QUATERNION ALGEBRAS: SET 5

KEITH CONRAD

1. Write each of the matrices $\left(\begin{smallmatrix} 9 & 5 \\ 7 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 9 & -13 \\ 7 & -10 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 21 & 8 \\ 55 & 21 \end{smallmatrix}\right)$ as products of the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

2. (Constructing units)

a) In $(5,7)_{\mathbf{Q}}$ (with usual basis $1, u, v, w$), show $\mathbf{Z} + \mathbf{Z}(1+u)/2 + \mathbf{Z}(v+w)/2 + \mathbf{Z}w$ is an order and it contains $(5,7)_{\mathbf{Z}}$. Find four pairwise noncommuting units of this larger order which have norm 1 and which do not lie in $(5,7)_{\mathbf{Z}}$.

b) In $(2,3)_{\mathbf{Q}}$, show $\mathbf{Z} + \mathbf{Z}u + \mathbf{Z}(1+v+w)/2 + \mathbf{Z}u(1+v+w)/2$ is an order and it contains $(2,3)_{\mathbf{Z}}$. Find four pairwise noncommuting units of this larger order which have norm 1 and which do not lie in $(2,3)_{\mathbf{Z}}$. Show another $\mathbf{Z}$-basis for this larger order is $\{1, (u+2v+w)/2, (1+v+w)/2, w+2v\}$.

c) Write a typical element of the larger order in part b as

$$q = x_0 + x_1 u + x_2(1+v+w)/2 + x_3 u(1+v+w)/2,$$

where $x_i \in \mathbf{Z}$. Show $\mathrm{N}(q) = x_0^2 + x_0x_2 + x_2^2 - 2(x_1^2 + x_1x_3 + x_3^2)$, so the elements with norm one in this order can be described as the 4-tuples of integers (x_0, x_1, x_2, x_3) that satisfy the equation

$$x_0^2 + x_0x_2 + x_2^2 - 2(x_1^2 + x_1x_3 + x_3^2) = 1.$$

What are the coordinates of q^{-1} when $\mathrm{N}(q) = 1$?

3. (Reduction mod p)

a) For each prime p, reduction mod p gives a group homomorphism $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{F}_p)$. Show this is surjective. That is, any 2×2 integer matrix whose determinant is $\equiv 1 \bmod p$ is the mod p reduction of a 2×2 integer matrix with determinant 1.

b) Let Γ be the norm-one elements of the larger order in part b of exercise 2. We can view Γ as the set of integer solutions to a certain polynomial equation in four variables, as in part c of exercise 2. Reducing the coordinates mod p gives a finite group $\Gamma(\mathbf{F}_p)$ and a group homomorphism $\Gamma \to \Gamma(\mathbf{F}_p)$. Is this onto for all primes p?

4. It was noted in the lectures that any two quaternion algebras over $\mathbf{Q}$ are linked: they can be written as $(c, *)_{\mathbf{Q}}$ for a common $c \in \mathbf{Q}^\times$. Prove $(-1,-1)_{\mathbf{Q}(t)}$ and $(-7,t)_{\mathbf{Q}(t)}$ are unlinked: they can't be written as $(f, *)_{\mathbf{Q}(t)}$ for a common $f \in \mathbf{Q}(t)^\times$.

5. Let $B = (K/F, b)$ be a quaternion *division* algebra over a field F of any characteristic.

a) For every $q \in B^\times$, show the function $R_q \colon B \to B$ given by $R_q(r) = qrq^{-1}$ is an F-algebra isomorphism of B with itself. (These are called *inner automorphisms* of B. Notice the composite of two inner automorphisms is also an inner automorphism. This will be useful in part c.)

b) Suppose $f \colon B \to B$ is an F-algebra isomorphism of B with itself such that f fixes all the elements of K pointwise. Prove $f = R_q$ for some $q \in K^\times$.

c) Suppose $f \colon B \to B$ is an F-algebra isomorphism of B with itself. Prove $f = R_q$ for some $q \in B^\times$. (Hint: Compose f with a suitable inner automorphism to reduce to the case of part b.)

d) In previous parts, B was a division algebra. What if B is split? In other words, is every F-algebra isomorphism of $\mathrm{M}_2(F)$ with itself an inner automorphism, *i.e.*, does it have the form R_q for some $q \in \mathrm{M}_2(F)^\times$?

6. Let Λ be an order in a quaternion algebra over $\mathbf{Q}$. Prove, for each non-zero $m \in \mathbf{Z}$, that up to left multiplication by a unit there are only finitely many $q \in \Lambda$ with norm m. (Hint: Suppose

$N(q_1) = N(q_2) = m$ and $q_1 \equiv q_2 \bmod \Lambda m$. Prove q_1 and q_2 are both right divisors of each other, so $q_1 = \varepsilon q_2$ for some $\varepsilon \in \Lambda^\times$. Note there are only m^4 congruence classes mod Λm.)

Discriminants

For any basis $\mathcal{B} = \{e_1, e_2, e_3, e_4\}$ of a quaternion algebra B over a field F, define its discriminant to be

$$\mathrm{disc}_F(\mathcal{B}) = \det(\mathrm{Tr}(e_i e_j)) \in F.$$

This is the determinant of a 4×4 matrix whose (i, j) entry is $\mathrm{Tr}(e_i e_j)$.

7. (Initial calculations and properties)

a) Show the basis $\{(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}), (\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}), (\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}), (\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix})\}$ of $M_2(\mathbf{R})$ has discriminant -1 and the basis $\{1, i, j, k\}$ of $\mathbf{H}$ has discriminant -16.

b) If $\mathcal{B}' = \{e_1', e_2', e_3', e_4'\}$ is another basis for B, and (a_{ij}) is the change-of-basis matrix expressing the e_i's in terms of the e_i's, show we have an equation of 4×4 matrices

$$(\mathrm{Tr}(e_i' e_j{}')) = (a_{ij})(\mathrm{Tr}(e_i e_j))(a_{ij})^\top.$$

Conclude $\mathrm{disc}_F(\mathcal{B}') = \det(a_{ij})^2 \, \mathrm{disc}_F(\mathcal{B})$, so the discriminants of $\mathcal{B}$ and $\mathcal{B}'$ differ by a non-zero square factor.

c) Use parts a and b to show any basis of a quaternion algebra over $\mathbf{Q}$ has a negative discriminant.

c) Let Λ be an order in a quaternion algebra over $\mathbf{Q}$. Show any two $\mathbf{Z}$-bases of Λ have the same discriminant. This common value is called the discriminant of Λ.

d) For non-zero integers a and b, show the order $(a, b)_{\mathbf{Z}}$ in $(a, b)_{\mathbf{Q}}$ has discriminant $-16a^2b^2$.

8. Show the discriminant of $M_2(\mathbf{Z})$ is -1 and the discriminant of the Hurwitz order $\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}(1 + i + j + k)/2$ in $\mathbf{H}(\mathbf{Q})$ is -4.

9. For two orders Λ_1 and Λ_2 in a quaternion algebra B over $\mathbf{Q}$, with $\Lambda_1 \subset \Lambda_2$, the following results are known:

- $\mathrm{disc}(\Lambda_2) | \mathrm{disc}(\Lambda_1)$
- if $\mathrm{disc}(\Lambda_1) = \mathrm{disc}(\Lambda_2)$, then $\Lambda_1 = \Lambda_2$.

a) Conclude from these properties and earlier exercises that every order in B is contained in a *maximal order*, which is an order contained in no larger order. (Hint: minimize the absolute value of a discriminant containing the given order.) Show $M_2(\mathbf{Z})$ in $M_2(\mathbf{Q})$ and the Hurwitz order in $\mathbf{H}(\mathbf{Q})$ are examples of maximal orders.

b) While B has many maximal orders, a difficult theorem says all *maximal* orders in B have the same discriminant. This common value is called the discriminant of B. (For example, the discriminant of $\mathbf{H}(\mathbf{Q})$ is -4.) A further difficult theorem says this common discriminant of any maximal order in B is always of the form $-d^2$ where d is a product of distinct primes, and that every quaternion algebra over $\mathbf{Q}$ is determined up to isomorphism by its discriminant.

Use these facts and your earlier work to show the order $(a, b)_{\mathbf{Z}}$, for integers a and b, is never a maximal order. (Thus maximal orders never admit a quaternionic $\mathbf{Z}$-basis.) Also show that the only quaternion *division* algebra over $\mathbf{Q}$ which can be written in the form $(a, b)_{\mathbf{Q}}$ and $(c, d)_{\mathbf{Q}}$ for integers a, b, c, d with ab relatively prime to cd is $\mathbf{H}(\mathbf{Q})$. (Recall from exercises 2 and 3 on set 3 that $\mathbf{H}(\mathbf{Q}) \cong (-2, -3)_{\mathbf{Q}} \cong (-5, -29)_{\mathbf{Q}}$.)

10. Consider the following alternate definition of the discriminant of a basis $\{e_1, e_2, e_3, e_4\}$ of a quaternion algebra: $\det(\mathrm{Tr}(e_i \overline{e}_j))$. How do its properties compare to the previous discriminant? Are these two kinds of discriminants always related in a definite way?