A Survey of the Classification of Division Algebras over Fields

by

Michelle Roshan Marie Ashburner

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2008

Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

For a given field F we seek all division algebras over F up to isomorphism. This question was first investigated for division algebras of finite dimension over F by Richard Brauer. We discuss the construction of the Brauer group and some examples. Crossed products and PI algebras are then introduced with a focus on Amitsur's non-crossed product algebra. Finally, we look at some modern results of Bell on the Gelfand-Kirillov dimension of finitely generated algebras over F and the classification of their division subalgebras.

Acknowledgements

I would like to thank my supervisor Professor John Lawrence for his many hours of help in preparing this thesis. My understanding and appreciation of the concepts in this thesis have greatly increased due to his patience and instruction. Many thanks also to my readers Professor Ross Willard and Professor Frank Zorzitto who have helped eliminate this text of conceptual and typographical errors. I am very grateful for the help and encouragement provided by my student colleagues of the Department of Pure Mathematics, as well as the guidance on the latex program provided by Collin Roberts, Eric Martin and Dr. Nico Spronk.

Dedication

This thesis is dedicated to my parents, my sister Tina and my brother Ramadhani

Contents

Chapter 1

Introductory Remarks

1.1 Basic Definitions and Facts

Assumed Background Knowledge The reader should be familiar with senior level ring and group theory. Concepts not routinely taught in an undergraduate mathematics program are defined within the text. Many fundamental results are presented in this chapter as well as any definitions necessary to the presentation of later material.

Notation All scalar multiplication and conjugation is defined using left multiplication, and all one-sided ideals are assumed to be left ideals. Thus all function symbols act on their arguments from the left.

Definition 1.1.1. Ring *We define a ring* $(R, +, \bullet)$ *to be an abelian group under the binary operation* $+$*, equipped with an associative multiplication* $\bullet$*, left and right distributivity across* $+$ *and containing the multiplicative identity* 1*.*

Definition 1.1.2. Matrix Ring *We denote the* $n \times n$ *matrix ring with entries from a field* F *by* $M_n(F)$

Definition 1.1.3. Algebra *An algebra A is a vector space over a field F equipped with an associative multiplication $\bullet$. For any algebra A we have the following:*

$a(x \bullet y) = (ax) \bullet y = x \bullet (ay)$
$a(x + y) = ax + ay$
$(x + y)a = xa + ya$

$\forall x, y \in A$ and $a \in F$. In all cases the centre of A is a commutative ring; in particular the following definition deals with the specific class of algebras with the scalar field F as their centres. We write A/F to denote that A is an algebra over F.

One can generalize the above definition to include all rings A with scalars coming from a commutative ring R.

Definition 1.1.4. Simple Ring *A ring R is called simple if the only two-sided ideals of R are $\{0\}$ and R.*

Definition 1.1.5. Central Simple Algebra *A Central Simple Algebra (CSA) is a simple algebra A/F such that $Z(A) = F$. When denoting a CSA with centre F, we write F-CSA instead of A/F.*

Definition 1.1.6. Division Algebra *Let F be a field. A division algebra (or division ring) is an algebra D/F such that $\forall d \in D$ $\exists u \in D$ such that $d \bullet u = u \bullet d = 1_D$. We denote u by d^{-1} and refer to it as the two-sided inverse of d. If $F = Z(D)$ then D is an F-CSA. We are mainly interested in central division algebras over a given field.*

Remark 1.1.7. *Division algebras were probably first investigated in 1843 when Hamilton invented the quaternion algebra $\mathbf{H} = \{a+bi+cj+dk \colon a, b, c, d \in \mathbf{R}, i^2 = j^2 = k^2 = -1, ij = k\}$. The inverse of a general element in $\mathbf{H}$ is $(a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$.*

Definition 1.1.8. Algebra Map *Let A and B be algebras over F. Then a homomorphism $f\colon A \to B$ is called an algebra map if f fixes F element-wise. This definition may be extended to R-module homomorphisms where R is any ring.*

Definition 1.1.9. Tensor Product *Let U, V be vector spaces over a field F. Let X denote the free abelian group on the set $U \times V$. Let Y be the subgroup of X generated by the following set:*

$\{(a,b)+(a',b)-(a+a',b), (a,b)+(a,b')-(a,b+b'), (\lambda a,b)-(a,\lambda b)\}$ *where $a \in U$ $b \in V$ and $\lambda \in F$*

Then we define the tensor product of U and V over F, $U \otimes_F V$, to be the quotient X/Y.

We write $a \otimes b \in U \otimes_F V$ for the class represented by (a,b) and refer to $a \otimes b$ as an elementary tensor. Clearly $U \otimes V$ is an abelian group under $+$ but we now make it into an F-vector space by defining $\lambda(a \otimes b) = (\lambda a) \otimes b$. The rule for multiplying elementary tensors uses the associative multiplication from the algebras A and B: $(a \otimes b)(a' \otimes b') = (aa' \otimes bb')$. Any element in $A \otimes B$ can be expressed as an F-linear combination of elementary tensors. We note here that if $dim(U) = m$ and $dim(V) = n$ then given a basis $\{u_1, ..., u_m\}$ for U and a basis $\{v_1, ..., v_n\}$ for V the set $\{u_i \otimes v_j\colon 1 \leq i \leq m \text{ and } 1 \leq j \leq n\}$ of elementary tensors is a basis for $U \otimes_F V$.

Notation 1.1.10. *We write $U \otimes V$ if it is clear which field the tensor product is taken over. We write 0 as shorthand for $(0 \otimes 0) = (a \otimes 0) = (0 \otimes b)$.*

Definition 1.1.11. Multiplication of Algebras *Let A and B be F-CSAs. Then as above their tensor product $A \otimes B$ can always be constructed. As shown below $A \otimes B$ is also an F-CSA. Furthermore, if A and B are division algebras over F, their tensor product $A \otimes B$ is again an F-CSA but need not be a division algebra. An example of this will be presented below.*

Lemma 1.1.12. Products of Simple Algebras *Let A be an F-CSA and let B be a simple algebra over F, so we have $F \subseteq Z(B)$. Then $A \otimes_F B$ is simple.*

Proof: let I be a non-zero ideal in $A \otimes B$. We must show that $I = A \otimes B$. For $u \in I$, $u \neq 0$ we may write $u = \sum a_i \otimes b_i$ for $a_i \in A$ and $b_i \in B$. Moreover, without loss of generality the b_i can be taken to be linearly independent over F. We call the number of non-zero a_i in the expression the length of u. Choose $u \in I$ of minimal length m. Let $r, s \in A$. Then $(r \otimes 1)u(s \otimes 1)$ $= (r \otimes 1) \sum a_i \otimes b_i (s \otimes 1) = \sum r a_i s \otimes b_i$ is again in I, since I is an ideal. Now since A is simple, the ideal generated by a_i, Aa_iA, is equal to A whenever $a_i \neq 0$. Thus for all $a_i' \in A$ there are $r_j, s_j \in A$ such that $\sum_j r_j a_i s_j = a_i'$. In particular choose $a_1' = 1$. Now, since $u \in I$ we may construct the element $u_1 = \sum (r_j \otimes 1)(a_i \otimes b_i)(s_j \otimes 1)$ which is again in I. Rearranging the order of summation and properties of $\otimes$ gives $u_1 = \sum_i (\sum_j r_j a_i s_j) \otimes b_i \in I$. After making the substitution $\sum_j r_j a_i s_j = a_i'$ with our choice for a_1', we finally have: $u_1 = 1 \otimes b_1 + a_2' \otimes b_2 + \cdots + a_m' \otimes b_m$. Moreover u_1 has the same length as u, so that $a_i \neq 0$. Now we note that for each $a \in A$ we have $(a \otimes 1)u_1 - u_1(a \otimes 1) \in I$, which gives $(a \otimes 1)(1 \otimes b_1 + \cdots + a_m' \otimes b_m) - (1 \otimes b_1 + \cdots + a_m' \otimes b_m)(a \otimes 1) \in I$, that is, $(a_2'a - aa_2') \otimes b_2 + \cdots + (a_m'a - aa_m') \otimes b_m \in I$. However since the first term vanishes, we have that the length of this element is always less than that of u_1, so must equal 0. Now since the b_i are linearly independent over F we have that the $1 \otimes b_i$ are linearly independent over $A \otimes 1$. Thus we must have $(a_i'a - aa_i') = 0$, $i = 2, \cdots m$, therefore $a_i'a = aa_i'$ so that a_i' lies in F, the centre of A. Rewrite $a_i' = \alpha_i \in F$, giving us that $u_1 = 1 \otimes b_1 + \alpha_2 \otimes b_2 + \cdots + \alpha_m \otimes b_m = 1 \otimes (b_1 + \alpha_2 b_2 + \cdots + \alpha_m b_m) \in I$ by properties of $\otimes$. Letting $b = b_1 + \alpha_2 b_2 + \cdots + \alpha_m b_m$ we know $b \neq 0$ because the b_i are independent over F and $a_i' \neq 0$. Recall $(1 \otimes b_1)(u_1)(1 \otimes b_2) \in I$ for all $b_1, b_2 \in B$, which gives $(1 \otimes B)(1 \otimes b)(1 \otimes B) \subseteq I$, therefore $(1 \otimes BbB) \subseteq I$, so that $1 \otimes B \subseteq I$ by B simple. But then $(a \otimes 1)(1 \otimes b) \in I$, thus $(A \otimes 1)(1 \otimes B) \subseteq I$ so we get that $A \otimes B = I$. Thus $A \otimes B$ is simple. ■

Proposition 1.1.13. $A \otimes B$ is a CSA *Let A and B be F-CSAs. Then their tensor product $A \otimes B$ is again a CSA with centre $F \otimes F \cong F$.*

Proof: $A \otimes B$ is an F-vector space, thus it follows from the associativity of the multiplications in A and B that $\bullet$ is associative, that is, $A \otimes B$ is an F-algebra. We examine the centre of $A \otimes B$: let $0 \neq z \in Z(A \otimes B)$. We write $z = a_1 \otimes b_1 + ... + a_n \otimes b_n$ where n is the length of z. As in the above lemma, the b_i are F-independent, thus as above we have for each $a \in A$, $0 = (a \otimes 1)z - z(a \otimes 1) = \sum_i (aa_i - a_i a) \otimes b_i$ which implies that $(aa_i - a_i a) \otimes b_i = 0$ for each i. Thus $aa_i - a_i a = 0$, so that $aa_i = a_i a$ for all i and for each $a \in A$. Thus each $a_i \in F$, the centre of A. Setting $b = a_1 b_1 + ... + a_n b_n \in B$ we have $z = 1 \otimes b$. If $b' \in B$ we have: $0 = z(1 \otimes b') - (1 \otimes b')z = (1 \otimes b)(1 \otimes b') - (1 \otimes b')(1 \otimes b) = 1 \otimes (bb' - b'b)$, therefore $bb' = b'b$, so that b lies in F. Therefore $z = 1 \otimes b$ for some $b \in F$, which gives us that $z \in F \otimes F$. So $Z(A \otimes B) \subseteq F \otimes F$; however the reverse inclusion is very easy to show. We may conclude that $Z(A \otimes B) = F \otimes F$. It therefore remains to prove that $A \otimes B$ is indeed simple, but this is a special case of the above lemma. ■

Products of Division Algebras Consider the following algebras over $\mathbf{R}$: $\mathbf{C}$ and $\mathbf{H}$, Hamilton's quaternions. These are both division algebras, yet their tensor product $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{H}$ is not, as it is isomorphic to $M_2(\mathbf{C})$ in which live non-zero, non-invertible elements. An example is the singular element $\begin{bmatrix} i & 1 \\ -1 & i \end{bmatrix}$. Thus in many cases, our study of division algebras over a field F will begin with an examination of the wider class of F-CSAs, which is closed under tensor products.

Lemma 1.1.14. Algebras as Tensor Products *Let A be any finite dimensional algebra over a field F. Suppose we have F-subalgebras S, T of A such that the following three statements hold:*

1) $st = ts \ \forall s \in S \ \forall t \in T$
2) $A = ST$ *as a product of rings*
3) $[A\colon F] = [S\colon F][T\colon F]$

Then $A \cong S \otimes_F T$.

Proof: Consider the mapping $\phi\colon S \times T \to A$, $\phi\colon (s,t) \mapsto st$. Then we have an F-linear map $f\colon S \otimes_F T \to A$ such that $f\colon s \otimes t \mapsto st$. Therefore, $f((s \otimes t)(s' \otimes t')) = f(ss' \otimes tt') = ss'tt' = sts't'$ by 1), which is $f(s \otimes t)f(s' \otimes t')$. So we have that f is an F-algebra map. Moreover f is surjective since 2) gives us $A = ST$. Finally, 3) tells us that $dim_F(S \otimes T) = dim_F(A)$, thus f is an F-isomorphism. We have $A \cong S \otimes_F T$. ■

Definition 1.1.15. Opposite Algebra *Let* A/F *be an algebra. Define* A^{op} *to be the vector space* A *equipped with multiplication* $a \cdot b = ba \ \forall a, b \in A$, *where* ba *is the usual product in* A. *It is easily shown that if* A *is an* F*-CSA then* A^{op} *is again a CSA.*

Definition 1.1.16. Bimodule *Let* R, S *be associative rings, and let* M *be an abelian group. Then we can view* M *as a left* R*-module as well as a right* S*-module. Then we call* M *an* (R,S)*-bimodule if* $\forall r \in R, s \in S$ *and* $m \in M$ *we have:* $(rm)s = r(ms)$.

Lemma 1.1.17. Bimodules and Tensor Products *Let* R, S *be algebras over a field* F. *If* M *is an* (R,S)*-bimodule then* M *is automatically a left* $R \otimes_F S^{op}$*-module, with* $(r \otimes s)m = rms$.

Proof: Consider the mapping $f\colon R \times S^{op} \times M \to M$, $f\colon (r,s,m) \to rms$. Then the first step is to ensure that the multiplication $(r \otimes s)m = rms$ is well-defined. This follows from the universal property and the fact the map is k-trilinear. We now verify the module axioms for M. We have $(r \otimes s)(m + m') = r(m + m')s = rms + rm's = (r \otimes s)m + (r \otimes s)m'$ from

the supposition; similarly $[(r \otimes s) + (r' \otimes s')]m = (r \otimes s)m + (r' \otimes s')m$. To show associativity across multiplication in $R \otimes S^{op}$ and M let $s * s'$ be the multiplication in S^{op}, i.e. $s * s' = s's \in S$. Then: $[(r \otimes s)(r' \otimes s')]m = [rr' \otimes s * s']m = (rr')m(s * s') = (rr')m(s's) = r(r'ms')s = (r \otimes s)[r'(ms')] = (r \otimes s)[(r' \otimes s')m]$. The fourth axiom is straightforward. ■

Definition 1.1.18. Algebraic Splitting Field *Let A be an F-CSA. A splitting field of A is a field extension K/F such that $\exists n \in \mathbf{N}$ with $K \otimes_F A \cong M_n(K)$. An example of a splitting field for A is $\bar{F}$, the algebraic closure of F.*

1.2 Some Fundamental Theorems

The Artin-Wedderburn Theorem, originally proven for F-algebras and later expanded to include any simple Artinian ring, is used heavily in chapters 2 and 3. The result leads to many structure theorems about rings and algebras, as we will soon see. The proof can be found in [11], p48.

Theorem 1.2.1. Artin-Wedderburn *A non-trivial right-Artinian simple ring is isomorphic to $M_n(D)$ for D a division ring. Moreover, if we have such a ring R such that $R \cong M_{n_1}(D_1) \cong M_{n_2}(D_2)$, we can conclude that $n_1 = n_2$ and $D_1 \cong D_2$.*

Corollary 1.2.2. Matrix Realizations *Let A be an F-CSA of finite dimension. Then we have an isomorphism $A \cong D \otimes M_n(F)$ for some division ring D with centre F and $n \in \mathbf{N}$.*

Theorem 1.2.3. Schur's Lemma *Let R be any ring and let A, B be simple left R-modules. Then we have:*

1) If $f\colon A \to B$ is a non-zero R-map, then f is an R-isomorphism.
2) $End_R(A)$ is a division algebra.

Proof: 1) A is simple, therefore its submodules are A and $\{0\}$. Consider the submodule $ker(f) \subseteq A$. It cannot equal A since f is non-zero. Thus $ker(f) = \{0\}$ so f is injective. Moreover, consider the submodule $im(f) \subseteq B$. Then the same reasoning gives us that $im(f) \neq \{0\}$, so $im(f) = B$. So f is an R-isomorphism.

2) By part 1) we know that if f is a non-zero R-map $f\colon A \to A$, then f is an isomorphism so that an inverse f^{-1} exists. Since these f are precisely the elements of $End_R(A)$, we conclude it is a division algebra. ■

Definition 1.2.4. Algebraic and Separable Extensions *Let D/F be a division algebra. We say D/F is algebraic if $\forall a \in D\ \exists f(x) \in F[x]$ with $f(a) = 0_D$. Suppose D/F is algebraic and $a \in D$. Then we say $f(x) \in F[x]$ is the minimal polynomial of a if it is irreducible and of smallest degree in $F[x]$ such that $f(a) = 0$. Without loss of generality we suppose $f(x)$ is monic, thus making it unique. An element $a \in D$ is called separable if $f(x)$ has no repeated roots, and D/F is then called separable if every element of D is separable.*

Theorem 1.2.5. Jacobson-Noether *Let D/F be a non-commutative division algebra such that D is algebraic over F. Then there is an element in $D\backslash F$ that is separable over F.*

Proof: Case D/F is of characteristic 0: then the extension is separable and there is nothing to prove. Case D/F is of characteristic $p \neq 0$: suppose for contradiction that there are no separable elements in $D\backslash F$, i.e. D is purely inseparable over F. Thus for any $a \in D$ we have $a^{p^n} \in F$ for some $n \geq 0$. It follows that there is a $b \in D\backslash F$ such that $b^p \in F$.

Consider the map $\delta\colon D \to D$ by $\delta\colon x \mapsto xb - bx$. Since $p \neq 0$, p applications of δ gives $xb^p - b^p x$ and this is 0 since $b^p \in F$, the centre of D. Furthermore, we know that $\delta \neq 0$ since $b \neq F$. Thus if $\delta(y) \neq 0$, then there exists a $k > 1$ with $\delta^k(y) = 0$ but $\delta^{k-1}(y) \neq 0$. We set $x = \delta^{k-1}(y)$. Because $k > 1$

we may write $x = \delta(\delta^{k-2}(y)) = \delta(w)$ for some $w \in D$. So $x = wb - bw$. We also have $\delta(x) = 0$, i.e. $xa = ax$. Since D is a division algebra, we set $u = xa^{-1}$ to write $x = au$. From the above equation we have $au = wa - aw$, therefore $a = (wa - aw)u^{-1} = (wu^{-1})a - a(wu^{-1})$, since it is easy to show that u commutes with a. Setting $c = wu^{-1}$ we have $a = ca - ac$, that is, $c = 1 - aca^{-1}$. There exists a $t \geq 0$ such that $c^{p^t} \in F$, giving us that $c^{p^t} = (1 + aca^{-1})^{p^t} = 1 + (aca^{-1})^{p^t} = 1 + c^{p^t}$ since $c^{p^t} \in F$, the centre of D. Therefore $c^{p^t} - c^{p^t} = 1$, which proves that there must exist a separable element in $D \backslash F$. ■

Chapter 2

The Brauer Group

2.1 The Noether-Skolem Theorem

The following Theorem is an essential tool to proving some technical results that follow, and a powerful result in its own right. Below we present a version using F-algebras. For a more general statement the reader can consult [11], p99.

Theorem 2.1.1. Generalization of Noether-Skolem *Let F be a field, and A be an F-CSA and let B/F be a simple algebra. If there are algebra maps $f, g\colon B \to A$, then there is a unit $u \in A$ such that $g(b) = uf(b)u^{-1}$ $\forall b \in B$.*

Proof: Define an action $*$ of B on A by: $b * a = f(b)a$. Then $*$ allows us to view A as a left B-module. Moreover we may view this left B-module as a right A-module, since for each $x \in A$ we have $(f(b)x)a = f(b)(xa)$. Thus we have A a (B, A)-bimodule, we denote it by ${}_fA$, By the Bimodules and Tensor Products Lemma, this (B, A)-bimodule is a left $(B \otimes_F A^{op})$-module, where $(b \otimes a)a' = ba'a$ for all $a \in A$. Similarly we can form ${}_gA$, another left $(B \otimes A^{op})$-module. By Lemma 1.1.10 $(B \otimes A^{op})$ is a simple F-algebra, and since A itself can be viewed as a $(B \otimes A^{op})$-module using $id\colon B \to A$, we have

$[{}_fA\colon \Delta] = [A\colon \Delta] = [{}_gA\colon \Delta]$ for Δ the division ring associated with A. One can now show ([20], p566 for example) that ${}_fA \cong {}_gA$ as $(B \otimes A^{op})$-modules, so we have an algebra isomorphism $\phi\colon {}_fA \to_g A$. We have the identity

$$\phi(f(b)aa') = g(b)\phi(a)a' \forall b \in B; a, a' \in A \qquad (\star)$$

Moreover ϕ is also an automorphism of A as a right A-module, so that $\phi(a) = \phi(1a) = \phi(1)a = ua$ for $u = \phi(1) \in A$. We note here that $\phi^{-1}(a) = \phi^{-1}(1)a = u'a$, where $u' = \phi^{-1}(1)$. Then if $a \in A$, we have $a = \phi\phi^{-1}(a) = \phi(u'a) = uu'a$. When $a = 1$, we have $1 = uu'$. Similarly we can show $1 = u'u$, so u is a unit in A. Finally equation $(\star)$ becomes $uf(b)a = \phi(f(b)a) = g(b)\phi(a) = g(b)ua$ for each $a \in A$. Once more setting $a = 1$, we see that $uf(b) = g(b)u$ implies that $g(b) = uf(b)u^{-1}$, as desired. ■

Corollary 2.1.2. Noether-Skolem *Let A be an F-CSA and let $C/F, C'/F$ be isomorphic simple subalgebras. If $\psi\colon C \to C'$ is an algebra isomorphism then there exists an invertible element $u \in A$ with $\psi(c) = ucu^{-1}$ $\forall c \in C$.*

Proof: In the above theorem, take f to be the inclusion $C \hookrightarrow A$, take $C' = \text{im}\psi$ and $g = i\psi$ where $i\colon C' \hookrightarrow A$.

2.2 Maximal Subfields

Definition 2.2.1. Maximal Subfield *Let A be an F-CSA of finite dimension. A maximal subfield of A is a field $L \subseteq A$ such that for any field K with $F \subseteq K \subseteq A$ we have $L \subseteq K$ implies $L = K$.*

Definition 2.2.2. Extending the Base Field *Let A be an F-CSA and K/F a field extension. If K is maximal, then $A \otimes_F K$ is a K-CSA. This is a direct consequence of universal property of free groups. Taking the tensor product of a CSA with a maximal subfield is called extending the base*

field. This will become helpful later when we require the base field of A to be separable.

Definition 2.2.3. Centralizer *Let D/F be a division algebra and let $S \subseteq D$. The centralizer of S in D is defined as $C_D(S) = \{x \in D \colon xs = sx \ \forall s \in S\}$ When it is clear which algebra we are taking centralizers in, we omit the subscript and simply write $C(S)$ for $C_D(S)$.*

Proposition 2.2.4. Centralizers and Subalgebras *Let A be an F-CSA of finite dimension and let B be a simple subalgebra. Then we may conclude:*

1) $C_A(B)$ is also a simple F-algebra
2) $B \otimes_F A^{op} \cong M_m(D)$ and $C_A(B) \cong M_n(D)$ where $m, n \in \mathbf{N}$ such that $n \mid m$ and D is a division algebra over F
3) $[B \colon F][C_A(B) \colon F] = [A \colon F]$
4) $C_A(C_A(B)) = B$

The fourth result is the most important one to this section. The proofs of statements 1) - 3) are omitted, but can be found in most comprehensive algebra texts, including [20], p731. Below we prove statement 4).

Proof: Let $b \in B$ and $u \in C_A(B) = C(B)$. Then $bu = ub$, so that $b \in C(C(B))$, therefore $B \subseteq C(C(B))$. However by statement 1), $C(B)$ is a simple subalgebra of A, thus the equation $[A \colon F] = [B \colon F][C(B) \colon F]$ above can be used with $C(B)$ substituted for the simple subalgebra B to give: $[A \colon F] = [C(B) \colon F][C(C(B)) \colon F]$. Equating the above gives us $[B \colon F] = [C(C(B)) \colon F]$. In light of this and the fact that $B \subseteq C(C(B))$, we conclude that $C(C(B)) = B$. ■

Lemma 2.2.5. Characterization of Maximal Subfields *Let D/F be a division algebra of finite dimension and K a subfield of D. Then K is a maximal subfield of D if and only if $K = C(K)$.*

Proof: ($\Longrightarrow$) Let K be a maximal subfield of D. It is clear that $K \subseteq C(K)$, so we wish to show $C(K) \subseteq K$. Let $a \in C(K)$. Then $K \subseteq K(a)$, where $K(a)$ is a field extension of K contained in D. However by K maximal, we must have $K(a) = K$, which means that $a \in K$. Therefore $C(K) \subseteq K$ and we are done. ■

($\Longleftarrow$) Suppose $K = C(K)$ and let L be a subfield of D such that $K \subseteq L$. It follows that every element of L commutes with any element of K. Thus $L \subseteq C(K) \rightarrow L \subseteq K \rightarrow L = K$. Thus K is maximal. This concludes the proof. ■

Theorem 2.2.6. Maximal Subfield Theorem I *Let D/F be a division algebra of finite dimension. Then D contains a maximal subfield L such that the field extension L/F is separable.*

Proof: Case $D = F$: We take $L = F$ and obtain a separable extension. Case $D \neq F$: Then since D/F is finite-dimensional, it is an algebraic extension. We may appeal to the Jacobson-Noether Theorem to find an element $a \in D \backslash F$ that is separable over F. Thus there exist separable subfields of D with $F \subsetneq D$. Let K be maximal with this property.

Claim: K is a maximal subfield of D. Proof: We appeal to the above lemma and show that $K = C_D(K)$. K is commutative, thus we have $K \subseteq C(K)$. Moreover K is certainly simple, thus we employ Proposition 2.2.4 part 4) to see that $K = C(C(K))$. In other words, K is the centre of $C(K)$. Suppose now for contradiction that $C(K) \neq K$. Then by Jacobson-Noether there is an element $u \in C(K) \backslash K$, which is separable over K, thus we have that $K(u)/F$ is a separable extension properly containing K. However we chose K the largest field separable over F, thus we have a contradiction. We conclude that $K = C(K)$, therefore K is a separable, maximal subfield of D by the Characterization of Maximal Subfields. ■

Lemma 2.2.7. Subalgebras and Tensor Products *Let A be an F-CSA and B be a simple subalgebra. Then there is a division ring D with centre F such that $B^{op} \otimes_F A \cong M_n(D)$.*

Proof: By Proposition Centralizers and Subalgebras, we know that $B \otimes A^{op} \cong M_k(D')$ for some division algebra D'/F. Thus $(B \otimes A^{op})^{op} \cong (M_k(D'))^{op}$. However it is not difficult to show that $(M_k(D'))^{op} \cong M_k(D'^{op})$, or that $(B \otimes A^{op})^{op} \cong B^{op} \otimes A$. Thus setting $D = D'^{op}$ and $k = n$ gives the desired result. ■

Theorem 2.2.8. Degree of Maximal Subfields *Let A be an F-CSA and let L, M be maximal fields of A. Then $[L : F] = [M : F]$, that is, all maximal subfields of an F-CSA A have the same degree over F.*

Proof: We begin by proving the following result: let D/F be a finite-dimensional division algebra and let L be a maximal subfield of D. Then $L \otimes_F D \cong M_n(L)$ for some $n \in \mathbf{N}$, i.e. L is a splitting field for D. Furthermore $n = [D\colon L] = [L\colon F]$. First of all we know that $C(L) = L$, thus $L \cong M_n(D')$ for some division ring D' over F and $n \in \mathbf{N}$ by Centralizers and Subalgebras. This tells us since L is commutative that n must be 1. Thus $D' \cong L$. We appeal to the above lemma to give $L^{op} \otimes D \cong M_n(L)$, so that $L \otimes D \cong M_n(L)$. We now compute n. Again by Centralizers and Subalgebras we have $[D\colon F] = [L\colon F][L\colon F] = [L\colon F]^2$, since L is maximal. On the other hand $[L \otimes D\colon F] = [M_n(L)\colon F] = n^2[L\colon F]$ by the above computation. Thus $n^2 = [D\colon L]$ for the degrees to agree. So $n^2 = [D\colon F] = [L\colon F]^2$, therefore $n = [L\colon F]$. Now, since all we used was the maximality of L in D, the same argument shows that $[D\colon F] = [M\colon F]^2$, therefore $[L\colon F] = [M\colon F]$. ■

Lemma 2.2.9. Maximal Subfields are Conjugate *Let A be an F-CSA. If L and L' are maximal subfields of A, then they are conjugate.*

Proof Outline: L and L' are certainly simple subalgebras of A; moreoever they are isomorphic as a consequence of A being a semisimple Artinian ring and L, L' being irreducible F-modules. For a proof of this see [11], p98. The Noether-Skolem Theorem then allows us to conclude L and L' are conjugate.

2.3 Building a Brauer Group

Lemma 2.3.1. Products with Opposite Algebras *Let A be an F-CSA and let A^{op} be the opposite algebra over F. Then we have $A \otimes_F A^{op} \cong M_n(F)$ where $n = [A : F]$.*

Proof: Let $L(A)$ denote the ring of linear transformations on A over F. Then $L(A) \cong M_n(F)$, thus it has dimension n^2 over F. Let $A_r = \{R_a \in L(A) \colon a \in A\}$, where R_a is the transformation $x \mapsto xa$ and let $A_l = \{L_a \in L(A) \colon a \in A\}$, where L_a is the transformation $x \mapsto ax$. Then we consider the maps: $A \longrightarrow A_r$, $a \mapsto R_a$ and $A^{op} \longrightarrow A_l$, $a \mapsto L_a$ One can check that these are F-isomorphisms. Thus we have: $A \otimes_F A^{op} \cong A_r \otimes_F A_l$. Now A_l and A_r are F-CSA's, thus so is $A_r \otimes A_l$. Consider the map $A_r \otimes A_l \longrightarrow A_r A_l$, $\sum R_a \otimes L_b \mapsto \sum R_a L_b$. By definition, this map is surjective and moreover is a homomorphism since elements of A_r and A_l commute pairwise with each other. Since the domain is simple, we must also have injectivity and so these are isomorphic. We now have $A \otimes A^{op} \cong A_r A_l \subseteq L(A)$.

Claim: $A_r A_l = L(A)$. Proof: $n^2 = [A \colon F]^2 = [A \otimes A^{op} \colon F] = [A_r A_l \colon F] \leq [L(A) \colon F] = n^2$. Thus they are equal and we conclude $A \otimes_F A^{op} \cong L(A) \cong M_n(F)$. ■

Lemma 2.3.2. Matrix Rings as Tensor Products *Let A be an F-algebra and $n \geq 1$. Then we have $A \otimes_F M_n(F) \cong M_n(A)$.*

Proof: Let e_{ij} be the matrix with 1 in the ij^{th} position and 0 elsewhere. If $\{a_1, ..., a_m\}$ is a F-basis for the CSA A then the elementary tensors $\{a_k \otimes e_{ij}\}$ as $1 \leq k \leq m$ and $1 \leq i, j \leq n$ forms a basis for $A \otimes_F M_n(F)$. For a basis element $a_k \otimes e_{ij}$ we have the corresponding basis element $(a_k)_{ij}$ for $M_n(A)$, i.e. the $n \times n$ matrix with a_k in the ij^{th} position and 0 elsewhere. This describes completely the required isomorphism. ■

Lemma 2.3.3. Products of Matrix Rings *Let F be a field and $r, s \in \mathbf{N}$. Then $M_r(F) \otimes_F M_s(F) \cong M_{rs}(F)$.*

Proof: Suppose we have F-vector spaces V and W such that $[V\colon F] = r$ and $[W\colon F] = s$. it can be shown that $End_F(V) \otimes_F End_F(W) \cong End_F(V \otimes_F W)$. If we take S to be the subalgebra of $End_F(V \otimes W)$ consisting of all $f \otimes 1_W$ and T to be the subalgebra of $End_F(V \otimes W)$ consisting of all $1_V \otimes g$ then S and T satisfy the three conditions of Lemma 1.1.14, thus we have $End_F(V \otimes W) \cong S \otimes T$, therefore $M_{rs}(F) \cong M_r(F) \otimes M_s(F)$. ■

Lemma 2.3.4. $[A\colon F]$ **is a Square** *Let A be a finite dimensional F-CSA. Then its dimension $[A\colon F]$ as a vector space over F is a square.*

Proof: We first prove the result when A is a central division algebra. Let D be a division algebra with centre F and consider the product $D \otimes_F \overline{F}$, call this $\overline{D}$. Since D is an F-CSA and the algebraic closure $\overline{F}$ is clearly an $\overline{F}$-CSA. Thus we know the product $\overline{D}$ is an $\overline{F}$-CSA, in particular it is simple. By a degree argument we have that $[\overline{D}\colon F] = [\overline{D}\colon \overline{F}][\overline{F}\colon F] = [D\colon F][\overline{F}\colon F]$, thus $[\overline{D}\colon \overline{F}] = [D\colon F]$. Invoking the Wedderburn-Artin Theorem we have that $\overline{D} \cong M_n(F)$ for some $n \in \mathbf{N}$ and division algebra D. We have that $[\overline{D}\colon \overline{F}] = n^2$, thus $[D\colon F] = n^2$.

Now consider a F-CSA A. Then Wedderburn-Artin gives us $A \cong M_m(D)$ for some $m \in \mathbf{N}$ and division algebra D over F. By the above argument

$[D\colon F] = n^2$, giving us that $[A\colon F] = [A\colon D][D\colon F] = m^2n^2$. This proves the lemma. ■

Definition 2.3.5. Brauer Equivalence *Let A and B be F-CSAs. We say $A \sim_{\mathcal{B}} B$ if $\exists\ r, s \in \mathbf{N}$ such that $M_r(A) \cong M_s(B)$. We read this as: A is Brauer Equivalent to B.*

Proposition 2.3.6. Brauer Equivalence is an Equivalence Relation *Let $\mathcal{C}$ denote the class of F-CSAs. Then the relation $\sim_{\mathcal{B}}$ on $\mathcal{C}$ is an equivalence relation.*

Proof: Let A be an F-CSA such that $[A : F] = n$. Then $A \cong M_1(A)$ so we take $r = s = 1$ to see that $A \sim_{\mathcal{B}} A$. Suppose now that $A \sim_{\mathcal{B}} B$ for F-CSAs A and B. Then $M_r(A) \cong M_s(B)$ so in this case we switch r and s to see that $B \sim_{\mathcal{B}} A$. Finally suppose that $A \sim_{\mathcal{B}} B$ and $B \sim_{\mathcal{B}} C$ for F-CSAs A, B, C. Then there are $r, s, t, u \in \mathbf{N}$ such that $M_r(A) \cong M_s(B)$ and $M_t(B) \cong M_u(C)$. On the other hand we have: $M_r(A) \cong_F A \otimes M_r(F)$, $M_s(B) \cong B \otimes M_s(F)$, $M_t(B) \cong B \otimes M_t(F)$ and $M_u(C) \cong C \otimes M_u(F)$. Thus $A \otimes M_r(F) \otimes M_t(F) \cong A \otimes M_{rt}(F)$ by the Products of Matrix Rings Lemma. At the same time we have $A \otimes M_r(F) \otimes M_t(F) \cong B \otimes M_s(F) \otimes M_t(F) \cong B \otimes M_t(F) \otimes M_s(F) \cong C \otimes M_u(F) \otimes M_s(F) \cong C \otimes M_s(F) \otimes M_u(F) \cong C \otimes M_{su}(F)$. Equating both sides we get $A \otimes M_{rt}(F) \cong C \otimes M_{su}(F)$, thus $M_{rt}(A) \cong M_{su}(C)$. Thus $A \sim_{\mathcal{B}} C$ and $\sim_{\mathcal{B}}$ is an equivalence relation. ■

Definition 2.3.7. Brauer Multiplication *Let A be an F-CSA and let $[A] = \{B\colon B$ is an F-CSA and $B \sim_{\mathcal{B}} A\}$. It is easy to see that the mapping $A \to [A]$ is well defined. Thus $[A]$ is an equivalence class of F-CSAs, called an F-Brauer equivalence class. Then we define the multiplication of such classes by: $[A][B] = [A \otimes_F B]$. This multiplication is closed on the class of F-Brauer equivalence classes since we know that $A \otimes B$ is again an F-CSA.*

Definition 2.3.8. Brauer Identity and Inverse *Let F be a given field. Then the F-Brauer equivalence class $[F]$ is called an F-Brauer identity since*

$F \otimes_F A \cong A$. If A is an F-CSA, then we call $[A^{op}]$ a Brauer inverse. Note that Lemma 2.3.1 gives us: $A \otimes_F A^{op} \cong M_n(F)$ where $n = [A\colon F]$. Thus under the Brauer multiplication we have $[A \otimes_F A^{op}] = [A][A^{op}] = [F]$.

Definition 2.3.9. *Let F be a given field. We define the set $\mathcal{B}(F) = \{[A]\colon$ A is an F-CSA $\}$.*

Theorem 2.3.10. The Brauer Group *Let F be a given field. The set $\mathcal{B}(F)$ is an abelian group with identity element $[F]$.*

Proof: From the properties of the tensor product $\otimes_F$ we can see that the multiplication is both associative and commutative. By the above arguments we are assured an inverse $[A^{op}]$ for each element $[A]$ and an identity element $[F]$. It is easy to show that the identity and inverse are unique. We call $\mathcal{B}(F)$ the Brauer group over F.

For any field F we have constructed an abelian group of F-CSAs modulo Brauer equivalence. Since the aim of this section is to build a tool to classify division algebras over a given field F, our next theorem will relate the group element $[A]$ with an element $[D]$, where D is a division algebra.

Theorem 2.3.11. Class Representatives *Let F be a given field and suppose A is a F-CSA. Then we have $[A] = [D]$ for a unique division ring D up to isomorphism. Moreover $[A] = [B]$ if and only if both classes have the same representative division ring.*

Proof: Let A be an F-CSA. Then $A \cong M_r(D)$ for some central division algebra D over F. Moreover we know that D is unique by the Artin-Wedderburn Theorem and that $F = Z(D)$. Now since D is an F-CSA, $[D] \in \mathcal{B}(F)$. In particular, $M_r(D) \cong A \cong M_1(A)$, therefore $D \sim_{\mathcal{B}} A$ if and only if $[D] = [A]$.

For the second part of the theorem, suppose $[A] = [B]$ in $\mathcal{B}(F)$ if and only if $M_r(A) \cong M_s(B)$ if and only if $M_r(M_m(D_1)) \cong M_s(M_n(D_2))$, which is

equivalent to $M_{rm}(D_1) \cong M_{sn}(D_2)$. The uniqueness part of the Wedderburn-Artin Theorem gives us $D_1 \cong D_2$ and incidentally that $rm = sn$. ■

Let F be a given a field. Denote by $\mathcal{D}$ the set of isomorphism classes of finite dimensional division algebras over F. We now address the 1-1 correspondence between $\mathcal{D}$ and $\mathcal{B}(F)$.

Theorem 2.3.12. Power of Brauer *Let F be a given field. Then there is a bijection from $\mathcal{B}(F)$ to $\mathcal{D}$.*

Proof: Let ϕ: $\mathcal{B}(F) \to \mathcal{D}$ be such that ϕ maps $[A]$ to the isomorphism class of D, where D is the representative division algebra, equivalently $A \cong M_r(D)$ for some r. Claim ϕ is well-defined: $[D] = [D']$ in $\mathcal{B}(F)$, therefore $D \sim_{\mathcal{B}} D'$. This gives us that there are r, s such that $M_r(D) \cong M_s(D')$. By the uniqueness part of Artin-Wedderburn this gives $D \cong D'$, that is: $\phi([D]) = \phi([D'])$.

Claim ϕ is onto: Suppose D is a finite dimensional division algebra over F. Then D belongs to the isomorphism class $\phi([D])$, so that $[D] \in \mathcal{B}(F)$. Thus ϕ is onto.

Claim ϕ is 1-1: Suppose $\phi([D]) = \phi([D'])$ in $\mathcal{D}$. Therefore we have $D \cong D'$ so that $M_1(D) \cong M_1(D')$, giving us that $D \sim_{\mathcal{B}} D'$. Thus $[D] = [D']$ in $\mathcal{B}(F)$. Thus ϕ is 1-1. We have our bijection. ■

Corollary 2.3.13. Non-Commutative Division Algebras *Let F be a given field. Then there exists a finite-dimensional non-commutative division algebra with centre equal to F if and only if $\mathcal{B}(F) \neq \{1\}$.*

Proof: Since there is a bijection from $\mathcal{B}(F)$ to $\mathcal{D}$ we have $|\mathcal{B}(F)| = |\mathcal{D}|$. Thus $\mathcal{B}(F) = \{1\}$ if and only if $|\mathcal{D}| = 1$ if and only if $\mathcal{D} = \{F\}$ since F is indeed a division algebra over itself. Hence there are no non-commutative division algebras over F. ■

2.4 Examples of Brauer Groups

We discuss below some simple yet fundamental examples of Brauer groups, one arising from the choice of $\mathbf{R}$ as our field, and the classification of finite division algebras.

Theorem 2.4.1. Algebraically Closed Fields *Let F be an algebraically closed field. Then $\mathcal{B}(F) = \{1\}$.*

Proof: Let A be an F-CSA. Then by Lemma 1.1.12 $\overline{F} \otimes_F A$ is again simple as an F-algebra. Thus by the Wedderburn-Artin Theorem, $\overline{F} \otimes A \cong M_n(D)$ for some $n \in \mathbf{N}$ and D a division algebra with centre F. We claim $D = F$. Suppose for contradiction this was not the case, then there is an $a \in D \backslash F$, therefore $F(a)$ is an algebraic extension of F with $F \subsetneq F(a)$. Since $F = \overline{F}$ this is a contradiction, thus $D = F = \overline{F}$ and our claim is proven. ■

For any F-CSA A we have $F \otimes_F A \cong M_n(F)$ implies that $A \cong M_n(F)$, that is, $[A] = [F] = 1_{\mathcal{B}(F)}$. Therefore $\mathcal{B}(F) = \{1\}$. Another way to see this is to employ corollary 2.3.13 along with the fact that any division ring over an algebraically closed field F is commutative, so that the Brauer group of F is trivial.

Theorem 2.4.2. Finite Fields *Let F be a finite field. Then $\mathcal{B}(F) = \{1\}$.*

Proof: Let A be an F-CSA, where F is finite. We have $A \cong M_n(D)$ where D is a division algebra with centre F. Now since $[A\colon F] < \infty$, A is also finite, so that D is finite, thus $D = L$ where L is a field extension of F. Therefore $Z(D) = D$, so that $D = F$, and we have $[D] = [F]$ in $\mathcal{B}(F)$. ■

Theorem 2.4.3. Frobenius *Let D be a division ring such that $Z(D) = \mathbf{R}$. If D is not commutative, then we have $D \cong \mathbf{H}$.*

Let A be an $\mathbf{R}$-CSA. Then in $\mathcal{B}(\mathbf{R})$, $[A] = [D]$ for D a field or $D \cong \mathbf{H}$. Thus $\mathcal{B}(\mathbf{R}) = \{[\mathbf{R}], [\mathbf{H}]\}$ by Corollary 2.3.13, so $\mathcal{B}(\mathbf{R})$ is the group of order two.

We complete this discussion by stating some deeper results for $\mathcal{B}(F)$ given $F = \mathbf{Q}$. For p a prime in $\mathbf{Z}$, we denote by $\mathbf{Q}_p$ the field of p-adic numbers. Then due to a famous result of Brauer, Hasse, and Noether one can show that $\mathcal{B}(\mathbf{Q_p})$ is isomorphic to $\mathbf{Q}/\mathbf{Z}$. The proof of this result comes from a branch of mathematics called Class Field Theory, which originally developed around the 1930's when advances in modern abstract algebra were a common occurrence. This isomorphism gives what is known as a local structure theorem for the Brauer Group of any p-adic completion of $\mathbf{Q}$. Moreover for any algebraic number field K and its p-adic completion K_p we have the following: $\mathcal{B}(K_p) \cong \mathbf{Q}/\mathbf{Z}$. Finally the structure of $\mathcal{B}(\mathbf{Q})$ and more generally for $\mathcal{B}(K)$ has also been determined. These are best presented here in terms of exact sequences.

Structure of the Brauer Group Let p be a finite prime of a number field K, that is, p corresponds to a prime ideal of the ring of integers of K. Then we have the existence of the following isomorphism:

$$\phi_p \colon \mathcal{B}(K_p) \to \mathbf{Q}/\mathbf{Z}$$

Furthermore we consider the cases where p is an infinite prime of K, that is, p corresponds to an archimedean valuation. Then we have: $\phi_p \colon \mathcal{B}(K_p) \to \frac{1}{2}\mathbf{Z}/\mathbf{Z}$ if p is real and $\phi_p \colon \mathcal{B}(K_p) \to \{0\}$ if p is complex. Now we define the sum $S(K) = \bigoplus \sum_p \mathbf{Q}/\mathbf{Z} \bigoplus \sum_{p'} \frac{1}{2}\mathbf{Z}/\mathbf{Z} \bigoplus \sum_{p^*} \{0\}$, where p denotes a finite prime, p' denotes an infinite real prime and p^* denotes an infinite complex prime. Then we have the sequence:

$\{1\} \longrightarrow \mathcal{B}(K) \xrightarrow{\phi_p} S(K) \xrightarrow{\psi} \mathbf{Q}/\mathbf{Z} \longrightarrow \{1\}$

where ψ adds the coordinates of the direct sum.

When $K = \mathbf{Q}$ we have:

$\{1\} \longrightarrow \mathcal{B}(\mathbf{Q}) \longrightarrow \mathcal{B}(\mathbf{R}) \bigoplus \sum_p \mathcal{B}(\mathbf{Q}_p) \xrightarrow{\psi} \mathbf{Q}/\mathbf{Z} \longrightarrow \{1\}$

where $\mathcal{B}(\mathbf{R})$ is identified with $\langle \frac{1}{2} + \mathbf{Z} \rangle$.

For more details on these sequences please see [19], chapter 6. A thorough understanding of the above concepts requires a familiarity with class field theory and crossed product algebras, which arose as a solution to determining the explicit structure of many CSAs including the subclass of cyclic algebras. The latter are discussed in the next two chapters.

Chapter 3

Crossed Products

3.1 Separable Maximal Fields

Let A be an F-CSA. Then we know there exists a division algebra D such that $A \cong D \otimes M_k(F)$ for some $k \in \mathbf{N}$. Let $L \subseteq D$ be a maximal subfield such that L/F is separable. Then we have $[D\colon F] = n^2$ for some $n \in \mathbf{N}$ by Lemma 2.3.4. Since $[D\colon F] = [L\colon F]^2$, we have $[L\colon F] = n$.

Now let L_1 be the normal closure of L and suppose $[L_1\colon L] = m$, $m \in \mathbf{N}$. We note here that $D \otimes M_m(F) \cong A_1$ where A_1 is an F-CSA. Claim: $L_1 \subseteq A_1$. Proof: $L \otimes M_m(F) \cong M_m(L) \subseteq A_1$, since $M_m(L)$ is certainly contained in $M_m(D) \cong D \otimes M_m(F)$. Moreoever $L_1 \subseteq M_m(L)$ as a consequence of the Artin-Wedderburn, thus $L_1 \subseteq A_1$. Moreover $[A_1\colon F] = [D\colon F][M_m(F)\colon F] = n^2m^2 = [L_1\colon F]^2$.

Thus we may conclude that for an arbitrary F-CSA A, we may identify an F-CSA A_1 such that $[A_1\colon F] = [L_1\colon F]^2$ for a normal maximal subfield L_1 of A_1. We complete this discussion with the fact that in $\mathcal{B}(F)$, $[A_1] = [A]$. Too see this, we appeal to the usual representation of A as $M_k(D)$ and A_1 as $M_m(D)$. Thus by definition of $\sim_{\mathcal{B}(F)}$ we have $[A] = [A_1]$.

For the rest of this chapter if A is an F-CSA, we assume without loss of

generality that A has a normal and separable maximal subfield L. Thus L/F is a Galois extension. Let $G = Gal_F(L)$ and $n = [L\colon F] = |G|$.

3.2 Crossed Product Algebra

Let A, L and G be as above and let $\sigma \in G$. The Noether-Skolem Theorem gives us an invertible element $x_\sigma \in A$ such that $\sigma(a) = x_\sigma a x_\sigma^{-1}$ for all $a \in L$.

Lemma 3.2.1. $A = \{\sum_{\sigma\in G} x_\sigma a_\sigma \colon a_\sigma \in L\}$.

Proof: We show that the x_σ's are linearly independent over L and span A. We may write $\sum_\sigma x_\sigma a_\sigma = \sum_\sigma \sigma(a_\sigma)x_\sigma$ where $\sigma(a_\sigma) \in L$. Then if $\sum_\sigma \sigma(a_\sigma)x_\sigma = 0$, then $\sigma(a_\sigma) = 0$ for all $\sigma \in G$, since any element of A can be expressed as an F-linear, thus an L-linear combination. This implies $a_\sigma = 0$ for all $\sigma \in G$, so we have independence. Moreoever $|G| = n$, or put another way, $|\ \{x_\sigma \colon \sigma \in G\}\ | = n$. Thus $dim_L\{Span_L\{x_\sigma \colon \sigma \in G\}\} = n$ gives us that $dim_F\{Span_L\{x_\sigma \colon \sigma \in G\}\} = n^2$. So the span of the x_σ over L has the same dimension as A, therefore $A = Span_L\{x_\sigma \colon \sigma \in G\}$. Thus the x_σ form a basis for A as a right vector space over L and we have $A = \{\sum_{\sigma\in G} x_\sigma a_\sigma \colon a_\sigma \in L\}$. ■

Let $\sigma, \tau \in G$, $a \in L$. Then $(x_\sigma x_\tau)a(x_\sigma x_\tau)^{-1} = x_\sigma x_\tau a x_\tau^{-1} x_\sigma^{-1} = x_\sigma \tau(a) x_\sigma^{-1} = \sigma\tau(a) = x_{\sigma\tau} a x_{\tau\sigma}^{-1}$. Therefore if $a \in L$ then $x_{\sigma\tau}(x_\sigma x_\tau)^{-1}a = a x_{\sigma\tau}(x_\sigma x_\tau)^{-1}$, therefore $x_{\sigma\tau}(x_\sigma x_\tau)^{-1} \in C_A(L) = L$ since L is maximal. Hence $x_{\sigma\tau}(x_\sigma x_\tau)^{-1} = l$, $l \in L\backslash\{0\}$, so that $x_\sigma x_\tau x_{\sigma\tau}^{-1} = l^{-1}$, that is, $x_\sigma x_\tau = l^{-1} x_{\sigma\tau}$, giving us that $x_\sigma x_\tau = x_{\sigma\tau}\sigma\tau(l^{-1})$. $\sigma\tau(l^{-1}) \in L$ so we set $f(\sigma, \tau) = \sigma\tau(l^{-1})$ and conclude that

$$x_\sigma x_\tau = x_{\sigma\tau} f(\sigma, \tau) \tag{1}$$

Let $f\colon G\times G \to L\backslash\{0\} = L^\times$ be the mapping assigning the element $f(\sigma,\tau)$ to the pair (σ,τ). We investigate some properties of f. Recall A is associative so that given $\sigma,\tau,\nu \in G$ we have $x_\sigma(x_\tau x_\nu) = (x_\sigma x_\tau)x_\nu$

$\Rightarrow x_\sigma x_{\tau\nu} f(\tau,\nu) = x_{\sigma\tau} f(\sigma,\tau) x_\nu$
$\Rightarrow x_{\sigma\tau}^{-1} x_\sigma x_{\tau\nu} f(\tau,\nu) = f(\sigma,\tau)x_\nu$
$\Rightarrow x_\nu^{-1} x_{\sigma\tau}^{-1} x_\sigma x_{\tau\nu} f(\tau,\nu) = x_\nu^{-1} f(\sigma,\tau)x_\nu$
$\Rightarrow (x_{\sigma\tau}x_\nu)^{-1} x_\sigma x_{\tau\nu} f(\tau,\nu) = \nu(f(\sigma,\tau))$.

Therefore $[x_{\sigma\tau\nu} f(\sigma\tau,\nu)]^{-1} x_{\sigma\tau\nu} f(\sigma,\tau\nu) f(\tau,\nu) = \nu(f(\sigma,\tau))$, so that $f(\sigma\tau,\nu)^{-1} f(\sigma,\tau\nu) f(\tau,\nu) = \nu(f(\sigma,\tau))$, which gives

$$f(\sigma,\tau\nu)f(\tau,\nu) = f(\sigma\tau,\nu)\nu(f(\sigma,\tau)) \tag{2}$$

This identity is called the Factor Set Condition.

Definition 3.2.2. Factor Set *Let L/F be a Galois extension with $G = Gal_F(L)$. Then a mapping $f\colon G\times G \to L^\times$ is called a factor set if (2) is satisfied $\forall \sigma,\tau,\nu \in G$.*

Note here that if we choose $\tau = \nu = 1 \in G$ and σ arbitrary then (2) gives $f(\sigma,1) = f(1,1)$. If we choose $\sigma = \tau = 1 \in G$ and ν arbitrary then we have $f(1,\nu) = \nu(f(1,1))$.

Definition 3.2.3. Crossed Product *Let L/F be a Galois extension with $G = Gal_F(L)$ and let $f\colon G\times G \to L^\times$ be a mapping. Then we call (L,G,f) a crossed product if the following conditions hold:*

i) $(L,G,f) = \{\sum_{\sigma\in G} x_\sigma a_\sigma \colon a_\sigma \in L\}$.
ii) Equality and addition in (L,G,f) are term-wise, that is: $x_\sigma a_\sigma + x_\sigma b_\sigma = x_\sigma(a_\sigma + b_\sigma)$
iii) Identity 1) above holds for all $a \in L$.
iv) Identity 2) above holds for all $\sigma,\tau\nu \in G$.

Theorem 3.2.4. Crossed Products are CSAs *Given a Galois extension L/F, $G = Gal_F(L)$ and a factor set f, the resulting crossed product $A = (L, G, f)$ is a central simple algebra over F.*

Proof: If we choose $\sigma = \tau = \nu = 1 \in G$ then iv) gives $(x_1 x_1) = x_1 f(1,1)$, that is, $1 = x_1 f(1,1)^{-1}$ so $x_1 f(1,1)^{-1}$ is the unity element for A. A is associative since the basis elements are associative by iv). Thus A is an associative algebra with twisted multiplication as defined in iii).

Claim: $Z(A) = F$. Proof: Since F is the fixed field of G, if we fix an $a \in F$ we have $\sigma(a) = a$ for each $\sigma \in G$. Multiplication by x_σ gives $ax_\sigma = x_\sigma a$, that is $F \subseteq Z(A)$. Conversely, if $x_\sigma \in Z(A)$, then $x_\tau x_\sigma = x_\sigma x_\tau$ for any $\tau \in G$. Moreover $Z(A) \subseteq C_A(L)$, so that $x_\tau x_\sigma = x_\sigma \sigma(x_\tau) = x_\sigma x_\tau$. Thus $\sigma(x_\tau) = x_\tau$ for all $\tau \in G$, so $\sigma = 1$. This gives us that $x_\sigma = x_1$ and $x_1 \in x_1 f(1,1)^{-1} F \cong F$. Therefore $Z(A) \subseteq F$ and we have shown that the centre of A is F.

Claim: A is simple. Proof: Let $I \neq \{0\}$ be an ideal of A, and let $u \in I, u \neq 0$ be of shortest length in the sense that fewest terms are needed to write $u = \sum \sigma x_\sigma a_\sigma$. Without loss of generality $a_1 \neq 0$, and for any $a \in L$, the element $ua - au \in I$ since I is an ideal. Thus we have $a \sum_\sigma x_\sigma a_\sigma - \sum_\sigma x_\sigma a_\sigma a \in I$, which gives $\sum_\sigma a x_\sigma a_\sigma - \sum_\sigma \sigma(a) x_\sigma a_\sigma \in I$, so that $\sum_\sigma x_\sigma (a a_\sigma - \sigma(a) a_\sigma) \in I$ implies that $\sum_\sigma x_\sigma (a - \sigma(a)) a_\sigma \in I$. When $\sigma = 1$, $a - \sigma(a) = 0$, so we have constructed an element in I of shorter length than u, which is a contradiction. Thus we must have $\sum_\sigma x_\sigma (a - \sigma(a)) a_\sigma = 0$ for each $a \in L$. Now given $\sigma \in G$, $\sigma \neq 1$, there exists an $a \in L$ such that $\sigma(a) \neq a$ gives $a - \sigma(a) \neq 0$. Therefore we must have $a_\sigma = 0$, that is $u = x_1 a_1 \in I$. However $x_1 a_1$ is invertible, so u^{-1} exists in A therefore $u u^{-1} = 1 \in I$, so that I is all of A. Thus A is an F-CSA. ■

Thus any crossed product $A = (L, G, f)$ is a CSA with centre equal to the base field of L. Additionally from our discussion above, given an F-CSA A and normal maximal subfield L, we can construct the crossed product

(L, G, f) where $G = Gal_F(L)$ and $f\colon G \times G \to L^\times$, $f\colon (\sigma, \tau) \mapsto f(\sigma, \tau)$. This crossed product has the property that in $\mathcal{B}(F)$, $[A] = [(L, G, f)]$.

3.3 Properties of Crossed Products

Definition 3.3.1. Equivalence *Let G, L be as above and let $f, g\colon G \times G \to L^\times$ be factor sets. We say f and g are equivalent if there exists a map $\lambda\colon G \to L$ such that for all $\sigma, \tau \in G$ $g(\sigma, \tau) = \lambda_{\sigma\tau}^{-1}\tau(\lambda_\sigma)\lambda_\tau f(\sigma, \tau)$.*

Lemma 3.3.2. Isomorphic Crossed Products *Let (L, G, f) and (L, G, g) be crossed products. Then $(L, G, f) \cong (L, G, g)$ if and only if f and g are equivalent.*

Proof: ($\Longrightarrow$). We have $\{x_\sigma\colon \sigma \in G\} \subseteq (L, G, f)$ and properties iii) and iv) of crossed products allow us to choose some $0 \neq \lambda_\sigma \in L$ such that setting $y_\sigma = x_\sigma\lambda_\sigma$ for $\sigma \in G$ gives:

1) $Span_L\{y_\sigma\colon \sigma \in G\} = (L, G, f)$ and
2) $y_\sigma a = \sigma(a)y_\sigma \ \forall a \in L \ \forall \sigma \in G$

Furthermore, $y_\sigma y_\tau = x_\sigma\lambda_\sigma x_\tau\lambda_\tau = x_\sigma x_\tau\tau(\lambda_\sigma)\lambda_\tau = x_{\sigma\tau}f(\sigma, \tau)\tau(\lambda_\sigma\lambda_\tau) = y_{\sigma\tau}\lambda_{\sigma\tau}^{-1}\tau(\lambda_\sigma)\lambda_\tau f(\sigma, \tau)$. Let $h(\sigma, \tau) = \lambda_{\sigma\tau}^{-1}\tau(\lambda_\sigma)\lambda_\tau f(\sigma, \tau)$. Then $y_\sigma y_\tau = y_{\sigma\tau}h(\sigma, \tau)$ so that we have constructed an algebra A isomorphic to (L, G, f). Let $B = (L, G, g)$ and let $\psi\colon B \to A$ be an isomorphism. Then without loss of generality ψ is an inner automorphism, or conjugation map. So we may assume ψ fixes L element-wise. This is because $\psi(L)$ is a maximal subfield and is thus conjugate to L by Lemma 2.2.9. So we have $\psi(a) = a$ for each $a \in L$. Let $\{z_\sigma\colon \sigma \in G\} \subseteq B$ be the basis elements, so that $z_\sigma z_\tau = z_{\sigma\tau}g(\sigma, \tau)$. Then $\psi(z_\sigma) = y_\sigma = x_\sigma\lambda_\sigma$. Therefore $\psi(z_\sigma z_\tau) = \psi(z_{\sigma\tau})g(\sigma, \tau)$, so that $\psi(z_\sigma)\psi(z_\tau) = \psi(z_{\sigma\tau})g(\sigma, \tau)$, so that we have $y_\sigma y_\tau = y_{\sigma\tau}g(\sigma, \tau)$, which gives us that $y_{\sigma\tau}\lambda_{\tau\sigma}^{-1}\tau(\lambda_\sigma)\lambda_\tau f(\sigma, \tau) = y_{\sigma\tau}g(\sigma, \tau)$, or equivalently, $g(\sigma, \tau) = \lambda_{\sigma\tau}^{-1}\tau(\lambda_\sigma)\lambda_\tau f(\sigma, \tau)$. Therefore f and g are equivalent.

($\Longleftarrow$). This direction is essentially a reversal of the above argument and is left to the reader. ■

Let f be a factor set and set $t = f(1,1)^{-1}$, $\lambda_\sigma = \sigma(t)$. Then if $g(\sigma,\tau) = \lambda_{\sigma\tau}^{-1}\tau(\lambda_\sigma)\lambda_\tau f(\sigma,\tau)$, therefore $g(\sigma,\tau) = \tau(t)f(\sigma,\tau)$ so $g(\sigma,1) = g(1,1) = f(1,1)^{-1}f(\sigma,1) = f(1,1)^{-1}f(1,1) = 1$ and $g(1,\sigma) = \sigma(t)f(1,\sigma) = \sigma(f(1,1))^{-1}\sigma(f(1,1)) = 1$. If f and g are equivalent, (L,G,f) and (L,G,g) are isomorphic. Thus without loss of generality when we study crossed products we need only consider those with factor sets f satisfying $f(\sigma,1) = f(1,\sigma) = 1$ for all $\sigma \in G$.

Definition 3.3.3. Factor Set Product *Let $f, g\colon G \times G \to L^\times$ be factor sets. Define $h\colon G \times G \to L^\times$ by $h(\sigma,\tau) = f(\sigma,\tau)g(\sigma,\tau)$ $\forall \sigma,\tau \in G$. We call h the product of f and g and write $h = fg$.*

A straightforward calculation shows that h is a factor set, so that (L,G,h) is a crossed product. An interesting fact to note here is that all the factor sets for a given pair L, G form a group under the product defined above. The unit element is $f(\sigma,\tau) = 1$ for each $\sigma,\tau \in G$ and the inverse $f^{-1}(\sigma,\tau)$ is defined pointwise by $(f(\sigma,\tau))^{-1}$.

3.4 Crossed Products and the Brauer Group

Lemma 3.4.1. *Let L, G be as above. Then $(L,G,1) \cong M_n(F)$ where $n = [L\colon F]$.*

Proof: $[L\colon F] = n$, which means that $[(L,G,f)\colon F] = n^2$. Now $L \subseteq (L,G,1)$ as a subfield and for all $\sigma \in G$ there is an $x_\sigma \in (L,G,1)$ such that $x_\sigma a = \sigma(a)x_\sigma$ for each $a \in L$ and $x_\sigma x_\tau = x_{\sigma\tau}$ $(\star)$. We define an action $*_x$ of $(L,G,1)$ on L by: for $a \in L$, $x = \sum_\sigma x_\sigma a_\sigma \in (L,G,1)$ $a*_x = \sum_{\sigma\in G}\sigma(a)a_\sigma$. Let $A_F(L)$ be the ring of F-linear transformations on L. Then using the

relations ($\star$) one can show $\phi\colon (L,G,1) \to A_F(L)$, $\phi(x) = *_x$ is a non-zero module homomorphism. Moreoever $(L,G,1)$ is simple, thus ϕ is an injection. Finally, $[(L,G,1)\colon F] = n^2 = [A_F(L)\colon F]$, thus ϕ is surjective. Therefore $(L,G,1) \cong A_F(L) \cong M_n(F)$. ■

Of course this means we may now represent the class $[(L,G,1)]$ in $\mathcal{B}(F)$ as $[F] = 1_{\mathcal{B}(F)}$. Next we connect multiplication in $\mathcal{B}(F)$ with taking products of factor sets.

Lemma 3.4.2. Idempotent Multiplication *Let L/F be a finite normal extension with $G = Gal_F(L)$. Then $L \otimes_F L = \bigoplus_{\sigma\in G} e_\sigma(L\otimes 1) = \bigoplus_{\sigma\in G} e_\sigma(1\otimes L)$, where $\{e_\sigma\colon \sigma \in G\}$ are mutually orthogonal idempotents such that $\forall a \in L$, $e_\sigma(a\otimes 1) = e_\sigma(1\otimes\sigma(a))$.*

Proof: There is more than one way to prove this lemma, but any proof is minimally relevant to our discussion, so it is omitted. The interested reader is directed to [11], p113 for one version.

Lemma 3.4.3. Idempotent Representation *Let A be an F-CSA and $0 \neq e$ an idempotent in A. Then in $\mathcal{B}(F)$ we have $[A] = [eAe]$.*

Proof: Wedderburn-Artin gives $A = M_m(D)$ for a division algebra D with centre F, $m \in \mathbf{N}$ and by Theorem 2.3.11 $[A] = [D]$ in $\mathcal{B}(F)$. Without loss of generality we may write $e = \begin{pmatrix} \mathbf{I} & 0 \\ 0 & 0 \end{pmatrix}$ where $\mathbf{I}_r$ is the $r \times r$ identity matrix. This is obtained by a change of basis via an inner automorphism of A. From here we see that $eAe = \begin{pmatrix} \mathbf{I} & 0 \\ 0 & 0 \end{pmatrix} M_r(D) \begin{pmatrix} \mathbf{I} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} M_r(D) & 0 \\ 0 & 0 \end{pmatrix}$ Therefore, $eAe \cong M_r(D)$, giving us $[eAe] = [D]$ in $\mathcal{B}(F)$ by the definition of $\sim_{\mathcal{B}}$. Therefore $[A] = [eAe]$ and we are done. ■

Theorem 3.4.4. Factor Sets in $\mathcal{B}(F)$ *Let L/F be a normal extension and $G = Gal_F(L)$. If $f, g\colon G\times G \to L^\times$ are factor sets then $[(L,G,f)][(L,G,g)] = [(L,G,fg)]$ in $\mathcal{B}(F)$.*

Proof: Let $E = (L,G,f) \otimes_F (L,G,g)$ with $L \otimes L \subseteq E$. Applying the Idempotent Multiplication Lemma, we have for all $\sigma \in G$ there exists a non-zero e_σ in $L \otimes L$ where the e_σ are idempotents such that $e_\sigma e_\tau = 0$ $\forall \sigma \neq \tau$ and $e_\sigma(a \otimes 1) = e_\sigma(1 \otimes \sigma(a))$ for $a \in L$. Now let $e = e_1$, so that $e(a \otimes 1) = e(1 \otimes a)$ for all $a \in L$. Let $\{x_\sigma\colon \sigma \in G\}$ be the basis elements for (L,G,f) and $\{y_\sigma\colon \sigma \in G\}$ the basis elements for (L,G,g). Then we have $x_\sigma^{-1} a x_\sigma = \sigma(a)$ for each $a \in L$, $x_\sigma x_\tau = x_{\tau\sigma} f(\sigma,\tau)$ and $y_\sigma^{-1} a y_\sigma = \sigma(a)$ for each $a \in L$, $y_\sigma y_\tau = y_{\tau\sigma} g(\sigma,\tau)$. We form a new idempotent $e' = (1 \otimes y_\sigma^{-1}) e (1 \otimes y_\sigma)$ of $L \otimes L$ such that $e'(1 \otimes a) = (1 \otimes y_\sigma^{-1}) e (1 \otimes y_\sigma a) = (1 \otimes y_\sigma^{-1}) e (1 \otimes \sigma(a))(1 \otimes y_\sigma) = (1 \otimes y_\sigma^{-1}) e (\sigma(a) \otimes 1)(1 \otimes y_\sigma) = (1 \otimes y_\sigma^{-1}) e (1 \otimes y_\sigma)(\sigma(a) \otimes 1) = e'(\sigma(a) \otimes 1)$. Thus for all $\sigma \in G$ we have $e' = e_\sigma$, so that $(1 \otimes y_\sigma^{-1}) e (1 \otimes y_\sigma) = e_\sigma$, giving us that $e(1 \otimes y_\sigma) = (1 \otimes y_\sigma) e_\sigma$, that is:

$$e(1 \otimes y_\sigma)e = (1 \otimes y_\sigma) e_\sigma e \tag{1}$$

Now if $\sigma \neq 1$ forces $e e_\sigma = 0$, then we have that $e(1 \otimes y_\sigma)e = 0$. Similarly, defining $e'' = (x_\sigma \otimes 1) e (x_\sigma^{-1} \otimes 1)$ results in

$$e'' = e_\sigma \, \forall \sigma \in G \tag{2}$$

Set $w_\sigma = x_\sigma \otimes y_\sigma$. Then we may use (1) and (2) to verify that $w_\sigma e = e w_\sigma$: when $\sigma = 1$ we have $e(1 \otimes y_\sigma) = (1 \otimes y_\sigma)e$ and $e(x_\sigma \otimes 1) = (x_\sigma \otimes 1)e$. On the other hand when $\sigma \neq 1$ we have $w_\sigma e = e w_\sigma = 0$. In turn, this gives $e w_\sigma e = e w_\sigma$. Let $u_\sigma = e w_\sigma$. Then we have $u_\sigma = e w_\sigma e \in eEe$ and $u_\sigma^{-1} = (e w_\sigma)^{-1} = (w_\sigma e)^{-1} = e w_\sigma^{-1}$. Moreover, $u_\sigma u_\tau = e w_\sigma e w_\tau = e w_\sigma w_\tau = e(x_\sigma x_\tau \otimes y_\sigma y_\tau) = e(x_{\sigma\tau} f(\sigma,\tau) \otimes y_{\sigma\tau} g(\sigma,\tau)) = e(x_{\sigma\tau} \otimes y_{\sigma\tau})(f(\sigma,\tau) \otimes g(\sigma,\tau)) = e w_{\sigma\tau} e(f(\sigma,\tau) \otimes g(\sigma,\tau)) = u_{\sigma,\tau} e(f(\sigma,\tau) g(\sigma,\tau) \otimes 1)$, that is

$$u_\sigma u_\tau = u_{\sigma,\tau} e(f(\sigma,\tau)g(\sigma,\tau) \otimes 1) \tag{3}$$

In addition, we have $u_\sigma(a \otimes 1)eu_\sigma^{-1} = u_\sigma(a \otimes 1)ew_\sigma^{-1}e = u_\sigma(a \otimes 1)w_\sigma^{-1}e = (x_\sigma \otimes y_\sigma)(a \otimes 1)(x_\sigma^{-1} \otimes y_\sigma^{-1})e = (x_\sigma a x_\sigma^{-1} \otimes y_\sigma y_\sigma^{-1})e = (\sigma(a) \otimes 1)e$, that is

$$u_\sigma(a \otimes 1)eu_\sigma^{-1} = (\sigma(a) \otimes 1)e \tag{4}$$

In summary, identities (3) and (4) along with the fact that $e(L\otimes 1) = (L\otimes 1)e$ lead to the construction of a new crossed product $(e(L\otimes 1), G, e(f\otimes 1)(g\otimes 1))$ contained in eEe.

Continuing on, we also have for $a, a' \in L$: $e(x_\sigma a \otimes y_\tau a')e = e(x_\sigma \otimes y_\sigma)(1 \otimes y_\sigma^{-1}y\tau)e(a \otimes a') = u_\sigma e(1 \otimes y_\sigma^{-1}y_\tau)e(aa' \otimes 1)$. If $\sigma \neq \tau$ then $e(1 \otimes y_\sigma^{-1}y_\tau)e = e(1 \otimes y_\sigma^{-1})ee(1 \otimes y_\tau)e$. But $e(1 \otimes y_\sigma^{-1})e = 0$, thus $e(1 \otimes y_\sigma^{-1}y_\tau)e = 0$. If $\sigma = \tau$, then $e(x_\sigma a \otimes y_\sigma a')e = u_\sigma e(aa' \otimes 1)$. Therefore in either case $eEe \subseteq (e(L \otimes 1), G, e(f \otimes 1)(g \otimes 1))$, so that $eEe = (e(L \otimes 1), G, e(fg \otimes 1))$. Since $e \in L \otimes L$, giving us that $e(L \otimes 1) \cong L$, so that $eEe \cong (L, G, fg)$. Now by the Idempotent Representation Lemma $[E] = [eEe]$, thus $[E] = [(L, G, fg)]$ and this completes the proof. ■

In conclusion, if $\mathcal{H} = \{[(L, G, f)]\}$ as f runs through all factor sets on $G \times G$ then $[(L, G, 1)] = 1_{\mathcal{B}(F)} \in \mathcal{H}$, $[(L, G, f)][(L, G, g)] = [(L, G, fg)] \in \mathcal{H}$ and if $[(L, G, f)] \in \mathcal{H}$ then $[(L, G, f)]^{-1} = ([L, G, f^{-1}]) \in \mathcal{H}$. Thus $\mathcal{H} \leq \mathcal{B}(F)$. This gives us the following theorem:

Theorem 3.4.5. *Let A be an F-CSA. Then A is Brauer equivalent to a crossed product algebra.*

Thus in studying $\mathcal{B}(F)$, we need only consider the set of classes $\mathcal{C} = \{[(L, G, f)]\}$ such that L runs over all normal extensions of F, $G = Gal_F(L)$ and f is a factor set from $G \times G$ to $L^\times$.

3.5 Crossed Products and Cohomology

In this section we briefly introduce some terminology and present two nice results connecting n^{th} cohomology groups with the Brauer group $\mathcal{B}(F)$.

Definition 3.5.1. G-Module *Let G, M be groups such that M is abelian under $+$. Let G act on M by left multiplication $g \cdot a$, such that:*

i) $g \cdot (a + a') = g \cdot a + g \cdot a'$
ii) $(gh) \cdot a = g \cdot (h \cdot a)$

Then we call M a left G-module.

Let G, M be as above. Let $C^n(G, M)$ denote the additive group of functions from G^n to $M.$, where G^n is the n-fold cartesian product. Now define a mapping $\delta^n \colon C^n \to C^{n+1}$ by

$$(\delta^n f)(x_1, ..., x_{n+1}) = f(x_2, ..., x_{n+1}) + \sum_{i=1}^{n} (-1)^i f(x_1, ..., x_i x_{i+1}, ..., x_{n+1}) + (-1)^{n+1} x_{n+1} f(x_1, ..., x_n)$$

Then it can be shown that $\delta^n \delta^{n-1} = 0$ for $n > 1$. We also define the following groups: $Z^n = \{f \in C^n \colon \delta^n f = 0\}$ and $B^n = \{\delta^{n-1} f \colon f \in C^n\}$. Note that if $\delta^{n-1} f \in B^n$, then $\delta^n(\delta^{n-1} f) = 0$.

Definition 3.5.2. n^{th} Cohomology Group *Let G, M be as above. Then we define $H^n(G, M) = Z^n / B^n$, this is the n^{th} cohomology group of G in M.*

Let L/F be a normal extension with $G = Gal_F(L)$. Then we can view $L^\times$ as a G-module with action $*$, where $\sigma * a = \sigma(a) \in L^\times$. We begin with two simple propositions.

Proposition 3.5.3. Factor Sets and H^2 I *Let G, L be as above. Then $f \colon G \times G \to L^\times$ is a factor set if and only if $f \in Z^2(G, L^\times)$.*

Proof: $f\colon G^2 \to L^\times$ is a factor set if and only if f satisfies $f(\sigma, \tau\nu) + f(\tau, \nu) = f(\sigma\tau, \nu) + \nu(f(\sigma, \tau))$ for all $\sigma, \tau, \nu \in G$ if and only if $f(\tau, \nu) - f(\sigma\tau, \nu) + f(\sigma, \tau\nu) - \nu(f(\sigma, \tau)) = 0$ for all $\sigma, \tau, \nu \in G$ if and only if $(\delta^2 f)(\sigma, \tau, \nu) = 0$ for all $\sigma, \tau, \nu \in G$ if and only if $Z^2(G, M)$. ■

Proposition 3.5.4. Factor Sets and H^2 II *Let G, L be as above. Then two factor sets f and g are equivalent if and only if $fg^{-1} \in B^2(G, L^\times)$.*

Proof: Suppose $fg^{-1} \in B^2(G, L^\times)$, that is $fg^{-1} = \delta^1\lambda$ for some $\lambda \in C^1$ if and only if $(\delta^1\lambda)(\sigma, \tau) = \lambda(\tau) - \lambda(\sigma\tau) + \tau(\lambda(\sigma))$. We now change notation to the more familiar λ_σ for $\lambda(\sigma)$ to see that our last line is equivalent to $(\delta^1\lambda)(\sigma, \tau) = \lambda_\tau - \lambda\sigma\tau + \tau(\lambda_\sigma)$ if and only if $f(\sigma, \tau) = \lambda_\tau - \lambda\sigma\tau + \tau(\lambda_\sigma)g(\sigma, \tau)$ if and only if f and g are equivalent. ■.

Now we are led to our first result, namely that the set of classes $\mathcal{H} = [(L, G, f)]$ is isomorphic to $H^2(G, L^\times)$. This can be seen by noting that a factor set f is equivalent to 1 if and only if $f1^{-1} = f \in B^2(G, L^\times)$, so that $Z^2(G, L^\times)/B^2(G, L^\times)$ is precisely the group of factor sets modulo those equivalent to 1. Let $\mathcal{C}$ be as defined in Section 3.4. Then we consider the mapping $\phi\colon H^2(G, L^\times) \to \mathcal{C}$, $\phi(f) = (G, L^\times, f)$, which gives us an explicit 1-1 correspondence between $\mathcal{C}$ and $H^2(G, L^\times)$. We summarize this result below before moving on to our next result.

Fact 3.5.5. $\mathcal{C} \cong H^2(G, L^\times)$.

Lemma 3.5.6. Finite Groups and Finite Quotients *Let G and M be groups with M abelian. If $|G| = k < \infty$ then $kH^n(G, M) = \{0\}$ for each $n \in \mathbf{N}$.*

Proof outline: Let $f \in Z^n(G, M)$. Then if $(x_1, ..., x_{n+1}) \in G$ we have $(\delta^n f)(x_1, ..., x_{n+1}) = 0$. We then write this out explicitly in terms of the definition for $(\delta^n f)$. Letting x_1 run over all elements of G, we define $h(x_2, ..., x_{n+1}) =$

$\sum_{x_1 \in G} f(x_1, ..., x_n)$ and some arithmetic along with the fact that $\sum_{x_1 \in G} f(x_1 x_2, x_3, ..., x_{n+1}) = h(x_3, ...x_{n+1})$ brings us to $kf(x_2, ...x_{n+1}) = -h(x_3, ..., x_{n+1}) + \sum_{i=2}^{n} (-1)^i h(x_2, ..., x_1 x_{i+1}, ..., x_{n+1}) - (-1)^{n+1} x_{n+1} h(x_2, ...x_n) = -(\delta^{n-1} h)(x_2, ..., x_{n+1}) \in B^n(G, M)$. We then conclude that $kZ^n(G, M) \subseteq B^n(G, M)$, thus $kH^n(G, M) = \{0\}$.

Theorem 3.5.7. $\mathcal{B}(F)$ a Torsion Group *Let F be a field. Then $\mathcal{B}(F)$ is a torsion group.*

Proof: Let $[A] \in \mathcal{B}(F)$. Then we have $[A] = [(L, G, f)]$ for some normal extension L/F. Now we know that $[A] \in H^2(G, L^\times)$ by Fact 3.5.5, thus the above lemma gives us $[A]^k = [(L, G, f)]^k = 1_{\mathcal{B}(F)}$, where $k = |G|$. Thus an arbitrary element in $\mathcal{B}(F)$ has finite order and we are done. ■

Theorem 3.5.7 concludes this chapter, yet opens new discussions on the decomposition of division algebras over a given field. It turns out that if D is any finite dimensional division algebra over its centre F, we may write D as a finite tensor product of other division rings D_i with centre F, such that $[D_i : F] = p_i^{m_i}$ for p_i prime and $m_i \in \mathbf{N}$. One can consult [11] for the necessary proofs for this result. We have focused on division algebras with finite dimension over their centres, and their Brauer equivalence to a crossed product. Theorem 3.2.4 leads to the question of whether or not all algebras are in fact isomorphic to a crossed product, a question answered finally by Amitsur and discussed in the next chapter.

Chapter 4

P.I. Algebras

Just as the study of polynomial rings over fields expands our knowledge of the fields themselves, examining identities satisfied by algebras within the appropriate framework allows us to draw some deep conclusions about these algebras. We begin this chapter with some definitions to set up our study of polynomial identity algebras.

4.1 Definitions and Examples

Definition 4.1.1. Free Monoid Algebra *We denote the free monoid by X, the collection of formal monomials or words in a countable set of variables $x_1, x_2, ...$ with juxtaposition as the multiplication and the symbol 1 as the identity. Let R be a commutative ring and consider the set $R\{X\} = \{\sum_{x\in X} a_x x : a_x \in R\}$. If we then define an addition $\sum a_x x + \sum b_x x = \sum (a_x + b_x)x$ and a scalar multiplication $a\sum a_x x = \sum a a_x x \ \forall a \in R$, then we may derive the following:*

$R\{X\}$ has a zero element $\sum_{x\in X}(0x)$ and an additive inverse $-\sum a_x x = \sum(-a_x)x$ and thus is an R-module. Moreover, by defining the multiplication $(\sum_{z\in X} a_z z)(\sum_{y\in X} b_y y) = \sum_{x\in X}(\sum_{zy=x} a_z b_y)x$, it can be shown that $R\{X\}$

is an algebra. The set $R\{X\}$ with this addition and multiplication is called the free R-algebra with a countable set of free generators.

Definition 4.1.2. Monoid Subalgebra *Let $f \in R\{X\}$ such that $f \in R\{x_1, ..., x_m\}$, the subalgebra with finitely many generators $x_1, ..., x_m$. We call this formal sum of monomials with coefficients in R a polynomial in m variables over R.*

Remark 4.1.3. Free Monoid Algebra over a Field *All the statements and derivations above hold if we replace our commutative ring R with a field F. We use either set of scalars depending on the generality desired.*

Definition 4.1.4. Set of Evaluations *Let A be any algebra over F. Given a polynomial f in m variables, we define the set $f(A) = \{$images of f under algebra homomorphisms from $F\{X\}$ to $A\}$. In other words we consider all possible evaluations $x_i \to a_i$ for all $a_i \in A$*

Definition 4.1.5. Polynomial Identity *We call f a Polynomial Identity (PI) for A if $f(A) = 0$. That is, $f(a_1, ..., a_m) = 0$ for all $a_i \in A$. We say f is satisfied by A. If A is an algebra over F, we call A a PI-algebra if $\exists f$ in $F\{X\}\backslash\{0\}$ such that f is a PI for A.*

Let A be a commutative algebra over F. A simple example of a polynomial identity is the commutator for rings $f(x_1, x_2) = x_1x_2 - x_2x_1 = [x_1, x_2]$. Another is if B is a subalgebra of a PI-algebra A/F, then B is a PI algebra over F.

Definition 4.1.6. Standard Polynomial S_k *Set $f = S_k = S_k(x_1, ..., x_k) = \sum_\pi (sgn\pi) x_{\pi(1)} \cdots x_{\pi(k)}$ where π ranges over all permutations of $\{1, ..., k\}$. S_k is called the standard polynomial of degree k. S_k is a PI for any F-Algebra that is generated by less than k elements as an F-module.*

A rather technical proof of this result can be found in [12].

Definition 4.1.7. Primitive Algebra *Let A be an F-algebra. A is called primitive if it contains an irreducible, faithful A-module M. A similar definition applies for associative rings.*

4.2 Kaplansky's Theorem

Definition 4.2.1. Dense Ring of Linear Transformations

Let V be any vector space and $\mathcal{L}$ the ring of linear transformations on V. A subring $L \subseteq \mathcal{L}$ is called dense if for each $n \in \mathbf{N}$ and for all choices $x_1, ..., x_n$ and $y_1, ..., y_n$ where the x_i are linearly independent, we have a transformation $\alpha \in L$ such that $\alpha x_i = y_i$, $i = 1, ..., n$.

Theorem 4.2.2. Density Theorem *Let A be a primitive ring and M a faithful irreducible left A-module. Then A is isomorphic to a dense ring of linear transformations on M, where we view M as a vector space over $D = End(M)$.*

Proof outline: We begin by appealing to Schur's Lemma to establish that D is a division ring and we regard M as a left vector space over D. It then turns out that in order to show density, it is enough to prove that for $E \subseteq M$ a subspace of finite dimension, if $x \in M \backslash E$ then there exists some $\alpha \in A$ such that $\alpha E = \{0\}$ but $\alpha x \neq 0$. This is proven by induction on the dimension of E. For full details please see [11].

Remark 4.2.3. *This technical yet deep theorem allows us to regard a seemingly arbitrary primitive ring A as a subring of an endomorphism ring, a result essential to proving Kaplansky's Theorem.*

Theorem 4.2.4. Maximal Subfield Theorem II *Let D be a division ring with centre F and let L be a maximal subfield of D. Then $L \otimes_F D$ is a dense ring of linear transformations on D as a left vector space over L.*

Proof: We recall that $End(D)$ is the ring of F-linear endomorphisms on D; set $D_r = \{T_a \colon a \in D\}$ where $T_a \colon D \to D$, $T_a(x) = xa$ and $L_l = \{U_k \colon k \in L\}$ where $U_k \colon D \to D$, $U_k(x) = kx$. Then D_r and L_l are the right and left multiplications by elements of D and L, respectively. One can easily see that D_r and L_l are in $End(D)$. Moreover let $T_a \in D_r$ and $U_k \in L_l$. Then: $U_kT_a(x) = U_k(xa) = k(xa)$ and $T_aU_k(x) = T_a(kx) = (kx)a$. Thus elements of D_r commute with those of L_l. Now, let $d \in D\backslash\{0\}$. Then $dD_r \subseteq D_r$ and D a division ring gives us that for all $b \in D$, $dT_{d^{-1}b} \colon x \to xd(d^{-1}b) = xb$, thus $dT_{d-1b} = T_b$. Thus $D_r \subseteq dD_r$ so they are equal. If we regard D as a (left) D_r-module, it is irreducible. Therefore D as an L_lD_r-module is also irreducible. Now viewing L_lD_r as a subring of $End(D)$, the action $U_kT_a \to (x \to kxa)$ for each $k \in L$, $x, a \in D$ must be faithful, for D is an integral domain. Thus we see that D is a faithful irreducible L_lD_r-module so the Density Theorem allows us to conclude that L_lD_r is isomorphic to a dense ring of linear transformations on D over L_l.

Now let $\Delta \subseteq End(D)$ be the centralizer of L_lD_r. Then Δ centralizes D_r implies that $\Delta \subseteq \{U_a \colon a \in D\} = D_l$, the extension of L_l to all elements of D. Similarly Δ centralizes $L_l \subseteq D_l$ and since L is a maximal subfield of D it is not difficult to show that L_l is a maximal subfield of D_l. Thus $\Delta \subseteq L_l$ and $L_l \subseteq \Delta$ trivially, so they are equal. It then follows that L_lD_r is isomorphic to a dense ring of linear transformations on D over L_l. Now we note that we may identify L with L_l by $L \to L_l$, $k \mapsto U_k$.

In our case D is central simple, being a division ring. Just having established that $L \cong L_l = \Delta$, Δ centralizes L_l and $F \subseteq L$, we may apply Lemma 1.1.12 to get $L \otimes_F D$ simple. Thus the mapping $L \otimes_F D \to L_lD_r$, $k \otimes a \mapsto U_kT_a$ is injective. Moreover it can be verified as a homomorphism. Lastly by virtue of the definitions of D_r and L_l it is onto. Thus $L \otimes_F D \cong L_lD_r$ so we have $L \otimes D$ isomorphic to a dense ring of linear transformations on D as required. ■

The idea behind Kaplansky's Theorem is that when an arbitrary primitive

algebra with centre R satisfies a polynomial identity, we obtain an upper bound on the dimension of A, and find that R must be a field.

Theorem 4.2.5. Kaplansky *Let A be a primitive algebra over its centre R satisfying a PI $f \in R\{X\}$ of degree k. Then R is a field, A is simple and finite-dimensional over R and if $dim_R(A) = n^2$ then $2n \leq k$.*

Proof: A primitive gives us that there is an A-module M such that M is faithful and irreducible, thus $M \cong A/I$, where I is a maximal right ideal of A. $I \subsetneq A$ and $1 \in A^2$, thus $A^2 \nsubseteq I$ implies that I is invariant under R, so that A/I invariant under R. Set $D = End(M)$. By Schur's Lemma D is a division ring with centre a field F. Consider the embedding $R/(I \cap R) \hookrightarrow D$. This shows a copy of R lies in D. It is an embedding because $M \cong A/I$ and there is a copy of M in D. Let $f = 0$ be our PI satisfied by A. Then f can be made into a multilinear identity, that is, one in which every variable occurs in at most one degree. This is done by considering a non-linear variable, say x_1, and applying the definition $g(u, v, x_2, ..., x_k) = f(u + v, x_2, ..., x_k) - f(u, x_2, ..., x_k) - f(v, x_2, ..., x_k)$. We now observe that if the degree of x_1 is n, it is replaced by two variables each of degree $n - 1$. This process may be repeated as many times as needed until we obtain a multilinear identity f. If f is not homogeneous, having variables failing to occur in each term, we simply set those variables to zero. Changing notation, we call this new PI f and its new degree k. Note here that if we show $k \leq 2n$ for this new PI, it certainly holds for the old degree as well. With relabeling if necessary we have $f = x_1 \cdots x_k + \sum_{\pi \neq id} x_{\pi(1)} \cdots x_{pi(k)}$ for some permutations $\pi \in S_k$.

Consider the list of matrices: $e_{11}, e_{12}, e_{22}, e_{23}, ..., e_{ii}, e_{i(i+1)}$ If they are chosen with the appropriate dimension so that we may list k of them (for example, if $k = 5$ then we would need 3×3 matrices), then substitution into f gives: $f(e_{11}, e_{12}, ...) = e_{11}e_{12}e_{22}...$ + some permutations of these. Only the first term fails to vanish since the only way to ensure a non-zero product of these elements is to have: $e_{ij}e_{kl}$ where $i = k$ or l *and* $j = k$ or l.

By the Density Theorem, A is a dense ring of linear transformations on M over D. If A was infinite-dimensional we could find k elements of A behaving like the basis vectors $e_{11}, e_{12}, e_{22}, e_{23}, ...$ and spanning a finite-dimensional subspace of A, as A consists of linear transformations. Then $f(e_{11}, e_{12}, ...) \neq 0$ so we arrive at a contradiction. Thus A is finite-dimensional and is dense, thus A is a matrix ring over D. This tells us that A is a simple algebra with centre a field, we call it F instead of R and write $A \cong M_m(D)$.

Let us now view D as an algebra over F: We know that f is a PI for D as well since we may identify $d \in D$ with $dI_m \in A$ where I_m is the $m \times m$ identity matrix. Let L be a maximal subfield of D and consider the tensor product $L \otimes_F D$. Because L is an extension field of F, $L \otimes_F D$ is again an algebra over L with a basis isomorphic to that of D. One sees that we have extended the base field here from F to L. Thus f is a PI for the tensor product $L \otimes D$, therefore by the Maximal Subfield Theorem II $L \otimes D$ is a dense ring of linear transformations on a vector space over L. We may also conclude that the dimension of $L \otimes D$ is finite in the same way A over D was shown to be finite-dimensional. Therefore $L \otimes D$ as viewed as a vector space over F, and thus over L is also finite. Hence we have A finite-dimensional over D and D finite-dimensional over F, so A is finite-dimensional over F. We conclude that $dim_F(A) = n^2$ for some n.

Now suppose $k \lneq 2n$. We may form a list $e_{11}, e_{12}, e_{22}, e_{23}, ...$ of k elements as before that fails to satisfy our PI. If, however, $k \geq 2n$ then we cannot form $f(e_{11}, e_{12}, e_{22}, e_{23}, ...)$, as we run out of matrices since the elements of A are $n \times n$. Thus f is satisfied as expected and we conclude that A is a simple, finite-dimensional algebra over its centre F such that $[A : F] = n^2$ and $2n \leq k$. This concludes the proof. ■

4.3 Cyclic Algebras

Let us continue our discussion of finite dimensional F-CSAs. A specific type of these are called cyclic algebras and were studied by some of the mathematicians most influential to modern algebra.

Definition 4.3.1. Cyclic Algebra *Let $A = (L, G, f)$ be a crossed product. Then if $G = \langle \sigma \rangle$ is cyclic we call A a cyclic algebra.*

Theorem 4.3.2. Brauer-Hasse-Noether *let D be a division algebra with $Z(D) = F$. If F is a number field then D is cyclic.*

This theorem was originally published in 1932 and was a notable discovery within both abstract algebra and number theory. It was Dickson who first formulated the construction of cyclic algebras as crossed products, so back then a cyclic algebra was called an algebra of Dickson type. The next step was to verify whether or not every CSA of finite dimension was cyclic. This brings us to a paper by Albert also presented in 1932, in which a finite dimensional non-cyclic CSA is constructed. By then it was already known that the proof of the Brauer-Hasse-Noether could not be extended to include a general field F.

Albert constructed a crossed product algebra A over a field F of characteristic 0, such that $[A\colon F] = 16$, then showed that A was not cyclic. The proof can be found in his paper [1]. After Albert's results were published, the next big question became whether or not all division algebras are isomorphic to a crossed product algebra. In Chapter 3 we discussed that although every construction of a crossed product is a CSA, given any CSA we find it is only Brauer equivalent to a crossed product. In 1971, Amitsur constructed a CSA that was not a crossed product. We discuss an outline of his proof in section 4.5.

4.4 Generic Matrices

One of the main tools used in Albert's proof is a PI algebra generated by a countable number of generic matrices. We discover some classical results about them below.

Definition 4.4.1. $F[\mathcal{X}]$ **and** $F(\mathcal{X})$ *Let* $\mathcal{X} = \{x_1, x_2, ...\}$. *We denote by* $F[\mathcal{X}]$ *the commutative polynomial algebra over* F. *We may construct the field of fractions of* $F[\mathcal{X}]$, *which we label as* $F(\mathcal{X})$.

If Y_k is an $n \times n$ matrix whose entries lie in $\mathcal{X}$, we can then consider the set $\mathcal{Y} \subseteq M_n(F[\mathcal{X}])$ as the set of all possible matrices Y_k.

Definition 4.4.2. Generic Matrix Algebra *Write* $F_n\mathcal{Y}$ *to denote the subalgebra of* $M_n(F[\mathcal{X}])$ *generated by* $\mathcal{Y}$ *and write* $F_nY_1, ..., Y_m$ *to denote the subalgebra generated by a finite subset of* $\mathcal{Y}$, $\{Y_1, ..., Y_m\}$. *Then* $F_n\mathcal{Y}$ *and* $F_nY_1, ..., Y_m$ *are called generic matrix algebras with generic matrices* Y_k. *We note here that* $F_n\mathcal{Y}$ *need not be finite dimensional but is always a finitely generated algebra.*

It is always true that a given generic matrix algebra A is an F-algebra with $F \subseteq Z(A)$, but its base field $Z(A)$ need not be F itself. In 1980, Formanek and others presented a result on the centre of a generic 2×2 matrix algebra generated by 2 matrices. Let F be a field and X, Y be two 2×2 generic matrices. We denote by A the algebra F_2X, Y. Even in this case, finding $Z(A)$ was non-trivial. We give a summary of the results below.

Definition 4.4.3. Prime Ring *Let* R *be a ring. We call* R *prime if given* $a, b \in R$ *with* $aRb = \{0\}$, *then* $a = 0$ *or* $b = 0$.

Lemma 4.4.4. A **is Prime** *Let* A *be a generic* $n \times n$ *matrix algebra. Then* A *is a prime ring.*

Proof: Let ξ and η be elements of A such that $\xi A\eta = \{0\}$. Then one can show that $\xi M_n(W)\eta = \{0\}$, where W is any subspace of F spanned by A. For verification of this result see [12], p90. But this implies that $\xi = 0$ or $\eta = 0$ since $M_n(W)$ is always prime. Thus we have A prime. ■

Theorem 4.4.5. A is a Domain *Let A be a generic $n \times n$ matrix ring. Then A has no zero divisors.*

Proof: Let A be any generic matrix ring generated by $n \times n$ matrices. Then A is a PI algebra and by the above lemma A is prime. Let Z denote the centre of A. Set $D = \{\frac{a}{b} \colon a \in A,\ b \in Z\backslash\{0\}\}$, where $\frac{a}{b} = \frac{a'}{b'}$ if $ab' = ba'$. Then D is a central simple algebra of dimension n^2 over its centre.

Now suppose for contradiction that D is not a division algebra. Then D contains a non-zero nilpotent element d, so A contains such an element. Thus we have an $f = f(Y_1, ...Y_m)$, which is not a PI for $M_n(F)$ but f^r is a PI for $M_n(F)$ for some $r \geq 2$. Let K/F be a field extension. Then we can construct a cyclic division algebra (K, σ, g) with dimension n^2 over its centre C. For details on this construction, see [12], p83. We also note here that $F \subseteq C$, so we have: $(K, \sigma, g) \otimes_C K \cong M_n(K)$, which implies that f is not a PI for (K, σ, g) but f^r is. However since (K, σ, g) is itself a division algebra, this cannot hold. Therefore D is a division ring, referred to as the generic division ring of dimension n^2. Furthermore we find that A cannot contain any non-zero nilpotent element d, so A is a domain. ■

The fact that any generic matrix algebra A is a domain, regardless of whether or not it is finite dimensional is used to make conclusions about the classification of division rings for finitely generated algebras. In this case, the central quotient ring D is also always a division ring, a fact used in the final chapter. We now continue our discussion on the centre of generic matrix rings.

Notation 4.4.6. *We let the mappings T, $D : A \to F[x_{ij}, y_{ij}]$ denote the trace and determinant respectively. Let $B = F[T(X), T(Y), D(X), D(Y), T(XY)]$ and $S = B\mathbf{I} + BX + BY + BXY$, where $\mathbf{I}$ is the identity matrix.*

By noting that $\{\mathbf{I}, X, Y, XY\}$ is an linearly independent set over $F[X, Y]$, we see it is also such over B. Consequently one can show that $B = Z(S)$. Moreover by appealing to the Cayley-Hamilton Theorem and performing some arithmetic, one shows that $S = BA$. If we denote by $[A, A]$ the commutator ideal $A(XY - YX)A$, we find that appropriate usage of the Cayley-Hamilton Theorem yields $[A, A] = S(XY - YX)$.

Theorem 4.4.7. Expressing A as a Vector Space *We denote the p^{th} power of a matrix X by X^p. We may view A as a vector space by writing it as a direct sum of F-vector spaces: $A = \bigoplus_{p,q\geq 0} FX^pY^q \bigoplus [A, A]$, where p, q run over all possible exponents.*

Proof: Let $\pi \colon A \to A/[A, A]$ be the projection mapping and write $\pi(X) = \overline{X}$, $\pi(Y) = \overline{Y}$. Then one sees immediately that $A/[A, A] = F[\overline{X}, \overline{Y}] = \bigoplus_{p,q\geq 0} F\overline{X}^p\overline{Y}^q$. Moreover since our matrix entries are commutative indeterminants we see this is a commutative polynomial ring over F. It then follows that $A = \bigoplus_{p,q\geq 0} FX^pY^q \bigoplus [A, A]$. ■

It is this theorem that allows us to find $Z(A)$ explicitly. We first present a technical lemma.

Lemma 4.4.8. $Z(A) \bigcap [A, A] = B[A, A]^2$.

The details of the proof may be found in [10], p108.

Theorem 4.4.9. Explicit Form for $Z(A)$ $Z(A) = F \bigoplus B[A, A]^2$.

Proof outline: We first make use of Theorem 4.4.7 by supposing we have a $U+V \in Z(A)$ such that $U \in \bigoplus_{p,q} FX^pY^q$ and $V \in [A,A]$. Then we define an F-algebra map θ by $\theta\colon x_{ii} \mapsto x_{ii}$, $y_{ii} \mapsto y_{ii}$ for $1 \leq i \leq 2$ and $x_{ij} \mapsto 0$, $y_{ij} \mapsto 0$ for $i \neq j$. Using the fact that $\theta(U+V)$ is a scalar matrix, we conclude that $U \in F$ and thus by the lemma stated above $V \in B[A,A]^2$.

We see that at this time conclusions about the centre of generic matrix algebras were drawn only for very specific rings. Formanek did publish another paper containing some more general results, including the construction of a family of polynomials in the centre of an $n \times n$ generic matrix algebra over F. Even recently the problem of finding central elements of these algebras remained an interesting one. In 1991 for example, Drensky published a result quite like Formanek's in its specificity: a central polynomial of degree 13 was found for the 4×4 generic matrix algebra over a field F with $char(F) = 0$. At the present time this problem in its generality remains open.

4.5 A Non-Crossed Product Division Ring

Amitsur constructed a family of division algebras to answer our above question. We now outline his construction but refer the reader to [3] for full details. Let $\mathbf{Q}(Y)$ be the generic division ring D from proof 4.4.5, where $Y = \{Y_1, ..., Y_m\}$ is a set of generic matrices.

In what follows, we suppose for contradiction that $\mathbf{Q}(Y)$ is a crossed product algebra. Then $\mathbf{Q}(Y) = (L, G, f)$ for a maximal normal subfield L of Z and Galois group $G = Gal_Z(L)$.

Lemma 4.5.1. Amitsur I *Let A be an F-CSA such that $char(F) = 0$. Suppose that $[A\colon F] = n^2$. Then A is also a crossed product with Galois group G as above.*

Definition 4.5.2. Laurent Series Field *Let F be a field with $char(F) = 0$ and let $F(t) = \{\sum_{\nu \geq m} a_\nu t^\nu\}$ with $a_\nu \in F$ and $m > -\infty$. We write $p(t) \in F(t)$. Then $F(t)$ is called a Laurent series field, or a power series field.*

Remark 4.5.3. *If $t_1, ..., t_r$ is a set of indeterminants we can recursively define $F(t_1, ..., t_r) = (F(t_1, ..., t_{r-1}))(t_r)$ with elements $p(t_1, ...t_r) = \sum_{\nu_1 \geq m_1} \cdot\cdot \cdot \sum_{\nu_r \geq m_r} a_{\nu_1} \cdots a_{\nu_r} t_1^{\nu_1} \cdots t_r^{\nu_r}$ then $F(t_1, ..., t_r)$ is a field extension of $F(t_1)$ and is also a Laurent series field.*

Lemma 4.5.4. Amitsur II *There exists a Laurent series field $K = F(t_1, ...t_r)$ such that any algebra A over K with $[A\colon K] = n^2$ is a crossed product with Galois group $G = C_{p_1} \times C_{p_2} \times \cdots C_{p_r}$, where the C_{p_i} are cyclic groups of prime order p_i and the p_i need not be distinct.*

Lemma 4.5.5. Amitsur III *There exists a prime p such that we have a division algebra Δ over the p-adic field $\mathbf{Q}_p$ with the following properties:*

1) $[\Delta\colon \mathbf{Q}_p] = n^2$.
2) For any maximal normal subfields $L \subseteq \Delta$, we have $G = Gal_{\mathbf{Q}_p}(L)$ such that $C_2 \triangleleft G$ and G/C_2 is cyclic.

Thus, Amitsur showed that only for $n = 2^i p_1, ..., p_r$, $i = 0, 1$ or 2 and $p_1, ..., p_r$ distinct odd primes can there exist Galois groups G of maximal normal subfields L satisfying Amitsur II and with property 2) of Amitsur III. Thus, $G = C \times C_{p_1} \times \cdots C_{p_r}$ where C is either trivial or equal to C_2 or $C_2 \times C_2$. This brings us to the following theorem.

Theorem 4.5.6. Non-Crossed Product Division Algebras *Given a division algebra $\mathbf{Q}(Y)$ over its centre Z with $[\mathbf{Q}(Y)\colon Z]$, we see that if $8 \mid n$ or if $p^2 \mid n$ for some odd prime p then $\mathbf{Q}(Y)$ fails to be a crossed product.*

In summary, we have investigated the development of the classification of finite dimensional division algebras with the Brauer group and crossed products as well as PI algebras. By the 1980's it was known that the class of finite dimensional division algebras over fields is much broader than the class of cyclic algebras or even crossed products. In the final chapters we will discuss a generalization of this study to finitely generated central simple algebras and the tools developed to classify these. One will find that the classification of finitely generated algebras has a different feel to it than the work proceeding it, in that the size of the class of algebras under this description is too large to give us the sense of concreteness that we have gotten used to thus far.

Chapter 5

Growth of Algebras

5.1 Growth of Finitely Generated Groups

In the classical study of finite-dimensional division algebras, tools like crossed products and the Brauer group enabled us to categorize these algebras over given fields up to isomorphism, or at least up to Brauer equivalence. In the cases where we wish to examine infinite dimensional F-algebras, we cannot have as concrete a classification. From about the 1970's growth of groups has been studied in order to find links between groups with certain properties and their growth functions. We begin the section with some definitions and statements.

Definition 5.1.1. Generated Subgroup *Let G be a group and let $S \subseteq G$ be any subset. Then we denote by $\langle S \rangle$ the subgroup of G generated by S.*

Definition 5.1.2. Length *Let G be a group and $S \subseteq G$. Let $g \in \langle S \rangle$. We define the length of g with respect to S as $\lambda_S(g) = min\{m \colon g = s_1 \cdots s_m$, $s_i \in S \cup S^{-1}\}$.*

Definition 5.1.3. Growth Function *Let G be a group and $S \subseteq G$ such that S is finite. The function $\gamma_S \colon \mathbf{N} \to \mathbf{N}$, $\gamma_S(m) = Card\{g \in \langle S \rangle \colon \lambda_S(g) \leq$*

$m\}$ is called the growth function of S. For the remainder of this discussion we deal only with finite subsets S of a group G.

Remark 5.1.4. *Let $m, n \in \mathbf{N}$. Then we have $\gamma_S(m+n) \leq \gamma_S(m)\gamma_S(n)$. As a consequence we see that $\gamma_S(m) \leq \gamma_S(1)^m$ gives us that $\gamma_S(m)^{\frac{1}{m}} \leq \gamma_S(1)$.*

Definition 5.1.5. Growth Rate *Let G be a group, S a finite subset of G and γ_S as above. Set $e_S = \lim_{m\to\infty} \gamma_S(m)^{\frac{1}{m}}$. If e_S exists we call it the growth rate of G with respect to S.*

Proposition 5.1.6. *Let G be a group with finite subset S. Then $\lim_{m\to\infty} \gamma_S(m)^{\frac{1}{m}}$ always exists.*

The proof of this proposition can be found in a paper by Milnor entitled *A note on curvature and the fundamental group*. It is important to note here that the growth function γ_S is dependent on our choice of subset S. We now turn to a discussion on groups generated by a finite subset S.

Proposition 5.1.7. *Let G be a group and $S, T \subseteq G$ such that S and T are finite and $\langle S\rangle = \langle T\rangle = G$. Then there exists $a, b \in \mathbf{N}$ such that $\gamma_T(m) \leq \gamma_S(am)$ and $\gamma_S(m) \leq \gamma_T(bm)$ $\forall m \geq 0$. This implies that $e_T \leq e_S^a$ and $e_S \leq e_T^b$.*

Proof: Set $a = 1 + max_{g\in T}\lambda_S(g)$ and $b = 1 + max_{g\in S}\lambda_T(g)$ and the first set of inequalities are satisfied. Moreover we note that $\gamma_T(m)^{\frac{1}{m}} \leq \gamma_S(am)^{\frac{1}{m}} = \gamma_S(am)^{\frac{a}{am}} = \gamma_S(am)^{\frac{1}{am}a}$. Thus taking limits $e_T \leq e_S^a$. By symmetry we have $e_S \leq e_T^b$. ■

Corollary 5.1.8. *Let G be a group with finite generating set S. Then if T is another generating set for G we have $e_S > 1 \Leftrightarrow e_T > 1$.*

Definition 5.1.9. Exponential Growth *Let G be a group with finite generating set S. Then if $e_S > 1$ we say that G has exponential growth rate or is of exponential growth. Otherwise $e_S = 1$ and we say G has polynomial growth rate or is of polynomial growth.*

Remark 5.1.10. *Given a group G with any finite generating set S, the determination of whether the growth rate of G is exponential or polynomial is independent of the choice of generators. We therefore call e_S the growth rate of G.*

Let G be a group with finite generating set S. Let $P(x), Q(x) \in \mathbf{Q}[x]$, and set $d = deg(P)$, $e = deg(Q)$ and suppose we have $P(m) \leq \gamma_S(m) \leq Q(m)$ for all but finitely many $m \in \mathbf{N}$. Then we can find positive real constants A and B such that $Am^d \leq \gamma_S(m) \leq Bm^e$. Now let T be another finite generating set for G. By the above proposition there exists $a, b \in \mathbf{N}$ such that $\gamma_S(m) \leq \gamma_T(am)$ and $\gamma_T(m) \leq \gamma_S(bm)$ for $m \in \mathbf{N}$. With these inequalities we can show:

1) γ_T is bounded below: $\gamma_T(m) \geq \gamma_T(a\lfloor \frac{m}{a} \rfloor) \geq A\lfloor \frac{m}{a} \rfloor^d$, since $\gamma_T(am) \geq \gamma_S(m) \geq Am^d$; moreoever $A\lfloor \frac{m}{a} \rfloor^d \geq (\frac{A}{a^d})(m-a)^d$, a polynomial of degree d in m.

2) γ_T is bounded above: $\gamma_T(m) \leq \gamma_S(bm) \leq B(bm)^e = Bb^e(m^e)$, a polynomial of degree e in m.

Thus the bounds on γ_S are polynomials of the same degree as those bounding γ_T. Our discussion leads us to a definition of polynomial growth of groups wherein the degree of growth is independent of the chosen generating set for G.

Definition 5.1.11. Polynomial Growth of Degree d *Let G be a group with finite generating set S. If $\exists d \in \mathbf{N}$ and constants $A, B > 0$ such that $Am^d \leq \gamma_S(m) \leq Bm^d$ $\forall m \in \mathbf{N}$ then we say G has polynomial growth of degree d.*

Whereas calculating e_S allows distinction between exponential growth and polynomial growth, this definition is useful in distinguishing between various degrees of polynomial growth.

5.2 Growth of Finitely Generated Algebras

The study of algebra growth is younger than the study of group growth and is closely related. We begin this section with some definitions leading to Gelfand-Kirillov dimension, the main tool in the modern classification of algebras.

Definition 5.2.1. Generating Vector Space *Let A be a finitely generated F-algebra, that is: we have $\{a_1, ..., a_m\} \subseteq A$ such that every element $a \in A$ has the form $a = \sum_{i=1}^{n} b_i$, where b_i is a monomial in $\{a_1, ..., a_n\}$. Then denote by V_A the F-vector space spanned by the a_i. We write V when the associated algebra is known from context and call V the generating subspace of A.*

Let $\mathcal{P}$ denote the set of sequences of real numbers that eventually become positive and increasing.

Definition 5.2.2. Ordering on P *Let $f, g \in \mathcal{P}$. We write $f \leq_{\mathcal{P}} g$ if there exist $c, m \in \mathbf{N}$ so that eventually $f(n) \leq cg(mn)$. We write $f \sim g$ if $f \leq_{\mathcal{P}} g$ and $g \leq_{\mathcal{P}} f$.*

Definition 5.2.3. Growth of f *Let $f \in \mathcal{P}$. Then $\mathcal{G}(f) = \{g \in \mathcal{P} \colon f \sim g\}$ is called the growth class, or simply growth, of f. We write $(\overline{\mathcal{P}}, \leq)$ to denote the poset of growth classes.*

Remark 5.2.4. *Let $f = f(x)$ and $g = g(y)$ be monic polynomial functions. Then $\mathcal{G}(F) = \mathcal{G}(g)$ if and only if $deg(f) = deg(g)$.*

Definition 5.2.5. *Let $\epsilon \geq 0$. Then we denote by P_ϵ the growth of the function $\mathbf{N} \to \mathbf{R}$, $n \mapsto n^\epsilon$. If $\epsilon > 0$, we denote by E_ϵ the growth of the function $\mathbf{N} \to \mathbf{R}$, $n \mapsto e^{n^\epsilon}$.*

Let ϵ, $\eta \geq 0$. Then $\epsilon < \eta$ if and only if $E_\epsilon < E_\eta$. An important example of function growth is logarithmic growth: let $f(n) = \log(n)$. Then f is in $\mathcal{P}$ and $\mathcal{G}(f) > P_0$, however if $\epsilon > 0$ then $\mathcal{G}(f) < P_\epsilon$.

Remark 5.2.6. *Since $(\overline{\mathcal{P}}, \leq)$ is a poset, there is no guarantee that the growth of two arbitrary functions in $\mathcal{P}$ are comparable.*

Given an algebra A finitely generated over F, we know from Definition 5.2.1 that A has finite dimensional generating subspaces. Let V, W be such subspaces. We label as $d_V(n)$ the dimension of $\sum_{i=0}^{n} V^i$, where $V^0 = F$, $d_W(n)$ the dimension of $\sum_{i=0}^{n} W^i$ and set $A_n = F + V + V^2 + ... + V^n = F + W + W^2 + ... + W^n$. We note that if A is finite-dimensional, then $A = A_n$ for some $n < \infty$, and in this case $d_V(n) = dim_F(\sum_{i=0}^{n} V^i) = dim_F(A_n)$ becomes eventually constant. In all cases we have $A = \bigcup_{n \in \mathbf{N}} A_n$ and d_V is increasing. Similar remarks can be made about d_W.

Lemma 5.2.7. Growth of d_V *Let A be a finitely generated algebra over F with generating subspaces V and W. Let $d_V(n), d_W(n)$ be as above. Then $\mathcal{G}(d_V) = \mathcal{G}(d_W)$.*

Proof: $A = \bigcup_{n=0}^{\infty}(F + V + V^2 + ... + V^n) = \bigcup_{n=0}^{\infty}(F + W + W^2 + ... + W^n)$ so there are $s, t > 0$ such that $W \subseteq \sum_{i=0}^{s} V^i$ and $V \subseteq \sum_{j=0}^{t} W^j$ but this means $d_W(n) \leq d_V(sn)$ and $d_V(n) \leq d_W(tn)$, so by definition $d_V \sim d_W$, thus $\mathcal{G}(d_V) = \mathcal{G}(d_W)$. ■

Definition 5.2.8. Growth of A *Let A be a finitely generated F-algebra and let V be any finite dimensional generating subspace of A. Without loss of generality $1 \in V$ so we have $\sum_{i=0}^{n} V^i = V^n$. We define the growth of A to be $\mathcal{G}(d_V)$ and we write $\mathcal{G}(A) = \mathcal{G}(d_V)$.*

By the above lemma, $\mathcal{G}(A)$ is independent of the choice of the generating subspace we use to measure it. This is a tool that vastly increases the sizes of algebras we can concretely study. Under this definition of growth, any finite-dimensional algebra A over F will have constant growth. More generally we say A has polynomial growth if $\mathcal{G}(A) = P_m$ for some $m \in \mathbf{N}$, exponential growth if $\mathcal{G}(A) = E_\epsilon$ for some $\epsilon > 0$, and subexponential growth if $P_m < \mathcal{G}(A) < E_1$ for all $m \in \mathbf{N}$. At this point we ask whether, given any m, there exists a finitely generated F-algebra A such that $\mathcal{G}(A) = P_m$. We answer this with the following proposition.

Proposition 5.2.9. *Let $A = F[x_1, ..., x_d]$ be the commutative polynomial ring in d variables. Then $\mathcal{G}(A) = P_d$.*

Proof Outline: We regard A as an F-algebra with generating subspace $V = Fx_1 + ... + Fx_d$. Then it is not difficult to show that $dim(V^{n+1}) = \binom{n+d}{d-1}$, which we view as a polynomial $p(n)$ of degree $d-1$. We have $d_V(n+1) - d_V(n) = dim(V^{n+1})$ and one can show that resultantly, $d_V(n)$ is a polynomial $p(n)$ with degree d. For a proof of this, see [16], p8. Thus we have $\mathcal{G}(A) = \mathcal{G}(d_V(n)) = d$. ■

We end this section with another result on finitely generated algebra growth.

Proposition 5.2.10. *Let A be a finitely generated F-algebra such that A is not finite dimensional. Then $P_1 \leq \mathcal{G}(A) \leq E_1$.*

A proof of this proposition can be found in [16], p9.

5.3 Gelfand-Kirillov Dimension

There are different ways of measuring the growth of algebras, including the GK-dimension. However, this tool also helps us to classify subalgebras such

as division algebras living inside a finitely generated algebra A in an efficient way. The key is to look at the asymptotic behaviour of growth functions. In the study of modern division algebra classification, Gelfand-Kirillov dimension is the most widely used invariant, although there are some others. An example is a paper published in 1976 of Borho and Kraft focusing on the *superdimension* of an algebra. We begin with introducing the connection between $\mathcal{G}(A)$ and GK-dimension.

Notation 5.3.1. *We write* $\log_n f(n)$ *to denote* $\frac{\log f(n)}{\log n}$ *and* $\overline{\lim}$ *for the limit superior.*

Lemma 5.3.2. Relationship Between Logarithm and Growth *Let* $f, g \in \mathcal{P}$. *Then:*

1) $\overline{\lim} \log_n f(n)$
$= inf\{r \in \mathbf{R}\colon f(n) \leq n^r$ *for all but finitely many* $n\}$
$= inf\{r \in \mathbf{R}\colon \mathcal{G}(f) \leq P_r\}$
2) If $\mathcal{G}(f) = \mathcal{G}(g)$ *then* $\overline{\lim} \log_n f(n) = \overline{\lim} \log_n g(n)$

Proof: For part 1) we set $R = \overline{\lim} \log_n f(n)$, $S = inf\{r \in \mathbf{R}\colon f(n) \leq n^r$ for all but finitely many $n\}$, and $T = inf\{r \in \mathbf{R}\colon \mathcal{G}(f) \leq \mathcal{G}(g)\}$. Then if any of R, S, T are infinite, so the others must be. Suppose $f(n) \leq n^r$ for all but finitely many n. Then $\mathcal{G}(f) \leq n^r$ so that $\{r \in \mathbf{R}\colon f(n) \leq n^r$ for all but finitely many $n\} \subseteq \{r \in \mathbf{R}\colon \mathcal{G}(f) \leq \mathcal{G}(r)\}$, therefore $T \leq S$. Now let $\epsilon > 0$. Then $\log_n f(n) \leq R + \epsilon$ for all but finitely many $n \in \mathbf{N}$, that is $f(n) \leq n^{R+\epsilon}$, which gives us $S \leq inf\{R + \epsilon\colon \epsilon > 0\}$, therefore $S \leq R$. Suppose now for contradiction that $R > T$ and consider $\epsilon = \frac{R-T}{3}$. Then $\mathcal{G}(f) \leq \mathcal{G}(T + \epsilon)$, so $f(n) \leq (mn)^{T+\epsilon}$ for some $m \in \mathbf{N}$ and all but finitely many n. Choose n large enough so that $m^{T+\epsilon} \leq n^{\epsilon}$. Then $f(n) \leq n^{T+2\epsilon}$ for all but finitely many n. This contradicts $\log_n f(n) > \overline{\lim} \log_n f(n) - \epsilon = R - \epsilon = T + 2\epsilon$ for all but finitely many n. Thus $R \leq T$ and we have established equality. Part 2) is left to the reader, as it is a direct consequence of 1). ■.

Let C be any F-algebra, not necessarily finitely generated. The Gelfand-Kirillov (GK) dimension of C is defined as $GKdim(C) = sup_V\{\overline{\lim}\log_n d_V(n)\}$, where V runs over all finite-dimensional subspaces of C.

Let A be a finitely generated F-algebra. Then the above definition can be written as $GKdim(A) = \overline{\lim}\log_n d_V(n)$, where V is any finite dimensional generating subspace of A. This is because Lemma 5.2.7 tells us the GK-dimension of a finitely generated F-algebra will be independent of the choice of generating subspace. We note a similarity to the growth functions of finitely generated groups. We note here that if V is a finite dimensional subspace of any F-algebra C, it is certainly a generating subspace for a finitely generated subalgebra $A \subseteq C$. Thus we have $GKdim(C) = sup_A\{GKdim(A)\colon A$ is a finitely generated subalgebra of $C\}$. The generality of this definition is part of its power. We now investigate some properties of GK-dimension for any F-algebra C.

Definition 5.3.3. Locally Finite Dimensional *let C be an F-algebra. Then C is called locally finite dimensional if every finitely generated subalgebra A of C is finite dimensional.*

Let C be an F-algebra. Then C is locally finite dimensional exactly when $GKdim(C) = 0$. Otherwise $GKdim(C) \geq 1$ follows from Proposition 5.2.10. We recall Proposition 5.2.9 to give us that for each n there exists an A such that $GKdim(A) = n$. What about non-integer dimensions? A theorem by Satz shows that if $r \in \mathbf{R}$ such that $2 < r \leq 3$ then there exists an algebra C such that $GKdim(C) = r$. [16] has details on Satz's construction and in fact there are other methods of constructing these algebras. Moreover we are guaranteed that for any F-algebra C, $GKdim(C[x_1, ..., x_d]) = GKdim(C) + d$. Thus if $r \geq 2$ Satz's Theorem verifies the existence of an algebra C with $GKdim(C) = r$. Some time passed after this discovery with the existence problem for GK-dimension between 1 and 2 remaining open, but in 1978 Bergman showed that if $r \in \mathbf{R}$ such that $r \in (1, 2)$ then there can be no

algebra with GK-dimension equal to r. The proof of Bergman's Theorem can be found in [16], pages 15-18.

Our goal remains to classify division algebras over a given field. With such a broad class of algebras at our disposal we must find a way to determine the behaviour of GK-dimension when relating an algebra to its subalgebras and homomorphic images. We focus here on finitely generated F-algebras; however, many of the results have generalizations to any F-algebra.

Proposition 5.3.4. Subalgebras and Homomorphic Images *Let A be a finitely generated F-algebra and let B be a subalgebra or homomorphic image of A. Then $GKdim(B) \leq GKdim(A)$.*

Proof: For a subalgebra B, the definition of GK-dimension leads immediately to the inequality. Now let $\pi\colon A \to B$ be a projection homomorphism. Then if $\overline{V}$ is a finite dimensional generating subspace for B we have $dim(\overline{V}^n) \leq dim(V^n)$ for all $n \in \mathbf{N}$, where V is the generating subspace formed by the pullback of the basis elements of $\overline{V}$. ■

Proposition 5.3.5. Tensor Products *Let A_1, A_2 be finitely generated F-algebras. Then $GKdim(A_1 \otimes_F A_2) \leq GKdim(A_1) + GKdim(A_2)$.*

Proof: Let A_1, A_2 be as above and let V_1, V_2 be finite dimensional generating subspaces for A_1, A_2 respectively and containing 1. Set $W = (V_1 \otimes 1_{A_1}) + (1_{a_2} \otimes V_2)$. Then W is a finite dimensional generating subspace for $A_1 \otimes A_2$. Moreover $V_1^n \otimes V_2^n \subseteq W^{2n} \subseteq V_1^{2n} \otimes V_2^{2n}$, which gives: $d_{V_1}(n)d_{V_2}(n) \leq d_W(2n) \leq d_{V_1}(2n)d_{V_2}(2n)$. Thus $GKdim(A_1 \otimes A_2) = \overline{\lim} \log_n d_W(2n) = \overline{\lim} \log_n (d_{V_1}(n)d_{V_2}(n)) = \overline{\lim}(\log_n d_{V_1}(n) + \log_n d_{V_2}(n)) \leq \overline{\lim} \log_n d_{V_1}(n) + \overline{\lim} \log_n d_{V_2}(n) = GKdim(A_1) + GKdim(A_2)$. ■

Remark 5.3.6. *We consider the sequences* $\{\log_n d_{V_1}(n)\}$, $\{\log_n d_{V_2}(n)\}$. *Warfield showed that if either of these sequences is convergent then we have* $GKdim(A_1 \otimes A_2) = GKdim(A_1) + GK(A_2)$ $(\star)$. *In particular, if one of the* A_i *is such that* $GKdim(A_i) \leq 2$ *then* $(\star)$ *holds. Should both* A_1 *and* A_2 *have GK-dimension greater than two, then although equality need not hold, we can find lower bounds for the growth of the sum of the dimensions. For example one can show that if* $2 < GKdim(A_1) \leq GKdim(A_2)$ *then* $GKdim(A_2)+2 \leq GKdim(A_1 \otimes A_2) \leq GKdim(A_1) + GKdim(A_2)$.

In addition to the above, similar results on GK-dimensions of finitely generated F-algebras are presented in [16], chapter 3. Although much can be said about GK-dimension of algebras, we bring our focus now to subfields of division algebras arising from the study of finitely generated F-algebras and their algebras of central quotients.

5.4 Bell's Results on Subfields of Division Algebras

This section must overlook certain details to present an overview of some modern results related to classifying algebras. Depending on the properties of a finitely generated algebra A, we can determine the nature of the division algebras that lie in A. Some theorems in this section have proofs which are beyond the scope of this chapter. In these cases a reference is provided.

We recall that we defined the generic division algebra D associated with a generic matrix algebra A as $D = \{\frac{a}{b} : a \in A, b \in Z(A)\backslash\{0\}\}$, where $\frac{a}{b} = \frac{a'}{b'}$ if and only if $ab' = ba'$. Given a field F and a finitely generated algebra A over F with no zero divisors, we can define the quotient algebra as above. We denote by $Q(A)$ the quotient algebra of A and note that it always exists but need not be a division algebra. From here on, D will denote a division subalgebra of $Q(A)$.

Fact 5.4.1. Quotient Algebras and GK-Dimension *Let A be any finitely generated algebra such that A is a domain with finite GK-dimension. Then $Q(A)$ is a division algebra.*

The proof of this fact can be found in chapter 4 of the revised edition of [16]. There is no method of determining whether or not $Q(A)$ is a division algebra when $GKdim(A) = \infty$. We present below some results on the subfields of the quotient division rings of algebras with finite GK-dimension.

Suppose our finitely generated domain A is such that $GKdim(A) < 3$ and let $D \subseteq Q(A)$ be a division subalgebra. If $Z(D) = K$ then we consider a field extension E/K such that $K \subseteq E \subseteq D$.

We note here that if we have sets $S \subseteq E$ and $T \subseteq D$, such that S is linearly independent over K and T is right-linearly independent over E, then the set $\{ts\colon s \in S, t \in T\}$ is linearly independent over K. This fact was discovered to be essential in proving Smoktunowicz's Gap Theorem, which deals with the GK-dimension of connected finitely generated domains. A generalization of this theorem is stated below.

Definition 5.4.2. Transcendence Basis and Degree *Let K and E be fields such that $K \subseteq E$. We call the set $B \subseteq E$ a transcendence basis of E if E is algebraic over $K(B)$ and B is algebraically independent over K. One can show that every field has a transcendence basis and that any two transcendence bases have the same cardinality, called the transcendence degree of E/K.*

Theorem 5.4.3. Bell I *Let A be a finitely generated F-algebra with $GKdim(A) < 3$ and with no zero divisors, and let D be a finitely generated division subalgebra of $Q(A)$. If $GKdim(D) \geq 2$ then $Q(A)$ is finite dimensional as a left D-vector space.*

A proof of this result can be found in [5]

Lemma 5.4.4. *Let A be a finitely generated F-algebra with no zero divisors such that $dimGK(A) < 3$ and suppose $Z(A) = F$. Then if $F = D_0 \subseteq D_1 \subseteq D_2 \subseteq ... \subseteq D_m \subseteq Q(A)$ is a chain of division subalgebras such that D_i is a finitely generated division algebra, yet infinite dimensional as a left vector space over D_{i-1} then $m \leq 2$.*

The proof of this lemma can be found in [6].

Theorem 5.4.5. *Let F be an algebraically closed field and let A be a finitely generated F-algebra such that A is a domain with $GKdim(A) < 3$. If D is a division subalgebra of $Q(A)$, then exactly one of the following must hold:*

1) D is a field with transcendence degree at most 1 over F
2) $Q(A)$ is finite dimensional as a left and right vector space over D.

Proof Outline: First we deal with the case where A is a PI-algebra. It then follows that $Q(A)$ is finite dimensional over its centre and thus over D. Otherwise, if D is commutative its transcendence degree will be at most 1. Suppose that D is not commutative. Choose $x, y \in D$ such that $xy \neq yx$ and let D' be the division algebra generated by x and y. A theorem of Tsen tells us that D' is infinite dimensional as a left $F(x)$-vector space. Thus we may conclude that $F \subseteq F(x) \subseteq D' \subseteq Q(A)$. By the above lemma we have that $Q(A)$ is finite dimensional over D' and $D \supseteq D'$, therefore $Q(A)$ is finite dimensional as a left D'-vector space and we are done. ■

The full proof can be found in [5]

A conjecture by Small states that if A is a finitely generated F-algebra such that A is a domain, $GKdim(A) = d$ and A is non-PI, then for any subfield $E \subseteq Q(A)$ we have the transcendence degree of E is at most $d - 1$ over F. In [5], Small's conjecture has been proven for several classes of algebras

satisfying the supposition. We appeal to what we saw in chapters 2 and 3 as an illustration of this conjecture's breadth: maximal subfields are useful tools in studying finite dimensional division algebras, so that in a more general setting it is not difficult to see the same is true for maximal subfields E of division subalgebras of $Q(A)$.

Definition 5.4.6. Straightening Property *Let A be a finitely generated F-algebra such that $GKdim(A) = d$ for some $d \geq 1$. Then A has the straightening property if there are $x_1, ..., x_d \in A$ such that $S = \{x_1^{i_1} x_2^{i_2} ... x_d^{i_d} : i_1, ..., i_d \geq 0\}$ is a vector space basis for A. In this case we call S a straightening basis for A.*

The terminology *straightening property* was invented by Small and used by Bell in discussing the following theorem.

Theorem 5.4.7. Bell II *Let A be a finitely generated F-algebra with $GKdim(A) = d$ for some $d \geq 1$ and suppose A has the straightening property. If $E \subseteq Q(A)$ is a subfield and $Q(A)$ is left algebraic over F, then $Q(A)$ is finite dimensional over F.*

The proof of this theorem can be found in [5].

Remark 5.4.8. *The end result of [5] is the proof that if an F-algebra A satisfies the conditions of Small's conjecture as well as the straightening property, then Small's conjecture holds for maximal subfields E of $Q(A)$. Algebras with no zero divisors that have the straightening property include: polynomial rings over any field, certain algebras related to finite dimensional Lie algebras and the tensor product of a finite number of algebras with the property.*

5.5 Concluding Remarks

We see that throughout the last 150 years, the classification of division algebras over fields has grown in complexity and generality. As with any mathematical problem, the most basic of cases were studied first, after which more general assertions were made and more abstract questions were posed. Even though one may find that we are currently unable to expand upon the older results, the classical theorems in chapters 2, 3 and 4 will always retain their beauty and remain the foundation of this study. At this time the investigation into properties of finitely generated algebras over fields continues, with broad classification theorems concerning GK-dimension waiting to be discovered and proven.

This Master's thesis is in no way a complete summary of the classification of division algebras or growth of algebras; rather it highlights many important historical results and provides a small taste of the modern ones. The interested reader is encouraged to take advantage of the bibliographical listings to pursue further reading material on all of the subjects discussed.

Bibliography

[1] Albert, A. A., *A Construction of Non-Cyclic Normal Division Algebras*, Bulletin of the American Mathematical Society, Volume 38 (1932), 449-456

[2] Alperin, Roger C., *Uniform Growth of Polycyclic Groups*, Geometriae Dedicata, Volume 92 (2002), 105-113

[3] Amitsur, S. A., *On Central Division Algebras*, Israel Journal of Mathematics, Volume 12 (1972), 408-420

[4] Bass, H., *The Degree of Polynomial Growth of Finitely Generated Nilpotent Groups*, Proceedings of the London Mathematical Society, Third Series, Volume 25 (1972) 603-614

[5] Bell, Jason P., *On the transcendence degree of subfields of division algebras*, preprint

[6] Bell, Jason P., *Division algebras of Gelfand-Kirillov transcendence degree 2*, preprint

[7] Drensky, V. and Cattaneo, G. M. P., *A central Polynomial of Low Degree for* 4×4 *Matrices*, Journal of Algebra, Volume 168 (1994), 469-478

[8] Dummit, David S. and Foote, Richard M., *Abstract Algebra*, Wiley & Sons, Hoboken, New Jersey, 2004

[9] Formanek, E., *Central Polynomials for Matrix Rings*, Journal of Algebra, Volume 23 (1972), 129-132

[10] Formanek, E., Halpin, P. and Li, W. W., *The Poincare Series of the Ring of* 2×2 *Generic Matrices*, Journal of Algebra, Volume 69 (1981), 105-112

[11] Herstein, I. N., *Noncommutative Rings*, Wiley & Sons, Hoboken, New Jersey, 1968

[12] Jacobson, Nathan, *PI-Algebras: An Introduction*, Springer-Verlag, Heidelberg, Germany, 1975

[13] Jacobson, Nathan, *Finite Dimensional Division Algebras over Fields*, Springer Books, Heidelberg, Germany, 1996

[14] Kaplansky, Irving, *Rings with a Polynomial Identity*, Bulletin of the American Mathematical Society, Volume 53 (1947), 575-580

[15] Kaplansky, Irving, *Fields and Rings*, University of Chicago Press, Chicago, 1969

[16] Krause, Gunter R. and Lenagan, Thomas H., *Growth of Algebras and Gelfand-Kirillov Dimension*, American Mathematical Society, Providence, Rhode Island, 2000

[17] Lambek, Joachim, *Lectures on Rings and Modules*, Blaisdell Publishing, Waltham, Massachusetts, 1966

[18] Reiner, I., *Maximal Orders*, Academic Press, London, England, 1975

[19] Roquette, Peter, *The Brauer-Hasse-Noether Theorem in Historical Perspective*, Springer Books, Heidelberg, Germany, 2005

[20] Rotman, Joseph J., *Advanced Modern Algebra 1st edition*, Prentice Hall, 2002

[21] Rowen, Louis H., *Polynomial Identities in Ring Theory*, Academic Press, New York, New York, 1980

[22] Saltman, David J., *Lectures on Division Algebras*, American Mathematical Society, Providence, Rhode Island, 1999