ISRAEL JOURNAL OF MATHEMATICS, Vol. 63, No. 1, 1988

THE CENTERS OF GENERIC DIVISION ALGEBRAS WITH INVOLUTION

BY

ALLAN BERELE[†] AND DAVID J. SALTMAN[††]

Department of Mathematics, DePaul University, Chicago, IL 60614, USA; and Department of Mathematics, The University of Texas at Austin, Austin, TX 78712, USA

ABSTRACT

The main goal of this paper is a study of the centers of the generic central simple algebras with involution. These centers are shown to be invariant fields under finite groups in a way analagous to the center of the generic division algebras. The centers of the generic central simple algebras with involution are also described as generic splitting fields (i.e. function fields of Brauer–Severi varieties) over the centers of generic division algebras. Finally, a generic central simple algebra is described for the class of central simple algebras with subfields of a certain dimension.

Introduction

Let $R = R(F, n, k)$ be the ring of generic matrices over an infinite field F, viewed as follows. Form the polynomial ring $S = F[x_{ij}^{(r)} \mid 1 \leqq i, j \leqq n$ and $1 \leqq r \leqq k]$. Let $X_r \in M_n(S)$ be the matrix with (i,j) entry $x_{ij}^{(r)}$. R is the F subalgebra of $M_n(S)$ generated by the "generic" matrices X_r. As is well known, R is a domain with a central quotient ring $UD(F, n, k)$ which is a division ring, and can be viewed as a subring of $M_n(K)$ where K is the field of fractions of S. The algebra $M_n(K)$ has two well known involutions, called the transpose and skew involutions, which will be explicitly defined in the first section. Let T, S denote these involutions respectively. We define $R^T = R^T(F, n, k) \subseteq M_n(S)$ to be the F algebra generated by the X's and the X^T's. We make a similar definition for $R^S(F, n, k)$. Both R^T and R^S are prime rings with central simple

[†] The first author would like to thank the Department of Mathematics of The University of Texas at Austin for its hospitality and the NSF for its support under grant DMS 585-05767.

[††] The second author would like to thank the NSF for its support under grants DMS 8303356 and DMS 8601279.

Received September 3, 1987 and in revised form February 29, 1988

rings of quotients $UD^T(F, n, k)$ and $UD^S(F, n, k)$ respectively. Obviously, R^T and UD^T are closed under T, while R^S and UD^S are closed under S. It is known that the UD's are division rings when n is a power of 2, and that, in any case, they are "generic central simple algebras with involution".

The main goal of this paper is a study of the centers $Z^T(F, n, k)$ and $Z^S(F, n, k)$ of UD^T and UD^S respectively. In the first section, these centers are shown to be invariant fields under finite groups in a way analagous to the known description (due to Procesi [P]; see also [F] whose treatment we have followed) of the center, $Z(F, n, k)$, of $UD(F, n, k)$. In the second section, the field extensions $Z^T(F, n, k)/Z(F, n, k)$ and $Z^S(F, n, k)/Z(F, n, k)$ are shown to be certain generic splitting fields, that is, to arise from the function fields of Brauer Severi varieties. In particular, Z^S can be viewed as a subfield of Z^T and Z^T/Z^S is a rational (purely transcendental) field extension.

In the third section, the ideas of the first section are used in a slightly different setting. In that section, a generic division algebra is described which is generic for the class of division algebras with a subfield of a certain dimension. Its center is also described as the invariant field of a finite group.

Let us mention some notation and definitions. We will say A/F is a central simple algebra when A is simple and finite dimensional over its center the field F. An involution $J: A \to A$ which fixes F is said to be of transpose (skew) type if the following holds. Let $L \supseteq F$ be a splitting field for A. Then there are matrix units for $A \otimes_F L$ such that $J \otimes I$ is the transpose (skew) involution with respect to those units. All involutions of a central simple algebra are of either transpose or skew type, and not both. If U is any commutative ring, let $M_n(U)$ denote the ring of $n \times n$ matrices over U. If $\psi: U \to V$ is any ring homomorphism, let $M_n(\psi): M_n(U) \to M_n(V)$ denote the induced homomorphism of matrix algebras.

For $n > 1$ any integer, let S_n be the symmetric group on n elements. If G is any group, let $G' = G \oplus \cdots \oplus G$ be the n fold direct sum of G. S_n acts on G' by permuting the direct summands and we can define the wreath product $G \wr S_n$ as the semidirect product of G' and S_n. In section one, we will be especially interested in $B_n = S_2 \wr S_n$ and $\bar{B}_n = (Z/4Z) \ S_n$. In section three, we will encounter $S_a \wr S_b$ for any a and b.

Section One: Splitting fields and Galois groups

Let F be a field of characteristic zero, let V be an n-dimensional vector space over F and let $\langle \ , \ \rangle$ be a nondegenerate bilinear form on V which

is either symmetric or skew symmetric. If $n = 2p$ is even, then V has a basis $e_1, \ldots, e_p, f_1, \ldots, f_p$ such that, for all i, $\langle e_i, f_i \rangle = \pm \langle f_i, e_i \rangle = 1$ and all other products of basis elements are zero; and if $n = 2p + 1$ is odd, then V has a basis $e_1, \ldots, e_p, f_1, \ldots, f_p, g$ such that, for all i, $\langle e_i, f_i \rangle = \langle f_i, e_i \rangle = \langle g, g \rangle = 1$ and all other products of basis elements are zero. (If n is odd there is no nondegenerate skew symmetric form on V.) This bilinear form and basis induce an adjunction on $n \times n$ matrices in a standard manner. Explicitly, if $A = (a_{ij})$ has adjoint $B = (b_{ij})$, then

$$b_{ij} = \begin{cases} a_{j+p,i+p} & \text{if } 1 \leqq i, j \leqq p \\ \pm a_{j-p,i+p} & \text{if } 1 \leqq i \leqq p, p+1 \leqq j \leqq 2p \\ \pm a_{j+p,i-p} & \text{if } p+1 \leqq i 2p, 1 \leqq j \leqq p \\ a_{j-p,i-p} & \text{if } p+1 \leqq i, j \leqq 2p \end{cases}$$

where the signs depend on whether the inner product is symmetric or skew; and if $n = 2p + 1$, then $b_{n,j} = a_{j \pm p,n}$, $b_{i,n} = a_{n,i \pm p}$ and $b_{n,n} = a_{n,n}$, for $1 \leqq i$, $j \leqq 2p$. This adjunction will be regarded as an involution $*$, and can be extended to $n \times n$ matrices over any extension field of F. When it is necessary to distinguish, we will denote $*$ as T in the symmetric case and S in the skew case.

Now fix an integer $k > 1$. Let R be the F-algebra generated by the k generic $n \times n$ matices $X_1, \ldots, X_k \in M_n(F[x_{ij}^{(r)}])$ together with their adjoints $X_1^*, \ldots, X_k^*$. R is a prime p.i. algebra with involution and so it may be embedded in a quotient ring Q by Posner's theorem. Q is a central simple algebra with involution, but it will be a division algebra only if n is a power of 2. Let C be the center of R, Z the center of Q. Z is the field of fractions of C. When necessary, we will use the more precise notation of $Z = Z^S(F, n, k)$ or $Z = Z^T(F, n, k)$. Our main result in this section is that Q is split by a rational function field L with $\mathrm{Gal}(L/Z) = B_n$. This affords a fairly explicit description of Z.

The first step is to make a "change of model", i.e., to replace R with an algebra isomorphic to it which will prove easier to work with. Let $S_1, \ldots, S_k$ be generic symmetric $n \times n$ matrices and $K_1, \ldots, K_k$ be generic skew symmetric $n \times n$ matrices. For example, we could take $S_i = X_i + X_i^*$ and $K_i = X_i - X_i^*$ for all $i = 1, \ldots, k$. Now $R \cong F[S_1, \ldots, S_k, K_1, \ldots, K_k]$ and we shall use the two interchangeably. The following two lemmas provide a less obvious isomorphic image of R.

LEMMA 1.1. *Let K_1 be a generic skew symmetric $n \times n$ matrix. Then K_1 has distinct eigenvalues and so is diagonalizable.*

PROOF. Without loss of generality we may take K_1 to be $X_1 - X_1^*$.

If the lemma were false then K_1 would satisfy some monic degree n polynomial $f(x)$ which had multiple roots in some extension field. Also, if $\phi: F[x_{ij}^{(1)}] \to L$ is any F-homomorphism, then $\phi(K_1)$ would also satisfy $f(x)$. Let $\lambda_1, \ldots, \lambda_p$ be independent indeterminants and define $\phi: F[x_{ij}^{(1)}] \to F(\lambda_1, \ldots, \lambda_p)$ by $\phi(x_{ij}^{(1)}) = 0$ if $i \neq j$ or $i = j \geqq p+1$ and $\phi(x_{ii}) = \lambda_i$ if $1 \leqq i = j \leqq p$. Then if n is even $\phi(K_1)$ is the diagonal matrix $\operatorname{diag}(\lambda_1, \ldots, \lambda_p, -\lambda_1, \ldots, -\lambda_p)$ and if n is odd then $\phi(K_1)$ is the diagonal matrix $\operatorname{diag}(\lambda_1, \ldots, \lambda_p, -\lambda_1, \ldots, -\lambda_p, 0)$. In either case $\phi(K_1)$ satisfies no degree n equation with multiple roots and the lemma is proven.

We define G to be the group $\{A \in \mathrm{GL}(V) \mid \langle Av, Aw \rangle = \langle v, w \rangle$ for all $v, w \in V\}$, possibly over an extension field of F. So G is either the symplectic group $\mathrm{Sp}(n)$ in the case $* = S$ or orthogonal group $\mathrm{O}(n)$ in the case $* = T$.

LEMMA 1.2. *Let K_1 be a generic skew symmetric matrix and G as above. Then there exists $A \in G$ such that AK_1A^{-1} is a diagonal matrix.*

PROOF. Extending scalars, let $v_1, \ldots, v_n$ be a basis of eigenvectors for K_1 with eigenvalues $\lambda_1, \ldots, \lambda_n$. Since $\langle \ , \ \rangle$ is non-degenerate, for each v_i there is at least one v_j with $\langle v_i, v_j \rangle \neq 0$. We now calculate

$$\lambda_i \langle v_i, v_j \rangle = \langle \lambda_i v_i, v_j \rangle = \langle K_1 v_i, v_j \rangle = \langle v_i, K_1^* v_j \rangle$$

$$= \langle v_i, -K_1 v_j \rangle = \langle v_i, -\lambda_j v_j \rangle = -\lambda_j \langle v_i, v_j \rangle.$$

Hence $\lambda_i = -\lambda_j$.

If $n = 2p$ is even then, since the eigenvalues are distinct, we may enumerate the eigenvectors as $v_1, \ldots, v_p, w_1, \ldots, w_p$ where $K_1 v_i = \lambda_i v_i$ and $K_1 w_i = -\lambda_i w_i$. By the above calculation and a normalization we may conclude that $\langle v_i, w_i \rangle = \pm \langle w_i, v_i \rangle = 1$ and all other products of basis elements are zero. Now if A is the change-of-basis matrix from $\{e_1, \ldots, e_p, f_1, \ldots, f_p\}$ to $\{v_1, \ldots, v_p, w_1, \ldots, w_p\}$ then A preserves the inner product and AKA^{-1} is diagonal.

The case of $n = 2p + 1$ is entirely similar. In this case the new basis will be $v_1, \ldots, v_p, w_1, \ldots, w_p, z$ and z will correspond to the eigenvalue zero. We omit the details in this case.

Let Λ be a generic skew symmetric diagonal matrix,

$$\Lambda = \operatorname{diag}(\lambda_1, \ldots, \lambda_p, -\lambda_1, \ldots, -\lambda_p) \quad \text{or} \quad \operatorname{diag}(\lambda_1, \ldots, \lambda_p, -\lambda_1, \ldots, -\lambda_p, 0).$$

Let $R' = F[\Lambda, K_2, \ldots, K_k, S_1 \ldots, S_k]$ be the algebra gotten from R by replacing K_1 by Λ, let Q' be the quotient ring of R' and Z' the center of Q'. The following is known, but a reference is diffcult to find.

THEOREM 1.3. *There is an F-isomorphism from R to R' preserving* $*$. *Hence Q is isomorphic to Q' and Z to Z'.*

PROOF. Let A be as in the previous lemma. Since $A \in G$, $(ABA^{-1})^* = AB^*A^{-1}$ for any matrix B. It is now easy to see that $ARA^{-1} \cong R'$.

Hence we may replace R by R' for the remainder of this section without affecting the properties of Z. Before we can discuss Z directly we need to construct some B_n modules.

LEMMA 1.4. (a) *B_n may be embedded in O_{2n} and O_{2n+1}.*

(b) *$\bar{B}_n$ may be embedded in Sp_{2n}.*

(c) *Let $H \subset \bar{B}_n$ be the subgroup $\{(h_1, \ldots, h_n; \mathrm{id}) \mid h_1, \ldots, h_n \in 2Z/4Z\}$. Then $\bar{B}_n/H \cong B_n$.*

PROOF. (a) We identify B_n with a set of permutations of the basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$. Define Y via $Y(e_i) = f_i$ and $Y(f_i) = e_i$, $i = 1, \ldots, n$. Then B_n is isomorphic to the set of permutations of $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ which commute with Y. Explicitly, if $\varepsilon_1, \ldots, \varepsilon_n \in Z/2Z$ and $\sigma \in S_n$ so $(\varepsilon_1, \ldots, \varepsilon_n; \sigma) \in Z/2Z \wr S_n = B_n$ then $(\varepsilon_1, \ldots, \varepsilon_n; \sigma)e_i = Y^{\varepsilon_{\sigma(i)}} e_{\sigma(i)}$ and $(\varepsilon_1, \ldots, \varepsilon_n; \sigma) f_i \in Y^{\varepsilon_{\sigma(i)}} f_{\sigma(i)}$. Each such permutation can be extended by linearity to all of V, fixing g in the odd case. This gives the desired embedding.

(b) Let $Y: V \to V$ be given by $Y(e_i) = f_i$ and $Y(f_i) = -e_i$, $i = 1, \ldots, n$. Note that $Y^4 = I$. As above, the action of $\bar{B}_n = Z/4Z \wr S_n$ on V is defined by $(g_1, \ldots, g_n; \sigma)e_i = Y^{g_{\sigma(i)}} e_{\sigma(i)}$ and $(g_1, \ldots, g_n; \sigma) f_1 = Y^{g_{\sigma(i)}} f_{\sigma(i)}$. Again we leave to the reader the verification that this gives an embedding of $\bar{B}_n$ into $\mathrm{Sp}(V)$.

(c) Identifying $Z/2Z$ with $2Z/4Z$ we map $\bar{B}_n$ onto B_n via $(g_1, \ldots, g_n; \sigma) \to (2g_1, \ldots, 2g_n; \sigma)$. The kernel will be H.

The significance of belonging to Sp or O lies in the following familiar lemma.

LEMMA 1.5. *Let T be either a generic symmetric matrix or a generic skew symmetric matrix with entries $\{Y_\alpha\}$, and let $A \in G$. Then there is a well-defined automorphism of $F[Y_\alpha]$ given by: for all (i, j) the (i, j)-entry of T is mapped to the (i, j)-entry of ATA^{-1}.*

PROOF. It is only necessary to check that if the (i, j)-entry of T equals plus or minus the (i', j')-entry then the (i, j)- and $(i'-, j')$-entries of ATA^{-1} will also be equal or inverse. If $T^* = \pm T$ then, since $A^* = A^{-1}$, $(ATA^{-1})^* = \pm ATA^{-1}$.

But, since T is generic among symmetric or skew symmetric matrices, T specializes to ATA^{-1} and so relations among the entries of T also hold among the entries of ATA^{-1}.

At this point we need to distinguish between the cases in which the inner product used to define R is symmetric or alternating. We handle the symmetric case first.

Enumerate $\Lambda, S_1, X_2, X_2^*, \ldots, X_k, X_k^*$ as $U_1, \ldots, U_{2k}$ and let $u_{ij}^{(r)}$ denote the (i,j)-entry of U_r, $i,j = 1, \ldots, n$, $r = 1, \ldots, 2k$. These entries are not all distinct or even all nonzero. Let M be the (multiplicative!) group generated by all nonzero products $u_{i_1i_2}^{(r_1)}u_{i_2i_3}^{(r_2)}\cdots u_{i_mi_1}^{(r_m)}$. (Note that there are m equalities of indices.) This $u_{i_1i_2}^{(r_1)}\cdots u_{i_mi_1}^{(r_m)}$ is a monomial in the (i_1, i_1) entry of $U_{r_1}\cdots U_{r_m}$. We claim that M is a module over B_p where $p = [n/2]$. If $\sigma \in B_p$ we can think of σ as a matrix $A \in O_n$ as in Lemma 4(a) or as an element of the symmetric group S_{2p} identifying $\{e_1, \ldots, e_p, f_1, \ldots, f_p\}$ with $\{1, \ldots, n\}$. Now define $\sigma(u_{ij}^{(r)}) =$ the (i,j)-entry of AU_rA^{-1}. It is easy to verify that $Ae_{ij}A^{-1} = e_{\sigma i,\sigma j}$ and so A takes $u_{ij}^{(r)}$ to $u_{\sigma i,\sigma j}^{(r)}$. We claim that this gives a well-defined action of B_p on $F[u_{ij}^{(r)}]_{i,j,r}$. The issue involved in proving that this action is well-defined is that the letters $u_{ij}^{(r)}$ are not all independent by virtue of the relations

(1) $U_1^* = -U_1$, $U_2^* = U_2$,

(2) $U_{2r} = U_{2r+1}^*$, $r = 1, \ldots, k-1$,

(3) U_1 is diagonal.

However, since $B_p \subseteq O_n$, conjugation by B_p preserves the involution and so preserves (1) and (2) and the corresponding relations among the $u_{ij}^{(r)}$. Moreover, since $\sigma(u_{i,j}^{(1)}) = u_{\sigma i,\sigma j}^{(1)}$, the operation will permute the zero entries of U_1 amongst themselves. And so the action is well-defined. The permutation definition of the action also makes it clear that $F(M) \subseteq F(u_{ij}^{(r)})_{i,j,r}$, the field generated by F and M, is a faithful B_p-submodule.

A bit more is true: if r is any element of R and if $f =$ the (i,j)-entry of r, then $\sigma(f) =$ the (i,j)-entry of ArA^{-1}.

The symplectic case is more subtle. The module M is defined as above. Since $\bar{B}_p \subseteq \mathrm{Sp}_n$, $n = 2p$, we may define a $\bar{B}_p$ action on $F(u_{ij}^{(r)})$ by conjugation as above.

The embedding of $\bar{B}_p$ into Sp_n described in Lemma 4(b) has the property that if the linear transformation $A \in \mathrm{Sp}_n$ corresponds to an element of $\bar{B}_p$ then A takes each basis element to plus or minus another basis element. Hence there is a permutation $\sigma \in S_n$ such that $Ae_{ij}A^{-1} = \pm e_{\sigma i,\sigma j}$. To describe the sign, consider the case in which $Y(e_i) = f_i$, $Y(f_i) = -e_i$ and Y acts as identity on all other basis elements. Then, in $Ye_{ij}Y^{-1} = \pm e_{\sigma(j)\sigma(k)}$ the sign will be minus

precisely when one of the indices j, k corresponds to the basis element f_i. Hence, if such a Y acts on an element of M the sign will be plus, since each index occurs an even number of times. Likewise, if any element of $\bar{B}_p$ acts on any element of M the sign will be positive. And it follows as before that $F(u_{ij}^{(r)})_{i,j,r}$ is a well-defined $\bar{B}_p$ module and that M is a submodule. Note, moreover, that elements of H are represented by diagonal matrices and so act trivially on elements of M, which are diagonal entries. Finally, if $(g_1, \ldots, g_h; \sigma) \notin H$, then $\sigma \notin \mathrm{id}$ or some $g_i \notin 2Z$. If $g_i \notin 2Z$ then the corresponding A takes e_i to $\pm f_{\sigma(i)}$ and if $\sigma(i) \neq i$ then the corresponding A takes e_i to $\pm e_{\sigma i}$ or $\pm f_{\sigma i}$ and so A will not act trivially on M by conjugation.

We have now proven the following basic lemma:

LEMMA 1.6. *Let* $(U_1, \ldots, U_{2k}) = (\Lambda, S_1, X_2, X_2^*, \ldots, X_k, X_k^*)$ *and write* $u_{ij}^{(r)}$ *for the* (i,j)*-entry of* U_r*, Let* $M =$ *the abelian group generated by all products of the form* $u_{i_1 i_2}^{(r_1)} u_{i_2 i_3}^{(r_2)} \cdots u_{i_m u_1}^{(r_m)}$*. Then there is a well-defined, faithful action of* B_p *on* M*.*

The main theorem of this section is

THEOREM 1.7. $F(M)^{B_p} = Z$*, the center of* Q*.*

In order to prove this theorem we require one more lemma.

LEMMA 1.8. *Let*

$$\Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_p, -\lambda_1, \ldots, -\lambda_p) \quad \textit{or} \quad \mathrm{diag}(\lambda_1, \ldots, \lambda_p, -\lambda_1, \ldots, -\lambda_p, 0).$$

Then the degree of $Z(\lambda_1, \ldots, \lambda_p)$ *over* Z *is* $\leqq 2^p p!$.

PROOF. Consider the inclusion fields $Z \subseteq Z(\lambda_1^2, \ldots, \lambda_p^2) \subseteq Z(\lambda_1, \ldots, \lambda_p)$. The degree of the second inclusion $Z(\lambda_1, \ldots, \lambda_p)/Z(\lambda_1^2, \ldots, \lambda_p^2)$ is $\leqq 2^p$. For the first extension note that, by the Cayley–Hamilton theorem $\det(xI - \Lambda) \in Z[x]$. And, $\det(xI - \Lambda) = \Pi_{i=1}^{p}(x^2 - \lambda_i^2)$ or $x\,\Pi_{i=1}^{p}(x^2 - \lambda_i^2)$ so $\Pi_{i=1}^{p}(x^2 - \lambda_i^2) \in Z[x]$. Therefore the degree of $Z(\lambda_1^2, \ldots, \lambda_p^2)$ over Z is $\leqq p!$. The lemma follows.

PROOF OF THEOREM 1.7. Since B_p acts on R by conjugation all central elements are fixed and so $Z \subseteq F(M)^{B_p}$.

Now let $\tilde{Z} = Z(\lambda_1, \ldots, \lambda_p)$ be as in the previous lemma. We claim that each of the primitive idempotents $e_{11}, \ldots, e_{nn}$ is contained in $Q \otimes_Z \tilde{Z}$. If $n = 2p$ is even and $i \leqq p$ then

$$e_{ii} = (\Lambda + \lambda_i I) \prod_{j \neq i} (\Lambda - \lambda_j I)(\Lambda + \lambda_j I)/2\lambda_i \prod_{j \neq i} (\lambda_j^2 - \lambda_i^2).$$

The case of $p + 1 \leqq i \leqq 2p$ is similar with the factor of $(\Lambda + \lambda_i I)$ replaced by $(\Lambda - \lambda_i I)$. If $n = 2p + 1$ is odd, then for $i \leqq 2p$ the above formulas are modified by multiplying the right hand sides by a factor of Λ/λ_i and

$$e_{nn} = \prod_{i=1}^{p} (\Lambda - \lambda_i)(\Lambda + \lambda_i) \Big/ \prod_{i=1}^{p} (-\lambda_i^2).$$

Moreover, $u_{ij}^{(r)} e_{ij} = e_{ii} X^{(r)} e_{jj} \in Q \otimes \bar{Z}$ and so each

$$u_{i_1 i_2}^{(r_1)} \cdots u_{i_m i_1}^{(r_m)} e_{i_1 i_1} \in Q \otimes \bar{Z}.$$

If the indices $i_1, \ldots, i_m$ contain all of the integers $1, \ldots, n$ then, since each $u_{i_1 i_2}^{(r_1)} \cdots u_{i_m i_m}^{(r_m)} e_{i_j i_j} \in Q \otimes \bar{C}$ we have $u_{i_1 i_2}^{(r_1)} \cdots u_{i_m i_1}^{(r_m)} I \in$ the center of $Q \otimes \bar{C}$, which equals $\bar{C}$. But every element of M is a quotient of such terms and so $F(M) \subseteq \bar{C}$.

Now consider the inclusions

$$Z \subseteq F(M)^{B_p} \subseteq F(M) \subseteq \bar{Z}.$$

By Galois theory $\deg(F(M)/F(M)^{B_p}) = O(B_p) = 2^p \cdot p!$ But, by the preceding lemma $\deg(\bar{Z}/Z) \leqq 2^p \cdot p!$ and hence $Z = F(M)^{B_p}$ and $\bar{Z} = F(M)$.

COROLLARY 1.9. *Q is split by $F(M)$, with Galois group* $\mathrm{Gal}(F(M)/Z) = B_p$. *Hence, every simple algebra with involution of first kind and dimension n^2 is split by a subgroup of B_p.*

QUESTION. If Q is a simple algebra of dimension n^2 and prescribed exponent $k < n$ in the Brauer group is it possible to draw any conclusions about the splitting fields for Q and their Galois groups?

We conclude this section with a calculation of the transcendence degree of Z over F. In order to do this we need the following straight-forward lemma which we state without proof.

LEMMA 1.10. *Let $F(g_1, \ldots, g_n)$ be a purely transcendental field extension of F. Suppose M is a subgroup of the multiplicative group generated by the g_i's. Let L be the subfield of $F(g_1, \ldots, g_n)$ generated by F and M. Then the transcendence degree of L/F equals the rank of M.*

THEOREM 1.11. (a) *If the involution is of transpose type then* $\mathrm{tr.deg}(Z/F) = (k-1)n^2 + \binom{n+1}{2}$.

(b) *If the involution is of symplectic type then* $\operatorname{tr.deg}(Z/F) = (k-1)n^2 + n^2/2 - n/2$.

PROOF. (a) Assume n is even. Since $F(M)$ is a finite extension of Z, $\operatorname{tr.deg} Z = \operatorname{tr.deg} F(M) = \operatorname{rank} M$. In order to calculate the rank of M we define two subgroups $A, B \subseteq M$ with the properties

(i) $A \cap B = (1)$,

(ii) $\operatorname{rk} A = (k-1)n^2 + n^2/2 + 1$, $\operatorname{rk} B = n/2 - 1$,

(iii) $A + B = M$.

To define A, first let K be the free abelian group generated by the alphabet

$$\{\lambda_i\}_{i=1}^{p} \cup \{x_{ij}^{(r)} \mid i,j = 1,\dots,n,\ r = 2,\dots,k\}$$
$$\cup \{s_{ij}\}_{i,j=1}^{p} \cup \{s_{ij} \mid i = p+1,\dots,2p,\ j = 1,2,\dots,j-p\}$$
$$\cup \{s_{ij} \mid j = p+1,\dots,2p,\ i = 1,2,\dots,j-p\}.$$

These last three sets record the entries of S without repetitions. Let $T =$ the free abelian group on $\{t_1,\dots,t_n\}$ and construct a homomorphism $\phi: K \to T$ via $x_{ij}^{(r)} \to t_i t_j^{-1}$, $s_{ij} \to t_i t_j^{-1}$ and $\lambda_i \to 1$, for all i, j, r. Then A will be the kernel of ϕ. It is clear from the definition of M that $A \subseteq M$. Moreover, since ϕ has cokernel of rank 1 it follows that the rank of $A = \operatorname{rank}(K) - n + 1 = (k-1)n^2 + n^2/2 + 1$.

The subgroup B is defined to be the subgroup generated by $\{x_{1i}^{(2)} x_{1+p,i+p}^{(2)}\}_{i=2}^{p}$. To simplify the notation we will denote $x_{ij}^{(2)}$ as x_{ij} for the remainder of this proof. Since $x_{1+p,i+p}$ is the $(i,1)$-entry of X_2^*, $x_{1i}x_{1+p,i+p} \in M$. B is a free abelian group of rank $p - 1 = n/2 - 1$. To see that $A \cap B = (1)$, consider $\phi(B)$. Each $\phi(x_{1i}x_{1+p,i+p}) = t_1 t_{1+p} t_i^{-1} t_{i+p}^{-1}$, $i = 2,\dots,p$. No nontrivial product of these is 1 since they involve distinct letters, and since $A = \ker \phi$ this implies that $A \cap B = (1)$.

Finally, we show that $A + B = M$. First

$$x_{i1}x_{i+p,1+p} = (x_{i1}x_{1i})(x_{i+p,1+p}x_{1+p,i+p})(x_{1i}x_{1+p,i+p})^{-1} \in A + B.$$

Next, for all $i, j < p$, $x_{ij}x_{i+p,j+p} \in A + B$ and $x_{ij+p}x_{i+p,j} \in A + B$. For

$$x_{ij}x_{i+p,j+p} = \frac{(x_{1i}x_{ij}x_{j1})(x_{1+p,i+p}x_{i+p,j+p}x_{j+p,1+p})}{(x_{1i}x_{1+p,i+p})(x_{j1}x_{j+p,1+p})}$$

and

$$x_{i,j+p}x_{i+p,j} = \frac{(x_{1i}x_{i,j+p}x_{j+p,1+p}x_{1+p,i+p}x_{i+p,j}x_{j,1})}{(x_{1i}x_{1+p,i+p})(x_{j+p,1+p}x_{j1})}.$$

Now, in K

$$x_{i,j+p}^{(r)} = x_{j,i+p}\frac{(x_{i,j+p}^{(r)}x_{j+p,i})}{(x_{j,i+p}x_{j+p,i})} \equiv x_{j,i+p} \bmod A + B$$

and

$$x_{i+p,j+p}^{(r)} = x_{ji}\frac{(x_{i+p,j+p}^{(r)}x_{j+p,i+p})}{(x_{ji}x_{j+p,i+p})} \equiv x_{j,i} \bmod A + B.$$

Similarly $x_{j,i+p}^{(r)} \equiv x_{i,j+p}$ and $x_{j,i}^{(r)} \equiv x_{i+p,j+p}$. Note that $x_{i,j+p}^{(r)}$ is the $(j, i+p)$-entry of X_r^*, $x_{i+p,j+p}^{(r)}$ is the (j, i)-entry of X_r^*, etc. So, for *all* (i, j), the (i, j)-entry of X_r^* is congruent to the (i, j)-entry of X_2, modulo $A + B$. And the same is true for the entries of S.

Consider any of the generators of M, $u_{i_1,i_2}^{(r_1)}u_{i_2,i_3}^{(r_2)}\cdots u_{i_m,i_1}^{(r_m)}$. For each $u_{i_\alpha,i_{\alpha+1}}^{(r_\alpha)}$, if r_α is odd so that U_{r_α} is Λ or X_s, $s = (r_\alpha - 1)/2$ we leave it as it is; and if r_α is even > 2 we use the preceding calculation to replace $u_{i_\alpha,i_{\alpha+1}}^{(r_\alpha)}$ with the corresponding entry of X_2, $x_{i_\alpha,i_{\alpha+1}}$, modulo $A + B$. The resulting monomial is in A and so $M \subseteq A + B$. This completes the calculation in this case.

If $n = 2p + 1$ is odd this argument can be repeated with the following minor modifications: K, the free group on the alphabet will have rank $(k-1)n^2 + 2p^2 + 4p + 1$. And so the group A will have rank $(k-1)n^2 + 2p^2 + 2p + 1$. The group B will be generated by $\{x_i^{(2)}x_{1+p,i+p}^{(2)}\}_{i=2}^{p} \cup \{x_n^{(2)}x_{1+p,n}^{(2)}\}$. Again, one may show that $A + B = M$ and, since rank $(B) = p$,

$$\text{rank}(M) = (k-1)n^2 + 2p^2 + 3p + 1 = (k-1)n^2 + \binom{n+1}{2}.$$

(b) The argument in the symplectic case is the same as in the transpose type case, with $n = 2p$ even. The only change involved is that $s_{i,i+p} = = s_{i+p,i} = 0$ for $i = 1, \ldots, p$ and so the alphabet has $2p = n$ fewer letters. Hence the rank of M will be n less, as claimed.

Section Two: Involutions and generic splitting fields

In this section we give the promised description of $Z^T(F, n, k)$ and $Z^S(F, n, k)$ as field extensions of $Z(F, n, k)$. In order to do this, we must draw a connection between involutions and certain minimal right ideals. This connection is the heart of this section, so it should be mentioned that it is implicit in, and we obtained it from, an unpublished proof of Tamagawa's of Albert's theorem on involutions.

Let B/F be any central simple algebra of degree n over the field F. For the

moment, let F be an arbitrary field of characteristic not 2. The algebra $B \otimes_F B =$ (by definition) B'' has an automorphism τ defined by $\tau(a \otimes b) = b \otimes a$. Of course, τ has order 2. By [KO] p. 112 (result attributed to Goldman), there is an $\alpha \in B''$ such that the following holds. First, $\alpha\beta\alpha^{-1} = \tau(\beta)$ for all $\beta \in B''$ and $\alpha^2 = 1$. In addition, let $L \supseteq F$ be any splitting field of B. We may write $B \otimes_F L \cong \mathrm{End}_L(V)$ for V an L vector space. Then $B'' \otimes_F L$ can be identified with $\mathrm{End}_L(V \otimes_L V)$ and the image of α in $\mathrm{End}_L(V \otimes V)$ is just the map $\alpha(v \otimes w) = w \otimes v$.

If $F[\alpha]$ is the subalgebra of B'' generated over F by α, then $F[\alpha]$ is isomorphic to $F \oplus F$. In other words, if $e = (1 + \alpha)/2$, then e is an idempotent and $F[\alpha] = Fe + F(1 - e)$. Also, if we set $B' = \{\beta \in B'' \mid \tau(\beta) = \beta\}$, then B' is obviously the centralizer in B'' of α. That is, B' is the centralizer of e and so $B' = eB''e + (1 - e)B''(1 - e)$. We write

$$B_1 = eB''e \qquad \text{and} \qquad B_2 = (1 - e)B''(1 - e).$$

Since $eB''e \cong \mathrm{End}_{B'}(eB'')$ and similarly for $1 - e$, the B_i are central simple algebras Brauer equivalent to $B'' = B \otimes_F B$. We compute the degree of the B_i in the next lemma.

LEMMA 2.1. *B_1 has degree $n(n + 1)/2$ and B_2 has degree $n(n - 1)/2$.*

PROOF. Let $L \supseteq F$ be a splitting field for B, so that $B \otimes_F L$ can be identified with $\mathrm{End}_L(V)$ for V an L vector space. Also $B'' \otimes_F L$ can be identified with $\mathrm{End}_L(V \otimes_L V)$. Now $B_1 \otimes_F L \cong e(B'' \otimes L)e \cong \mathrm{End}_L(e(V \otimes V))$. Similarly,

$$B_2 \otimes_F L \cong (1 - e)(B'' \otimes L)(1 - e) \cong \mathrm{End}_L((1 - e)(V \otimes V)).$$

Given the above description of α as a map $\alpha : (V \otimes V) \to (V \otimes V)$, it is clear that $e(V \otimes V)$ is the vector space of symmetric tensors and $(1 - e)(V \otimes V)$ is the space of antisymmetric tensors. Thus $e(V \otimes V)$ has dimension $n(n + 1)/2$ and $(1 - e)(V \otimes V)$ has dimension $n(n - 1)/2$. This proves the lemma.

While the above argument is still fresh, let us use the above machinery to investigate τ invariant right ideals of $B'' = B \otimes B$.

LEMMA 2.2. *Let $R' \subseteq B''$ be a right ideal of dimension n^2 and assume $\tau(R') = R'$. Then $R' \cap B' = R$ is a right ideal of $B' = B_1 \oplus B_2$, $R \subseteq B_1$ or $R \subseteq B_2$, and R has dimension $n(n + 1)/2$ or $n(n - 1)/2$ respectively.*

PROOF. Let $L \supseteq F$ be as above and make the same identifications. Then there is a unique one dimensional L subspace $W \subseteq V \otimes V$ such that $R'L \subseteq$

$\mathrm{End}_L(V \otimes V)$ is exactly $\{\beta \mid \beta \text{ has image in } W\}$. Since $\tau(R') = R'$, $\alpha(W) = W$. Since $\alpha^2 = 1$, the map α restricted to W is either the identity or the -1 map. Thus $W \subseteq e(V \otimes V)$ or $W \subseteq (1-e)(V \otimes V)$. It follows that $(1-e)R'L = 0$ or $eR'L = 0$. Hence $R' \cap B' = eR'e$ or $(1-e)R'(1-e)$ and only one is nonzero. If $eRe \neq (0)$ then

$$e(R'L)e = \{\beta \in \mathrm{End}_L(e(V \otimes V)) \mid \beta(e(V \otimes V)) \subseteq W\}$$

and so R has dimension $n(n+1)/2$ over F. A similar argument holds if $(1-e)R'(1-e) \neq (0)$ and the lemma follows.

In an unpublished proof, Tamagawa used τ invariant idempotents to prove Albert's theorem on involutions. We next take that proof and extend it slightly to get the relationship we desire between involutions and minimal right ideals.

Let $J: B \to B$ be any involution of B fixing F. Define $L(J)$ to be the left ideal of $B'' = B \otimes B$ generated by all elements of the form $(b \otimes 1) - (1 \otimes J(b))$ where $b \in B$. Now set $R'(J)$ to be the right annihilator of $L(J)$ in B'', and $R(J) = R'(J) \cap B'$.

THEOREM 2.3. (a) *$L(J)$ is a left ideal of B'' of dimension $n^4 - n^2$ over F.*

(b) *$R'(J)$ is a right ideal of B'' of dimension n^2 over F.*

(c) *$R(J) \subseteq B_1$ or $R(J) \subseteq B_2$ and has dimension $n(n+1)/2$ or $n(n-1)/2$ respectively.*

(d) *$R(J) \subseteq B_1$ if and only if J is of transpose type and $R(J) \subseteq B_2$ if J is of skew type.*

(e) *The mapping $J \to R(J)$ is injective. An ideal R of B_1 or B_2 of the right dimension is of the form $R(J)$ if and only if the following holds. For all $b \in B$, $(b \otimes 1)R = (0)$ implies that $b = 0$.*

PROOF. Let B^o be the opposite algebra of B. We can consider J to be an isomorphism $J: B \to B^o$. Then $1 \otimes J: B \otimes B \to B \otimes B^o$ maps $L(J)$ onto the left ideal, L, generated by all elements of $B \otimes B^o$ of the form $b \otimes 1 - 1 \otimes b$. But L is the kernel of the surjection $\mu: B \otimes B^o \to B$ defined by $\mu(a \otimes b) = ab$. Thus L, and hence $L(J)$, has the desired dimension. This proves (a) and (b) immediately follows. Next observe that since J has order 2, $L(J)$ is τ invariant. Thus $R'(J)$ is τ invariant. By 2.2, part (c) follows.

We next do a part of (e). Suppose $(b \otimes 1)R(J) = (0)$ for some nonzero $b \in B$. Then $B''(b \otimes 1) \subseteq L(J)$. But if $(\Sigma b_i b \otimes c_i) \in B''(b \otimes 1)$, then

$$\sum((b_i b \otimes c_i) - (1 \otimes c_i J(b) b_i)) \in L(J),$$

so $\Sigma(1 \otimes c_i J(bb_i)) \in L(J)$. Since B is simple, this implies that $1 \otimes B \subseteq L(J)$ and

is a contradiction. We have shown that if $(b \otimes 1)R(J) = (0)$, then $b = 0$. In particular, $J(b)$ is the unique element of B such that $((b \otimes 1) - (1 \otimes J(b)))R(J) = (0)$. This proves the injectivity part of (e).

To show the rest of (e), suppose $R \subseteq B_1$ or B_2 is of the right dimension and $(b \otimes 1)R = (0)$ implies that $b = 0$. Choose $f \in R$ such that $fB' = R$. The map $b \to (b \otimes 1)f$ is an injection. Let $L \supseteq F$ split B and apply the identifications of the proof of Lemma 2.1. Then f considered as an endomorphism of $e(V \otimes V)$ or $(1 - e)(V \otimes V)$ has rank one. Thus considering f as an endomorphism of $V \otimes V$, it also has rank one. Finally, we can conclude that $B''f$ has dimension n^2 and so $B''f = (B \otimes 1)f$. Since $\tau(f) = f$, $(1 \otimes B)f = B''f = (B \otimes 1)f$. We conclude that for any $b \in B$, there is a unique $J(b) \in B$ such that $((b \otimes 1) - (1 \otimes J(b))f = 0$. Applying τ to both sides of this equation shows that $J(J(b)) = b$. Finally,

$$((ab) \otimes 1)f = ((a \otimes 1)(b \otimes 1))f = ((a \otimes 1)(1 \otimes J(b)))f$$

$$= ((1 \otimes J(b))(a \otimes 1))f = ((1 \otimes J(b))(1 \otimes J(a)))f = (1 \otimes J(b)J(a))f.$$

Thus $J(ab) = J(b)J(a)$ and J is an involution. It is clear that $R = R(J)$ and so (e) is proved.

In order to prove (d), again choose $f \in R(J)$ such that $R(J) = fB'$. Then $L(J)$ is the left annihilator of f. Define $\Gamma : B \to B'$ by setting $\Gamma(b) = [(b \otimes 1) + (1 \otimes b)]f$. Obviously, Γ is F linear and $\Gamma(B) \subseteq B'f$. But

$$((a \otimes b) + (b \otimes a))f = ((1 \otimes b)(a \otimes 1) + (b \otimes 1)(1 \otimes a))f$$

$$= ((1 \otimes bJ(a)) + (bJ(a) \otimes 1))f,$$

so it follows that $\Gamma(B) = B'f$. Observe that $R(J) \subseteq B_i$ if and only if $f \in B_i$. Also, $B'f = B_i f$ if $f \in B_i$. The kernel of Γ is

$$\{b \in B \mid ((b \otimes 1) + (1 \otimes b))f = 0\} = \{b \in B \mid J(b) = -b\}.$$

This kernel is then the space of skew symmetric elements of B with respect to J, and we call this kernel B^a. If $R(J) \subseteq B_1$, then $B'f = B_1 f$ has dimension $n(n + 1)/2$ and so B^a had dimension $n(n - 1)/2$. Similarly, if $R(J) \subseteq B_2$, B^a has dimension $n(n + 1)/2$. Since J has transpose or skew type if and only if B^a has

dimension $n(n-1)/2$ or $n(n+1)/2$ respectively, part (d) and the whole theorem is proved.

Underlying the above result is an isomorphism of varieties, which we will now describe. Let $\mathrm{GL}(B)$ be the variety of linear isomorphisms of B. The set of involutions form a (Zariski) closed subspace of $\mathrm{GL}(B)$, since the conditions of antiautomorphism, order 2, and fixing F are closed conditions. Let In denote this closed subspace, which we can think of as a scheme with the reduced induced structure. Let V_1 and V_2 be the Brauer Severi schemes of B_1 and B_2 respectively. That is, the V_i have points over any K corresponding to the right ideals of $B \otimes_F K$ of dimension $n(n+1)/2$ or $n(n-1)/2$ respectively. For any such right ideal R, the condition that $(b \otimes 1)R = 0$ implies $b = 0$, is an open condition that defines open subsets $U_i \subseteq V_i$. Theorem 2.3 above can be expanded to show that In is isomorphic to the disjoint union of U_1 and U_2. The idea, of course, is that the map $J \to R(J)$ is an isomorphism of varieties. The proof of this is neither short (including all details) nor difficult.

Instead of proving directly that the map in 2.3 is an isomorphism of varieties, we proceed in a slightly different manner. Let A/F be any central simple algebra of degree m and let $L \subseteq A$ be a maximal subfield. Denote by $e_1, \ldots, e_m$ a basis of L over F. Let $W \subseteq A$ be an F subspace such that $L \cap W = (0)$ and $L + W = A$. Choose $d \in W$. Let $n : A \to F$ be the reduced norm map and $f(x_1, \ldots, x_m)$ the polynomial $n(x_1e_1 + \cdots + x_me_m + d)$. Associated with L is an affine open subset of $V =$ the Brauer Severi variety of A. To be precise, let V' be the variety whose K points are the left ideals of $B \otimes K$ of dimension $m^2 - m$. The map taking an ideal to its annihilator defines an isomorphism between V and V'. Let U' be the open subset of V' whose points over any $K \supseteq F$ are the left ideals $N \in V'$ such that $N \cap (LK) = (0)$. Let $U \subseteq V$ be the corresponding open subset of V. According to [S], p. 343, there is a Zariski open subset of choices of d such that $f(x_1, \ldots, x_m)$ is absolutely irreducible. Let X be the affine variety defined as the zeroes of f. If $N \in U'$, there is a unique element of N of the form $c_1e_1 + \cdots + c_me_m + d$. This defines a morphism of varieties from U to X. It is further shown in [S] that there is a Zariski open subset of choices of d such that $c_1e_1 + \cdots + c_me_m + d$ has rank $n - 1$. With this choice of d the above morphism is birational and so V and X have the same function field $F(X)$.

We can finally apply all of this to the particular case at hand. Let $Z = Z(F, n, k)$ and $B = UD(F, n, k)$. Use B to form $B'' = B \otimes B$, B', B_1, B_2 as above. Let B^T be the generic division algebra with transpose involution,

written $UD^T(F, n, k)$, and defined in the introduction. Let Z^T be the center of B^T. The definition of B^T implies that $B \subseteq B^T$ canonically. Hence $Z \subseteq Z^T$. Now

$$\text{tr.deg } Z^T/Z = \text{tr.deg } Z^T/F - \text{tr.deg } Z/F$$

$$= \left((k-1)n^2 + \binom{n+1}{2}\right) - ((k-1)n^2 + 1)$$

by 1.11 and [F] so

$$\text{tr.deg } Z^T/Z = \binom{n+1}{2} - 1.$$

Also note that B^T has an involution we will call T, and that B^T is the central quotient ring of the F algebra generated by the generic matrices $X_1, \ldots, X_k$ and their transposes $X_1^T, \ldots, X_k^T$. Use B^T to form B_1^T as above. Of course, $B_1^T = B_1 Z^T$. In a similar manner, let B^S be the generic division algebra $UD^S(F, n, k)$ with skew involution. Define Z^S, and B_2^S in an analagous manner. Our main theorem is the following

THEOREM 2.4. *Z^T is isomorphic to the function field of the Brauer Severi variety of B_1 over Z. That is, Z^T is isomorphic to the Amitsur generic splitting field of B_1 over Z. Similarly, Z^S is isomorphic to the function field of the Brauer-Severi variety (generic splitting field) of B_2 over Z.*

PROOF. Let L be a maximal subfield of B_1 with basis $e_1, \ldots, e_m$ where $m = n(n+1)/2$. Choose $d \in B_1 - L$ as above. Let T be the given involution of B^T. Define $R = R(T) \subseteq B_1^T$ as in 2.3 and let $N \subseteq B_1 T$ be the left annihilator of R. Since L is a field, $R(T) \cap L = (0)$. Let

$$z = c_1 e_1 + \cdots + c_m e_m + d$$

be the unique element of N of that form. Arguing again as in [S] p. 343, there is a Zariski open subset of choices of d in $B_1 - L$ so that z has rank $n-1$. Then $R(T)$ is the right annihilator of z. Set $Z' = Z(c_1, \ldots, c_m) \subseteq Z^T$. Since $z \in B_1 Z'$, there is an ideal $R' \subseteq B_1 Z'$ such that $R' Z^T = R(T)$. The ideal R' defines an involution of BZ' which is the restriction of T. Thus $X_1^T, \ldots, X_s^T \in BZ'$ and so $BZ' = B^T$. It follows that $Z^T = Z' = Z(c_1, \ldots, c_m)$.

Let $f(x_1, \ldots, x_m)$ be the polynomial defined as above using B_1, L, d etc. Since Z'/Z has transcendence degree $m-1$, f must generate the ideal of polynomials with $(c_1, \ldots, c_m)$ as a zero. Thus Z' is isomorphic to the function field of the variety defined by f. But this is the function field of the Brauer Severi variety of

B_1. Arguing in an exactly parallel way we get the result for B^S also, and the whole theorem is proved.

Of course, neither B_1 nor B_2 above can be division algebras (except when $n = 2$), but are matrices over the division algebra, D, Brauer equivalent to $B \otimes B$. Thus Z^T and Z^S are both rational field extensions of the function field of the Brauer Severi variety of D. Since $n(n+1)/2 > n(n-1)/2$, it is in fact true that Z^S is isomorphic to a subfield of Z^T and Z^T/Z^S is rational.

Section Three: A related construction

Let F be an infinite field of any characteristic, $n = ab$ and let S be the polynomial ring

$$F[\lambda_l, x_{ij}^{(r)} \mid 1 \leqq l \leqq b, 1 \leqq i, j \leqq n, 1 \leqq r \leqq k].$$

Denote by $X_r \in M_n(S)$ the generic matrix with (i,j)-entry $x_{ij}^{(r)}$ and let $\Lambda \in M_n(S)$ be the diagonal matrix $\operatorname{diag}(\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots, \lambda_2, \ldots, \lambda_b)$ where each entry appears a times. We will consider R, the F subalgebra of $M_n(S)$ generated by the X's and Λ.

We first show that R is a prime domain which is "generic" with respect to a certain class of central simple algebras. To begin, let $S' \subseteq S$ be the polynomial ring in the x's alone and let $R' \subseteq M_n(S') \subseteq M_n(S)$ be the F subalgebra generated by the X's alone. If K' is the field of fractions of S', then we know that $R'K' = M_n(K')$, and in particular, $R'K'$ contains the matrix units. Thus if K is the field of fractions of S, $RK = M_n(K)$. Thus R is prime. Also, if C is the center of R, then $C \subseteq K \cap M_n(S) = S$. Let Z be the field of fractions of C. It follows from standard arguments that $Q = RZ$ is the central quotient ring of R and is central simple of degree n with center Z.

Next we proceed to show in what way R is "generic". To begin this discussion, we consider a class of homomorphisms from R to central simple algebras of degree n.

Suppose A/F' is central simple of degree n and $F' \supseteq F$. Assume $s \in A$ is such that $F'(s)/F'$ is a separable field extension of degree dividing b. Let $t_1, \ldots, t_k \in A$ be arbitrary. We claim there is an (obviously unique) F algebra map $\phi : R \to A$ with $\phi(\Lambda) = s$ and $\phi(X_r) = t_r$. To construct ϕ, choose a field $L' \supseteq F'$ such that $L' \supseteq F'(s)$, L'/F' is Galois, and L' splits A. Then $A \otimes_{F'} L' \cong M_n(L')$. We can identify $A \otimes L'$ with $M_n(L')$ in such a way that $s \in M_n(L')$ is a diagonal matrix. If $f(x)$ is the characteristic polynomial of s and $g(x)$ is the minimal polynomial of s, then both are polynomials in $F'[s]$. Since $F'(b)$ is a field, $g(x)$

is irreducible over F'. Thus $f(x) = g(x)^{a'}$ where a divides a'. Thus each root of $g(x)$ appears in the diagonal matrix s exactly a' times. After reordering, we can write $s = \text{diag}(s_1, \ldots, s_b)$ where duplication is introduced so that each s_i appears exactly a times. Of course, t_r is some matrix $(t_{ij}^{(r)})$. Define $\psi: S \to L'$ by $\psi(\lambda_i) = s_i$ and $\psi(x_{ij}^{(r)}) = t_{ij}^{(r)}$. Then $M_n(\psi)(\Lambda) = s$ and $M_n(\psi)(X_r) = t_r$. If we call ϕ the restriction of $M_n(\psi)$ to R, then ϕ is the required map. Note that it is automatically the case that $\phi(Z(R)) \subseteq F''$.

Let us view these maps ψ in another way. Let A/F' be as above and let $L \subseteq A$ be a subfield such that L/F' is separable of degree b. Choose $L' \supseteq L$ such that L'/F' is Galois and L' splits A. S is the affine ring of the affine space, V, of degree $(b + rn^2)$. Maps from S to L' can be identified with L' points of V, which are just the points of the L' vector space

$$V(L') = L' \otimes L' \otimes \cdots L' \otimes M_n(L') \otimes \cdots M_n(L')$$

(bL's and $kM_n(L')$'s). Maps $\psi: S \to L'$ such that $M_n(\psi)(R) \subseteq A$ and $M_n(\psi)(\Lambda) \in L$ are a subset $U \subseteq V(L')$.

LEMMA 3.1. *U is Zariski dense in V.*

PROOF. Since L' is infinite, $V(L')$ is dense in V. The conditions on $M_n(\psi)$ defining U say precisely that the point ψ lies in the F' space $L \otimes A \otimes \cdots \otimes A$ viewed as a subset of $V(L')$. Thus up to a choice of basis of $V(L')$, U is just $V(F')$ and is therefore dense.

We are ready for:

PROPOSITION 3.2. *Let $0 \neq s \in C$ and let A/F' be a central simple algebra of degree n. Assume $L \subseteq A$ is a subfield such that L/F' is separable of degree b. Then there is an F algebra map $\phi: R \to A$ such that $\phi(s) \neq 0$, $\phi(C) \subseteq F'$, and $\phi(\Lambda) \in L$.*

PROOF. Choose a $\psi: S \to L'$ in set U above such that $\psi(s) \neq 0$. This is possible since U is Zariski dense and $s \in S$. Let ϕ be the restriction of $M_n(\psi)$ to R. Since, by definition, $M_n(\psi)(S) \subseteq L'$, $\phi(C) \subseteq A \cap L' = F'$. This proves the result.

COROLLARY 3.3. *Q is a division ring and R is a domain.*

PROOF. Of course, if Q is a division ring R must be a domain. Suppose Q is not a division ring. Then $Q = M_t(D)$ for some division ring D. There is an $0 \neq s \in Z(R)$ such that the (standard) matrix units of $M_t(D)$ are in $R(1/s)$.

Choose $F' \supseteq F$ and D'/F' a cyclic division algebra of degree n. Clearly, D has a subfield L separable of degree b over F'. Choose $\phi : R \to D'$ as in 3.2 such that $\phi(s) \neq 0$. Then ϕ extends to an F algebra map $\phi : R(1/s) \to D'$. But $R(1/s)$ has nontrivial matrix units that map to nontrivial such units in D', a contradiction.

REMARK. To be fully precise, R or Q is generic for the class of central simple algebras A/F' of degree n with subrings $F' \subseteq L \subseteq A$ such that A is free as an L module and L/F is separable of degree b, but L need not be a field.

In the rest of this section we will describe the center of Q as a field of invariants with respect to the group $S_a \wr S_b$. To put those remarks in perspective, we mention the following fact.

LEMMA 3.4. *Let $L' \supseteq L \supseteq F'$ be fields such that L'/F' has degree n and L/F' has degree b. Then the Galois group of a splitting field of L' over F is naturally a subgroup of $S_a \wr S_b$.*

PROOF. Let G be the Galois group of a splitting field of L'/F'. Then G has subgroups $H, K \subseteq G$ corresponding to L' and L respectively. We conclude that $H \subseteq K$, $[G : H] = n$ and $[G : K] = b$. G acts faithfully on the set of n left cosets $T = \{gH \mid g \in G\}$ via $g'(gH) = g'gH$. The left cosets of K partition T onto b sets of a elements each, and G must preserve this partition. But the subgroup $G' \subseteq S_n$ that preserves this partition is isomorphic to $S_a \wr S_b$.

As a consequence of the above, if A/F' is a central simple algebra of degree n with a subfield $L \subseteq A$ such that L/F' is separable of degree b, then A is split by a Galois extension L''/F' such that the Galois group of L''/F' is a subgroup of $S_a \wr S_b$.

LEMMA 3.5 (Change of Model). *There is a matrix A such that $A\Lambda A^{-1} = \Lambda$ and AX_1A^{-1} is of the form*

$$\begin{bmatrix} D_1 & & & * \\ & D_2 & & \\ & & \ddots & \\ * & & & D_b \end{bmatrix}$$

where $D_1, \ldots, D_b$ are $a \times a$ diagonal matrices.

PROOF. Consider the idempotents

$$E_1 = e_{11} + e_{22} + \cdots + e_{aa},$$

$$E_2 = e_{a+1,a+1} + \cdots + e_{2a,2a}, \ldots, \qquad E_b = e_{ab-a+1,ab-a+1} + \cdots + e_{ab,ab}.$$

Each $E_iX_1E_i$ is of the form

$$\begin{bmatrix} 0 & & 0 \\ & Y_i & \\ 0 & & 0 \end{bmatrix}$$

where Y_i is a generic $a \times a$ matrix and lies across the diagonal. Let A_i be such that $A_iY_iA_i^{-1}$ is a diagonal matrix. Now it is easy to see that

$$A = \begin{bmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_b \end{bmatrix}$$

has the required properties.

As in the previous sections, we now redefine R by redefining X_1 to be as in Lemma 3.5, i.e., we assume that $x_{ij}^{(1)} = 0$ if $1 < |i-j| < a-1$. This redefinition of R replaces it with an isomorphic ring and so does not affect Q or Z. As above, we define M to be the multiplicative abelian group generated by all nonzero products of the form

$$\lambda_1^{\alpha_1} \cdots \lambda_b^{\alpha_b} x_{i_1i_2}^{(m_1)} \cdots x_{i_pi_1}^{(m_p)}$$

with the above restriction on the $x_{ij}^{(1)}$.

LEMMA 3.6. (a) *M is a free abelian group of* rank $kn^2 - na + n + 1$.
(b) *M is a faithful module for $S_1 \wr S_b$.*

PROOF. (a) Let $B =$ the free abelian group

$$\langle \lambda_i, x_{ij}^{(m)} \mid i,j = 1, \ldots, n,\ m = 1, \ldots, k; \text{ if } m = 1, \text{ then } i = j \text{ or } |i-j| > a \rangle,$$

let $T = \langle t_1, \ldots, t_n \rangle$ and $V = \langle v \rangle$. Map $\alpha : B \to T$ via $\lambda_i \to 1$, $x_{ij}^{(m)} \to t_it_j^{-1}$ and map $\beta : T \to V$ via $t_i \to v$. Then there is an exact sequence

$$1 \to M \to B \to T \to V \to 1.$$

Hence

$$\operatorname{rk}(M) = \operatorname{rk}(B) - \operatorname{rk}(T) + \operatorname{rk}(V) = n + kn^2 - b(a^2 - a) + 1 - n$$

$$= kn^2 - na + n + 1.$$

(b) $S_a \wr S_b$ is embedded in S_{ab} as

$$\left\{\sigma \;\middle|\; \text{for all } i,j \text{ such that } \left[\frac{i-1}{a}\right] = \left[\frac{j-1}{a}\right],\right.$$

$$\left.\sigma \text{ acts in such a way that } \left[\frac{\sigma(i)-1}{a}\right] = \left[\frac{\sigma(j)-1}{a}\right]\right\}.$$

Since $S_{ab} \subseteq \mathrm{GL}_{ab}$, $S_a \wr S_b$ acts on $n \times n$ matrices by conjugation. As in the previous case this induces as action of $S_a \wr S_b$ on $F[\lambda_r, x_{ij}^{(m)}]$: We enumerate $\Lambda, X_1, \ldots, X_k$ as $U_1, \ldots, U_{k+1}$ and let $u_{ij}^{(m)} =$ the (i,j)-entry of U_m. Then set $\sigma(u_{ij}^{(m)}) =$ the (i,j)-entry of the conjugate of U_n by σ. As in the previous sections $\sigma(u_{ij}^{(m)}) = u_{\sigma(i),\sigma(j)}^{(m)}$ and so one easily sees that the action is well defined and that M is a submodule.

Now let $L = Z(\lambda_1, \ldots, \lambda_b)$ and

$$K_i = L\left(u_{ij}^{(1)} \;\middle|\; \left[\frac{j-1}{a}\right] = i - 1\right)$$

and let $K = K_1 K_2 \cdots K_b$.

LEMMA 3.7. *The degree of K over Z is $\leqq b!(a!)^b = 0(S_a \wr S_b)$.*

PROOF. The characteristic polynomial for Λ is $(x - \lambda_1)^a \cdots (x - \lambda_b)^a \in Z[x]$. Since Z is separable $(x - \lambda_1) \cdots (x - \lambda_b) \in Z[x]$ and so the degree of L over Z is $< b!$

If $E_1, \ldots, E_b$ are as in the proof of Lemma 3.5 then

$$E_i = \prod_{j \neq i} (\Lambda - \lambda_j I) \Big/ \prod_{j \neq i} (\lambda_i - \lambda_j) \in Q \otimes_Z Z(\lambda_1, \ldots, \lambda_b).$$

Hence $E_i X_1 E_i \in Q \otimes_Z Z(\lambda_1, \ldots, \lambda_b)$ and has characteristic equation in $L = Z(\lambda_1, \ldots, \lambda_b)$. But the characteristic equation for $E_i X_1 E_i = \Pi(x - \lambda_j)$, product over

$$\left[\frac{j-1}{a}\right] = i - 1.$$

So the degree of K_i over L is $\leqq a!$. The lemma now follows.

THEOREM 3. $Z = F(M)^{S_a \wr S_b}$.

PROOF. Same as Theorem 1.7 using $Z \subseteq F(M)^{S_a \wr S_b} \subseteq F(M) \subseteq L$.

COROLLARY. *Z is a unirational field of transcendence degree $kn^2 + na - n + 1$.*

REFERENCES

[A] S. A. Amitsur, *Generic splitting fields of central simple algebras*, Ann. Math. **62** (1955), 8–43.

[Ar] M. Artin, *Severi varieties*, in *Brauer Groups in Ring Theory and Algebraic Geometry*, Springer-Verlag, Berlin/Heidelberg/New York, 1982 (LNM #917).

[F] E. Formanek, *The center of 3×3 generic matrices*, Lin. and Multilin. Alg. **7** (1979), 203–212.

[KO] M. A. Knus and M. Ojanguren, *Theorie de la Descente et Algebres d'Azumaya*, Springer-Verlag, Berlin, 1974 (LNM #389).

[P] C. Procesi, *Noncommutative affine rings*, Atti, Acc. Naz. Lincei, s.VIII, v.VIII, f.6 (1967), 239–255.

[R] P. Roquette, *On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras*, Math. Ann. **150**, 411–439.

[S] D. J. Saltman, *Norm polynomials and algebras*, J. Alg. **62**, No. 2 (1980), 333–345.