Arithmetic in Quaternion Algebras

31st Automorphic Forms Workshop

Jordan Wiebe

University of Oklahoma

March 6, 2017

Outline

Quaternion Algebras

Quaternion algebras are incredibly useful for various computations, including computing modular forms. We'll construct quaternion algebras, orders, and discuss their arithmetic and applications.

Quaternion Algebras

Quaternion algebras are incredibly useful for various computations, including computing modular forms. We'll construct quaternion algebras, orders, and discuss their arithmetic and applications.

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

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

Quaternion Algebras

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

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

induces an algebra isomorphism

$$\left(\frac{a,b}{F}\right) \simeq \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in F(\sqrt{a}) \right\}.$$

Quaternion Algebras

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

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

induces an algebra isomorphism

$$\left(\frac{a, b}{F}\right) \simeq \left\{ \begin{pmatrix} \alpha & b\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in F(\sqrt{a}) \right\}.$$

So we can represent $\left(\frac{a,b}{F}\right)$ (a 4-dimensional F-algebra) in matrix form over the quadratic extension $F(\sqrt{a})$.

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.

Level

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

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

for $\mathfrak{p}$ the prime ideal of $\mathfrak{o}_F$.

Level

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

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

for $\mathfrak{p}$ the prime ideal of $\mathfrak{o}_F$.

Definition (Level)

Let $\mathcal{O}$ be an order in B split. We say $\mathcal{O}$ has level $\mathfrak{p}^n$ if $\mathcal{O}$ is isomorphic (as a ring and as an $\mathfrak{o}_F$ module) to $\mathcal{O}_B(n)$.

Level

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

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

for $\mathfrak{p}$ the prime ideal of $\mathfrak{o}_F$.

Definition (Level)

Let $\mathcal{O}$ be an order in B split. We say $\mathcal{O}$ has level $\mathfrak{p}^n$ if $\mathcal{O}$ is isomorphic (as a ring and as an $\mathfrak{o}_F$ module) to $\mathcal{O}_B(n)$.

Note: not every order has level. There are conditions depending on whether B is split or ramified which determine whether an order has level as desired.

Specific Example

Consider the algebra ramified at p and ∞, so $\Delta = p$, and a level $N = p^{2k+1}M$ for M relatively prime to p. Write $M = M_1^2 M_2$, where M_2 is square-free.

Specific Example

Consider the algebra ramified at p and ∞, so $\Delta = p$, and a level $N = p^{2k+1}M$ for M relatively prime to p. Write $M = M_1^2 M_2$, where M_2 is square-free. We can find a d so that $K = \mathbb{Q}(\sqrt{-d})$ is unramified at p and split at every other prime dividing the level N via CRT and Dirichlet's theorem on primes in arithmetic progression.

Specific Example

Consider the algebra ramified at p and ∞, so $\Delta = p$, and a level $N = p^{2k+1}M$ for M relatively prime to p. Write $M = M_1^2 M_2$, where M_2 is square-free. We can find a d so that $K = \mathbb{Q}(\sqrt{-d})$ is unramified at p and split at every other prime dividing the level N via CRT and Dirichlet's theorem on primes in arithmetic progression. Then we can represent B in matrix form as

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

Specific Example

Consider the algebra ramified at p and ∞, so $\Delta = p$, and a level $N = p^{2k+1}M$ for M relatively prime to p. Write $M = M_1^2 M_2$, where M_2 is square-free. We can find a d so that $K = \mathbb{Q}(\sqrt{-d})$ is unramified at p and split at every other prime dividing the level N via CRT and Dirichlet's theorem on primes in arithmetic progression. Then we can represent B in matrix form as

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

and the order

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & pM_2\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_K, \beta \in M_1\mathfrak{o}_K \right\}$$

has level N.

Proof

The proof here relies on the behavior of B and K locally, splitting into cases based on whether B is ramified or split, and whether K is split, ramified, or unramified.

Proof

The proof here relies on the behavior of B and K locally, splitting into cases based on whether B is ramified or split, and whether K is split, ramified, or unramified. In the case of the order presented above, we have

		K_p		
		K_p split	K_p ramified	K_p unramified
B_p	B_p split	✓	✓	✓
	B_p ramified	×	×	✓

Applications to Modular Forms

The construction of the order of level N above can be used to construct a basis for the space of newforms of weight k and level N via Arnold Pizer's algorithm. The new order presented above expands the current algorithm implemented in Sage to include higher powers of the discriminant in the level, as well as more general algebras.

Thank you!