Maximal Orders of Quaternions

Alyson Deines

December 8th Math 581b Final Project

A non-commutative analogue of Rings of Integers of Number Field

Abstract

Abstract

I will define maximal orders of quaternion algebras, give examples, discuss how they are similar to and differ from rings of integers, and then I will discuss one of their applications .

Quaternion Algebras over Number Fields

Definition

- Let F be a field and $a, b \in F$.
- A quaternion algebra over F is an F-algebra $B = \left(\frac{a,b}{F}\right)$ with basis

$$i^2 = a, j^2 = b, \text{ and } ij = -ji.$$

Examples:

- $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$
- $F = \mathbb{Q}(\sqrt{5}),\ B = \left(\frac{-1,-1}{F}\right)$
- Let F be any number field, $\left(\frac{1,b}{F}\right) \cong M_2(F)$ via

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

Maximal Orders

Lattices

- Let F be a number field with ring of integers R and let V be a finite dimensional F-vector space.
- An R-lattice of V is a finitely generated R-submodule $\mathcal{O} \subset V$ such that $\mathcal{O}F = V$.

Orders

- Let F be a number field with ring of integers R and let B be a finite dimensional F-algebra.
- An R-order $\mathcal{O} \subset B$ is an R-lattice of B that is also a subring.
- A maximal R-order $\mathcal{O} \subset B$ is an order which is not properly contained in any other orders.

Examples

Example

- Let F be a number field with ring of integers R and take $B = \left(\frac{1,1}{F}\right) \cong M_2(F)$.
- Then $M_2(R)$ is a maximal order.

Non-maximal Example

- Let $F = \mathbb{Q}(\sqrt{5})$ and $B = \left(\frac{-1,-1}{F}\right)$.
- Then $R = \mathbb{Z}[\gamma]$ where $\gamma = \frac{1+\sqrt{5}}{2}$.
- $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rij$ is a non-maximal order.

Examples

Maximal Example

- Let
$$e_1 = \frac{1}{2}(1 - \overline{\gamma} i + \gamma j)$$
$$e_2 = \frac{1}{2}(-\overline{\gamma} i + j + \gamma k)$$
$$e_3 = \frac{1}{2}(\gamma i - \overline{\gamma} j + k)$$
$$e_4 = \frac{1}{2}(i + \gamma j - \overline{\gamma} k)$$
- $\mathcal{O}_B = Re_1 \oplus Re_2 \oplus Re_3 \oplus Re_4$ is a maximal order.

Norm and Trace

Definition

- Let $x = u + vi + wj + zij \in B$.
- $\overline{x} = u - vi - wj - zij$
- $\text{nrd}(x) = x\overline{x} = u^2 - av^2 - bw^2 + abz^2$
- $\text{trd}(x) = x + \overline{x} = 2u$

Definition

- We say an element $x \in B$ is integral over R if it satisfies a monic polynomial with coefficients in R.
- If $x \in B$ and $x \notin F$, then x has minimal polynomial $t^2 - \text{nrd}(x)t + \text{trd}(x)$.
- So $x \in B$ is R-integral if and only if $\text{nrd}(x), \text{trd}(x) \in R$.

Integrality Issues

Now that we have a concept of integrality, we can see ways in which maximal orders fail as an analogue to rings of integers and Dedekind domains

Definition

- Take $B = M_2(\mathbb{Q})$ with elements $x = \begin{pmatrix} 0 & 0 \\ 1/2 & 0 \end{pmatrix}$ and $x = \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix}$.
- Then $x^2 = y^2 = 0$, so x and y are integral over $\mathbb{Z}$ but not in $M_2(\mathbb{Z})$.
- Additionally $\mathrm{nrd}(x + y) = 1/4$ so $x + y$ is not integral.
- Thus the set of all integral elements is not closed under addition and can't be a ring.

Local Fields

Local Quaternion Algebra

- Let v be a valuation of F.
- Then $B_v = B \otimes F_v$ is a quaternion algebra over F_v.
- If $\mathcal{O} \subset B$ is an R-order, $\mathcal{O}_v = \mathcal{O} \otimes R_v$ is an R_v-order.
- $\mathcal{O}$ is maximal if and only if $\mathcal{O}_{\mathfrak{p}}$ is maximal for every prime $\mathfrak{p}$ of R.
- For v a noncomplex valuation there is up to F_v-algebra isomorphism, a unique division ring B_v over F_v.

Ramification/Splitting

Definition

- We say that B is ramified at v if B_v is a division ring.
- Otherwise, we say that B is split at v (i.e. $B_v \cong M_2(F_v)$).
- The number of places of F where B is ramified is finite.

Discriminant

- The discriminant of B (relative to R) is the R-ideal $\text{disc}_R(B) = \prod_{\mathfrak{p} \text{ ramified}} \mathfrak{p} \subset R$.
- Let $\mathcal{O} \subset B$ be an R-order. Then the discriminant of $\mathcal{O}$ is the ideal $\text{disc}(\mathcal{O})$ of R generated by $\{d(x_1, x_2, x_3, x_4) : x_1, ..., x_n \in \mathcal{O}\}$ and $d(x_1, x_2, x_3, x_4) = \det(\text{trd}(x_i x_j))_{i,j=1,2,3,4}$.
- Let $\mathcal{O}$ be an R-order in B. Then $\mathcal{O}$ is maximal if and only if $\text{discred}(\mathcal{O}) = \text{disc}_R(B)$.

The Hilbert Symbol

Hilbert Reciprocity

- The Hilbert symbol

$$(a,b)_F = \begin{cases} 1 & \text{when } B = \left(\frac{a,b}{F}\right) \text{ is split.} \\ -1 & \text{otherwise.} \end{cases}$$

- If F is a number field and $a, b \in F^\times$ then

$$\prod_v (a,b)_{F_v} = 1.$$

Hilbert Modular Forms

There are two ways to compute Hilbert Modular Forms, both of which involve quaternion algebras and their maximal orders.

Computing Maximal Orders

- Using the Hilbert symbol you can compute maximal orders
- Can use maximal orders to work with Shimura curves and compute Hilbert Modular Forms

Hecke Operators

- Let $\mathcal{O}_{\mathfrak{c}}$ be the intersection of two maximal orders
- We can use this order to create a space which we can compute Hecke operators one.
- These Hecke operators correspond to the Hecke operators of certain Hilbert modular forms.