Quadratic Forms (Math 520/620/702)

Problem Set #3 Due Wed., Nov. 9, 2011, in class.

1. Let $\mathbb{H}$ be the usual (Hamiltonian) quaternion algebra over $\mathbb{R}$.

a) Show by example that a polynomial of degree n over $\mathbb{H}$ can have more than n roots in $\mathbb{H}$.

b) Explain where the usual proof that this cannot happen in a field breaks down in the division algebra $\mathbb{H}$.

c) Explain why a factorization $f(X) = g(X)h(X)$ of polynomials over $\mathbb{H}$ does not in general imply that $f(c) = g(c)h(c)$ for $c \in \mathbb{H}$, though it does if the coefficients of f, g, h lie in $\mathbb{R}$. [Note: this is related to part (b).]

2. Let $f(X) \in \mathbb{R}[X]$.

a) Show that if $\alpha \in \mathbb{H}$ is a root of $f(X)$, then so is $\beta\alpha\beta^{-1}$ for all $\beta \in \mathbb{H}^\times$.

b) Find all the square roots of -1 in $\mathbb{H}$, and show that this is consistent with part (a).

3. Let $a \in \mathbb{H}$.

a) Write $f(X) = X^2 - a$, $\bar{f}(X) = X^2 - \bar{a}$, and $F(X) = \bar{f}(X)f(X)$. Show that $F(X) \in \mathbb{R}[X]$, and that $F(X)$ has a root α in $\mathbb{C} = \mathbb{R}[i] \subset \mathbb{H}$.

b) Show by direct computation that if $c := f(\alpha) \neq 0$ then $\beta := \overline{c\alpha c^{-1}}$ is a root of $f(X)$.

c) Conclude that a has a square root in $\mathbb{H}$.

[Note: This argument can be generalized to show that $\mathbb{H}$ is "algebraically closed" as a division algebra.

4. Let $a \in \mathbb{H}$ such that $a \notin \mathbb{R}$.

a) Show that $K := \mathbb{R}(a) \subset \mathbb{H}$ is a degree two field extension of $\mathbb{R}$; that K is a maximal subfield of $\mathbb{H}$; and that the centralizer $C_{\mathbb{H}}(K) = K$.

b) Show that a has *exactly* two square roots in $\mathbb{H}$. [Hint: Show that any square root of a must commute with a and must therefore lie in K, which is a field.]

c) Where did you use that $a \neq \mathbb{R}$? What happens if $a \in \mathbb{R}$?

5. Let M be the $n \times n$ matrix over $\mathbb{Z}[X_1, \dots, X_n]$ whose (i,j) entry is X_i^{j-1}.

a) Show that the determinant of M is equal to $\prod_{i>j}(X_i - X_j)$. [Hint: Show that $X_i - X_j$ divides the determinant for all $i < j$, and consider the degrees of the polynomials.]

b) Deduce that if $z_1, \dots, z_n$ are distinct elements of a field L, then the vectors $v_i := (1, z_i, \dots, z_i^{n-1})$, for $i = 1, \dots, n$, are linearly independent in L^n.

c) Let $\beta, z \in L^\times$ be such that $1, z, \dots, z^{n-1}$ are distinct, and let N be the $n \times n$ diagonal matrix over L with diagonal entries $\beta, \beta z, \beta z^2, \dots, \beta z^{n-1}$. Show that the matrices $I, N, N^2, \dots, N^{n-1}$ are linearly independent. [Hint: Use (b).]

d) Let $a \in L^\times$ and let $M = (m_{ij})$ be the $n \times n$ matrix over L with $m_{i,i+1} = 1$ for $1 \leq i < n$; $m_{n,1} = a$; and $m_{ij} = 0$ otherwise. Show that the (i,j) entry of M^r is non-zero if and only if $j \equiv i + r \pmod{n}$. Deduce that if $\sum_{i,j=1}^n c_{ij} M^i N^j = 0$ for some choice of n^2 elements $c_{ij} \in L^\times$, then the matrices $S_i := \sum_{j=1}^n c_{ij} M^i N^j$ are equal to 0 for all $i = 1, \dots, n$. [Hint: Which entries of S_i can be non-zero?]

6. Let K be a field that contains a primitive n-th root of unity ζ. Let $a, b \in K^\times$, and let $\beta \in L := \bar{K}$ be an n-th root of b in the algebraic closure (so $\beta \in L^\times$). Consider the K-algebra A with generators u, v and relations $u^n = a$, $v^n = b$, $uv = \zeta vu$.

a) Let M, N be the $n \times n$ matrices over L given in parts (c),(d) of problem 5, with $z = \zeta$. Show that $M^n = aI$, $N^n = bI$, and $MN = \zeta NM$. (Here I is the $n \times n$ identity matrix.) Use this to find a surjective K-algebra homomorphism h from A to the K-algebra $A' \subseteq M_n(\bar{K})$ that is generated by M, N.

b) Show that for each $i = 1, \dots, n$, the n matrices $M^i N^j$ (for $j = 1, \dots, n$) are linearly independent. Then deduce that the n^2 matrices $M^i N^j$ (for $i, j = 1, \dots, n$) are linearly independent. [Hint: First use 5(c); then use 5(d).]

c) Find the dimensions of A and A' over K, and then show that $h : A \to A'$ is an isomorphism of K-algebras.

d) Show that A' is a simple K-algebra. [Hint: Show that $A' \otimes_K L$ is isomorphic to $M_n(L)$, and then consider $I \otimes_K L$ for any ideal $I \subset A'$.]

e) Deduce that A is a central simple algebra over K. [Hint: Show that A' is central, by considering the center of the tensor product $A' \otimes_K L$.]

f) What does this say if $n = 2$?

7. Fill in the details of Examples 2.13 and 2.17 in Chapter III of Lam. (In particular, in 2.13, show that the two norm forms in the display are isometric as claimed, and that 7 is not a sum of three squares in the field $\mathbb{Q}$.)

8. Do the following problems from Lam, Chapter III (pages 75-77):

a) Exercise 2.

b) Exercise 5.

c) Exercise 6. [Hint: Use equivalent conditions for a quaternion algebra to be split.]