Selectivity in Quaternion Algebras

Benjamin Linowitz

Dartmouth College
Outline

• Orders in quaternion algebras

• Type numbers

• A few embedding theorems

• Determining when an order is selective
Let $F$ be a field.

A **quaternion algebra** over $F$ is a central simple $F$-algebra of dimension 4.

By Wedderburn’s theorem, every quaternion algebra is either a division $F$-algebra or isomorphic to $M_2(F)$.

If $\text{char}(F) \neq 2$ then every quaternion algebra $\mathcal{A}$ over $F$ has an $F$-basis $\{1, i, j, ij\}$ satisfying

$$i^2 = a, \quad j^2 = b, \quad ij = -ji, \quad a, b \in F^*.$$ 

Conversely, such an $F$-basis completely determines a quaternion algebra, typically denoted $(\frac{a,b}{F})$.

**Example** If $F = \mathbb{R}, a = b = -1$ then we have $\mathbb{H}$, Hamilton’s quaternions.
Let $K$ be a number field with ring of integers $\mathcal{O}_K$.

Let $\mathfrak{A}$ be a quaternion algebra over $K$ and $p$ a prime (possibly infinite) of $K$.

Then $\mathfrak{A}_p := \mathfrak{A} \otimes_K K_p$ is a quaternion algebra over $K_p$.

If $\mathfrak{A}_p \cong M_2(K_p)$ then $p$ splits in $\mathfrak{A}$. Otherwise $p$ ramifies in $\mathfrak{A}$.

**Fact** Only a finite, even number of primes ramify in $\mathfrak{A}$.

**Example** Every prime $p$ of $K$ splits in the matrix algebra $M_2(K)$. 
The quaternionic case of a classical theorem:

**Theorem (Albert-Brauer-Hasse-Noether).** Let $\mathcal{A}$ be a quaternion algebra over a number field $K$ and let $L$ be a quadratic field extension of $K$. Then there is an embedding of $L$ into $\mathcal{A}$ over $F$ if and only if no prime of $K$ which ramifies in $\mathcal{A}$ splits in $L$. 
If $\mathbb{A}$ is a quaternion algebra over a number field $K$, then an order $\mathcal{R} \subset \mathbb{A}$ is a subring of $\mathbb{A}$ which is a rank 4 $\mathcal{O}_K$-module and satisfies $\mathcal{R} \otimes K \cong \mathbb{A}$.

**Example** $M_2(\mathcal{O}_K)$ is an order in the algebra $M_2(K)$.

**Local Theory** If $\mathcal{R}$ is an order of $\mathbb{A}$ and $p$ is a finite prime, then its local factor $\mathcal{R}_p := \mathcal{R} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_p}$ is an order of $\mathbb{A}_p$.

**Local-Global Principle** Suppose that for every finite $K$-prime $p$ we have an order $\mathcal{R}_p$ of $\mathbb{A}_p$. If there exists an order of $\mathbb{A}$ whose local factors are almost always equal to $\mathcal{R}_p$, then there exists a *unique* order $\mathcal{R}$ of $\mathbb{A}$ whose local factors are always $\mathcal{R}_p$. 

6
3 Classes of Orders

1. An order is **maximal** if it is maximal with respect to inclusion.

2. An order is **Eichler** if it is the intersection of two maximal orders.

3. An order is **primitive** if it contains the ring of integers of a maximal subfield of \( \mathfrak{A} \).
Type numbers

Note From this point on, we assume that there exists an infinite prime which is split in \( \mathcal{A} \) (i.e. \( \mathcal{A} \) satisfies the Eichler condition).

Two orders \( \mathcal{R}, \mathcal{S} \subset \mathcal{A} \) are of the same genus if \( \mathcal{R}_p \cong \mathcal{S}_p \) for all finite primes \( p \).

The type number \( t(\mathcal{R}) \) is the number of isomorphism (conjugacy) classes in the genus of \( \mathcal{R} \).

Fact The type number \( t(\mathcal{R}) \) is always finite.
We can say more then just $t(\mathcal{R}) < \infty$. It turns out that $t(\mathcal{R})$ is a power of 2.

To show this, one proves that there is a bijection between the representatives of orders in the genus of $\mathcal{R}$ and the quotient

$$I_K/H_{\mathcal{R}}$$

where $H_{\mathcal{R}}$ is a subgroup of $I_K$ containing $I_{K}^2$ and $P_{K,\infty}$, the principal ideals of $I_K$ whose generators are positive at the elements of $Ram_\infty(\mathfrak{A})$.

The proof of this bijection makes critical use of the assumption that $\mathfrak{A}$ satisfies the Eichler condition.

Let $K(\mathcal{R})$ be the class field corresponding to the above quotient. Then $[K(\mathcal{R}) : K] = t(\mathcal{R})$. 
Recall the ABHN Theorem:

**Theorem (Albert-Brauer-Hasse-Noether).** Let $\mathbb{A}$ be a quaternion algebra over a number field $K$ and let $L$ be a quadratic field extension of $K$. Then there is an embedding of $L$ into $\mathbb{A}$ over $F$ if and only if no prime of $K$ which ramifies in $\mathbb{A}$ splits in $L$.

Chinburg and Friedman proved an integral refinement of this theorem by considering when an order $\Omega \subset L$ embeds into a maximal order of $\mathbb{A}$. It is assumed that an embedding of $L$ into $\mathbb{A}$ exists.

**Theorem (Chinburg and Friedman)** *Assumptions as above, an order $\Omega \subset L$ can be embedded into either all maximal orders of $\mathbb{A}$ or into those belonging to exactly half of the isomorphism classes of maximal orders.*
This generalizes to arbitrary orders $\mathcal{R} \subset \mathfrak{A}$.

**Theorem (L.)** The proportion of the genus of $\mathcal{R}$ into which an order $\Omega \subset L$ can be embedded is $0, \frac{1}{2}$ or $1$.

In the maximal case, $\Omega$ is always contained in a maximal order.

If $\mathcal{R}$ is not a maximal order, then it is possible to have an embedding of $\Omega$ into $\mathfrak{A}$ but not into the genus of $\mathcal{R}$.

**Example** Let $\mathcal{R}$ be any order which is not primitive. If $L$ is any quadratic extension field of $K$ contained in $\mathfrak{A}$ then $\mathcal{O}_L$ embeds into $\mathfrak{A}$ but not into the genus of $\mathcal{R}$ by definition of primitivity.
We now have two questions to answer:

(1) When does $\Omega$ embed into an order in the genus of $\mathcal{R}$?

(2) If $\Omega$ does embed into the genus of $\mathcal{R}$, when is it selective?
(1) When does $\Omega$ embed into the genus of $\mathcal{R}$?

An **optimal embedding** of $\Omega$ into $\mathcal{R}$ is an embedding

$$\varphi : L \rightarrow \mathcal{A} \quad \varphi(\Omega) = \varphi(L) \cap \mathcal{R}.$$  

**Proposition 1** $\Omega$ embeds into the genus of $\mathcal{R}$ if and only if there is an overorder $\Omega^*$ of $\Omega$ and an optimal embedding of $\Omega^*$ into the genus of $\mathcal{R}$.

**Proposition 2** There is an overorder $\Omega^*$ of $\Omega$ and an optimal embedding of $\Omega^*$ into the genus of $\mathcal{R}$ if and only if, for all $K$-primes $\mathfrak{p}$, there is an overorder $\Omega^*_\mathfrak{p}$ of $\Omega_\mathfrak{p}$ which optimally embeds into $\mathcal{R}_\mathfrak{p}$.

These propositions reduce (1) to local optimal embedding theory, which exists for Eichler and primitive orders.
(2) If $\Omega$ does embed into the genus of $\mathcal{R}$, when is it selective?

In the maximal case,

**Theorem (Chinburg and Friedman)** $\Omega$ is selective for maximal orders in $\mathfrak{A}$ if and only if the following conditions hold:

1. The extension $L/K$ and the algebra $\mathfrak{A}$ are unramified at all finite primes and ramify at exactly the same real primes.

2. All prime ideals of $K$ dividing the relative discriminant ideal $d_{\Omega/\mathcal{O}_K}$ of $\Omega$ split in $L/K$. 
If \( \mathcal{R} \subset \mathfrak{A} \) is an arbitrary order,

**Theorem (L.)** \( \Omega \) is selective for \( \mathcal{R} \) if and only if the following conditions hold:

1. There is a containment of fields \( L \subset K(\mathcal{R}) \).

2. All prime ideals of \( K \) dividing the relative discriminant ideal \( d_{\Omega/\mathcal{O}_K} \) of \( \Omega \) split in \( L/K \).