Lecture 2

Q: How can we tell whether two quaternion algebras A, A' are "the same"?

Def: An isomorphism of (quaternion) algebras A, A' over F is a ring isomorphism $f: A \xrightarrow{\sim} A'$ s.t. $f(c) = c$ for all $c \in F$.

So ring and vector space structure are preserved.

For quaternion algebras specifically, we'll use a particular type of basis to show that two are isomorphic.

Def: A basis of the quaternion algebra $A := (a,b)_F$ of the form $\{1, u, v, uv\}$ with $u^2, v^2 \in F^\times$ and $uv = -vu$ is called a quaternionic basis of A.

One can check that $(uv)^2 = -u^2v^2 \in F^\times$ and u, v, uv all pairwise anticommute.

Q: What are some other bases of $A = (a,b)_F$ aside from $\{1, i, j, ij\}$?

- $\{1, j, i, ji\}$ is one! So immediately we get $(a,b)_F \simeq (b,a)_F$.
- $\{1, i, ij, \underbrace{aj}_{i^2 j}\}$ is a basis. Thus $(a,b)_F \simeq (a, \underbrace{-ab}_{(ij)^2})_F$

- Similarly $\{1, j, ij, \underbrace{-bi}_{jij=-j^2 i}\}$ is a basis. Hence $(a,b)_F \simeq (b,-ab)_F$

- Finally, $\{1, ci, dj, cdij\}$ is a basis $\forall c,d \in F^\times$. Thus $(a,b)_F \simeq (ac^2, bd^2)_F$.

<u>Note</u>: By taking $b=1$, we get $(a,1)_F \simeq (a,-a)_F$ and $b=-1$ gives $(a,-1)_F \simeq (a,a)_F$

Since $(a, c^2)_F = (a,1)_F = (1,a)_F$

and

$(c^2, b)_F = (1,b)_F = (b,1)_F$

the isom. class of a quat. alg. depends on $a,b \in F^\times / F^{\times 2}$.

<u>Important exercise (2.4)</u>: Given $u,v \in (a,b)_F$ s.t. $u,v \notin F$ but $u^2, v^2 \in F^\times$ and $uv = -vu$, show that $\{1, u, v, uv\}$ is a quaternionic basis of $(a,b)_F$.

Some familiar algebraic objects turn out to be isom. to quat. algs.

> <u>Prop</u>: For all $a \in F^\times$, there is an isomorphism of F-algebras : $(1,a)_F \simeq M_2(F)$.

<u>Proof sketch</u>: Assume $\{1,i,j,ij\}$ is a basis for $(1,a)_F$. Consider the map $(1,a)_F \longrightarrow M_2(F)$ defined by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad ij \longmapsto \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}$$

and extend F-linearly to $(1,a)_F$.

Check that the image forms a linearly indep. set of size 4 in $M_2(F)$, the map is multiplicative, and $c \in F \mapsto \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$. ∎

Splitting of quaternion algebras:

Def: A quaternion algebra over F is called <u>split</u> if it is isomorphic to $M_2(F)$ as an F-algebra.

Example: Up to isomorphism, there are only two quaternion algebras over $\mathbb{R}$ and only one over $\mathbb{C}$:

$$(a,b)_{\mathbb{R}} \simeq \begin{cases} \mathbb{H}, & \text{if } a,b \text{ are negative} \\ M_2(\mathbb{R}), & \text{if } a \text{ or } b \text{ is positive} \end{cases}$$

Since all elements of $\mathbb{C}^\times$ are squares in $\mathbb{C}$, we have $(a,b)_{\mathbb{C}} \simeq M_2(\mathbb{C})$ for all $(a,b) \in \mathbb{C}^\times$, i.e, all quat. algs. over $\mathbb{C}$ are split!

Over $F=\mathbb{Q}$, the situation is VERY different! Eventually we'll show that there are infinitely many non-isom. quat. algebras over $\mathbb{Q}$!

So far, we've seen that $b \in F^{\times 2}$ guarantees $(a,b)_F$ is split. But this condition can be weakened. To do so, need to understand a subgroup of $F^\times$.

Let $N_a := \{x^2 - ay^2 : x,y \in F\} \setminus \{0\} \subseteq F^\times$.

In the lecture notes we show that N_a is a <u>subgroup</u> of $F^\times$ and equal to $F^\times$ if a is a square.

Lemma: For $a \in F^\times$, the set N_a of nonzero elts of the form $x^2 - ay^2$ with $x, y \in F$ is a subgroup of $F^\times$.

Proof: First observe that $1 \in N_a$ since we can write $1 = 1^2 - a \cdot 0^2$.

Next, N_a is closed under multiplication since

$$(x_1^2 - ay_1^2)(x_2^2 - ay_2^2) = (x_1x_2 + ay_1y_2)^2 - a(x_1y_2 + x_2y_1)^2.$$

Finally, N_a is closed under inversion since

$$\frac{1}{x^2 - ay^2} = \frac{x^2 - ay^2}{(x^2 - ay^2)^2} = \left(\frac{x}{x^2 - ay^2}\right)^2 - a\left(\frac{y}{x^2 - ay^2}\right)^2. \blacksquare$$

Note that N_a always contains all squares in $F^\times$ by taking $y = 0$. In the notes, we show further that if a is a square, then $N_a = F^\times$.

Theorem (characterization of splitness)

The following are equivalent for $(a,b)_F$:

1. The algebra is split.

2. The algebra is NOT a division algebra

3. The norm map $N : (a,b)_F \longrightarrow F$ has a nontrivial zero

4. The element b is a norm from the field extension $F(\sqrt{a})/F$, i.e., $b \in N_a$.

Proof: (1) $\Rightarrow$ (2) is immediate from the defn of split. (2) $\Longleftrightarrow$ (3) is the content of the earlier proposition.

To prove (3) $\Rightarrow$ (4), we may assume that a is not a square in F. (Why?)

Suppose that $v = v_0 + v_1 i + v_2 j + v_3 ij$ is a nonzero element w/ $N(v) = 0 = v_0^2 - a v_1^2 - b v_2^2 + ab v_3^2$. Then

$$\underbrace{(v_2^2 - a v_3^2)}_{\text{nonzero since } a \notin F^{\times 2}} b = v_0^2 - a v_1^2.$$

Thus $b = \underbrace{(v_0^2 - a v_1^2)}_{\in N_a} \underbrace{(v_2^2 - a v_3^2)^{-1}}_{\in N_a} \in N_a$ by Lemma.

Finally, we prove (4) $\Rightarrow$ (1): Again assume $a \notin F^{\times 2}$. If $b \in N_a$ then $b^{-1} \in N_a$ too, hence $\exists\, r, s \in F$ s.t.

$$b^{-1} = r^2 - as^2.$$

Let $u = rj + sij$ and $v = (1+a)i + (1-a)ui$. We claim that $\{1, u, v, uv\}$ is a quaternionic basis of $(a,b)_F$. We compute

$$\begin{aligned} u^2 &= r^2 j^2 + rs\,jij + s^2 (ij)^2 + rs\,ij^2 \\ &= br^2 - \cancel{brsi} - abs^2 + \cancel{brsi} \\ &= br^2 - abs^2 \\ &= b(r^2 - as^2) \\ &= b b^{-1} \\ &= 1 \end{aligned}$$

Similarly, one checks that $v^2 = 4a^2$ and that $uv = -vu$. By Exercise 2.4, this implies our claim is true. Thus

$$\begin{aligned} (a,b)_F &\simeq (u^2, v^2)_F \\ &= (1, 4a^2)_F \\ &\simeq M_2(F) \text{ by our earlier Proposition} \quad \blacksquare \end{aligned}$$

<u>Corollary</u>: A quaternion algebra $(a,b)_F$ is either a division algebra over F or it is isomorphic to $M_2(F)$, i.e., split.