1

Applications algébriques de la cohomologie des groupes. II : théorie des algèbres simples

This is my translations of the results of Serre's paper *Application algébriques de la cohomologies des group: Théorie des algèbre simple.* the prerequisites are a basic course in algebra, including some representation theory. With this background assumed, I add a few definitions that may not be known to the reader. I also reference a few results from [1] which could be considered "classical" results whose proofs need not be repeated due to the amount of build-up that would be required.

Before starting his translation, I will quickly put the definition of a representation of an algebra for the reader to recall:

Definition 1.0.1: Algebra Representation

Let A be a finite dimensional (associative) algebra over k. Then a *representation* of A is a k-homomorphism:

$$\rho : A \to \operatorname{End}_k(V)$$

for some vector space V.

Recall that one definition of an R-module is given by a ring homomorphism $\rho : R \to \operatorname{End}_{\mathrm{Ab}}(M)$ for an abelian group M. If we restrict to k-homomorphisms and k-endomorphisms, we can define the A-module $\rho : A \to \operatorname{End}_k(V)$, hence we can think of representation of and algebra A as a left A-modules. This makes sense, as representation theory can be thought of the study of associative algebras (the study of group representation is the study of group algebras, the study of the representation of lie algebras is universal enveloping algebras, the study of the representation of quiver algebras is the study of path algebras, and so forth). You can find everything you need about the basic of representation theory in [1, chapter 23]. Because of this, we shall see that many of the results for the representation of associative algebras outlined bellow to be familiar to anyone who has taken a basic course in representation theory.

Next, we define the object that shall represent the generalization of number rings:

Definition 1.0.2: Central Simple Algebra

Let A be an algebra over a field k. Then A is called *simple* if it is a simple ring. It is called a *central simple algebra* (CSA) if it is simple, is finite dimensional over k, and its center is k.

The idea behind this definition is that it generalizes field extensions F/k, for we have a distinguished field k, and we are interested in the "algebraic case", hence the extension ought to be finite. Contrasting to fields, a CSA need not be commutative and need be a division ring

Example 1.1: Simple and Central Simple Algebras

1. Naturally, $M_n(k)$ is a central simple algebra of dimension n^2
2. It is possible to be simple and have center k but not be finite: the Weyl algebra $k[x, \delta_x]$ is infinite dimensional over k.
3. $\mathbb{C}$ is a central simple algebra over $\mathbb{C}$, but not over $\mathbb{R}$ (as it's center contains more than $\mathbb{R}$
4. Let $A = \mathbb{H}$ be the quaternions (or Hamiltonians). Then this is a CSA over $\mathbb{R}$ with dimension 4. We shall soon define a quaternion algebra, and see that all 4-dimensional central simples algebra's over a field k is a quaternion algebra, and it shall be limited to 2-by-2 matrices or division algebras.

1.1 Artin-Wederburn and elementary Results

A central result in the study of simple rings and algebras is the Artin-Wederburn theorem, which we remind the reader as well as some useful corollaries:

Theorem 1.1.1: Artin-Wedderburn

Let R be a ring. Then R is a semi-simple ring if and only if

$$R \cong_{\mathbf{Ring}} M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

where each D_k is a division ring and $M_{n_i}(D_i)$ is the matrix ring over D_i, and each D_i n_i are unique up to isomorphism

Proof **:**
See [1]

most of the time, we are working with k-algebras. These corollaries provide useful insights:

Corollary 1.1.2: Artin-Wedderburn For k-Algebras

Let R be a semi-simple k-algebra for some field k. Then

$$R \cong_{k\text{-}\mathbf{Alg}} M_{n_1}(D_1) \times \cdots \times M_{n_l}(D_l)$$

where each D_i is a divsion k-algebra, finite dimensional as a k-vector space:

$$\dim_k R = \sum n_i^2 \dim_k(D_i)$$

and has exactly l simple R-modules as we've classified before.

***Proof* :**
See [1]

Corollary 1.1.3: Artin-Wedderburn For $\overline{k}$-Algebras

Let R be a semi-simple k-algebra for some algebraically closed field $k = \overline{k}$. Then

$$R \cong_{k\text{-}\mathbf{Alg}} M_{n_1}(k) \times \cdots \times M_{n_l}(k)$$

showing that R is a finite dimensional vector-space over R with dimension:

$$\dim_k(R) = \sum_i^l n_i^2$$

and has exactly l simple R-modules as we've classified before.

As a consequence, if R is a simple $\overline{k}$-algebra,then $R \cong M_n(\overline{k})$.

***Proof* :**
See [1]

Let us now generalize some of basic representation theory results. Let E be an irreducible representation of A (take for example a minimal left ideal of A, see [1, chapter 23]).

Lemma 1.1.4: Schur's Lemma - updated

Let E be an irreducible representation of a k-algebra A, and let $K \subseteq \mathrm{End}_k(E)$ be the endomorphisms that commute with the operations of A: it is the centralizer of A in $\mathrm{End}_k(E)$, $K = C_{\mathrm{End}_k(E)}(A)$. Then K is a division ring.

Note that this makes K an A-algebra

***Proof* :**
Take $u \in K$. We want to show that $u^{-1} \in K$. Consider $u^{-1}(0) = V \subseteq E$. For $x \in V$, we have:

$$0 = a \cdot u(x) = u(a \cdot x)$$

hence, V is stable under A, and as $u \neq 0$ we must have $V = 0$ as u is invertible in $\mathrm{End}_k(E)$. It follows that $u^{-1} \in K$.

Notice from this that we may say that the representation E must be faithful (the map must be injective). Indeed, the kernel of this representation would be an ideal of A but

Lemma 1.1.5: Minimal Centralizer of Representations

Let E be a semi-simple an faithful representation of A, $K = C_{\mathrm{End}_k(E)}(A)$, $B = C_{\mathrm{End}_k(E)}(K)$ (i.e. the centralizer of A and K in $\mathrm{End}_k(E)$). Then

$$A = B$$

***Proof* :**
Let $x \in E$ and $b \in B$. We shall show that there exists an $a \in A$ such that $a(x) = b(x)$.

Let $Ax = V \subseteq E$ be a stable subspace. Then V admits a (stable) compliment: $E = V \oplus V^{\perp}$. Let $\pi : E \to V$ be the natural projection map. Then certainly π is A-linear and commutes with K, namely $\pi \in K$. Then:

$$\pi(b(x)) = b(\pi(x)) = b(x)$$

namely, $b(x) \in V = aX$, implying $a(x) = b(x)$, as we sought to show.

Lemma 1.1.6: Generator lemma

Let E be a semi-simple an faithful representation of A, $K = C_{\mathrm{End}_k(E)}(A)$, $B = C_{\mathrm{End}_k(E)}(K)$ (i.e. the centralizer of A and K in $\mathrm{End}_k(E)$). Let $x_1, ..., x_n \in E$ and $b \in B$. Then there exits values $a_i \in A$ such that:

$$ax_1 = bx_1, \; ax_2 = bx_2 \qquad \cdots \qquad ax_n = bx_n$$

***Proof* :**
Let F be the direct sum space of n copies of representation E. Then F is formed of elements $(y_1, ..., y_n)$, $y_i \in E$, on which A acts by

$$a \cdot (y_1, ..., y_n) = (ay_1, ..., ay_n)$$

The representation F is still semi-simple. The centralizer of A in $\mathrm{End}_k(F)$ is formed of matrices (u_{ij}), $u_{ij} \in K$, and it follows that, if we let B operate on F by the formula:

$$b \cdot (y_1, ..., y_n) = (by_1, ..., by_n)$$

the elements of $\mathrm{End}_k(F)$ thus defined will still be in the centralizer of the centralizer of A (in the theory of semi-groups, this is sometimes called the bicommutant). By lemma 1.1.5 applying to the point $x = (x_1, ..., x_n) \in F$, and to $b \in B$ giving us the desired result.

Serre write K_n for $M_n(K)$ for a division ring K, but we shall stick to $M_n(D)$ where our division ring is D instead of K. If D contains k in its center, we have:

$$M_n(D) = M_n(k) \otimes D$$

as can be easily seen.

We present one more important result that has two useful corollaries. Let A be a k-algebra. Then A acting on itself by left multiplication gives something called the *regular left representation*. If $A = M_n(D)$, it has basis e_{ij}, $1 \le i, j \le n$. The elements e_{i,j_0} for a fixed j_0 gives a subspace of $M_n(D)$, say $N_{j_0} \subseteq M_n(D)$. It is easy to see that N_{j_0} is a minimal left ideal (namely, an irreducible representation). Then we see that for any other choice of j_0, say j_1, we get an isomorphic irreducible representation N_{j_1}. Then this gives the following classical result:

Theorem 1.1.7: Representation of Simple Algebra

Let A be a simple k-algebra. Then all representation of A is isomorphic to the direct sum of irreducible representation

Proof **:**
see [1, chapter 23]

Corollary 1.1.8: Representation of Simple Algebra

Let A be a simple k-algebra. Then:

1. All representations of A are semi-simple (completely reducible in Serre's words)
2. Two representation of A which have the same dimension are isomorphic

Proof **:**
immediate from the above

Let us now turn towards the tensor product of simple algebras.

Lemma 1.1.9: Centralizer of Tensor Product of Algebras

Let A, A' be two k-algebras, B, B' be sub k-algebras of A, A' (respectively) with C, C' their centralizers on A, A' (respectively). Then the centralizer of $B \otimes B'$ in $A \otimes A'$ is $C \otimes C'$.

Proof **:**
Let us first find the centralizer of $B \otimes 1$. For this, let a'_i be a basis of A'. Any $x \in A \otimes A'$ can be

written uniquely in the form:

$$x = \sum_i a_i \otimes a_i' \qquad \text{for appropriate } a_i \in A$$

If x commutes with $b \otimes 1$, then $a_i b = b a_i$ that is $a_i \in C$ for all i. We thus see that the centralizer of $B \otimes 1$ is $C \otimes A'$. Similarly, that of $1 \otimes B'$ is $A \otimes C'$. It follows that the centralizer of $B \otimes B'$ is equal to the intersection of the centralizers of $B \otimes 1$ and $1 \otimes B'$, namely

$$(C \otimes A') \cap (A \otimes C') = C \otimes C'$$

as we sought to show.

Thus, the centre of the tensor product of two algebras is the tensor product of the centre of the two algebras. Applying this to the special case of $A = M_n(k) \otimes D$ for some division ring D, then:

$$Z(A) = k \otimes Z(D)$$

Corollary 1.1.10: Centre of simple algebra is A Field

Let A be a simple k-algebra, finitely generated over k. Then $Z(A)$ is a field.

***Proof* :**
Consider $Z(A)$. As A is a finitely generated k-algebra, $Z(A)$ is a finitely generated k-algebra. For any $0 \neq z \in Z(A)$, consider zA. As z is central,we have that zA is two-sided ideal. As A is simple, it must be that $zA = A$, that is z is there exists a $w \in A$ such that $za = 1$. Therefore, $Z(A)$ is a division ring. It is by definition commutative, and hence it is a field. Since z was an arbitrary nonzero element, $Z(A)$ is a division ring. It is by definition commutative, and hence it is a field.

We shall next require to see the interaction between the tensor product of central simple algebras. We require the following lemma:

Theorem 1.1.11: Ideal Generation Tensor Product

Let A be a k-algebra and K' a left division ring with center k. Then every ideal $N \subseteq A \otimes K'$ is generated (as a left module over K') by its intersection with $A \otimes 1$.

Note that neither A nor K' are assumed finite over k

***Proof* :**
We will first note that we can make K' operate on the left on $A \otimes K'$ by:

$$k'(a \otimes k'') = a \otimes k'k''$$

If N is an ideal of the algebra $A \otimes K'$, it is in particular a K'-module subspace of $A \otimes K'$.

Let a_i be a basis of A over k; the elements $a_i \otimes 1$ equally form a basis of the K'-module $A \otimes K'$. Let x be a primitive element of N with respect to this basis (Bourbaki, Alg.II, paragraph 5):

$$x = \sum_i a_i \otimes k_i'$$

Consider the element $x \cdot m$ ($m \in K'$); we have $x \cdot m \in N$ (N is an ideal), and on the other hand:

$$x \cdot m = \sum_i a_i \otimes k_i' m$$

It then follows from the properties of primitive elements that we have:

$$k_i' m = n k_i' \text{ for all } i \quad (n \in K')$$

Since one of the k_i' is equal to 1, we have $m = n$, and the preceding equality simply means that k_i' commutes with all $m \in K'$, i.e., that $k_i' \in k$. We can then write: $x = a \otimes 1$, by setting: $a = \sum_i k_i' a_i$. We have thus shown that every primitive element x is in $A \otimes 1$; the theorem follows immediately since every vector space is generated by its primitive elements.

Theorem 1.1.12: Tensor Product CSA

Let A, A' be simple k-algebras finitely generated over k, where one of them is a CSA. Then $A \otimes A'$ is a simple k-algebra

***Proof* :**
Suppose that $A' = M_n(k) \otimes K'$ is central, in other words that the center of the left field K' is reduced to k. It will suffice to show that $A \otimes K'$ is a simple algebra. Indeed, if this is demonstrated, $A \otimes K' = M_m(k) \otimes K''$, and $A \otimes A' = M_m(k) \otimes M_n(k) \otimes K'' = M_{mn}(k) \otimes K'' = M_{nm}(K'')$. The algebra $A \otimes A'$ will thus be isomorphic to a matrix algebra for which simplicity is immediately verified. Then the general case of $A \otimes K'$ being simple follow from theorem 1.1.11, completing the proof.

Corollary 1.1.13: Tensor Product of Two CSA's

The tensor product of two CSA is a CSA

***Proof* :**
In the previous proof, it was enough for one of them to be a CSA.

Corollary 1.1.14: Opposite Algebra Tensoring

Let A be a CSA over k and A^{op} the opposite algebar. Then:

$$A \otimes A^{\mathrm{op}} \cong M_{n^2}(k)$$

***Proof* :**
Let us denote by E the algebra A considered as a vector space over k. We can make A naturally on E on the left or right by multiplication to create a left or right A-module. This amounts to identifying A and A^{op} as sub-algebras of the algebra $\mathrm{End}_k(E)$ of k-endomorphisms of E. Since the algebras A and A^{op} commute in $\mathrm{End}_k(E)$, we can define a canonical homomorphism of $A \otimes A^{\mathrm{op}}$

into $\mathrm{End}_k(E)$ which extends the isomorphisms: $A \to \mathrm{End}_k(E)$ and $A^{\mathrm{op}} \to \mathrm{End}_k(E)$. The algebra $A \otimes A^{\mathrm{op}}$ being simple, this homomorphism is an isomorphism; moreover, as;

$$[A \otimes A^{\mathrm{op}} : k] = [A : k]^2 = n^2 = [\mathrm{End}_k(E) : k]$$

this isomorphism maps $A \otimes A^{\mathrm{op}}$ onto $\mathrm{End}_k(E) = M_{n^2}(k)$, as we sought to show.

1.2 Brauer Group

Let A be a CSA over k. As A is simple, we get by Artin-Wedderburn that it is isomorphic to $M_n(D) \cong M_n(k) \otimes D$. For example, if $n = 1$ and $k = \mathbb{R}$ we get (by a classical theorem from algebraic topology) that $A \cong \mathbb{R}$ or $A \cong \mathbb{H}$ (the quaternions). If $n > 1$, we get $M_n(\mathbb{R})$ and $M_n(\mathbb{H})$ (which are no longer division algebras). We see that the division ring is one of the "characterizing" feature of the CSA (the other being its matrix ring), especially that up to Morita-equivalence we get the same category. We thus have the following natural equivalence we may define:

Definition 1.2.1: Brauer Equivalence

Let k-**CSA** be a collection of central simple algebras over k. Then define the equivalence relation $A \sim A'$ where the two are equivalent if and only if their associated division rings are isomorphic.

Proposition 1.2.2: Brauer Group

The Brauer equivalence on a collection of CSA's forms a commutative group under the tensor product. This group will be denoted $\mathrm{Br}(k)$.

In Serre, this group is denoted G_k.

***Proof* :**
By corollary 1.1.13, it is closed under the tensor product, the equivalence class containing k is certainly the identity, and corollary 1.1.14 shows that every equivalence class has an inverse. Associativity and commutativity is a classical result from tensor products.

Example 1.2: Brauer Groups

1. Let $k = \overline{k}$. Then $\mathrm{Br}(\overline{k}) = 0$ by corollary 1.1.3.
2. If $k = \mathbb{R}$, then we shall show in the next section that $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$, namely we shall have $\mathbb{R}$ and $\mathbb{H}$, the quaternions.
3. Let k be a finite field. Then $\mathrm{Br}(k) = 0$, as all finite division rings are fields.
4. If $k = \mathbb{Q}_p$, then $\mathrm{Br}(k) \cong \mathbb{Q}/\mathbb{Z}$ (Serre references Algebren - Chap. VII - 2nd paragarph).
5. If $k = \mathbb{Q}$, $\mathrm{Br}(\mathbb{Q})$ will be a subgroup of

$$\mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Q}/\mathbb{Z})^{\oplus \mathbb{N}}$$

which can be thought of as a result similar to that in number theory where we study the "global field" $\mathbb{Q}$ by looking at all its localizations (note that $\mathbb{Z}/2\mathbb{Z}$ comes from $\mathrm{Br}(\mathbb{R})$!) Serre references Deuring for the proof (see Sere p.8)

Theorem 1.2.3: Field Extensions and CSA

Let A be a CSA over k, L/k a field extension (either finite or infinite). Then $A \otimes L$ is simple

Proof **:**
If A is a division ring, then all ideals of $A \otimes L$ will be given with in part with the intersection of the ideals of L, which is simply (0), making $A \otimes L$ simple.

If A is any CSA, write $A \cong M_n(k) \otimes D$. Then:

$$A \otimes L \cong M_n(k) \otimes (D \otimes L) \stackrel{!}{=} M_n(k) \otimes M_m(D')$$

where for $\stackrel{!}{=}$, D' is the division ring naturally given by $D \otimes_k L$! But this gives the result.

Corollary 1.2.4: Index of CSA

Let A be a simple, central and finite algebra over k. Then $[A : k]$ is a perfect square.

Proof **:**
Let L be an algebraically closed extension of k. The algebra $A \otimes L$ can be endowed with an algebra structure over L, and we have:

$$[A \otimes L : L] = [A : k]$$

But $A \otimes L$ is a simple algebra, central over L, and finite over L. It then follows from example 1.2[1] that it is a matrix algebra over L, and $[A \otimes L : L]$ is indeed a perfect square.

Looking at the field extension of a k-algebra, it is natural to consider that $- \otimes_k L$ gives a homomorphism of Brauer groups $\varphi_{k,L} : \mathrm{Br}(k) \to \mathrm{Br}(L)$, namely due to the following result from linear algebra:

$$(A \otimes_k L) \otimes_L (A' \otimes_k L) \cong (A \otimes_k A') \otimes_k L$$

The kernel $\ker \varphi_{k,L}$ consists of all k-algebra's that become trivial (matrix algebras) when extending to L. Serre calls these algebras the algebras that *admit L as a field of decomposition.* (or admit a decomposition by L). More recently, the term *splitting field* . Naturally, if $L = \overline{k}$, then every algebra admits a decomposition as $\mathrm{Br}(\overline{k}) = 0$. We only require a finite extension:

Theorem 1.2.5: Splitting Field is Finite

The Brauer group $\mathrm{Br}(k)$ is the union of $\ker \varphi_{k,L}$ going over each L/k where L is a finite field extension. In particular, there exists a finite extension L/k such that for a CSA A over k, $[A \otimes_k L] = [1]$ in $\mathrm{Br}(L)$.

Proof **:**
By example 1.2[1] we have that for a CSA A over $\overline{k}$, $A \otimes_k \overline{k} \cong M_n(D)$. Then the right hand side is generated by finitely many elements of the left hand side. We need only take the elements that map to the generators of the right hand side and to choose the appropriate field elements to get find L/k, as we sought to show.