)[N(F(\xi_1\xi_2)/F) \cap N(F_1/F) \\ &\subseteq N(F(\xi_1)/F)[N(F(\xi_1\xi_2)/F) \cap N(F(\xi_2\xi_3)/F)] \end{aligned}$$

□

Lemma 3.11. *Let $b \in F(\xi_2, \xi_3)$, then $b \in F(\xi_2)N_1(K)$ iff $N_3(b) \in N(F(\xi_1, \xi_2)/F(\xi_2))$.*

Proof. For some $a_2 \in F(\xi_2)$ and $k \in K$, let $b = a_2 N_1(k)$. We have;

$$N_3(b) = N_3(a_2 N_1(k)) = a_2^2 N_1(N_3(k)) = N_1(a_2 N_3(k))$$

so $a_2 N_3(k) \in F(\xi_1, \xi_2)$.

Conversely, suppose $N_3(b) = N_1(k_0)$, for some $k_0 \in F(\xi_1, \xi_2)$. Let $k = b + k_0$. To simplify notation, let $k' = k_0 + \sigma_1(k_0) \in F(\xi_2)$. Then;

$$N_1(k) = N_1(b + k_0) = b^2 + bk' + N_1(k_0) = b^2 + bk' + N_3(b) = b(b + \sigma_3(b) + k').$$

Notice that $(b + \sigma_3(b)) + k' \in F(\xi_2)$. If $b = -k_0$, then take $k_0 = 1$, otherwise, we are done. □

Corollary 3.12. *If $b \in F(\xi_2\xi_3)$, then $b \in F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$ iff;*

$$N_2(b) = N_3(b) \in N[F(\xi_1, \xi_2)/F(\xi_2)] \cap N[F(\xi_1, \xi_3)/F(\xi_3)]$$

3.5 The counterexample

Let $F = \mathbb{Q}(\lambda)$, the field of rational functions in the indeterminate λ over $\mathbb{Q}$. Take $\xi_1^2 = -1$, $\xi_2^2 = -(\lambda^2 + 1)$ and $\xi_3^2 = \lambda$. Set $b = \xi_2\xi_3 \in F(\xi_2\xi_3)$. Then, we have;

$$\begin{aligned} N_2(b) = N_3(b) &= \lambda(\lambda^2 + 1) \\ = \frac{1}{4} N_1 &\left(\xi_2[\lambda - 1 - \xi_2) + (\lambda - 1 + \xi_2)\xi_1]\right) \\ &= N_1[(\xi_1, \xi_3)(\lambda\xi_1 - 1)] \end{aligned}$$

Therefore, we must have $b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$. Suppose, to the contrary,

$$N(b; F_1/F) = N_1(f_1)[N(f_2; F(\xi_1\xi_2)/F)] = N_1(f_1)[N(F(f_3; \xi_2\xi_3)/F)]$$

for appropriately chosen f_1, f_2, f_3. For some polynomials $g, g_1, g_2, g_3, g_4, g_5, g_6 \in \mathbb{Z}[\lambda]$, we must have $f_1^{-1} = (g_1 + g_2\xi_1)g^{-1}$, $f_2 = (g_3 + g_4\xi_1\xi_2)g^{-1}$, and $f_3 = (g_5 + g_6\xi_2\xi_3)g^{-1}$. Clearing out g^{-1}, we obtain;

$$\lambda(\lambda^2+1)(g_1^2+g_2^2) = g_3^2 - (\lambda^2+1)g_4^2 = g_5^2 + \lambda(\lambda^2+1)g_6^2.$$

We assume that none of the g_i's have any common divisor, but this proves to be impossible, as seen by taking the cannonical homomorphism into $\frac{\mathbb{Z}}{2\mathbb{Z}}[\lambda]$, and nullifying all g_i's. (Note that in $\frac{\mathbb{Z}}{2\mathbb{Z}}$, $\bar{c}^2 + \bar{d}^2 = (\bar{c}+\bar{d})^2$). We have;

$$\bar{\lambda}(\bar{\lambda}+1)^2(\bar{g_1}+\bar{g_2})^2 = (\bar{g_3} + (\bar{\lambda}+1)\bar{g_4})^2 = \bar{g_5}^2 + \bar{\lambda}(\bar{\lambda}+1)^2\bar{g_6}^2.$$

Since all the powers of $\bar{\lambda}$ in the middle are even, but odd on the other sides, by unique factorization, all sides must be zero. Therefore, $\bar{g_1} = \bar{g_2}$, $\bar{g_3} = (\bar{\lambda}+1)\bar{g_4}$, $\bar{g_5}^2 = \bar{\lambda}(\bar{\lambda}+1)^2\bar{g_6}^2$. We can apply the same argument to the last equation, and obtain $\bar{g_5} = \bar{g_6} = 0$. Therefore, $2|g_5$ and $2|g_6$, implying that $4|g_5^2 + \lambda(\lambda^2+1)g_6^2$, and similarly, $4|g_3^2 - (\lambda^2+1)g_4^2$, $4|\lambda(\lambda^2+1)(g_1^2+g_2^2)$. For appropriately chosen polynomials h_1, h_2, write $g_1 = g_2 + 2h_1$ and $g_3 = (\lambda+1)g_4 + 2h_2$.

We see that $4|2g_2^2 + 4g_2h_1 + 4h_1^2$ and $4|2\lambda g_4^2 + 4(\lambda+1)g_4h_2 + 4h_2^2$. Therefore, $2|g_1$, $2|g_2$, $2|g_3$, $2|g_4$, and we obtain a contradiction.

Appendix A

Brauer groups of some fields

Let A be a central simple algebra over a field K and let L be a splitting field for A. Choose an L-isomorphism $\Phi : L \otimes A \leftrightarrow \mathbb{M}_n(L)$. For any $x \in A$ the element $det(\Phi(1 \otimes x))$ is independent of the isomorphism Φ. In fact, if $\Phi' : L \otimes A \leftrightarrow \mathbb{M}_n(L)$ is another L-isomorphism, then by Skolem-Noether theorem, there exists an invertible element $u \in \mathbb{M}_n(L)$ such that $\Phi'(z) = u\Phi(z)u^{-1}$ for every $z \in L \otimes A$ so that

$$det(\Phi'(1 \otimes x)) = det(u\Phi(1 \otimes xu^{-1}) = det(\Phi(1 \otimes x))$$

We will call $det(\Phi(1 \otimes x))$ the reduced norm of x (with respect to L) and denote it by $N_{rd}^L(x)$.

We shall show that $N_{rd}^L(x)$ belongs to K, and that it is independent of L. Let L, L' be splitting fields for A and let $\theta : L \to L'$ be a K-monomorphism. Let $\Phi : L \otimes A \leftrightarrow \mathbb{M}_n(L)$ be an L-isomorphism. Then there exists an L'-isomorphism;

$$\Phi' : L' \otimes A \cong L' \otimes_L L \otimes A \leftrightarrow L' \otimes_L \mathbb{M}_n(L) \cong \mathbb{M}_n(L')$$

such that $\Phi' \circ (\theta \otimes 1) = \mathbb{M}_n(\theta) \circ \Phi$. It follows from this that we have for any $x \in A$,

$$N_{rd}^{L'}(x) = \theta(N_{rd}^L(x))$$

Let now L be a Galois splitting field for A. Then, for any element $\sigma \in \mathfrak{G}(L|K)$, we have that,

$$N_{rd}^{L}(x) = \sigma(N_{rd}^{L}(x))$$

This shows that $N_{rd}^{L}(x)$ belongs to K.

Let now L' be any splitting field of A. There exists a field extension L'' of K and K-monomorphisms $\theta : L \to L'', \theta' : L' \to L''$. Therefore,

$$\theta'(N_{rd}^{L'}(x)) = N_{rd}^{L''}(x) = \theta(N_{rd}^{L}(x)) = N_{rd}^{L}(x)$$

This shows that $N_{rd}^{L'}(x)$ is independent of L', and we call it the reduced norm of x and denote it by $N_{rd}(x)$.

Theorem A.1. *Let A be a central simple K-algebra of dimension n^2. Then, for any $x \in A$, if L_x denotes the left multiplication by x in A, we have $det(L_x) = (N_{rd}(x))^n$.*

Proof. Let L be an extension of K such that $L \otimes A \cong \mathbb{M}_n(L)$. Since $det(L_{1\otimes x}) = det(L_x)$, we assume by replacing A by $L \otimes A$ that A is a matrix algebra over K. Thus, we have to show that if $x \in \mathbb{M}_n(K)$, and L_x denotes the left multiplication by x in $\mathbb{M}_n(K)$, then $det(L_x) = (det(x))^n$. Let $\mathbb{M}_n(K) = S \oplus \cdots \oplus S$ (n times), where S is the unique simple (left) $\mathbb{M}_n(K)$-module. If l_x denotes the endomorphism of S induced by x, then we have $det(L_x) = (det(l_x))^n$. But, with respect to a suitable K-basis for S, we can choose the matrix of l_x as x itself. This proves the theorem.

□

Let $\mathbb{H}$ denote the algebra of quaternions over $\mathbb{R}$. For any $x \in \mathbb{H}$, given by $x = a + bi + cj + dk$, denote $\overline{x} = a - bi - cj - dk$. It is easy to show that $\mathbb{H}$ is a central division algebra over $\mathbb{R}$.

It is easy to check that $\overline{x+y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{yx}$ for $x, y \in \mathbb{H}$. This means that $x \to \overline{x}$ defines an isomorphism of $\mathbb{H}$ onto its opposite $\mathbb{H}^\circ$. Hence we have an

$\mathbb{R}$-algebra isomorphism of $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$ onto $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{\circ}$ and the latter is isomorphic to $\mathbb{M}_4(\mathbb{R})$. This shows that the class of $\mathbb{H}$ in $Br(\mathbb{R})$ is of order 2. This gives us some motivation for the following theorem.

Theorem A.2. *The Brauer group of* $\mathbb{R}$ *is cyclic of order two and is generated by the class of* $\mathbb{H}$.

Proof. Let D be any finite dimensional division algebra over $\mathbb{R}$. The center K of D, being a finite algebraic extension of $\mathbb{R}$, is isomorphic to either $\mathbb{C}$ or $\mathbb{R}$. In case $K = \mathbb{C}$, we have $D = \mathbb{C}$, since $\mathbb{C}$ is algebraically closed. Suppose $K = \mathbb{R}$. Then any maximal subfield of D being a proper extension of R is isomorphic to $\mathbb{C}$. Hence, we must have $dim_{\mathbb{R}}(D) = 4$. We fix a maximal subfield L of D and choose $i \in L$ such that $i^2 = -1$. Then $L = \mathbb{R}(i)$. By the Skolem-Noether Theorem, the automorphism $z \to \overline{z}$ of L, given by $a + ib \to a - ib$, can be extended to an inner automorphism of D. This means that there exists an element $u \in D$ such that $uzu^{-1} = \overline{z}$ for all $z \in L$. Since $z \to \overline{z}$ is an automorphism of order 2, we have $u^2 z = zu^2$ for all $z \in L$. Since L is a maximal subfield of D, we have $u^2 \in L$. We claim that u^2 is actually in $\mathbb{R}$. For, if $u^2 \notin \mathbb{R}$, then $\mathbb{R}(u^2) = L$ and $uzu^{-1} = z$ for all $z \in L$, which is a contradiction. Hence $u^2 \in \mathbb{R}$. We assert that $u^2 < 0$. Indeed, if $u^2 = a > 0$, then $u = \pm\sqrt{a}$. This is impossible. Hence $u^2 = -a$ for some $a \in \mathbb{R}$, $a > 0$. We put $j = u/\sqrt{a}$ and $ij = k$. Then we have $j^2 = -1$. Since $j^{-1}ij = -i$, we see that $k = ij = -ji$ and $k^2 = ijij = -i^2 j^2 = -1$. Moreover $k \notin L$, since $k \in L$ implies $j \in L$. Since $dim_L(D) = 2$, $\{1, j\}$ is a basis for D as a vector space over L. Hence $\{1, i, j, k\}$ is a basis for D over R. Thus we have shown that any finite dimensional division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{C}, \mathbb{R}$ or $\mathbb{H}$. Thus the only central division algebras over $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{H}$. □

Definition A.3. Let f be a form (a homogeneous polynomial in one or more variables) over a field K. A field K is said to be C_i if every form $f(X_1, \cdots, X_n)$ in n variables and of degree d, with $n > d^i$, has a non-trivial zero in K; there exist $a_1, \cdots, a_n \in K$, not all zero, such that $f(a_1, \cdots, a_n) = 0$.

The following lemma is stated without proof;

Lemma A.4. *Let K be a C_1 field. Then $Br(K) = \{1\}$.*

We shall use this in order to prove that the Brauer Group of a finite field is always trivial. If we show that all finite fields are C_1, then we are done.

Theorem A.5 (Chevalley)**.** *A finite field is C_1.*

Proof. Let K be a finite field of characteristic p and let $q = p^r$ be the number of elements in K. For a polynomial $f \in K[X_1, \cdots, X_n]$, let $Z(f)$ denote the number of zeros of f in K^n. We may assume that f is a non-constant polynomial. In the field K, we have the identity

$$Z(f) \cdot 1 = \sum_{(x_1, \cdots, x_n) \in K^n} (1 - f^{q-1}(x_1, \cdots, x_n))$$

The polynomial $F(X_1, \cdots, X_n) = 1 - f^{q-1}(X_1, \cdots, X_n)$ is of degree $d(q-1)$. We write,

$$Z(f) \cdot 1 = \sum_{(x_1, \cdots, x_n) \in K^n} F(X_1, \cdots, X_n)$$

For $a_{i_1 \cdots i_n} \in K$, let,

$$F = \sum_{i_1 + \cdots + i_n \leq d(q-1)} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

The above formula can be written as;

$$Z(f) \cdot 1 = \sum_{i_1 + \cdots + i_n \leq d(q-1)} a_{i_1 \cdots i_n} \sum_{(x_1, \cdots, x_n) \in K^n} x_1^{i_1} \cdots x_n^{i_n}$$

We have,

$$\sum_{(x_1, \cdots, x_n) \in K^n} x_1^{i_1} \cdots x_n^{i_n} = (\sum_{x \in K} x^{i_1})(\sum_{x \in K} x^{i_2}) \cdots (\sum_{x \in K} x^{i_n})$$

Since $i_1 + \cdots + i_n \leq d(q-1) < n(q-1)$, we have $i_k < q-1$ for some k. Consider $\sum_{x \in K} x^{i_k}, i_k < q-1$. If $i_k = 0$, then $\sum_{x \in K} x^{i_k} = q = 0$. Suppose $i_k > 0$. Since K is finite, K^* is cyclic. Let $\theta \in K^*$ generate K^*. We then have

$$\sum_{x \in K} x^{i_k} = \sum_{x \in K^*} x^{i_k} = \sum_{0 \leq m \leq q-2} \theta^{m i_k} = \sum_{0 \leq m \leq q-2} (\theta^{i_k})^m$$

Now,

$$(\theta^{i_k} - 1) \sum_{0 \leq m \leq q-2} (\theta^{i_k})^m = (\theta^{i_k})^{q-1} - 1 = 0$$

Since $i_k < q-1, \theta^{i_k} \neq 1$. Hence,

$$\sum_{0 \leq m \leq q-2} (\theta^{i_k})^m = 0$$

Thus $\sum_{x \in K} x^{i_k} = 0$. This shows that $Z(f) \cdot 1 = 0$, so $Z(f) \equiv 0 (\text{mod } p)$. This proves the theorem. □

Corollary A.6. *If K is a finite field, then $Br(K) = \{1\}$.*

Appendix B

Construction of abelian crossed products

In this chapter, we shall talk about how the properties (A) - (D) (modify $b_i = z_i^{q_i}$, instead of $b_i = z_i^2$) determine a unique abelian crossed product, for some Galois extension K over F with Galois group $G = \langle\sigma_1\rangle \oplus \langle\sigma_2\rangle \oplus \cdots \langle\sigma_r\rangle$, where each σ_i has order q_i, for all r, in G.

Consider the ring of polynomials $K[x_1, x_2 \cdots x_r]$ with non-commutative variables satisfying $x_i k = \sigma_i(k) x_i$, for all $k \in K$ and $x_i x_j = u_{ij} x_j x_i$, for all i, j. Call this domain A_r. Consider the left ideal M of A_r generated by $\{x^{q_i} - b_i | 1 \leq i \leq r\}$ and $M_i = \langle x^{q_i} - b_i \rangle$. Notice that these ideals are both two-sided ideals. The algebra (K, G, U, B) is defined as the quotient ring A_r/M. It remains to show that it is an abelian crossed product.

Write $\bar{m} = (m_1, m_2, \cdots m_r)$ for a set of non-negative integers m_i, and $a^{\bar{m}} = a_1^{m_1} a_2^{m_2} \cdots a_r^{m_r}$, for elements of a group or ring $a = (a_1, a_2, \cdots a_r)$. Notice that all elements in G have the form $\sigma^{\bar{m}}$ ($\bar{m}$ is not fixed for each element) and $x^{\bar{m}}$ forms a basis for A_r over K. For some $a \in K$, we can see that $x^{\bar{m}} x^{\bar{n}} = a x^{\bar{m}+\bar{n}}$. Therefore, any monomial $a x^{\bar{m}}$ has a unique degree, and the product $a x^{\bar{m}} b x^{\bar{n}}$ has degree $deg(a x^{\bar{m}}) + deg(b x^{\bar{n}})$.

We shall now show that $z^{\bar{m}} = x^{\bar{m}} + M$ forms a basis of A_r/M over K. For any $f[x] \in A_r$, we can write $f[x] = g[x](x_i^{q_i} - b_i) + h[x]$, where each monomial h has degree less than q_i in x_i. Therefore, $z^{\bar{m}}$ spans A_r/M. It now suffices to show that any for monomial $f[x]$ in M that has degree less than q_i will automatically be 0. Let $f[x] = \sum_{j=1}^{r} h_j[x](x_j^{q_j} - b_j)$. We can assume that each h_j other than h_r has degree less than q_r in x_r. But, $h_r[x](x_r^{q_r} - b_r)$ has degree more than q_r in x_r, unless $h_r = 0$. Inductively, we can see that $f[x] = 0$.

Therefore, $[A_r/M : K] = q_1 q_2 \cdots q_r = n$, and $[A_r/M : F] = n^2$. A_r/M has its maximal subfield as K and its center as F; if $a(\sum a_m z^{\bar{m}}) = (\sum a_m z^{\bar{m}})a$, for all $a \in K$, then $\sum a_m(a - \sigma^{\bar{m}}(a))z^{\bar{m}} = 0$. Thus, if $a_m \neq 0$, $a = \sigma^{\bar{m}}(a)$, for all $a \in K$, so $\bar{m} = (0, 0 \cdots 0)$. Therefore, we must have $a_0 \in K$. If a is central, then $az^{\bar{m}} - z^{\bar{m}}a$ or $\sigma^{\bar{m}}(a) - a$ is 0 for all $\bar{m}$, so $a \in F$. This concludes the construction of the abelian crossed product from our hypothesis.

Bibliography

[1] R. Sridharan. TIFR notes on semisimple rings, central simple algebras, etc., 2007. URL https://drive.google.com/open?id=0B0P0giWGP2NyQndRd2Z2SXUzZDQ.

[2] SA Amitsur, Louis H Rowen, and JP Tignol. Division algebras of degree 4 and 8 with involution. *Bulletin of the American Mathematical Society*, 1(4): 691–693, 1979.

[3] Louis Halle Rowen. Central simple algebras. *Israel Journal of Mathematics*, 29(2):285–301, 1978.

[4] SA Amitsur and D Saltman. Generic abelian crossed products and p-algebras. *Journal of Algebra*, 51(1):76–87, 1978.