Topics in Algebra – Math 702

Problem Set #3

1. Let M be the $n \times n$ matrix over $\mathbb{Z}[X_1, \ldots, X_n]$ 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, \ldots, z_n are distinct elements of a field L, then the vectors $v_i := (1, z_i, \ldots, z_i^{n-1})$, for $i = 1, \ldots, n$, are linearly independent in L^n . c) Let $\beta, z \in L^{\times}$ be such that $1, z, \ldots, z^{n-1}$ are distinct, and let N be the $n \times n$

c) Let $\beta, z \in L^{\times}$ be such that $1, z, \ldots, z^{n-1}$ are distinct, and let N be the $n \times n$ diagonal matrix over L with diagonal entries $\beta, \beta z, \beta z^2, \ldots, \beta z^{n-1}$. Show that the matrices $I, N, N^2, \ldots, N^{n-1}$ 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 $i = 1, \ldots, n$. [Hint: Which entries of S_i can be non-zero?]

2. Let K be a field that contains a primitive n-th root of unity ζ . Let $a, b \in K^{\times}$, and let $\beta \in L := \overline{K}$ 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 1, 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, ..., n, the *n* matrices $M^i N^j$ (for j = 1, ..., n) are linearly independent. Then deduce that the n^2 matrices $M^i N^j$ (for i, j = 1, ..., n) are linearly independent. [Hint: First use 1(c); then use 1(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?

3. Let A be a central simple algebra over F, and let E be a field that contains F and is contained in A.

a) Show that the centralizer $C_A(E)$ contains E, and is an E-algebra.

b) Show that $\dim_F(C_A(E)) = \dim_E(C_A(E))[E:F].$

c) Deduce that [E : F] divides the degree of the *F*-algebra *A*, with equality if and only if $C_A(E) = E$. [Hint: What is $\dim_F(E) \cdot \dim_F(C_A(E))$?]

d) Show that if [E:F] is equal to the degree of A, then E is a maximal subfield of A (i.e. E is not strictly contained in any other field E' with $F \subseteq E' \subseteq A$).

e) Show that if A is a division algebra over F then the converse of (d) holds. [Hint: If not, show there exists $a \in C_A(E)$ that does not lie in E, and consider $E(a) \subseteq A$.]

4. a) Let D be a non-commutative division ring that is also a finite dimensional \mathbb{R} algebra. Show that the center must be \mathbb{R} , and hence D is a (central) division algebra over \mathbb{R} . [Hint: If not, D is a non-trivial central simple algebra over the field Z(D). What can
that field be?]

b) Let E be a maximal subfield of the \mathbb{R} -division algebra D. Show that $E \cong \mathbb{C}$ and that the degree of D over \mathbb{R} is 2. Deduce that D is a quaternion algebra over \mathbb{R} .

c) Conclude that $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. (This proves a theorem due to Frobenius.)