Arithmetic in Quaternion Algebras

Graduate Algebra Symposium

Jordan Wiebe

University of Oklahoma

November 5, 2016

Outline

1. Groundwork
   - Definitions
   - Local-Global Connections
   - Integrality
   - Properties
2. Orders
   - Level & Discriminant
3. Results
   - Local-Global Connection
   - Global Example

Quaternion Algebras

Recall Hamilton's quaternions ($\mathbb{H}$): the four-dimensional vector space over $\mathbb{R}$ with basis $\{1, i, j, k\}$ made into a ring via the operations $i^2 = j^2 = k^2 = ijk = -1$.

Quaternion Algebras

Recall Hamilton's quaternions ($\mathbb{H}$): the four-dimensional vector space over $\mathbb{R}$ with basis $\{1, i, j, k\}$ made into a ring via the operations $i^2 = j^2 = k^2 = ijk = -1$.

Definition (Quaternion Algebra)

A 4-dimensional central simple algebra over a field F is called a quaternion algebra, and can be given via the (algebra) Hilbert symbol $\left(\frac{a,b}{F}\right)$ denoting the algebra with F-basis $\{1, i, j, k\}$ with multiplication satisfying $i^2 = a$, $j^2 = b$, and $ij = -ji = k$.

Quaternion Algebras

It's worth noting (for later) that the map given by

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, i \mapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}, j \mapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, k \mapsto \begin{pmatrix} & i \\ i & \end{pmatrix}$$

Quaternion Algebras

It's worth noting (for later) that the map given by

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, i \mapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}, j \mapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, k \mapsto \begin{pmatrix} & i \\ i & \end{pmatrix}$$

induces an algebra isomorphism

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}.$$

Quaternion Algebras

It's worth noting (for later) that the map given by

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, i \mapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}, j \mapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, k \mapsto \begin{pmatrix} & i \\ i & \end{pmatrix}$$

induces an algebra isomorphism

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}.$$

So we can write $\mathbb{H}$ (a 4-dimensional $\mathbb{R}$-algebra) in matrix form over the (2-dimensional) $\mathbb{R}$-algebra $\mathbb{C}$.

Number Fields

A number field K is a finite extension of $\mathbb{Q} = \mathbb{Q}(\alpha)$ for some algebraic α. These extensions have a number of important properties, but perhaps the most important concept here is that of absolute values (usual definition). There is an equivalence on absolute values, and the equivalence classes of absolute values are called *places*. The classic example here is the rationals $\mathbb{Q}$ and their p-adic absolute values (which corresponds to the primes) and the archimedean absolute value (the usual one). We can complete our field using one of the absolute values, and this completion is denoted K_v.

Number Fields

A number field K is a finite extension of $\mathbb{Q} = \mathbb{Q}(\alpha)$ for some algebraic α. These extensions have a number of important properties, but perhaps the most important concept here is that of absolute values (usual definition). There is an equivalence on absolute values, and the equivalence classes of absolute values are called *places*. The classic example here is the rationals $\mathbb{Q}$ and their p-adic absolute values (which corresponds to the primes) and the archimedian absolute value (the usual one). We can complete our field using one of the absolute values, and this completion is denoted K_v.

We will call a finite extension of $\mathbb{Q}_p$ a p-adic field.

Basic Results

- Any algebra with dimension < 4 is a field.

Basic Results

- Any algebra with dimension < 4 is a field.
- Any quaternion algebra over F is either a noncommutative division algebra D or the matrix algebra $M_2(F)$.

Basic Results

- Any algebra with dimension < 4 is a field.
- Any quaternion algebra over F is either a noncommutative division algebra D or the matrix algebra $M_2(F)$.

Definition (Split/Nonsplit)

We call a quaternion algebra B over a p-adic field F split if $B \simeq M_2(F)$, and nonsplit if $B = D$ is division.

Local-Global Results

Let F be a number field (a finite field extension of $\mathbb{Q}$). For a place v of F, write $B_v = B \otimes F_v$. Then B_v is a quaternion algebra over the field F_v.

Local-Global Results

Let F be a number field (a finite field extension of $\mathbb{Q}$). For a place v of F, write $B_v = B \otimes F_v$. Then B_v is a quaternion algebra over the field F_v.

Theorem (Albert-Brauer-Hasse-Noether for QAs)

For two quaternion algebras B and B' over a number field F, $B \simeq B'$ if and only if $B_v \simeq B'_v$ for all places v.

Local-Global Results

Let F be a number field (a finite field extension of $\mathbb{Q}$). For a place v of F, write $B_v = B \otimes F_v$. Then B_v is a quaternion algebra over the field F_v.

Theorem (Albert-Brauer-Hasse-Noether for QAs)

For two quaternion algebras B and B' over a number field F, $B \simeq B'$ if and only if $B_v \simeq B'_v$ for all places v.

So if we understand the local components of a quaternion algebra, we can differentiate between global objects.

Integrality

The ring of integers $\mathfrak{o}_F$ for a number field $F = \mathbb{Q}(\alpha)$ yields a number of useful results about the number field, and we wish to generalize the concept of a ring of integers to (quaternion) algebras.

Integrality

The ring of integers $\mathfrak{o}_F$ for a number field $F = \mathbb{Q}(\alpha)$ yields a number of useful results about the number field, and we wish to generalize the concept of a ring of integers to (quaternion) algebras.

Definition (Order)

Let V be a finite-dimensional vector space over F, the fraction field of a Dedekind domain R. An R-lattice in V is a subset $\Gamma \subset V$ such that Γ is a finitely-generated module over R. Call an R-lattice Γ complete if $V = F \cdot \Gamma$. An order in an F-algebra A over R is a complete R-lattice $\mathcal{O}$ in A which is a subring of A.

Order Examples

- Let $B = \left(\frac{a,b}{F}\right)$ and $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rk$. Then $\mathcal{O}$ is an order.

Order Examples

- Let $B = \left(\frac{a,b}{F}\right)$ and $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rk$. Then $\mathcal{O}$ is an order.
- In the matrix representation of B, we can write

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in R \oplus Ri \right\}.$$

Order Examples

- Let $B = \left(\frac{a,b}{F}\right)$ and $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rk$. Then $\mathcal{O}$ is an order.
- In the matrix representation of B, we can write

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in R \oplus Ri \right\}.$$

- In the matrix algebra $M_n(\mathbb{Q})$, $M_n(\mathbb{Z})$ is an order. Similarly, in the matrix algebra $M_n(\mathbb{Q}_p)$, $M_n(\mathbb{Z}_p)$ is an order.

Key Properties

Definition (Ramified/Split)

We call a quaternion algebra B over a number field F split at p if $B_p \simeq M_2(F_p)$. If B_p is not split, then by the classification of quaternion algebras we know that B_p must be division, and is called ramified. Any quaternion algebra B over a number field F is unramified at almost all primes, so $\mathrm{Ram}(B) = \{p_1, \ldots, p_r\}$ is finite (and in fact determines B!). In particular, $B_{p_i} \simeq D_i$ for D_i division and for all $1 \leq i \leq r$.

Key Properties (ctd)

Definition (Ramified/Unramified/Split)

For a quadratic field extension $K = F(\sqrt{d})$, we say K_p is split if $K_p = F_p \oplus F_p$. If we write $p\mathfrak{o}_{K_p} = \varpi^e \mathfrak{o}_{K_p}$, then we call K_p ramified if $e > 1$ and unramified otherwise.

The Split Case

Let $B = M_2(F)$ (split) for F a p-adic field and define

$$\mathcal{O}_B(n) = \left\{ \begin{pmatrix} \mathcal{O}_F & \mathcal{O}_F \\ \mathfrak{p}^n & \mathcal{O}_F \end{pmatrix} \right\}.$$

The Split Case

Let $B = M_2(F)$ (split) for F a p-adic field and define

$$\mathcal{O}_B(n) = \left\{ \begin{pmatrix} \mathcal{O}_F & \mathcal{O}_F \\ \mathfrak{p}^n & \mathcal{O}_F \end{pmatrix} \right\}.$$

Then we say this order is of level $\mathfrak{p}^n$. Note that this order often arises in the theory of modular forms.

The Unramified Case

Let E be the unramified quadratic extension of a p-adic field F. For a division algebra D over F, we can write $D = E \oplus Ej$. In fact, we can write $j^2 = \varpi$ for ϖ a uniformizer for E. In matrix form, we can write

$$D = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in E \right\}.$$

The Unramified Case

Let E be the unramified quadratic extension of a p-adic field F. For a division algebra D over F, we can write $D = E \oplus Ej$. In fact, we can write $j^2 = \varpi$ for ϖ a uniformizer for E. In matrix form, we can write

$$D = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in E \right\}.$$

Then the lattice

$$\mathcal{O}_D(2n+1) = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_E, \beta \in \varpi^n \mathfrak{o}_E \right\}$$

in an order, and we say this order has level $\mathfrak{p}^{2n+1}$.

The Ramified Case

Let K be a ramified quadratic extension of a p-adic field F. For a division algebra D over F, we can write

$$D = \left\{ \begin{pmatrix} \alpha & u\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\},$$

as before.

The Ramified Case

Let K be a ramified quadratic extension of a p-adic field F. For a division algebra D over F, we can write

$$D = \left\{ \begin{pmatrix} \alpha & u\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\},$$

as before. Then for u a uniformizer for K, the lattice

$$\mathcal{O}'_D(2n+1) = \left\{ \begin{pmatrix} \alpha & u\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{Z} + u^n \mathfrak{o}_E \right\}$$

in an order, and we say this order has level $\mathfrak{p}^{2n+1}$.

Level

Definition (Level)

Let $\mathcal{O}$ be an order in B. We say $\mathcal{O}$ has level $\mathfrak{p}^n$ if $\mathcal{O}$ is isomorphic (as a ring and as a module) to $\mathcal{O}_B(n), \mathcal{O}_D(n)$, or $\mathcal{O}'_D(n)$, depending on whether B is split or ramified.

Level

Definition (Level)

Let $\mathcal{O}$ be an order in B. We say $\mathcal{O}$ has level $\mathfrak{p}^n$ if $\mathcal{O}$ is isomorphic (as a ring and as a module) to $\mathcal{O}_B(n), \mathcal{O}_D(n)$, or $\mathcal{O}'_D(n)$, depending on whether B is split or ramified.

Note: in the nonsplit (ramified) setting, every order has level. In the split case, not every order has level.

Global Connection

For B a quaternion algebra over a number field F, define $\mathcal{O}_v = \mathcal{O} \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_v}$. Then

$$\operatorname{level}(\mathcal{O}) = \prod \operatorname{level}(\mathcal{O}_v).$$

So we can derive information about a global order by investigating its local orders.

A Global Example

Let B be a definite quaternion algebra over $\mathbb{Q}$ with $\mathrm{Ram}(B) = \{p_1, \ldots, p_r\}$ such that $d = p_1 \cdots p_r \equiv 7 \bmod 8$. Let $K = \mathbb{Q}(\sqrt{-d})$ and write

$$B = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\},$$

where $b \in \mathbb{Z}$ such that $\gcd(b, d) = 1$ and $\left(\frac{-d}{p}\right) = 1$ for each $p \mid b$.

A Global Example

Let B be a definite quaternion algebra over $\mathbb{Q}$ with $\mathrm{Ram}(B) = \{p_1, \ldots, p_r\}$ such that $d = p_1 \cdots p_r \equiv 7 \bmod 8$. Let $K = \mathbb{Q}(\sqrt{-d})$ and write

$$B = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\},$$

where $b \in \mathbb{Z}$ such that $\gcd(b, d) = 1$ and $\left(\frac{-d}{p}\right) = 1$ for each $p \mid b$. Then

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathfrak{o}_K \right\}$$

is an order in B of level $\prod p_i \cdot \prod_{p \mid b} p^{v_p(b)}$.

Proof

In this situation, we want to examine the situation locally, so we compute $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$. This breaks down into cases based on whether p is ramified or unramified or split.

Proof

In this situation, we want to examine the situation locally, so we compute $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$. This breaks down into cases based on whether p is ramified or unramified or split.

- If B is ramified at p, then $\mathcal{O}_p$ is maximal and has level p.

Proof

In this situation, we want to examine the situation locally, so we compute $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$. This breaks down into cases based on whether p is ramified or unramified or split.

- If B is ramified at p, then $\mathcal{O}_p$ is maximal and has level p.
- If B is split at p, then $\mathcal{O}_p$ is the intersection of two maximal orders (called Eichler) and has level $p^{v_p(b)}$.

Current Work

I'm currently working on determining the level of an arbitrary order in a quaternion algebra over $\mathbb{Q}$. Using the quadratic subfield representation, we can determine what the level is locally, and piece it together into a global picture.

Thanks!