Generalities on Central Simple Algebras

Michael Lipnowski

Introduction

The goal of this talk is to make readers (somewhat) comfortable with statements like "*the* quaternion algebra over $\mathbb{Q}$ ramified at 2,5,7,11." Statements like this will come up all the time, when we use Jacquet-Langlands.

The Basic Theorems

Definition 1. *A **central simple algebra** (CSA) over a field k is a finite dimensional k-algebra with center k and no non-trivial two-sided ideals.*

Some examples:

- Any division algebra over k is clearly a central simple algebra since any non-zero element is a unit. For example, we have quaternion algebras:

  $$H(a,b) = span_k\{1,i,j,ij\}$$

  with multiplication given by

  $$i^2 = a, j^2 = b, ij = -ji.$$

  For example, when $k = \mathbb{R}, a = b = -1$, we recover the familiar Hamilton quaternions $\mathbb{H}$.

- Let G be a finite group and $\rho : G \to GL_n(k)$ be an irreducible k-representation. Then $End_G(\rho)$ is a division algebra by Schur's Lemma. Hence, it is a CSA.

- $M_n(k)$ is a CSA. Indeed the left ideals are of the form

  $$\begin{pmatrix} * & 0 & * & 0 \\ * & 0 & * & 0 \\ * & 0 & * & 0 \\ * & 0 & * & 0 \end{pmatrix}$$

  and right ideals have a similar "transpose" shape.

A first step to understanding division algebras are the following basic theorems.

Double Centralizer Theorem 1. *Let A be a k-algebra and V a faithful, semi-simple A-module. Then*

$$C(C(A)) = End_k(V),$$

where the centralizers are taken in $End_k(V)$.

Classification of simple k-algebras. *Every simple k-algebra is isomorphic to $M_n(D)$ for some division k-algebra D.*

Proof. Choose a simple A-module S (for example, a minimal left ideal of A).
A acts faithfully on S since the kernel of $A \to End_k(S)$ is a two-sided ideal not containing 1.
Let D be the centralizer of A in the k-algebra $End_k(S)$. By the double centralizer theorem, $A = C(D)$, i.e. $A = End_D(S)$.
But S is a simple A-module. Thus for $d \in D$ multiplication by d is an A-linear endomorphism $d : S \to S$ and hence is either 0 or invertible, by Schur's Lemma. Since the inverse is also A-linear and $D = C(A)$, it follows that D is a division algebra.
It follows that D is a division k-algebra and so $S \cong D^n$ for some n. Hence,

$$A = End_D(D^n) = M_n(D^{opp}).$$

□

Noether-Skolem Theorem. *Let A be a simple k-algebra and B a semi-simple k-algebra. If*

$$f, g : A \to B$$

are k-algebra maps, then there is an invertible $b \in B$ such that

$$f(a) = bg(a)b^{-1}$$

for all $a \in A$.

The Brauer Group

We note the two following facts:

Proposition. *If A and B are CSAs over k, then $A \otimes_k B$ is a CSA over k.*

Proposition. *Let A be a CSA over k. Then $A \otimes_k A^{opp} \cong End_k(V)$.*

We define an equivalence relation on the set of CSAs over k by

$$A \sim B \text{if} A \otimes_k M_n(k) \cong B \otimes_k M_m(k) \text{for some positive integers} n, m.$$

This allows us to define the **Brauer group of** $k, Br(k)$, to be the set of equivalence classes of CSAs over k.
As of right now, this is only a Bruaer set. But we can endow it with a group operation $[A][B] = [A \otimes_k B]$.

- This operation is well-defined on equivalence classes since $M_n(k) \otimes_k M_m(k) \cong M_{mn}(k)$.
- It is clearly associative and commutative.
- $[k]$ acts as the identity.
- $[A^{opp}]$ is the inverse of $[A]$

Some examples of Baruer groups:

- If k is algebraically closed, then $Br(k) = 0$. Indeed, any CSA A is isomorphic to $M_n(D)$ for some division k-algebra D. But for any element $d \in D, k[d]$ is a finite field extension of k. But k is algebraically closed! Hence, $D = k$. But then $A \sim k$.
- $Br(R) = \{[\mathbb{R}], [\mathbb{H}]\}$.
- By a theorem of Wedderburn, all division algebras over finite fields are commutative. Hence, $Br(\text{finite field}) = 0$.

Extension of Base Field

Proposition. *Let A be a CSA over $k, K \supset k$ a field extension. Then $A \otimes_k K$ is a CSA over K.*

In this statement, K need not necessarily be finite over k.

Corollary. *If A is a CSA over k, then $[A : k]$ is a square.*

Proof.

$$[A : k] = [A \otimes_k \overline{k} : \overline{k}].$$

But $A \otimes_k \overline{k}$ is a CSA over $\overline{k}$ and so is isomorphic to $M_n(\overline{k})$ for some n. Thus, $[A : k] = n^2$. □

Note that if L/k is any field extension, then

$$Br(k) \to Br(K) : A \mapsto A \otimes_k L$$

defines a homomorphism. We let $Br(L/k)$ denote its kernel.

Brauer Groups and Cohomology

There is a natural isomorphism $H^2(L/k) = H^2(G_{L/k}, L^\times) \to Br(L/k)$. This is very handy, as it allows $Br(L/k)$ and $H^2(L/k)$ to play off each other. For example, it is not otherwise clear that $Br(k)$ is torsion or that $H^2(G_k, k^\times) = H^2(G_k^{un}, k^\times)$ for a local field k.
Here is a slightly more general version of the double centralizer theorem that we'll find useful.

Theorem. *Let B be a simple k-subalgebra of A. Then $D = C_A(B)$ is simple, $B = C_A(D)$, and $[B : k][D : k] = [A : k]$.*

Proposition. *Let A be a CSA over k. Let $L \subset A$ be a (commutative) field containing k. Then TFAE:*

(a) $L = C_A(L)$.

(b) $[A : k] = [L : k]^2$

(c) L *is a maximal commutative subalgebra of* A.

Along with this criterion, the following is an exercise in using the double centralizer theorem.

Corollary (CFT, 3.6). *Let A be a central simple algebra over k. A field L of finite degree over k splits A iff there exists an algebra B representing the same Brauer group element containing L and such that $[B : k] = [L : k]^2$.*

We can give some additional information about splitting fields of A.
If A is any CSA over k with $[A;k] = n^2$, there is a variety/k $\underline{\text{Isom}}(A, M_n)$ which represents the functor

$$\underline{\text{k-algebras}} \to \underline{\text{Sets}} : R \to \{ \text{ isomorphisms } A \otimes_k R \to M_n(R)\}.$$

Indeed, this is easy to represent, since a map of k-algebras is a linear map determined by a non-vanishing determinant and preservation of the algebra's structure constants, all algebraic conditions. The variety is non-empty since it contains at least one $\overline{k}$ point (all CSAs split over an algebraically closed field). Furthermore, it can be checked that this is smooth (by Grothendieck's functorial criterion for smoothness). Hence, the k^{sep} points are dense. In particular, A-splits over some finite separable extension.

CSAs and 2-cocycles

This entire section follows Milne's treatement in **CFT** almost verbatim.

Let L/k be a finite Galois extension.
Let $\mathcal{A}(L/k) = \{A : A = \text{CSA over} k \text{containing} L \text{of degree} [A : k] = [L; k]^2\}$.

By Noether-Skolem, for any $\sigma \in G_{L/K}$, there exists some $e_\sigma \in A^\times$ such that

$$\sigma a = e_\sigma a e_\sigma^{-1} \text{ for all } a \in A. (1)$$

We see that $e_\sigma e_\tau e_{\sigma\tau}^{-1} = \phi_A(\sigma, \tau)$ (1) centralizes L and hence lies in $L^\times$. Because the multiplication in A is associative, we easily see that $\phi_A : G \times G \to L^\times$ is a 2-cocycle. Furthermore, it's clear that different choices of e'_σ lead to a cocycle ϕ'_A which differs from ϕ_A by a coboundary. Thus, we get a well-defined cohomology class.

Claim (CFT, 3.12). *The elements $e_\sigma, \sigma \in G$, are linearly independent over L.*

Proof. $\dim_L(A) = \dim_k(A)/\dim_k(L) = n = |G|$. Thus, it suffices to show that the e_σ are linearly indepedent.
Let $\{e_\sigma\}_J$ be a maximal L-linearly independent subset. We assume, for a contradiction, that $J \neq G$. If $\tau \notin J$, express

$$e_\tau = \sum_{\sigma \in J} a_\sigma e_\sigma. \ (*)$$

for some $a_\sigma \in L$. But we compute $e_\tau a$ in two different ways:
First, by the defining property $e_\tau a e_\tau^{-1} = \tau a$, we have

$$e_\tau a = \tau a e_\tau = \sum_{\sigma \in J} (\tau a) a_\sigma e_\sigma.$$

On the other hand, by our assumption (*) and the definiting property applied to each e_σ, we get

$$e_\tau a = \sum_{\sigma \in J} a_\sigma e_\sigma a = \sum_{\sigma \in J} a_\sigma (\sigma a) e_\sigma.$$

Hence $a_\sigma(\sigma a) = a_\sigma(\tau a)$ for each $\sigma \in J$. But a_σ is non-zero for some $\sigma \in J$, whence $\sigma = \tau$. This contradicts $\tau \notin J$. □

Suppose that A and A' are isomorphic elements of $\mathcal{A}(L/k)$. By Noether-Skolem, we can find an isomorphism $f : A \to A'$ such that $f(L) = L$ and $f|_L$ is the identity map.
Note that if we choose elements $e_\sigma \in A$ which satisfy $(1)_A, (2)_A$ then the elements $f(e_\sigma) \in A'$ satisfy $(1)_{A'}, (2)_{A'}$ with cocycle ϕ_A. Hence, the cohomology class only depends on the isomorphism class of A. Furthermore, if L-bases $\{e_\sigma\} \subset A$ and $\{e'_\sigma\} \subset A'$ both have the same cocycle, then extending $e_\sigma \to e'_\sigma$ by L-linearity clearly gives an isomorphism $A \cong A'$.
Hence, we have an injective map

$$\mathcal{A}(L/k)/\cong \to H^2(L/k).$$

But this map is surjective too. Given a 2-cocycle ϕ, we can just define an algebra by (1) and (2). Namely, let

$$A(\phi) = \oplus_{\sigma \in G} e_\sigma$$

with defining relations

$$e_\sigma a e_\sigma^{-1} = \sigma a \text{ for all } \sigma \in G, a \in L$$

$$e_\sigma e_\tau = \phi(\sigma, \tau) e_{\sigma\tau} \text{ for all } \sigma, \tau \in G.$$

By the cocycle relation for ϕ, it follows that the above defines a k-algebra.

Fact (CFT, 3.13). *$A(\phi)$ is a CSA over k. Furthermore, this construction is a group homomorphism: $[A(\phi)][A(\phi')] = [A(\phi + \phi')]$.*

This isomorphism is actually functorial:

$$\begin{array}{ccc} H^2(L/k) & \xrightarrow{Inf} & H^2(E/k) \\ \downarrow & & \downarrow \\ Br(L/k) & \xrightarrow{\text{inclusion}} & Br(E/k) \end{array}$$

where the vertical maps are $\phi \mapsto A(\phi)$. Since both the Brauer groups (resp. H^2s) are limits under inclusions (resp. inflation maps) of finite Galois extensions L/k, the above diagram implies that there is a canonical isomorphism

$$H^2(k) \xrightarrow{\sim} Br(k).$$

This implies the otherwise unobvious fact that

Corollary. *For any field k, $Br(k)$ is torsion. For any finite extension L/k, $Br(L/k)$ is killed by $[L : k]$.*

Proof. The same results are true for cohomology groups. □

Brauer Groups of Local Fields

Usually, the invariant map of local class field theory is constructed by pure group cohomology. We give an alternate presentation based more directly related to CSAs.

Let D be a central division algebra over non-archimedean local field K, say $n^2 = [D : k]$. Let K have ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{p} = (\pi)$, and residue field k of size q.
It has a valuation satisfying the usual properties:

- $|\alpha| = 0$ iff $\alpha = 0$.
- For all $\alpha, \beta \in D, |\alpha\beta| = |\alpha||\beta|$.
- For all $\alpha, \beta \in D, |\alpha, \beta| \leq \max\{|\alpha|, |\beta|\}$.

We define $|\alpha|$ as the scaling effect of right multiplication by α. This is equivalently the absolute value (in K) of the determinant of right multiplication by x as a map from D, as a K-vector space, to itself. Then it is clear that the first and second properties from the above list hold. But the triangle inequality is less obvious.
But this actually reduces to the commutative case.
Indeed, we want to show that if $|x| \leq 1$, then $|1 + x| \leq 1$. But the way we've defined it,

$$|x| = |N_{K[x]/K}(x)|_K^{[D:K[x]]}.$$

So we just need to show that if $|N_{K[x]/K}(x)|_K \leq 1$, then $|N_{K[x]/K}(1 + x)|_K \leq 1$. But this is a result that we know to be true of commutative field extensions. Hence, it's true here too.

Define $|\alpha| = (1/q)^{ord(\alpha)}$, giving the normalized valuation on D.
By the way we've defined the valuation, ord extends the usual valuation on any field extension L/K.
We know that any element $x \in D$ is contained in a field extension $K[x]/K$ of degree $\leq n$ (since any maximal subfield of D has degree n over K). Hence,

$$ord(D^\times) \subset n^{-1}\mathbb{Z}.$$

As usual, we define

$$\mathcal{O}_D = \{\alpha \in D : |\alpha| \leq 1\}$$

$$\mathcal{P} = \{\alpha \in D : |\alpha| < 1\}.$$

The absolute value is discrete and multiplicative. So, just as in the case of fields, any element π of largest absolute value generates the two sided ideal $\mathcal{P}$. And any element of $\mathcal{O}_D$ can be expressed uniquely as $u \times \pi^m$ for some $m \geq 0$. Thus, any two-sided ideal can be expressed uniquely as $\mathcal{P}^m$.
In particular, if $\mathfrak{p}$ denotes the prime ideal of K, then $\mathfrak{p}\mathcal{O}_D = \mathcal{P}^e\mathcal{O}_D$ for some integer e, the ramification index. In particular, $ord(D^\times) = e^{-1}\mathbb{Z}$, implying that $e \leq n$.
Also, if $|\alpha| = 1$ for some $\alpha \in D$, then $\alpha \in \mathcal{O}_D^\times$. Hence, $j = \mathcal{O}_D/\mathcal{P}$ is a finite division algebra, and hence a field. Let $f = [j : k]$. If $j = k[a]$ and α is a lift of a to $\mathcal{O}_D$, then

$$f = [j : k] \leq [K[\alpha] : K] \leq n.$$

Exactly as in the case of commutative fields, we see that $n^2 = ef$. Note that $\mathcal{O}_D$ is a free $\mathcal{O}_K$-module of some rank, say m.

- $\mathcal{O}_D \otimes_{\mathcal{O}_K} K = D$, so $m = n^2$.
- $\mathcal{O}_D \otimes_{\mathcal{O}_K} k = \mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$. Thus, $n^2 = \dim_k \mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$. But we can filter

$$\mathcal{O}_D \supset \mathcal{P} \supset ... \supset \mathcal{P}^e = \mathfrak{p}\mathcal{O}_D.$$

  Each successive quotient, of which there are e, has dimension f as a k-vector space. Hence, $n^2 = ef$.

But since $e, f \leq n$ the equality $ef = n^2$ implies that $e = f = n$.

$$n = [j : k] \leq [K[a] : K]$$

Also, we know that the field $k[a] = j$, so $K[\alpha]$ is an extension of K with residue field j.
But the maximal commutative subfield of D has degree n over K. Thus,

$$n \geq [K[a] : K] \geq [j : k] = n.$$

Thus $K[\alpha]/K$ has both degree and residue degree n. Thus, $K[\alpha]/K$ is unramified.
Since every CSA is in the same class as some division algebra, we know that every CSA is split by an unramified extension. Hence,

$$Br(K) = Br(K^{un}/K).$$

The Local Invariant Map

We can use this Brauer group perspective to directly define the invariant map

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z}$$

and the fundamental class of class field theory.

Any CSA over K is split by some unramified field extension $A \subset L/K$. By Noether Skolem, there is some $\alpha \in A^\times$ such that

$$Frob(x) = \alpha x \alpha^{-1} \text{ for all } x \in G_{L/K}.$$

We define

$$inv_K(A) = ord(\alpha) \ (mod\ \mathbb{Z}).$$

But Frobenii are compatible: if $L' \subset L \subset K$ is a tower of unramified field extensions, then $Frob_{L'/K}|_L = Frob_{L/K}$. Thus, this map does not depend on choice of splitting field.
Also, if A/K is split by L and A'/K is split by L', then $A \otimes_k A'/K$ is split by LL'.
Furthermore, if $Frob(x) = axa^{-1}, Frob(x') = a'xa$, then

$$Frob(x \otimes_k x') = (a \otimes_k 1)(1 \otimes_k a)(x \otimes_k x')(1 \otimes_k a)^{-1}(a \otimes_k 1)^{-1}.$$

Thus, we get a homomorphism from CSAs over K to $\mathbb{Q}/\mathbb{Z}$. Furthermore, $M_n(K) \mapsto 0$, because it is already split over K. Thus,

$$Br(K) \to \mathbb{Q}/\mathbb{Z} : A \mapsto inv_K(A)$$

is a well-defined group homomorphism. The above work we've done also easily shows that

$$Br(L/K) \to 1/[L:K]\mathbb{Z}/\mathbb{Z}$$

for an unramified extension L/K.
Here's the most important example of this:

- Let L/K be an unramified extension of degree n with $\sigma = Frob$. Let ϕ be the 2-cocycle

$$\phi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i+j \leq n-1 \\ \pi & \text{otherwise.} \end{cases}$$

  This is the 2-cocycle of the fundamental class $u_{L/K} \in H^2(L/K)$. In particular, it maps to $1/n \in 1/n\mathbb{Z}/\mathbb{Z}$ via the invariant map, $inv'_{L/K}$, of Galois cohomology.
  It has associated CSA $A(\phi) = \oplus_i e_i L$ with mutiplication determined by

$$e_i a e_i^{-1} = \sigma^i a \text{ for all } a \in L$$

  and

$$e_i e_j = \begin{cases} e_{i+j} & \text{if } i+j \leq n-1 \\ \pi e_{i+j-n} & \text{otherwise.} \end{cases}$$

  So in particular, e_0 is the identity and L is identified with Le_0. But $e_1^n = e_{n-1}e_1 = \pi e_0 = \pi$. Hence,

$$inv_K(A(\phi)) = ord(e_1) = \frac{1}{n}.$$

Hence, we have a commutative diagram

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{inv'_{L/K}} & 1/n\mathbb{Z}/\mathbb{Z} \\ \downarrow & & \downarrow \\ Br(L/K) & \xrightarrow{inv_{L/K}} & 1/n\mathbb{Z}/\mathbb{Z} \end{array}.$$

It commutes because it commutes on a generator ϕ of $H^2(L/K)$. Since the top row is an isomorphism, so is the bottom row. Hence, we get a canonical isomorphism

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z}$$

for any local field K.

Brauer Groups of Global Fields

The following is the fundamental exact sequence of class field theory

$$0 \to Br(K) \xrightarrow{\sum_v inv_v} \oplus_v Br(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

None of the exactness comes easily. In fact, it's not even immediately clear why the first map is well-defined, i.e. why is it impossible for infinintely many of the local invariants to be non-zero simultaneously?
For this, we could return to the variety of ismorphisms $\underline{\mathrm{Isom}}(A, M_n)$. This is a variety over k. If we spread it out to some ring of S-integers $\mathcal{O}_S$, then we'd get a variety $V/\mathcal{O}_S$ which represents the functor

$$\underline{\mathcal{O}_S\text{-algebras}} \to \underline{\mathrm{Sets}} : R \to \{ \text{ isomorphisms } A \otimes_k R \to M_n(R)\}.$$

We could check that this is a non-empty smooth variety. Furthermore, over the residue fields $k_v, v \notin S$ there is a point. By Hensel's Lemma, these lift to $\mathcal{O}_v$ points. (This is a "reason", but not a proof.)

Exactness of the above sequence is the essence of the proofs behind class field theory. For details, see **CFT**.
Another miracle happens over global fields (containing a primitive n^{th} root of 1, call it ζ).
We define the **Milnor K-group**, $K_2(K)$ to be $K^\times \otimes_{\mathbb{Z}} K^\times$ modulo the relation

$$u \otimes_{\mathbb{Z}} (1-u) = 1 \text{ whenever } u, 1-u \neq 1.$$

Now, consider the algebra $A(a, b; \zeta)$ over K generated by i, j subject to the relations:

$$i^n = a, j^n = b, ij = \zeta ji.$$

The Milnor relations are satisfied by the $A(a, b; \zeta)$ and so define a homomorphism

$$K_2(k) \to Br(k).$$

It turns out that

$$K_2(K)/nK_2(K) \to Br(K)[n]$$

is an isomorphism! (Merkuryev-Suslin)
In particular, combining the class field theory exact sequence with this miracle, we see that any 2-torsion element of $Br(K)$ is in the class of a unique quaternion algebra (up to isomorphism).

References

CFT J.S. Milne. *Class Field Theory (version 4.00).* Available at www.jmilne.org/math/