Lecture 2
Central Simple Algebras

Patricio Quiroz

Wesleyan University 04.08.2014

Remember that the theory of spinor genera is the "abelian part" in the problem of study the difference between local and global information, that is:

$$\begin{array}{rcl} gen(\Lambda) & = & G_{\mathbb{A}}.\Lambda \\ | & & \\ spn(\Lambda) & = & GG'_{\mathbb{A}}.\Lambda \\ || & & \text{If } G \text{ is not compact at some archimedean place.} \\ cls(\Lambda) & = & G.\Lambda \end{array}$$

where

$$\#\{\text{spinor genera in } gen(\Lambda)\} = |J_K/K^* H_{\mathbb{A}}(\Lambda)| = [\Sigma_\Lambda : K],$$

and $H_{\mathbb{A}}(\Lambda)$ is the "image" of the spinor norm[1] $\Theta_{\mathbb{A}} : G_{\mathbb{A}} \to J_K/J_K^n$. This theory can be used to study representation problems as:

Given a lattice $M \subset \Lambda$ (Λ fixed of maximal rank), how many classes (orbits $G.\Lambda$) in the genus of Λ (in the orbit $G_{\mathbb{A}}.\Lambda$) contain an isomorphic copy of M?

We will focus on the case of orders (lattices with additional structure) in central simple algebras (CSA's). So, we have to have some background material about CSA's and orders inside them.

Motivation. Central simple algebras and orders appear in different places, for instance:

1. Number theory. Brauer groups play a central role in class field theory.

2. Theory of hyperbolic varieties. Arithmetical Kleinian and Fuchsian groups can be described in terms of maximal orders[2].

[1] n is 2 in the cases of forms and the degree of the central simple algebra in that case.

[2] See for example, L.E. Arenas-Carmona, *Representation fields for cyclic orders*, Acta arithmetica, 156.2 (2012)

3. Theory of modular forms. Studying maximal orders in CSA's is one way to generalize the classic theory of modular forms[3]. There is also a connection between a certain space defined in terms of the ideal class group of a maximal order in a quaternion algebra and the space of modular forms of weight 2 and certain level[4] (related with the ramification of the quaternion algebra).

4. Wireless communication. There is a recent book[5] from the AMS showing applications of CSA's via the characterization of space-time codes problems in terms of matrices.

1 Central Simple Algebras (CSA's)

Let K be a field (we think K as a number field or one of its completions). Let A be a finite dimensional K-algebra[6].

Definition. We say that A is

1. *Central*, if $Z(A) = K$.

2. *Simple*, if it has no two-sided (non trivial) ideals.

3. *Central simple*, if it is central and simple.

Examples.

1. A field K is a K-CSA.

2. Quaternion algebras $\left(\frac{\alpha,\beta}{K}\right)$ are central simple. Hence, $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ and $\mathbb{M}_2(K) \cong \left(\frac{1,-1}{K}\right)$ are CSA's.

3. A K-division algebra D is simple and is central simple over its center[7] $Z(D)$.

4. $\mathbb{M}_n(K)$ is a CSA and it can be shown by using properties[8] of tensor product of algebras, that[9] $\mathbb{M}_n(D) \cong \mathbb{M}_n(K) \otimes_K D$ is a central simple algebra for any division CSA D over K.

[3] If you google for *Quaternion algebras and shimura curves* you will find a couple of short introductions that make use of maximal orders in quaternion algebras to produce curves.

[4] See A. Pacetti, G. Tornaria, *Shimura correspondence for level p^2 and the central values of L-series*, J. of Number Theory, 124 (2007)

[5] G. Berhuy, F Oggier, *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*, mathematical surveys and monographs, vol 191, AMS (2013)

[6] For us, an algebra A will always be an associative algebra with 1, so K" = "$1 \cdot K \subset A$.

[7] $Z(D)$ is a field because $xy = yx \Leftrightarrow y^{-1}x^{-1} = x^{-1}y^{-1}$ for every $x, y \in D$.

[8] E.g. Azumaya-Nakayama (1947) theorem concerning ideals in a tensor product in §5.1 of *Further Algebra and Applications* by P.M. Cohn.

[9] For any K-algebra B, $\mathbb{M}_n(B) \cong \mathbb{M}_n(K) \otimes_K B$.

Theorem. (Wedderburn[10], 1907) Let A be a finite dimensional simple K-algebra. Then there exists an integer $n \geq 1$ and a division ring $D \supset K$ such that $A \cong \mathbb{M}_n(D)$. Moreover, D is unique up to isomorphism.

As an immediate consequence, we have that a CSA over a finite field is a matrix algebra over a field[11].

Corollary. A CSA A over an algebraically closed field K satisfies $A \cong \mathbb{M}_n(K)$.
Proof. $A \cong \mathbb{M}_n(D)$, where $D \supset K$ is a division ring. Now, every element in D defines an algebraic extension of K, but K is algebraically closed, so $D = K$.

We conclude that there is always a field extension L/K such that $A \otimes_K L \cong \mathbb{M}_n(L)$. We say that a field L with the last property is a **splitting field** of the CSA A.

Example. If $A \cong \left(\frac{\alpha,\beta}{K}\right)$, then it is clear that $K(\sqrt{\alpha})$ is a splitting field for A.

It can be proved[12] that a CSA has always a separable[13] splitting field L with $L \subset A$ and $[L : K] = n$. As a consequence, a CSA A has square dimension and we say that $\sqrt{dim(A)}$ is the *degree* of A.

Now we proceed to state the beautiful Skolem-Noether theorem which implies that the group of automorphisms of a CSA A is isomorphic to A^*/K^*.

Theorem. (Skolem-Noether[14], 1927) Let A be a CSA over K and B a simple K-algebra. Let $\sigma, \tau : B \to A$ be two algebra homomorphisms. Then there exists an inner automorphism ϕ of A such that $\tau = \phi\sigma$.

If we take $B = A$ and $\sigma = id_A$ in the theorem, we conclude that every automorphism in a CSA is a conjugation (inner). Hence, we have a surjection $A^* \twoheadrightarrow Aut(A)$ with kernel K^*.

Example. We characterize[15] central simple algebras of dimension 4. Let A be a CSA with $dim_K(A) = 4$. By Wedderbun's we have $A \cong \mathbb{M}_n(D)$ and $4 = dim_K(A) = n^2 \cdot dim_K(D)$. We have two options: $n = 1$ or $n = 2$. If $n = 2$, we have $A \cong \mathbb{M}_2(K)$. If $n = 1$, A is a division algebra. Take a separable splitting field $L \subset A$. It is clear that $L = K(a)$ is a quadratic extension of K and we can choose a such that $a^2 \in K$. By Skolem-Noether's we have an element $b \in A^*$ such that $bab^{-1} = \sigma(a)$, where σ is the non trivial automorphism of $Gal(L/K)$. Hence, $A = L \oplus bL$ and $b^2 = \beta \in K = Z(A)$. So, if we define $\alpha = a^2$, we have $A \cong \left(\frac{\alpha,\beta}{K}\right)$.

Now, we will define an analogue to the determinant in a CSA. This map will be

[10] It is in everywhere, but you can see for instance §8 in W. Scharlau, *Quadratic and Hermitian forms*, Springer (1985).
[11] A finite division ring is commutative.
[12] See Scharlau's book.
[13] Hence, there is always a Galois extension of K (not necessarily contained in A) that is a splitting field of A. CSA's containing Galois splitting fields are called crossed products in the literature.
[14] See Scharlau's book.
[15] When the base field has characteristic different from 2.

essentially our spinor norm.

Reduced Norm.

We know that, going up, we have $A_L = A \otimes_K L \cong \mathbb{M}_n(L)$, so we have an inclusion $A \hookrightarrow A_L$ and we can see an element $a \in A$ as a matrix. Hence, we define the characteristic polynomial of $a \in A$ as $\chi_a(x) := \chi_{\phi(a)}(x) \in L[x]$, where ϕ is any isomorphism $\phi : A_L \to \mathbb{M}_n(L)$. This polynomial does not depend on ϕ because of Skolem-Noether's theorem. It can be proved that, $\chi_a(x)$ is independent of the field L and $\chi_a(x) \in K[x]$. Note that $\chi_a(0) = (-1)^n det(\phi(a))$.

Definition. We say that the map $N : A \to K$ given by $a \mapsto (-1)^n \chi_a(0) = det(\phi(a))$ is the **reduced norm** of $a \in A$. We have immediate consequences:

1. $N(ab) = N(a)N(b), \forall a, b \in A$.

2. $N(\lambda a) = \lambda^n N(a)$, $\forall a \in A, \lambda \in K$.

A less immediate consequence is (in the quaternionic case, this is immediate[16] because you can express the inverse of an element q as $(Nq)^{-1}\bar{q}$): $a \in A^*$ if and only if $N(a) \neq 0$. Let's prove it. It is clear that if a is invertible, then $N(a) \neq 0$. Now take $a \in A$ with $N(a) \neq 0$. We know that (taking a galois splitting field L and an isomorphism $\phi : A_L \to \mathbb{M}_n(L)$) $\phi(a) \in \mathbb{M}_n(L)$ is invertible because its determinant ($= N(a)$) is not 0. Let $b \in A_L$ be the inverse of a. If we prove that $b \in A$ we are done. Take $G = Gal(L/K)$ and $\hat{G} = id_A \otimes G \subset Aut(A \otimes_K L)$. It is clear that the set of fixed points of $\hat{G}$ is A. Hence, it is enough to prove that $\sigma(b) = b$ for every $\sigma \in \hat{G}$. If $\sigma(b) \neq b$, then $\sigma(b)$ would be another inverse of a, which can not occur by uniqueness of inverses.

Note that we used a (nice) "going up and down" or "descent" argument which is frequently used in field theory, galois cohomology and, of course, CSA's theory.

If $a \in A$, there is a relation between $N(a)$ and l_a, where $l_a : A \to A$ is the linear map given by $l_a(b) = ab$. The relation is (the matrix of l_a in a splitting field is $diag(a, ..., a)$)

$$det(l_a) = N(a)^n.$$

Finally, if $L \subset A$ is a maximal splitting field[17], then for every $a \in L$,

$$N(a) = N_{L/K}(a).$$

---

[16]It can be checked, by using the inclusion $\left(\frac{\alpha,\beta}{K}\right) \hookrightarrow \mathbb{M}_2(K(\sqrt{\alpha}))$ given by $i \mapsto \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}$, $j \mapsto \begin{pmatrix} 0 & 1 \\ \beta & 0 \end{pmatrix}$, that the quaternion norm $q \mapsto q\bar{q}$ is the reduced norm of the quaternion algebra.

[17]A splitting field $L \subset A$ with $[L : K] = n$, where $dim_K(A) = n^2$.