Division Algebra Theorems of Frobenius and Wedderburn

Christopher M. Drupieski
Nicholas A. Hamblet
University of Virginia
Algebra Seminar
November 9, 2005
Outline

I. Prerequisites
II. Elementary Consequences
III. Application of Wedderburn-Artin Structure Theorem
IV. Classification Theorems
V. Further Classification of Central Division Algebras
I. Prerequisites

- Wedderburn-Artin Structure Theorem
- Definition: Central Simple Algebra
- Examples
- Technical Lemma
Wedderburn-Artin Structure Theorem

Let $R$ be a left semisimple ring, and let $V_1, \ldots, V_r$ be a complete set of mutually nonisomorphic simple left $R$-modules. Say $R \cong n_1 V_1 \oplus \cdots \oplus n_r V_r$. Then

$$R \cong \prod_{i=1}^{r} M_{n_i}(D_i^\circ)$$

where $D_i = \text{End}_R(V_i)$ is a division ring. If $R$ is simple, then $r = 1$ and $R \cong \text{End}_D(V)$. 
Definition

Call $S$ a **central simple** $k$-algebra if $S$ is a simple $k$-algebra and $Z(S) = k$. 
Examples

• \( M_n(k) \) is a central simple \( k \)-algebra for any field \( k \).

• The Quaternion algebra \( \mathbb{H} \) is a central simple \( \mathbb{R} \)-algebra (Hamilton 1843).

• Any proper field extension \( K \supsetneq k \) is not a central simple \( k \)-algebra because \( Z(K) = K \neq k \).
Technical Lemma

Lemma 1. Let $S$ be a central simple $k$-algebra and let $R$ be an arbitrary $k$-algebra. Then every two-sided ideal $J$ of $R \otimes S$ has the form $I \otimes S$, where $I = J \cap R$ is a two-sided ideal of $R$. In particular, if $R$ is simple, then $R \otimes S$ is simple.
Counterexample

The simplicity of $R \otimes S$ depends on $S$ being central simple.

- $\mathbb{C}$ has the structure of a (non-central) $\mathbb{R}$-algebra.
- Let $e_1 = 1 \otimes 1$, $e_2 = i \otimes i$.
- Note that $(e_2 + e_1)(e_2 - e_1) = 0$.
- Then $0 \neq (e_2 + e_1)$ is a nontrivial ideal.
- $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not simple.
II. Elementary Consequences of Wedderburn Structure Theorem

- An isomorphism lemma
- A dimension lemma
Lemma (Isomorphism)

Lemma 2. Let $R$ be a finite dimensional simple $k$-algebra. If $M_1$ and $M_2$ are finite dimensional $R$-modules and $\dim_k M_1 = \dim_k M_2$, then $M_1 \cong M_2$. 
Proof of Lemma 2

Proof. Let $M$ be the unique simple $R$-module.

- Say $M_1 \cong n_1 M$ and $M_2 \cong n_2 M$.
- $n_1 \dim_k M = \dim_k M_1 = \dim_k M_2 = n_2 \dim_k M \Rightarrow n_1 = n_2 \Rightarrow M_1 \cong M_2$. 

\qed
Lemma (Dimension)

Lemma 3. If $D$ is a finite dimensional division algebra over its center $k$, then $[D : k]$ is a square.
Proof of Lemma 3

Proof. Let $K = \bar{k}$, the algebraic closure of $k$, and let $D^K = D \otimes_k K$.

- $[D^K : K] = [D : k] < \infty$.
- $D^K$ is a simple artinian $K$-algebra by Lemma 1.
- By the WA structure theorem, $D^K \cong M_n(K)$ for some $n \in \mathbb{N}$.
- $[D : k] = [D^K : K] = [M_n(K) : K] = n^2$.  \hfill $\square$
III. Application of Wedderburn-Artin Structure Theorem

- Skolem-Noether Theorem
- Corollary
- Centralizer Theorem
- Corollary
Theorem 4. [Skolem-Noether] Let $S$ be a finite dimensional central simple $k$-algebra, and let $R$ be a simple $k$-algebra. If $f, g : R \to S$ are homomorphisms (necessarily one-to-one), then there is an inner automorphism $\alpha : S \to S$ such that $\alpha f = g$. 

Skolem-Noether Theorem

Theorem 4. [Skolem-Noether] Let $S$ be a finite dimensional central simple $k$-algebra, and let $R$ be a simple $k$-algebra. If $f, g : R \to S$ are homomorphisms (necessarily one-to-one), then there is an inner automorphism $\alpha : S \to S$ such that $\alpha f = g$. 

15
Proof of Skolem-Noether

• $S \cong \text{End}_D(V) \cong M_n(D^\circ)$ for $k$-division algebra $D$ and finite-dimensional $D$-module $V$.

• $D$ central simple since $k = Z(S) = Z(D)$.

• $V$ has two $R$-module structures induced by $f$ and $g$.

• $R$-module structure commutes with $D$-module structure since $S \cong \text{End}_D(V)$.

• $V$ has two $R \otimes D$-module structures induced by $f$ and $g$. 
Proof (cont.)

• $R \otimes D$ is simple by Lemma 1, so the two $R \otimes D$ module structures on $V$ are isomorphic by Lemma 2.

• There exists an isomorphism $h : R^f \otimes_D V \rightarrow R^g \otimes_D V$ such that for all $r \in R$ and $d \in D$,
  
  (i) $h(rv) = rh(v)$, i.e., $h(f(r)v) = g(r)h(v)$, and
  
  (ii) $h(dv) = dh(v)$

• Now $h \in End_D(V) \cong S$ by (ii). By (i), $hf(r)h^{-1} = g(r)$, i.e., $hfh^{-1} = g$. 
Corollary

**Corollary.** If $k$ is a field, then any $k$-automorphism of $M_n(k)$ is inner.
Centralizer Theorem

**Theorem 5.** [Centralizer Theorem] Let $S$ be a finite dimensional central simple algebra over $k$, and let $R$ be a simple subalgebra of $S$. Then

(i) $C(R)$ is simple.

(ii) $[S : k] = [R : k][C(R) : k]$.

(iii) $C(C(R)) = R$. 
Proof of Centralizer Theorem

• $S \cong \text{End}_D(V) \cong M_n(D^\circ)$, $D$ a central $k$-division algebra and $V$ a finite dimensional $D$-module.

• $V$ is an $R \otimes D$ module, and $C(R) = \text{End}_{R \otimes D}(V)$.

• $R \otimes D$ is simple, so $R \otimes D \cong \text{End}_E(W)$, $W$ the simple $R \otimes D$-module and $E = \text{End}_{R \otimes D}(W)$.

• Say $V \cong W^n$ as $R \otimes D$-modules.
Proof (cont.)

• $C(R) = \text{End}_{R \otimes D}(V) \cong \text{End}_{R \otimes D}(W^n) \cong M_n(E)$, which is simple.

• (ii) follows from $C(R) \cong M_n(E)$, WA structure theorem, and mundane degree calculations.

• Apply (ii) to $C(R)$, get $[C(C(R)) : k] = [R : k]$. Then $R \subseteq C(C(R)) \implies R = C(C(R))$. 
Corollary

**Corollary 6.** Let $D$ be a division algebra with center $k$ and $[D : k] = n^2$. If $K$ is a maximal subfield of $D$, then $[K : k] = n$. 
Proof of Corollary

Proof.

• By maximality of $K$, $C(K) = K$.

• Then by the Centralizer Theorem,

$$n^2 = [D : k] = [K : k]^2 \Rightarrow [K : k] = n$$

\[\square\]
IV. Classification Theorems

• Finite Division Rings (Wedderburn)
• Group Theoretic Lemma
• Finite Dimensional Division $\mathbb{R}$-algebras (Frobenius)
Classification of Finite Division Rings

**Theorem 7** (Wedderburn, 1905). Every finite division ring is commutative, i.e., is a field.
Group Theoretic Lemma

Lemma. If $H \leq G$ are finite groups with $H \neq G$, then $G \neq \bigcup_{g \in G} gHg^{-1}$. 
Proof of Wedderburn Theorem

Let $k = Z(D)$, $q = |k|$, $K \supseteq k$ a maximal subfield of $D$. Assume $K \neq D$.

- $[D : k] = n^2$ for some $n$ by Lemma 3, and $[K : k] = n$ by Corollary 6. Then $K \cong F_{q^n}$.

- Since $F_{q^n}$ is unique up to isomorphism, any two maximal subfields of $D$ containing $k$ are isomorphic, hence conjugate in $D$ by the Skolem Noether Theorem.
Proof (cont.)

• Every element of $D$ is contained in some maximal subfield, so $D = \bigcup_{x \in D} xKx^{-1}$.

• Then $D^* = \bigcup_{x \in D^*} xK^*x^{-1}$, which is impossible by the group theoretic lemma above unless $K = D$. Conclude $K = D$, i.e., $D$ is a field.
Classification of Finite Dimensional Division \( \mathbb{R} \)-algebras

**Theorem 8** (Frobenius, 1878). If \( D \) is a division algebra with \( \mathbb{R} \) in its center and \([D : \mathbb{R}] < \infty\), then \( D = \mathbb{R}, \mathbb{C} \) or \( \mathbb{H} \).
Proof of Frobenius Theorem

Let $K$ be a maximal subfield of $D$. Then $[K : \mathbb{R}] < \infty$. We have $[K : \mathbb{R}] = 1$ or 2.

- If $[K : \mathbb{R}] = 1$, then $K = \mathbb{R}$ and $[D : \mathbb{R}] = 1$ by Lemma 3, in which case $D = \mathbb{R}$.
- If $[K : \mathbb{R}] = 2$, then $[D : K] = 1$ or 2 by Lemma 3.
- If $[D : K] = 1$, then $D = K$, in which case $D = \mathbb{C}$. 
Proof (cont.)

- Suppose \([D : K] = 2\). So \(K \cong \mathbb{C}\) and \(Z(D) = \mathbb{R}\).

- Complex conjugation \(\sigma\) is an \(\mathbb{R}\)-isomorphism of \(K\). Hence, by the Skolem-Noether Theorem there exists \(x \in D\) such that \(\varphi_x = \sigma\), where \(\varphi_x\) denotes conjugation by \(x\).

- \(\varphi_{x^2} = \varphi_x \circ \varphi_x = \sigma^2 = id\). Then \(x^2 \in C(K) = K\). In fact, \(\varphi_x(x^2) = \sigma(x^2) = x^2 \Rightarrow x^2 \in \mathbb{R}\).
Proof (cont.)

• If $x^2 > 0$, then $x = \pm r$ for some $r \in \mathbb{R}$, ($\Rightarrow\Leftarrow$). So $x^2 < 0$ and $x^2 = -y^2$ for some $y \in \mathbb{R}$.

• Let $i = \sqrt{-1}$, $j = x/y$, $k = ij$. Check that the usual quaternion multiplication table holds.

• Check that $\{1, i, j, k\}$ forms a basis for $D$. Then $D \cong \mathbb{H}$.
V. Further Classification of Central Division Algebras

- Equivalence Relation
- Observations
- Definition of Brauer Group
- Examples
Equivalence Relation

Define an equivalence relation on central simple $k$-algebras by

$$S \sim S' \iff S \cong M_n(D) \text{ and } S' \cong M_m(D)$$

for some central division algebra $D$. Denote the equivalence class of $S$ by $[S]$, and let $Br(k)$ be the set of all such similarity classes. Each element of $Br(k)$ corresponds to a distinct central division $k$-algebra. Can recover information about central division $k$-algebras by studying structure of $Br(k)$.
Observations

• If $S, T$ are central simple $k$-algebras, then so is $S \otimes_k T$.

• $[S] * [T] := [S \otimes_k T]$ is a well-defined product on $Br(k)$.

• $[S] * [T] = [T] * [S]$ for all $[S], [T] \in Br(k)$.

• $[S] * [k] = [S] = [k] * [S]$ for all $[S] \in Br(k)$.

• $[S] * [S^\circ] = [k] = [S^\circ] * [S]$ for all $[S] \in Br(k)$. (Follows from $S \otimes S^\circ \cong M_n(k)$.)
Definition of the Brauer Group

**Definition.** Define the Brauer group of a field $k$, denoted $Br(k)$, to be the set $Br(k)$ identified above with group operation $\otimes_k$. 
Examples

• $Br(k) = 0$ if $k$ is algebraically closed, since there are no nontrivial $k$-division algebras.

• $Br(F) = 0$ if $F$ is a finite field by Wedderburn’s Theorem on finite division rings.

• $Br(\mathbb{R}) = \mathbb{Z}_2$ by Frobenius’s Theorem and the fact that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$. 