NOTE ON CENTRAL SIMPLE ALGEBRAS AND THE BRAUER GROUP

YASSINE AIT MOHAMED

Abstract. The main goal of this note is the study of the important properties of central simple algebras.

1. Introduction

The theory of central simple algebras represents one of the most elegant and profound chapters in modern algebra, combining elements of ring theory, Galois theory, and algebraic number theory into a coherent framework with wide-ranging applications. The systematic study of these structures emerged in the early 20th century, although their origins can be traced to fundamental questions in 19th century mathematics. The initial investigations into what would later be recognized as central simple algebras began with Hamilton's discovery of quaternions in 1843. Hamilton's construction of a non-commutative division algebra over the real numbers challenged the prevailing algebraic paradigms and opened new avenues of research. Subsequent work by Cayley on octonions further expanded the landscape of algebraic structures beyond the commutative realm. A significant theoretical advancement occurred through Wedderburn's fundamental theorem (1907), which established that every simple algebra of finite dimension over a field is isomorphic to a matrix algebra over a division ring. This result, refined by Artin in the 1920s into what is now known as the Artin-Wedderburn theorem, provided the crucial structural characterization that serves as the foundation for the modern theory. The work of Emmy Noether and her school in the 1920s and 1930s placed the study of central simple algebras within the broader context of abstract algebra. Brauer's introduction of what is now called the Brauer group (1929) represented a particularly significant development, providing a means to classify central simple algebras over a given field and establishing profound connections to Galois cohomology. Albert's extensive investigations in the 1930s further enriched the theory, particularly through his work on crossed products and division algebras. The theory gained additional momentum through its connections to class field theory, as developed by Hasse, Brauer, and Noether, who established the local-global principles governing central simple algebras over number fields. The emergence of central simple algebras as a fundamental object of study was solidified by their connections to various areas of mathematics. Their relationship to projective representations of groups, established by Schur, their role in the theory of simple algebras with involution, and their connections to quadratic forms and algebraic groups all contributed to their centrality in algebraic theory. In contemporary mathematics, central simple algebras continue to play a pivotal role in various domains, including representation theory, algebraic K-theory, and arithmetic geometry. The Brauer group, in particular, has found applications in areas as diverse as the study of algebraic surfaces and modern cryptographic constructions.

2. Simple rings and modules

A ring here is assumed to be associative with a unity, but not necessarily commutative and modules will be assumed to be left modules, unless otherwise stated.

Definition 2.1. *Let R be a ring and M be an R-module. We say that M is a simple module if it is nonzero and the only R-submodules of M are 0 and M. The ring R is called a simple ring if it has no two-sided ideals but 0 and R.*

Examples 2.2.
1) *If k is a field, then the only simple k-modules are the 1-dimensional k-vector spaces.*
2) *Take $R = \mathbb{Z}$. Every abelian group of prime order is a simple R-module.*
3) *If R is a commutative ring, then every simple R-module is isomorphic (as an R-module) to a quotient ring $R/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal of R.*

Definition 2.3. *Let R be a nonzero ring with unit. We say that R is a division ring or a skew field if every nonzero element $x \in R$ has a multiplicative inverse, i.e, there exists $x' \in R$ such that $xx' = x'x = 1$.*

Example 2.4. *Let $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, where i, j and k are indeterminates elements subject to the following equalities $i^2 = j^2 = k^2 = -1$. The ring $\mathbb{H}$ (with basis $(1, i, j, k)$ and endowed with the nutural addition and the multiplication defined by linear extension of the above equalities) is called the ring of quaternions. We show that $\mathbb{H}$ is a skew field.*

Notation 1. *Let R be a ring and M be an R-module. We will denote the endomorphism ring of M by $End_R(M)$.*

Theorem 2.5. (*Schur's lemma*)
Let M and N be simple R-modules. If $f : M \longrightarrow N$ is a homomorphism of modules, then either $f = 0$ or f is an isomorphism. In particular, the ring $End_R(M)$ is a skew field.

Proof. The kernel of f is a submodule of M, so it is either 0 or whole of M. Likewise, the image of f is a submodule of of N and it must be 0 or whole of N. If $f \neq 0$, then $\ker(f) = 0$ and $im(f) = N$, hence f is an isomorphism. The second assertion follows then by taking $N = M$.

Theorem 2.6. *If D is a skew filed, then $M_n(D)$ is a simple ring, for every $n \in \mathbb{N}$.*

Proof. Let E_{ij} be the matrix with (i,j)-coefficient is equal to 1 and all other coefficients equal to 0. Let $A = (a_{mk})_{1 \le m,k \le n}$ be a nonzero matrix, i.e, there exist $i, j \in \{1, ..., n\}$ such that $a_{ij} \neq 0$. As D is a division ring, a_{ij} is invertible. One cane easily see that

$$a_{ij}^{-1}.E_{pi}AE_{jp} = E_{pp}.$$

It follwos that the two-sided ideal J generated by the matrix A contains the unit matrix I_n, since $I_n = E_{11} + ... + E_{nn}$. Hence J is equal to the ring $M_n(D)$, which shows that $M_n(D)$ is a simple ring.

Theorem 2.7. (*Wedderburn, Rieffel*)
Let R be a simple ring and M a nonzero left ideal of R. Then $R \cong End_D(M)$, where $D = End_R(M)$.

Proof. Let $A = End_D(M)$ and let $h: R \longrightarrow A$ be the map defined by $h(\alpha)x = \alpha x$, for all $\alpha \in R$ and $x \in M$. One can easily see that h is a ring homomorphism. As the ring R is simple and h is a nonzero ring homomorphism, then $\ker(h) = \{0\}$, i.e, h is injective. To prove the surjectivity of h we will show that $Im(h)$ is a left ideal of A which contains 1_A. It is clear that $h(1_R) = 1_A \in Im(h)$, since h is a ring homomorphism. Let $y \in M$ and denote by g_y the right multiplication by y, i.e, $g_y(x) = xy$ for all $x \in M$, Plainly, $g_y \in D$. Let $f \in A$, we have $f(xy) = f(g_y(x)) = g_y(f(x)) = f(x)y$.
It follows that $f \circ h(x)(y) = f(xy) = f(x)y = h(f(x))y$, which means, $f \circ h(x) = h(f(x))$, for all $x \in M$. If $\psi \in h(M)$, i.e, $\psi = h(x_0)$ for some $x_0 \in M$, then for all $f \in A$ we have:

$$f \circ \psi = f \circ h(x_0) = h(f(x_0)) \in h(M).$$

that is $h(M)$ is a left ideal of A. Since R is a simple ring, then $MR = R$, where MR coincides here with the two-sided ideal generated by M. Thus,

$$h(R) = h(MR) = h(M)h(R)$$

Hence $Im(h) = h(R)$ is a left ideal of A. Since it contains the unity element 1_A, then it is equal to A. This shwos that h is surjective.

Definition 2.8. *An algebra A over a commutative ring R is said to be a simple algebra if the ring A is simple.*

Theorem 2.9. *Let K be a field and R a finite-dimentional simple algebra over K. Then there exists a skew field D such that $R \cong M_n(D)$.*

Proof. Let M be a minimal left ideal of R. In particular, M is a simple R-module. By Schur's lemma $D = End_R(M)$ is a skew field and by Theorem 2.7 we have $R \cong End_D(M)$. Since M is finite-dimentional as a vector space over K, then it is finite-dimentional over D. It follows then that $End_D(M) \cong M_n(D)$, where $n = \dim_D(M)$, so $R \cong M_n(D)$.

Theorem 2.10. *Let D be a division ring and $R = M_n(D)$. Then the following statements hold*

1) *The ideals*
$$L_i = \left\{ \sum_{j=1}^{n} e_{ji}\alpha_j \mid \alpha_j \in D \right\}$$
are minimal left ideals of R. Moreover, R is a finite direct sum of the ideal L_i, that is,
$$M_n(D) = L_1 \oplus \ldots \oplus L_n.$$
2) *All simple modules over R are isomorphic.*
3) *If M is a nonzero R-module, then M is a direct sum of simple R-modules.*

Theorem 2.11. *Let D and Δ be skew fields. If $M_m(D) \cong M_n(\Delta)$, then $m = n$ and $D \cong \Delta$.*

Proof. Let $R = M_m(D)$ and $R' = M_n(\Delta)$. As one can see D^m can be considered (in a canonical way) as a left R-module and Δ^n as a left R'-module. Up to identification, one can use Theorem 2.10(1) to see that D^m is indeed a simple R-module and Δ^n is a simple R'-module. Hence, again by assertion 2 in the same theorem above, we have $D^m \cong \Delta^n$, therefore $End_R(D^m) \cong End_{R'}(\Delta^n)$. Now, we aim to show that $End_R(D^m) \cong D$ (as rings). For this, let $\psi : D \longrightarrow End_R(D^m)$ be the map defined by $\psi(\delta)(x) = x\delta$, for all $\delta \in D$ and $x \in D^m$. One can easily see that ψ is a ring homomorphism. If δ and γ are elements of D such that $\psi(\delta) = \psi(\gamma)$, then, in particular, $\delta = \psi(\delta)(1_D) = \psi(\gamma)(1_D) = \gamma$. This proves that ψ is injective. For the surjectivity, let $f \in End_R(D^m)$. It is clear that D^m is a free right D-module. Let $\{e_1, ..., e_m\}$ be the canonical basis of D^m. Plainly, there exists $\delta_1, ..., \delta_m \in D$ such that

$$f(e_1) = e_1\delta_1 + ... + e_m\delta_m.$$

We have also $f(e_1) = f(e_{11}e_1) = e_1\delta_1$. Therefore, for all $j \in \{1, ..., m\}$, we have

$$\begin{aligned} f(e_j) &= f(e_{j1}e_1) \\ &= e_{j1}(f(e_1)) \\ &= e_{j1}(e_1\delta_1) \\ &= e_j\delta_1. \end{aligned}$$

Consequently, $f(e_j) = \psi(\delta_1)(e_j)$. Since the e_j describe the elements of a basis of D^m, we get $f = \psi(\delta_1)$. Therfore, ψ is surjective. Subsequently,

$$D \cong End_R(D^m) \cong End_{R'}(\Delta^n) \cong \Delta.$$

Also, from the equality $m^2 = \dim_D(R) = \dim_\Delta(R') = n^2$, we get $m = n$.

Lemma 2.12. *Let R be a ring. If we consider R as a right R-module, then R is canonically isomorphic to the ring $End_R(R)$, i.e, $R \cong End_R(R)$.*

Proof. Let $\psi : R \longrightarrow End_R(R)$ be the map defined by $\psi(a) = L_a$ for all $a \in R$, where L_a is the left multiplication by a, i.e, $L_a(x) = ax$ for all $x \in R$. It is clear that $L_a \in End_R(R)$ and that ψ is a ring homomorphism. Let a be any element of R such that $L_a = 0$. In particular, $L_a(1_R) = a = 0$, that is ψ is injective. Let $f \in End_R(R)$. Since R is considered as a right R-module, then $f(x) = f(1x) = f(1)x$ for all $x \in R$, hence $f = L_{f(1)}$. Consequently, ψ is surjective.

Theorem 2.13. (*Wedderburn*)
Let R be a simple ring which has a minimal right ideal M. Then there is a skew field D such that $R \cong M_n(D)$.

Proof. Since R is simple, then $RM = R$. Therefore every element of R is a linear combination of elements of M. In particular,

$$1 = a_1x_1 + ... + a_nx_n$$

for some $a_i \in R$ and $x_i \in M$, $i \in \{1, ..., n\}$. Such a decomposition is not unique, we choose the shorten one, which means, with a minimal n. Plainly, we have

$$R = a_1M \oplus ... \oplus a_nM$$

Since M is a simple module, then we have $M \cong a_iM$ for all $i \in \{1, ..., n\}$. It follows that

$$R \cong M \oplus ... \oplus M = M^n$$

Let $D = End_R(M)$, which is a skew field, then by Lemma 2.12 we have

$$R \cong End_R(R) \cong End_R(M^n) \cong M_n(End_R(M)) \cong M_n(D)$$

3. Central simple algebras

Definition 3.1. *Let A be a K-algebra. We say that A is central, if its center is equal to the field K. i.e, $Z(A) = K$. To each subset B of A we associate the subalgebra (of A):*

$$Z_A(B) = \{a \in A \mid ab = ba \; for \; all \; b \in B\}$$

which is called the centralizer of B in A.

Examples 3.2.
1) *The quaternion algebra $\mathbb{H}$ defined in Example 2.4(2) is central over $\mathbb{R}$.*
2) *If K is an arbitrary field, then $M_n(K)$ is central simple over K.*
3) *Every algebra is central over its center.*

Lemma 3.3. *Let B and C be K-algebras, and let $A = B \otimes_K C$. Then we have:*

1) $Z_A(B \otimes_K K) = Z(B) \otimes_K C$.
2) $Z_A(K \otimes_K C) = B \otimes_K Z(C)$.

Proof. Let $\{y_1, \ldots, y_n\}$ be a basis of C. Every element w of A can be written as follows:

$$w = x_1 \otimes y_1 + \ldots + x_n \otimes y_n$$

where x_i are uniquely determined by w. If $w \in Z_A(B \otimes K)$, then $(x \otimes 1)w = w(x \otimes 1)$ for all $x \in B$. This implies that:

$$(xx_1 - x_1 x) \otimes y_1 + \ldots + (xx_n - x_n x) \otimes y_n = 0 \; for \; all \; x \in B.$$

It follows that $xx_i = x_i x$ for all $x \in B$ and $i \in \{1, \ldots, n\}$, that is, every x_i is an element of $Z(B)$. Consequently, $w \in Z(B) \otimes C$, which shows that $Z_A(B \otimes K) \subseteq Z(B) \otimes C$. The reverse inclusion is clear.

Proposition 3.4. *Let A, B and C as in the Lemma 3.3. Then we have*

$$Z(A) = Z(B) \otimes_K Z(C).$$

In particular, If B and C are central, then $A = B \otimes_K C$ is also central.

Proof. It is easy to see that $Z(A) = Z_A(B \otimes K) \cap Z_A(K \otimes C)$. It follows by Lemma 3.3 that:

$$Z(A) = (Z(B) \otimes C) \cap (B \otimes Z(C)) = Z(B) \otimes Z(C).$$

If B and C are central, then $Z(B) = K = Z(C)$. Therfore, $Z(A) = K \otimes K \cong K$, that is, A is central.

Lemma 3.5. *Let B and C be subalgebras of a K-algebra A with $C \subseteq Z_A(B)$. Assume that B is central simple (over K). If $x_1, \dots, x_n$ are linearly independent elements of B and $y_1, \dots, y_n \in C$ such that $x_1 y_1 + \dots + x_n y_n = 0$, then $y_i = 0$, for all $i \in \{1, \dots, n\}$.*

Remark 3.6. *The tensor product of simple algebras is not necessarily simple. For example the $\mathbb{R}$-algebra $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not simple, although $\mathbb{C}$ is simple over $\mathbb{R}$.*

The following theorem gives a sufficient condition for the simplicity of the tensor product of two algebras.

Theorem 3.7. *Let B and C be K-algebras. Then the following statements hold.*

1) *If B is central simple and C is simple, then $B \otimes_K C$ is simple.*
2) *If B and C are both central simple, then $B \otimes_K C$ is central simple.*

4. The Brauer group

Definition 4.1. *Let R be a ring. The opposite of R is defined to be the ring whose elements are the same elements as in R, with addition law defined to be the addition* *in R, but with multiplication performed in the reverse order, i.e, the opposite of* $(R,+,.)$ *is the ring* $(R,+,*)$ *whose multiplication* $*$ *is defined by* $x*y = y.x$ *for all* $x,y \in R$. *This ring will be denoted by* R^{op}.

Remarks 4.2. *The following statements hold.*

1) *The opposite of the opposite of R is isomorphic to R, i.e,* $(R^{op})^{op} = R$.
2) $R^{op} = R$ *if and only if R is commutative.*
3) *The right ideals of a ring R are the left ideal of its opposite, and vice versa.*
4) *A ring R is central (resp., simple; resp., a division ring) if and only if its opposite ring is so.*

Theorem 4.3. *If A is an n-dimentional central simple algebra over a filed K, then* $A \otimes_K A^{op} \cong M_n(K)$.

Proof. Since $M_n(K)$ is isomorphic to $End_K(A)$, it suffices to prove that $A \otimes A^{\mathbf{op}} \cong End_K(A)$. Let $a \in A$ and $b \in A^{\mathbf{op}}$. The map:

$$\begin{array}{rccc} \psi_{a,b}: & A & \longrightarrow & A \\ & x & \longmapsto & axb \end{array}$$

is clearly an element of $End_K(A)$. It induces a map

$$\begin{array}{rccc} \psi: & A \otimes_K A^{\mathbf{op}} & \longrightarrow & End_K(A) \\ & (a,b) & \longmapsto & \psi_{a,b} \end{array}$$

Plainly, ψ is bilinear and is also multiplicative since $\psi_{ac,db}(x) = acxdb = \psi_{a,b} \circ \psi_{c,d}(x)$, for all $x \in A$ and (a,b), $(c,d) \in A \otimes_K A^{\mathrm{op}}$. It follows by the universal property of the tensor product that there is an algebra homomorphism

$$\phi: A \otimes_K A^{\mathbf{op}} \longrightarrow End_K(A).$$

By the fourth assertion of the last remark and Theorem 3.7, the algebra $A \otimes A^{\mathbf{op}}$ is simple. Hence ϕ is injective. Moreover, we have $\dim(A \otimes_K A^{\mathbf{op}}) = n^2 =$

$End_K(A)$, so ϕ is bijective.

We define an equivalence relation on central simple algebras over a field K as indicated in the following definition.

Definition 4.4. *Let A and B be central simple K-algebras. We say that A and B are similar or Brauer equivalent and we denote $A \sim B$, if there is a division ring D such that $A \cong M_m(D)$ and $B \cong M_n(D)$, for suitable positive integers m, n. Equivalently, they are similar, if $M_n(A) \cong M_n(B)$, for some positive integer n.*

Notation: One can easily see that the similarity relation defined above, is an equivalence relation. The similarity class of a central simple algebra A will be denoted simply by $[A]$, and the set of all Brauer equivalence classes will be denoted by $Br(K)$. In particular, K and $M_n(K)$ have the same class in $Br(K)$, for all $n \in \mathbb{N}$.

Proposition 4.5. *The similarity relation is compatible with the tensor product, i.e, if A, B, A_1 and B_1 are central simple algebras over a field K with $A \sim B$ and $A_1 \sim B_1$, then $A \otimes_K A_1 \sim B \otimes_K B_1$.*

Proof. Indeed, let D and D_1 be division K-algebras such that

$$A \cong M_n(D),\ B \cong M_m(D),\ A_1 \cong M_p(D_1)\ \textit{ and }\ B_1 \cong M_s(D_1).$$

Then, we have

$$A \otimes_K A_1 \cong M_n(D) \otimes_K M_p(D_1) \cong M_{np}(D \otimes_K D_1),$$

$$B \otimes_K B_1 \cong M_m(D) \otimes_K M_s(D_1) \cong M_{ms}(D \otimes_K D_1).$$

Our result follows from these isomorphisms.

Theorem 4.6. *If K is an arbitrary field, then $Br(K)$ is an abelian group with respect to the law induced by the tensor product: $[A].[B] := [A \otimes_K B]$, for any central simple algebras A and B over K. This group is called the Brauer group of the field K.*

Proof. By Proposition 4.5 this law is well defined. Plainly, for any central simple K-algebra A, we have $A \otimes_K K \cong A$, so $[K](= [M_n(K)]$ for any positive integer n) is the identity element of $Br(K)$. By Therorem 4.3, the opposed element of $[A]$ in $Br(K)$ is given by the class of its opposite algebra, that is, $-[A] = [A^{\mathbf{op}}]$. Also, for any central simple K-algebras C, D, we have $C \otimes_K D \cong D \otimes_K C$, which shows that $Br(K)$ is an abelian group.

Definition 4.7. *Let A be a central simple K-algebra. The order of $[A]$ in the Brauer group is called the exponent of A and will be denoted by $exp(A)$.*

Example 4.8. *The exponent of the quaternion algebra $\mathbb{H}$ defined in Example 2.4 is 2.*

Proposition 4.9. *If A and B are central simple K-algebras, then $A \cong B$ if and only if $A \sim B$ and $\dim_K(A) = \dim_K(B)$.*

Proof. If $A \sim B$, then there is a skew field D such that $A \cong M_m(D)$ and $B \cong M_n(D)$ for some integer m, n. Since A and B have the same dimension, then $n = m$, hence $A \cong M_n(D) \cong B$. The reverse is obvious.

Lemma 4.10. *Assume that K is an algebraically closed field and let D be a division algebra over the field K, Then $D = K$. That is, the only division algebra over K is K itself.*

Proof. Let $\dim_K(D) = m$ and let $\alpha \in D$. Since the powers $1, \alpha, \ldots, \alpha^m$ are linearly dependent over K, α is a root of a monic polynomial $f \in K[X]$. We choose f with minimal degree; let β be a root of f in K, then $f(X) = g(X)(X - \beta)$

for some $g \in K[X]$. As the degree of f is minimal, then $g(\alpha) \neq 0$. Since D is a divison algebra, then necessarily $\alpha = \beta$ $(\in K)$. This proves that $D \subseteq K$. The reverse inclusion is clear.

Corollary 4.11. *The Brauer group of every algebraically closed field is trivial, i.e, if K is an algebraically closed field, then $Br(K) = \{1\}$.*

Proof. This follows from Lemma 4.10.

Definition 4.12. *Let A be a K-algebra and ψ an automorphism of A. We say that ψ in an inner automorphism, if there is an invertible element a of A such that $\psi(x) = axa^{-1}$ for all $x \in A$.*

Theorem 4.13. (*Skolem, Noether*)
Let A and B be K-algebras with A central simple and B simple. Let $f, g : B \longrightarrow A$ be two K-algebra homomorphisms. Then there is an invertible element $a \in A$ such that $f(b) = ag(b)a^{-1}$ for all $b \in B$.

Proof. We first suppose that $A = M_n(K)$, for some $n \in \mathbb{N}$. It is clear that K^n can be endowed with a natural $M_n(K)$-module and so, by means of the homomorphsim f (*resp.*, g) K^n can also be seen as a B-module. More explicitly, by means of the action $bx = f(b)x$ for all $b \in B$ and $x \in K^n$ (resp., $bx = g(b)x$ for $b \in B$ and $x \in K^n$). We denote these B-modules by V_f and V_g respectively. Since B is simple, it follows by Theorems 2.9 and 2.10 that V_f and V_g are isomorphic. Let $\psi : V_f \longrightarrow V_g$ be a B-isomorphism. Hence we have

$$\psi(f(b)x) = g(b)\psi(x) \; for \; all \; x \in K^n \; and \; b \in B.$$

Since ψ is an isomorphism, then $f(b) = \psi^{-1}g(b)\psi$ and ψ is clearly an element of $End_K(K^n) \cong M_n(K) = A$. This shows the result in this case.
For the general case, $A \otimes_K A^{\mathbf{op}}$ is a matrix algebra by Theorem 4.3 and the

algebra $B\otimes_K A^{\mathbf{op}}$ is simple by Theorem 3.7. We apply the fist part to the maps

$$f\otimes id, g\otimes id:\ B\otimes_K A^{\mathbf{op}} \longrightarrow A\otimes_K A^{\mathbf{op}}$$

There exists an invertible element $b\in A\otimes_K A^{\mathbf{op}}$ such that

$$(1)\quad f\otimes id(x\otimes y) = b(g\otimes id)(x\otimes y)b^{-1},\quad for\ all\ \ x\in B\ \ and\ \ y\in A^{\mathbf{op}}.$$

In particular, if we take $x=1$ we get $1\otimes y = b(1\otimes y)b^{-1}$ for all $y\in A^{\mathbf{op}}$, which means that, b is an element of $Z_{A\otimes_K A^{\mathbf{op}}}(K\otimes_K A^{\mathbf{op}})$, hence an element of $A\otimes_K K$ by the Lemma 3.3. Thus, $b = b'\otimes 1$ for some $b'\in A$. Taking $y=1$ in (1) we get $f(x) = b'g(x)b'^{-1}$ for all $x\in B$, which ends the proof.

Corollary 4.14. *Let A be a central simple K-algebra. Then every automorphism of A is an inner automorphism.*

Proof. Let ψ be an algebra automorphism of A. To show that ψ is an inner automorphism of A, it suffices to take in the previous theorem $B=A$, $f=id$ and $g=\psi$.

Theorem 4.15. *Let A be a central simple K-algebra and let B be a simple K-subalgebra of A. Then its centralizer $C=Z_A(B)$ is also simple. Moreover, we have:*

$$\dim_K(A) = \dim_k(B)\dim_K(C).$$

Proof. To show that C is simple, we will show that $C\cong End_T(A)$, where T is the simple K-algebra $B\otimes_K A^{\mathbf{op}}$. Note that the K-algebra A can be viewed as a left T-module for the operation defined by linearly extending the following equalites:

$$(\beta\otimes\alpha)x = \beta x\alpha,\ \ for\ all\ \ \alpha\in A^{\mathbf{op}},\ \beta\in B\ and\ x\in A.$$

Consider the map $\psi:\ C\longrightarrow End_T(A)$, defined by $\psi(c)(x)=cx$, for all $c\in C$ and $x\in A$. It is easy to see that ψ is a K-algebra homomrphsim. Let $c\in Ker(\psi)$, i.e,

$\psi(c)$ is the zero endomorphism. In particular, we have $c = \psi(c)(1) = 0$, hence ψ is injective. One can easily see that ψ is also surjective. Indeed, let $f \in End_T(A)$ and let $c = f(1)$, then for every element $b \in B$ we have:

$$cb = (1 \otimes b)c = (1 \otimes b)f(1) = f((1 \otimes b)1) = f(b).$$

we have also

$$bc = (b \otimes 1)c = (b \otimes 1)f(1) = f((b \otimes 1)1) = f(b).$$

Consequently, $bc = cb$, that is, $c \in C$. Moreover, for any $x \in A$, we have

$$\psi(c)(x) = cx = (1 \otimes x)c = (1 \otimes x)f(1) = f((1 \otimes x)1) = f(x)$$

Thus $f = \psi(c)$, which proves that ψ is surjective.
Now, we prove the dimention equality. From Theorem 3.7, the K-algebra T is simple and by Theorem 2.10, there is a unique T-module M, up to isomorphism, and every T-module is a finite direct sum of copies of M. In particular, $A \cong M^n$, for some $n \in \mathbb{N}$. Let $D = End_T(M)$. As M is a simple T-module, it follows by Schur's lemma that D is a division algebra. We proved above that $C \cong End_T(A)$. Hence we have

$$C \cong End_T(A) \cong End_T(M^n) \cong M_n(End_T(M)) = M_n(D).$$

Therfore, we have

$$\dim_K(C) = \dim_K(M_n(D)) = n^2 \dim_K(D). \quad (1)$$

It is clear that M is also a D-module, so by Theorem 2.10 we have $M \cong D^s$, for some $s \in \mathbb{N}$. we also have

$$T = End_D(M) \cong End_D(D^s) \cong M_s(D).$$

Thus $A \cong D^{ns}$, hence

$$\dim_K(A) = ns \dim_K(D). \quad (2)$$

On the other hand, we have

$$\dim_K(A)\dim_K(B) = \dim_K(T) = \dim_K(M_s(D)) = s^2\dim_K(D). \quad (3)$$

From the identities (1), (2) and (3) we get $\dim_K(B)\dim_K(C) = \dim_K(A) = ns\dim_K(D)$.

Corollary 4.16. *Let A, B and C as in the Theorem* 4.15. *Then the following properties hold.*

1) $Z_A(Z_A(B)) = B$. *In particular, we have* $Z(Z_A(B)) = Z(B)$.
2) *If B is central, then* $A \cong B \otimes_K C$.

Proof. Clearly we have $B \subseteq Z_A(Z_A(B))$. For the reverse inclusion, take $C' = Z_A(C)$. By Theorem 4.15 C is a simple algebra and we have :

$$\begin{cases} \dim_K(C)\dim_K(C') & = & \dim_K(A). \\ \dim_K(C) & = & \frac{\dim_K(A)}{\dim_K(B)} \end{cases}$$

So, $\dim_K(B) = \dim_K(C') = \dim_K(Z_A(Z_A(B)))$. This proves the reverse inclusion. It follows then that

$$Z(Z_A(B)) = Z_A(Z_A(B)) \cap Z_A(B) = B \cap Z_A(B) = Z(B).$$

Assume that B is central and let $\phi : B \otimes_K C \longrightarrow A$ be the K-algebra homomorphism defined by $\phi(b \otimes c) = bc$, for all $b \in B$ and $c \in C$. Since $B \otimes_K C$ is simple, then ϕ is injective. It is also surjective since A and $B \otimes C$ have the same dimension.

5. Central simple algebras under field extensions

In this section, we define the scalar extension of a K-algebra by an arbitrary field extension of K. We focus especially on the case where the algebra is simple, then we define and study properties of the reduced norm and trace which are natural generalisations of the classical norm and trace.

Definition 5.1. *Let A be a K-algebra and let L be a field extension of K. The L-algebra $A \otimes_K L$ is called the scalar extension of A by L. We will denote it simply by A_L.*

Remarks 5.2. *Let A and L as in Definition* 5.1. *Then we have:*
1. $\dim_K(A) = \dim_L(A_L)$.
2. *When A is a central simple K-algebra, then A_L is also central simple over L.*

Definition 5.3. *Let A be a central simple K-algebra. We say that A is split if $A = 1$ in $Br(K)$, that is, $A \cong M_n(K)$ for some $n \in \mathbb{N}$.*

Definition 5.4. *Let A be a central simple K-algebra and let L be a field extension of K. If the L-algebra A_L is split, then we say that L is a splitting field of A.*

An important example of splitting field will be given by the following lemma.

Lemma 5.5. *Let A be a central simple algebra over a field K. Then the algebraic closure $\overline{K}$ of K is a splitting field of A. Moreover, the dimension of A over K is a square.*

Proof. Extend the K-algebra A to the algebraic closure $\overline{K}$. As seen in Remark 5.2, $A_{\overline{K}}$ is simple and by the Wedderburn's theorem, there is a central divison $\overline{K}$-algebra D such that $A_{\overline{K}} \cong M_n(D)$, for some integer n. By Lemma 4.10, we get $D = \overline{K}$, thus $A_{\overline{K}} \cong M_n(\overline{K})$, that is, A is split by $\overline{K}$. We have also

$$\dim_K(A) = \dim_{\overline{K}}(A_{\overline{K}}) = \dim_{\overline{K}}(M_n(\overline{K}) = n^2.$$

Definition 5.6. *Let A be a central simple K-algebra with $\dim_K(A) = n^2$. The integer n is called the degree of A and will be denoted by $\deg(A)$.*

Definition 5.7. *Let $A = M_n(D)$ be a central simple K-algebra, where D is a division central K-algebra. The degree of D is called the index of A and will be denoted by $ind(A)$.*

Definition 5.8. *Let A be a central simple K-algebra. A subfield of A is a subalgebra E of A (over K) such that E is a field. We say that E is a maximal subfield of A, if there is no other subfield F of A that contains E. We say that E is a strictly maximal subfield of A if $dim_K E = deg(A)$.*

Theorem 5.9. *Let A be a central simple K-algebra and L a subfield of A. Let $B = Z_A(L)$, then $A_L \sim B$.*

Corollary 5.10. *Let A be a central simple K-algebra of degree n. If L is strictly maximal subfield of A, then L is a splitting field of A.*

Proof. Since L is assumed to be strictly maximal in A, then by definition $[L : K] = n$. Note that A can be seen as a left A-module and also as a right L-module. Consider the map $\psi : A \otimes_K L \longrightarrow End_L(A) \cong M_n(L)$ which is defined by

$$\psi(a \otimes \lambda)(b) = ab\lambda, \quad for\ all\ a, b \in A\ and\ \lambda \in L.$$

One can easily see that ψ is an L-algebra homomorphism. As seen in Remark 5.2(2), the L-algebra $A \otimes_K L$ is simple, hence ψ is injective. ψ is also surjective since $\dim_K(A_L) = n^3 = \dim_K(M_n(L))$. Consequently, $A_L \cong M_n(L)$, which means that L is a splitting field of the K-algebra A.

Definition 5.11. *Let K be a field of characteristic $p > 0$ and L a field extension of K. An element $\alpha \in K$ is called purely inseparable over K if there is $n \in \mathbb{N}$ such that $\alpha^{p^n} \in K$. The extension L/K is said to be purely inseparable if every element of L is purely inseparable over K.*

Remarks 5.12. (1) *Purely inseparable extensions are the extreme opposite of separable extensions.*

(2) *Recall that every extension of a field of characteristic zero is separable.*

Lemma 5.13. *Let D be a central division K-algebra. Then, there exists $d \in D\backslash K$ such that d is separable over K.*

Proof. If $char(K) = 0$, then we are done. Assume that $char(K) = p > 0$ and suppose that all elements of $D\backslash K$ are purely inseparable over K. Take $a \in D\backslash K$ with $a^{p^n} \in K$ for some integer n, then consider the K-linear map

$$\begin{array}{cccc} f: & D & \longrightarrow & D \\ & x & \longmapsto & xa - ax. \end{array}$$

By simple computation, one sees that $f^{p^n}(x) = xa^{p^n} - a^{p^n}x = 0$ because $a^{p^n} \in K$. As $a \notin K$, then f is not the zero homomorphism, so there is $y \in D$ such that $f(y) \neq 0$. Therefore, there exists $k \in \mathbb{N}^*$ such that $f^k(y) = 0$ and $f^{k-1}(y) \neq 0$. Let $x := f^{k-1}(y)$ and $z := f^{k-2}(y)$. We then have $xa - ax = f(x) = f^k(y) = 0$, thus $xa = ax$. We have also $f(z) = za - az = x$. It follows that $au = ua$ where $u = a^{-1}x$. Therefore, $au = x = za - az$. Since $au = ua$, then $au^{-1} = u^{-1}a$,. Let $c = zu^{-1}$, then

$$a = (za - az)u^{-1} = zu^{-1}a - azu^{-1} = ca - ac.$$

Thus, $c = 1 + aca^{-1}$. Since c is not in K, then by assumption it is purely inseparable over K, hence there is $m \in \mathbb{N}$ such that $c^{p^m} \in K$. Hence we have

$$\begin{array}{rcl} c^{p^m} & = & (1 + aca^{-1})^{p^n} \\ & = & 1 + (aca^{-1})^{p^m} \\ & = & 1 + ac^{p^n}a^{-1} \\ & = & 1 + c^{p^m}, \end{array}$$

which is not true.

The result of the last Lemma assures the existence of a separable splitting field for any central simple algebra; precisely, we have the following theorem.

Theorem 5.14. *Let D be a central division K-algebra. Then D has a maximal separable subfield. In particular, every central simple K-algebra has a separable splitting field.*

Let A be a central simple K-algebra of degree n and let L be any splitting field of A. Then, $A_L \cong M_n(L)$. Let $\phi : A_L \longrightarrow M_n(L)$ be an aribtrary isomorphism. The characteristic polynomial of a matrix $N \in M_n(L)$ is given by:

$$\chi(X,N) := \chi_L(X,N) := \det(XI_n - N) \in L[X].$$

$\chi(X,N) = X^n + \alpha_{n-1}X^{n-1} + ... + \alpha_0$, where $\alpha_0 = (-1)^n \det(N)$ and $\alpha_{n-1} = -tr(N)$.

Definition 5.15. *Let A, L and ϕ be as in above. The characteristic polynomial of an element $a \in A_L$ (with respect to the representation ϕ) is is defined by $\chi(X,a) := \chi(X,\phi(a))$.*

Lemma 5.16. *The definition of the characteristic polynomial does not depend of the choice of the isomorphism ϕ and the splitting field L.*

Proof. Let $f : A_L \longrightarrow M_n(L)$ be an other isomorphism. We have to check that $\chi(X,\phi(a)) = \chi(X,f(a))$. By Skolem-Noether theorem, there is an invertible matrix $N \in M_n(L)$ such that $\phi(a) = Nf(a)N^{-1}$. Hence, we have

$$\begin{aligned}
\chi(X,\phi(a)) &= \det(XI_n - \phi(a)) \\
&= \det(XI_n - Nf(a)N^{-1}) \\
&= \det(N(XI_n - f(a))N^{-1}) \\
&= \det(XI_n - f(a)) \\
&= \chi(X,f(a)).
\end{aligned}$$

Remark 5.17. *The K-algebra A can be seen as a sub-K-algebra of A_L via the map $x \longmapsto x \otimes 1$. Moreover, if a is an element of A, then $\chi(X,a) \in K[X]$.*

Definition 5.18. *Let A be a central simple K-algebra of degree n. Let $\chi(X,a)$ ($\in K[X]$) for an element $a \in A$, be defined as in above. Write $\chi(X,a) = x^n + \alpha^{n-1}X^{n-1} + ... + \alpha_0$, with $\alpha_i \in K$, the element $(-1)^n\alpha_0$ is called the reduced norm of a and will be denoted simply by $N(a)$ or $Nrd_A(a)$. The reduced trace of a is defined to be the element $-\alpha_{n-1}$, and will be denoted by $S(a)$ or $Trd_A(a)$.*

Remark 5.19. *The bilinear form trace $T: A \times A \longrightarrow K$ defined by $T(a,b) = Trd_A(ab)$ is nondegenerate.*

Corollary 5.20. *Let A be a central simple K-algebra of degree n. Then the following statement hold*

1) *The map $S: A \longrightarrow K$ is K-linear and $N(ab) = N(a)N(b)$, for all $a, b \in A$.*
2) *$S(ab) = S(ba)$, for all $a, b \in A$.*
3) *$S(\alpha) = n\alpha$ and $N(\alpha) = \alpha^n$, for all $\alpha \in K$.*
4) *Let $a \in A$, then a is invertible in A if and only if $N(a) \neq 0$. In particular, the restriction of N to $U(A)$ defines a group homomorphism $N: U(A) \longrightarrow K^*$, where $U(A)$ is the group of invertible elements of A.*

References

[1] R. Elman, N. Karpenko and A. Merkurjev, *The algebraic and geometry theory of quadratic forms* (2008).

[2] M. Knus, *Quadratic and Hermitian Forms over Rings*, Springer-Verlag, Berlin Heidelberg New York, London, Paris, Tokyo, Hong Kong, Barcelona (1990).

[3] M. Knus, A. Merkurjev, M. Rost, J. Tingol *The Book of Involutions*, American Mathematical Society (1998).

[4] Richard S. Pierce, *Associative algebras*, Springer-Verlag, New York Heidelberg Berlin (1982).