FIXED POINTS OF AUTOMORPHISMS OF LINEAR GROUPS

Sarah J. Gottlieb

INTRODUCTION

In the author's paper, *Algebraic Automorphisms of Algebraic Groups with Stable Maximal Tori,* a counterexample due to D. Winter was given, showing the existence of a solvable linear group in characteristic 2, with automorphism σ, which has two σ-stable maximal tori not conjugate by a σ-fixed point.

This paper generalizes that group for any characteristic $p > 0$. We define first an upper triangular group $\mathfrak{G}$ in $GL(p(p+1), \kappa)$ consisting of p diagonal block matrices, each block being upper triangular in $GL(p+1, \kappa)$. We then define a rational representation θ on $\mathfrak{G}_u$, the unipotent part of $\mathfrak{G}$:

$$\theta: (\mathfrak{G}_u, \cdot) \to (\kappa, +).$$

Our desired group is $G = T \cdot U$ where T is the diagonal maximal torus of $\mathfrak{G}$ and U is the kernel of θ. The automorphism σ of G cyclically permutes the p blocks of a matrix; that is, σ replaces the first block by the second, the second block by the third, etc., and the p^{th} block by the first. Having been previously defined on $\mathfrak{G}$, σ is used in the construction of θ.

PART I

Let $M_i \subseteq GL(p+1, \kappa)$ be upper triangular matrices, for $i = 1, \ldots, p$; κ an algebraically closed field with char $\kappa = p > 0$. Let M be the matrix in $GL(p(p+1), \kappa)$ with $M_1, \ldots, M_p$ along the diagonal, and zeroes elsewhere:

$$M = \begin{bmatrix} M_1 & & & & \\ & M_2 & & & \\ & & \ddots & & \\ & & & 0 & \\ & & & \ddots & \\ & 0 & & & \\ & & & & M_p \end{bmatrix}$$

Received February 18, 1977. Revision received October 16, 1978.

Michigan Math J. 27 (1980).

Denote by $\mathfrak{M}$ the set of all such matrices M. Then $\mathfrak{M}$ is an upper triangular algebraic group in $GL(p(p+1),\kappa)$.

It will be convenient to denote an entry of a matrix $M \in \mathfrak{M}$ by $(M_i)_{j,k}$, where M_i is the i^{th} block of M, and (j,k) are the local coordinates of the entry within the block.

There is an automorphism σ of order p on $\mathfrak{M}$, defined by:

$$\begin{cases} [(\sigma(M))_i]_{k,j} = (M_{i+1})_{k,j} & \text{for} \quad i = 1,\ldots,p-1 \\ [(\sigma(M))_p]_{k,j} = (M_1)_{k,j} \end{cases}$$

The effect of σ is to permute cyclically (upward) the blocks of a matrix $M \in \mathfrak{M}$. That is, $[\sigma(M)]_i = M_{i+1}$ for $1 \le i \le p-1$, and $[\sigma(M)]_p = M_1$. In fact, σ is conjugation by a permutation matrix of order p. For $p = 3$, for example, the permutation matrix would be:

$$\left[\begin{array}{ccc|ccc|ccc} & & & 1 & & & & & \\ & & & & 1 & 0 & & & \\ 0 & & & & & & & 0 & \\ & & & 0 & & 1 & & & \\ & & & & & & & & \\ \hline & & & & & & 1 & & \\ & & & & & & & 1 & 0 \\ 0 & & & 0 & & & 0 & & \\ & & & & & & & & 1 \\ \hline 1 & & & & & & & & \\ & 1 & 0 & & & & & & \\ & & & 0 & & & 0 & & \\ 0 & & 1 & & & & & & \\ & & & & & & & & \\ & & 1 & & & & & & \end{array}\right]$$

$\mathfrak{M}$ also admits an index-change automorphism τ, given by $[(\tau(M))_i]_{k,j} = (M_i)_{k-1,j-1}$ for $j,k \in \{2,\ldots,p+1\}$; and for $j = 1,\ldots,p+1$:

$$\begin{aligned} [(\tau(M))_i]_{1,j} &= (M_{i-1})_{1,j} \qquad (i = 2,\ldots,p), \\ [(\tau(M))_1]_{1,j} &= (M_p)_{1,j} \end{aligned}$$

For example, in the case $p = 3$, if

$$M_1 = \begin{bmatrix} t_1 & a_1 & a_2 & a_3 \\ & t_2 & b_1 & b_2 \\ & & t_3 & c_1 \\ & & & t_4 \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} t_5 & a_4 & a_5 & a_6 \\ & t_6 & b_3 & b_4 \\ & & t_7 & c_2 \\ & & & t_8 \end{bmatrix}, \quad \text{then}$$

$$(\tau(M))_2 = \begin{bmatrix} t_1 & a_1 & a_2 & a_3 \\ & t_5 & a_4 & a_5 \\ & & t_6 & b_3 \\ & & & t_7 \end{bmatrix}$$

Let $\alpha = \sigma \cdot \tau$. Then for $M \in \mathfrak{M}$, $N = \alpha(M)$, and $i = 1, \ldots, p-1$, we have

$$(N_i)_{k,j} = [(\sigma(\tau(M))_i]_{k,j} = [(\tau(M))_{i+1}]_{k,j} = (M_{i+1})_{k-1,j-1}$$

where $k, j \in \{2, \ldots, p+1\}$; and

$$(N_i)_{1,j} = [(\tau(M))_{i+1}]_{1,j} = (M_i)_{1,j}$$

where $j = 1, \ldots, p+1$. The case for $i = p$ is similar, with $i+1$ replaced by 1.

In particular, if M is a fixed point of α, then $N = M$ and:

$$(*): \quad \begin{cases} (M_i)_{k,j} = (M_{i+1})_{k-1,j-1} \\ \\ (M_p)_{k,j} = (M_1)_{k-1,j-1} \end{cases} \quad \text{for} \begin{cases} i = 1, \ldots, p-1 \\ j = 2, \ldots, p+1 \\ k = 2, \ldots, p+1 \end{cases}$$

Note that the condition (*) implies that for $j = p - i$:

$$\begin{aligned} (M_i)_{p+1,p+1} &= (M_{i+1})_{p,p} = \ldots = (M_p)_{p+1-j,p+1-j} = (M_1)_{p-j,p-j} \\ &= (M_1)_{i,i} = \ldots = (M_i)_{i-(i-1),i-(i-1)} = (M_i)_{1,1}. \end{aligned}$$

That is (**): $(M_i)_{1,1} = (M_i)_{p+1,p+1}$ for $i = 1, \ldots, p$.

Let $G = (\mathfrak{M}_\alpha)_0$ be the connected component of the fixed-point subgroup $\mathfrak{M}_\alpha$ of $\mathfrak{M}$ under α. Then $\mathfrak{G}$ is the semi-direct product $\mathfrak{G} = \mathfrak{T} \cdot \mathfrak{U}$ of its diagonal maximal torus $\mathfrak{T}$ and its maximal unipotent subgroup $\mathfrak{U}$.

A matrix in $\mathfrak{G}$ has entries in the first row of each block arbitrary in κ, while its remaining non-zero entries satisfy the conditions (*) and (**) above.

It is helpful to display representative elements $t \in \mathfrak{T}$, $u \in \mathfrak{U}$, for $p = 3$:

$$t = \left[\begin{array}{c|c|c} \begin{matrix} t_1 & & 0 \\ & t_2 & \\ 0 & & t_3 \end{matrix} & \begin{matrix} 0 \\ \\ \\ \end{matrix} & \begin{matrix} 0 \\ \\ \\ \end{matrix} \\ \hline \begin{matrix} & & \\ 0 & & \\ & & \end{matrix} & \begin{matrix} t_2 & & 0 \\ & t_3 & \\ 0 & & t_1 \end{matrix} & \begin{matrix} & & \\ 0 & & \\ & & \end{matrix} \\ \hline \begin{matrix} & & \\ 0 & & \\ & & \end{matrix} & \begin{matrix} & & \\ 0 & & \\ & & \end{matrix} & \begin{matrix} t_3 & & 0 \\ & t_1 & \\ 0 & & t_2 \end{matrix} \end{array}\right] \quad \begin{matrix} t_1, t_2, t_3 \in \kappa \\ t_1 t_2 t_3 \neq 0 \end{matrix}$$

$$u = \left[\begin{array}{ccc|c|c} 1 & a_1 & a_2 & a_3 & \\ & 1 & b_1 & b_2 & \\ 0 & & 1 & c_1 & 0 \\ & & & 1 & \\ \hline & & & 1 \; b_1 \; b_2 \; b_3 & \\ & 0 & & 1 \; c_1 \; c_2 & 0 \\ & & & 0 \quad 1 \; a_1 & \\ & & & \quad\quad 1 & \\ \hline & 0 & & & 1 \; c_1 \; c_2 \; c_3 \\ & & & 0 & 1 \; a_1 \; a_2 \\ & & & & 0 \quad 1 \; b_1 \\ & & & & \quad\quad 1 \end{array}\right] \left.\begin{array}{l} a_1, a_2, a_3 \\ b_1, b_2, b_3 \\ c_1, c_2, c_3 \end{array}\right\} \in \kappa$$

The groups $\mathfrak{G}$, $\mathfrak{T}$, and $\mathfrak{U}$ are clearly σ-stable; but we shall usually apply σ to the set of nilpotent matrices $\mathfrak{U}' = \{u - I \mid u \in \mathfrak{U}\}$. $\mathfrak{U}'$ is stabilized by σ. Moreover, $\mathfrak{U}'$ is closed under matrix addition and multiplication; and σ preserves both.

For $X \in \mathfrak{U}$ or $\mathfrak{U}'$, define $\phi(X) = \sum_{i=1}^{p} (\sigma^i(X))_{1,p+1}$ Then ϕ is additive since σ is; that is,

$$\phi(X + Y) = \phi(X) + \phi(Y) \text{ for } X, Y \in \mathfrak{U} \text{ or } \mathfrak{U}'.$$

We now define the function $\theta: \mathfrak{U} \to \kappa$ by

$$\theta(I + X) = \sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) \phi(X^i) + (X^p)_{1,p+1}.$$

for $X \in \mathfrak{U}'$. Then θ is a polynomial function in the entries of $(I + X)$ with integral coefficients. Hence it is a rational function defined over the prime field.

We wish to prove that θ is in fact a rational representation of $\mathfrak{U}$ in κ. Hence we must show that θ is a homomorphism from $\langle U, \cdot \rangle$ to $\langle \kappa, + \rangle$. This is the object of parts II and III.

PART II

Define matrix rings $\mathscr{M}$ and $\mathscr{G}$ over the ring $\mathfrak{W}_2(\kappa)$ of 2-dimensional Witt vectors over κ, using the same defining relations as in Part I for $\mathfrak{M}$ and $\mathfrak{G}$.

Addition $(\overset{\circ}{+})$ and multiplication $(\overset{\circ}{\cdot})$ in $\mathfrak{W}_2(\kappa)$ are defined as follows: for $w = (w_0, w_1)$ and $v = (v_0, v_1)$ in $\mathfrak{W}_2(\kappa)$, w_0, w_1, v_0, v_1 are in κ, and

$$w \overset{\circ}{+} v = \left(w_0 + v_0, w_1 + v_1 - \sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) w_0^i v_0^{p-i} \right)$$

$$w \overset{\circ}{\cdot} v = (w_0 v_0, w_0^p v_1 + w_1 v_0^p).$$

The natural projection R of $\mathfrak{W}_2(\kappa)$ onto κ, given by $R((w,v)) = w$, is a ring homomorphism.

The important facts for our purpose about $\mathfrak{W}_2(\kappa)$ are that addition and multiplication in κ are preserved in the first element while the characteristic of $\mathfrak{W}_2(\kappa)$ is p^2.

The identity "1" in $\mathfrak{W}_2(\kappa)$ is $(1,0)$; "i" is $(i,0)$ for $i = 1, \ldots, p-1$; "p" is represented by $(0,1)$, and "0" by $(0,0)$; "$p + i$" by $(i,1)$ and "$jp + i$" by (i,j) for $i,j = 1,2,\ldots,p-1$;

Let $\hat{I}$ denote the identity of $\mathscr{G}$, and let $\mathscr{U}$ denote the subset of $\mathscr{G}$ whose elements have all "1"'s on the diagonal, and define $\mathscr{U}' = \{u - \hat{I} \mid u \in \mathscr{U}\}$. Then $\langle \mathscr{U}, \cdot \rangle$ is a semi-group, and $\mathscr{U}'$ is closed under addition and multiplication.

There is a ring automorphism $\hat{\sigma}$ on $\mathscr{M}$ defined as was σ on $\mathfrak{M}$, which is also defined on $\mathscr{U}'$ and stabilizes $\mathscr{G}$, $\mathscr{U}$, and $\mathscr{U}'$.

Similarly, there is an additive mapping $\hat{\phi}$ from $\mathscr{U}$ or $\mathscr{U}'$ to $\mathfrak{W}_2(\kappa)$, given by

$$\hat{\phi}(X) = \sum_{i=1}^{p} (\hat{\sigma}^i(X))_{1,p+1} \qquad \text{for } X \in \mathscr{U} \text{ or } \mathscr{U}'$$

Define the mapping $\hat{\theta}\colon \mathscr{U} \to \mathfrak{W}_2(\kappa)$ by

$$\hat{\theta}(\hat{I} + X) = \sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) \hat{\phi}(X^i) + (X^p)_{1,p+1} \qquad \text{for } X \in \mathfrak{U}'.$$

The definition of $\hat{\theta}$ on $\mathscr{U}$ is strikingly similar to that of θ on $\mathfrak{U}$.

The proof of the following lemma is straightforward and will be omitted.

LEMMA 1. *If $\rho\colon \mathfrak{M} \to \mathscr{M}$ is the mapping defined by $[\rho(X)]_{j,k} = (X_{j,k}, 0)$, then for $x \in \mathfrak{U}'$, $R[\hat{\phi}(\rho(X))] = \phi(X)$, $R[(\rho(X)^p)_{1,p+1}] = (X^p)_{1,p+1}$, and $R[\hat{\phi}(\rho(X)^j)] = \phi(X^j)$ for $j = 1,2,\ldots$.*

COROLLARY 2. $\theta = R\hat{\theta}\rho$ *on* $\mathfrak{G}$.

Proof. For $X \in \mathfrak{U}'$, $\rho(I + X) = \hat{I} + \rho(X)$ where $\hat{I}$ denotes the identity matrix in $\mathscr{U}$ and $\rho(X) \in \mathscr{U}'$. We have:

$$R\hat{\theta}\rho(I + X) = R\left[\sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) \hat{\phi}(\rho(X)^i) + (\rho(X)^p)_{1,p+1} \right]$$

$$= \sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) R[\hat{\phi}(\rho(X)^i)] + R[(\rho(X)^p)_{1,p+1}]$$

$$= \sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) \phi(X^i) + (X^p)_{1,p+1} = \theta(I + X),$$

by Lemma 1.

THEOREM 3. *If $R\hat{\theta}$ is a homomorphism from $\langle \mathscr{U}, \cdot \rangle$ to $\langle \kappa, + \rangle$, then θ is a homomorphism from $\langle \mathfrak{U}, \cdot \rangle$ to $\langle \kappa, + \rangle$.*

Proof. Let A and B be any elements of $\mathfrak{U}'$, and note that for any $i = 1,2,\ldots$ there are numbers j_i and k_i such that

$$[\rho(A) + \rho(B) + \rho(A)\rho(B)]^i = \sum_{j=1}^{j_i} \left[\prod_{i=1}^{k_i} X(j,k) \right],$$

where $X(j,k) = \rho(A)$ or $\rho(B)$ or 1. Thus, using Lemma 1,

$$R\hat{\phi}\,[(\rho(A) + \rho(B) + \rho(A)\rho(B))^i] = \phi((A + B + AB)^i),$$

and

$$R\,[((\rho(A) + \rho(B) + \rho(A)\rho(B))^p)_{1,p+1}] = [(A + B + AB)^p]_{1,p+1}$$

Hence

$$\begin{aligned} R\hat{\theta}(\rho(I + A) \cdot \rho(I + B)) &= R\hat{\theta}((\hat{I} + \rho(A))(\hat{I} + \rho(B))) \\ &= R\hat{\theta}(\hat{I} + \rho(A) + \rho(B) + \rho(A)\rho(B)) \\ &= R\left[\sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) ((\rho(A) + \rho(B) + \rho(A)\rho(B))^i) \right. \\ &\quad \left. + ((\rho(A) + \rho(B) + \rho(A(\rho(B))^p)_{1,p+1} \right] \\ &= \sum_{i=1}^{p-1} \left(\binom{p}{i} \Big/ p \right) \phi((A + B + AB)^i) \\ &\quad + ((A + B + AB)^p)_{1,p+1} \\ &= \theta(I + A + B + AB) = \theta((I + A)(I + B)). \end{aligned}$$

So if $R\hat{\theta}$ is a homomorphism, then

$$\begin{aligned} \theta((I + A)(I + B)) &= R\hat{\theta}(\rho(I + A)\rho(I + B)) \\ &= [R\hat{\theta}(\rho(I + A)) + R\hat{\theta}(\rho(I + B))] \\ &= \theta(I + A) + \theta(I + B), \end{aligned}$$

by Cor. 2, as we wished to prove.

It remains now to prove that $R\hat{\theta}$ is indeed a homomorphism.

PART III

For this section, which deals only with matrices in $\mathscr{G}$, $\mathscr{U}$, $\mathscr{U}'$, etc., we may without confusion denote $\hat{\sigma}$, $\hat{\phi}$, $\hat{\theta}$, $\hat{I}$, etc., simply by σ, ϕ, θ, I, etc. (It should be noted, however, that the observations of Lemmas 4, 5, and 6 have corresponding formulations for $\mathfrak{G}$ over κ).

LEMMA 4. *For* $X \in \mathscr{U}'$, $p\theta(I+X) = \phi((I+X)^p) = \phi\left(\sum_{k=1}^{p} \binom{p}{k} X^k\right)$

Proof. For $x \in \mathscr{U}'$, $(X_i^p)_{1,p+1} = \prod_{j=1}^{p} (X_i)_{j,j+1}$, $(i = 1, \ldots, p)$.

So

$$\begin{aligned}(\sigma(X^p)_{1,p+1} &= (\sigma(X_1^p))_{1,p+1} = (X_2^p)_{1,p+1} \\ &= \prod_{j=1}^{p} (X_2)_{j,j+1} = \left[\prod_{j=1}^{p-1} (X_1)_{j+1,j+2}\right](X_1)_{1,2} \\ &= \prod_{j=1}^{p} (X_1)_{j,j+1} = (X_1^p)_{1,p+1} = (X^p)_{1,p+1}.\end{aligned}$$

That is,

$$[\sigma^i(X^p)]_{1,p+1} = (X^p)_{1,p+1} \text{ for } i = 1, \ldots, p.$$

So

$$\phi(X^p) = \sum_{i=1}^{p} [\sigma^i(X^p)]_{1,p+1} = p(X^p)_{1,p+1}.$$

Hence

$$\begin{aligned}\phi[(I+X)^p] &= \phi\left[\sum_{k=0}^{p} \binom{p}{k} X^k I^{p-k}\right] \\ &= \phi\left[I + X^p + \sum_{k=1}^{p-1} \binom{p}{k} X^k\right] \\ &= \phi(I) + \phi(X^p) + \phi\left[\sum_{k=1}^{p-1} \binom{p}{k} X^k\right] \\ &= 0 + p(X^p)_{1,p+1} + \sum_{k=1}^{p-1} \binom{p}{k} \phi(X^k) = p\theta(I+X)\end{aligned}$$

LEMMA 5. *Let* $X, Y \in \mathscr{U}'$. *Then* $\phi(XY) = \phi(YX)$.

Proof. Let $2 \leqq k \leqq p$. By (*), i.e., the condition defining $\mathscr{G}$:

$$(X_1)_{1,k} = (X_p)_{2,k+1} = \ldots = (X_{p-(p-k)})_{2+(p-k),k+1+(p-k)} = (X_k)_{p-k+2,p+1} = [\sigma^{(k-1)}(X_1)]_{p-k+2,p+1},$$

and

$$(Y_1)_{k,p+1} = (Y_2)_{k-1,p} = (Y_{1+(k-1)})_{k-(k-1),p+1-(k-1)} = (Y_k)_{1,p-k+2} = [\sigma^{(k-1)}(Y_1)]_{1,p-k+2}.$$

Hence

$$(X_1)_{1,k}(Y_1)_{k,p+1} = [\sigma^{(k-1)}(Y_1)]_{1,p-k+2}\,[\sigma^{(k-1)}(X_1)]_{p-k+2,p+1}$$

and for $i = 1, \ldots, p$

$$[\sigma^i(X_1)]_{1,k}\,[\sigma^i(Y_1)]_{k,p+1} = [\sigma^{(k-1+i)}(Y_1)]_{1,p-k+2}\,[\sigma^{(k-1+i)}(X_1)]_{p-k+2,p+1}$$

Thus:

$$\sum_{i=1}^{p} [\sigma^i(X_1)]_{1,k}\,[\sigma^i(Y_1)]_{k,p+1} = \sum_{j=1}^{p} [\sigma^j(Y_1)]_{1,p-k+2}\,[\sigma^j(X_1)]_{p-k+2,p+1},$$

and:

$$\begin{aligned}\sum_{i=1}^{p} [\sigma^i(XY)]_{1,p+1} &= \sum_{k=2}^{p}\left(\sum_{i=1}^{p} [\sigma^i(X_1)]_{1,k}\,[\sigma^i(Y_1)]_{k,p+1}\right)\\ &= \sum_{k=2}^{p}\left(\sum_{j=1}^{p} [\sigma^j(Y_1)]_{1,p-k+2}\,[\sigma^j(X_1)]_{p-k+2,p+1}\right)\\ &= \sum_{l=2}^{p}\left(\sum_{j=1}^{p} [\sigma^j(Y_1)]_{1,l}\,[\sigma^j(X_1)]_{l,p+1}\right)\\ &= \sum_{j=1}^{p} [\sigma^j(YX)]_{1,p+1}\end{aligned}$$

So: $\phi(XY) = \phi(YX)$.

COROLLARY 6. *For a set of n matrices* $\{\xi(1), \xi(2), \ldots, \xi(n)\} \subseteq \mathscr{U}'$; *and for numbers* $a_1, \ldots, a_m \in \mathfrak{W}_2(\kappa)$, *we have*

$$\phi[\xi(1) \cdot \xi(2) \ldots \xi(n-1) \cdot \xi(n)] = \phi[\xi(2) \ldots \xi(n-1)\,\xi(n)\,\xi(1)] = \ldots = \phi[\xi(n)\,\xi(1) \ldots \xi(n-1)];$$

and

$$\phi\,[a_1\xi(1)\,\xi(2)\,\ldots\,\xi(n) + a_2\,\xi(2)\,\ldots\,\xi(n)\,\xi(1) + \ldots + a_m\,\xi(n)\,\xi(1)\,\ldots\,\xi(n-1)]$$

$$= (a_1 + a_2 + \ldots + a_m)\,\phi\,[\xi(1)\cdot\xi(2)\,\ldots\,\xi(n)].$$

Choose A, B arbitrary in $\mathscr{U}'$. Then by Lemma 4

$$p\theta\,[(I+A)(I+B)] = p\theta(I + A + B + AB) = \phi\left(\sum_{k=1}^{p}\binom{p}{k}(A+B+AB)^k\right).$$

Let us denote the expression $\sum_{k=1}^{p}\binom{p}{k}(A+B+AB)^k$ by E, and the expression $\binom{p}{k}(A+B+AB)^k$ by E_k, for $k = 1,\ldots,p$. The terms of each $(A+B+AB)^k$ we may consider as words in the letters A and B. The collection of all words, including repetitions, appearing in E_k we shall call $\mathscr{W}_k$. Note that $\mathscr{W}_k$ contains $\binom{p}{k}$ copies of every word in $(A+B+AB)^k$. We set $\mathscr{W} = \bigcup_{k=1}^{p}\mathscr{W}_k$—the collection of all words, including repetitions, appearing in E. Note that any given word may have a number of copies in each of several $\mathscr{W}_k$'s. For example, there are p copies of the word AB in $\mathscr{W}_1$, and $\binom{p}{2}$ copies in $\mathscr{W}_2$, for a total of $p + \binom{p}{2}$ in $\mathscr{W}$.

We say that two words, $W, W' \in \mathscr{W}$ are *equivalent* if one is a cyclic permutation (abbreviate *c.p.*) of the other. For example, the words $ABBA$ and $AABB$ are equivalent. The relation of being in cyclic permutation is an equivalence relation.

For any word $W \in \mathscr{W}$, we denote by $\bar{W}$ the equivalence class in $\mathscr{W}$ which contains W.

LEMMA 7. $\phi(E) = \sum_{\bar{W}\subseteq\mathscr{W}} \operatorname{card}(\bar{W})\,\phi(W)$, *where the sum is over equivalence classes.*

Proof. By Cor. 6, for a word $W' \in \bar{W}$:

$$\phi(W') = \phi(W) \text{ and } \phi\left(\sum_{W'\in\bar{W}} W'\right) = \operatorname{card}(\bar{W})\,\phi(W).$$

Thus

$$\phi(E) = \phi\left(\sum_{W\in\mathscr{W}} W\right) = \phi\left(\sum_{\bar{W}\subseteq\mathscr{W}}\left(\sum_{W'\in\bar{W}} W'\right)\right)$$

$$= \sum_{\bar{W}\subseteq\mathscr{W}} \phi\left(\sum_{W'\in\bar{W}} W'\right) = \sum_{\bar{W}\subseteq\mathscr{W}} \operatorname{card}(\bar{W})\,\phi(W).$$

We have now a counting problem, to determine card$(\bar{W})$. If W is A^k or B^k for some $k \in \{1,\ldots,p\}$, then W has only one distinct *c.p.*, which appears only in E_k; so, $\bar{W} \subseteq \mathscr{W}_k$, and card$(\bar{W}) = \binom{p}{k}$. All the other words in $\mathscr{W}$ have at least one A and at least one B. These we shall call *mixed words.* We shall find that for a mixed word W, card $\bar{W}$ is a multiple of p^2.

Assume W is a mixed word. At least one *c.p.* of W starts with an A, so we may assume that W, which is simply a representative of $\bar{W}$, itself starts with an A. Since W also has a B, it must somewhere have an A and B in succession. The AB sequence we shall call a *diphthong.*

Suppose W has i letters and r diphthongs. Since a product of $(p+1)$ elements of $\mathscr{U}'$ is 0, we need only consider $1 \leqq i \leqq p$, and of course $1 \leqq r \leqq i/2$. There are i (not necessarily distinct) possible *c.p.*'s of W, all of which in fact occur in $(A + \mathrm{B} + AB)^i$. Of these, r would start with a B, end with an A, and have only $(r-1)$ diphthongs. (For example, the word $***AB***$ may be cyclically permuted to $B******A$). The remaining $(i-r)$ *c.p.*'s of W all have r diphthongs.

The class $\bar{W}$ is therefore the disjoint union $\bar{W} \cup \bar{W}_{r-1}$ of the sets

$$\bar{W}_r = \{W' \in \bar{W} \mid W' \text{ has } r \text{ diphthongs}\},$$

and

$$\bar{W}_{r-1} = \{W' \in \bar{W} \mid W' \text{ has } (r-1) \text{ diphthongs}\}.$$

So

$$\text{card}(\bar{W}) = \text{card}(\bar{W}_r) + \text{card}(\bar{W}_{r-1}).$$

Now suppose that W has only l *distinct c.p.*'s. (The number l of course depends on the exact configuration of W. For example, the word ABBA has 4 distinct *c.p.*'s, but the word $ABAB$ has only 2). If one *c.p.* of W occurs j times in the list of i possible *c.p.*'s of W, then each of the l distinct *c.p.*'s of W occurs j times in the list, and $i = j \cdot l$. Similarly, there are $(i-r)/j$ distinct *c.p.*'s of W with r diphthongs, and r/j distinct *c.p.*'s of W with $r-1$ diphthongs.

LEMMA 8. *Denote by* $\mathscr{W}_k$ *the set of words (including repetitions) appearing in* $(A + B + AB)^k$, *and suppose that* $\bar{W} \cap \mathscr{W}_k \neq \emptyset$. *Say that* W *has* i *letters,* r *diphthongs, and* $l = i/j$ *distinct c.p.*'s. *Then* $\text{card}(\bar{W} \cap \mathscr{W}_k) = \dfrac{k\binom{r}{i-k}}{j}$.

Proof. $\bar{W} \cap \mathscr{W}_k = (\bar{W}_r \cap \mathscr{W}_k) \cup (\bar{W}_{r-1} \cap \mathscr{W}_k$, and the union is disjoint; so $\text{card}(\bar{W} \cap \mathscr{W}_k) = \text{card}(\bar{W}_r \cap \mathscr{W}_k) + \text{card}(\bar{W}_{r-1} \cap \mathscr{W}_k)$.

Since $\bar{W} \cap \mathscr{W}_k \neq \emptyset$, k can be at most i, and at the least $i-r$, because 0 at the least and r at most of the k factors used can be AB, and the rest must be either A or B. Therefore, $i - r \leqq k \leqq i$.

Case 1. $k = i - r$. Then $\bar{W}_{r-1} \cap \mathscr{W}_{i-r} = \emptyset$, as we must use r factors of AB to form W. Each of the $(i-r)/j$ distinct *c.p.*'s in $\bar{W}_r$ appear exactly once in $\mathscr{W}_k$, by choosing the r factors of AB to correspond to the positions of the r diphthongs, and choosing the appropriate factors of either A or B in the remaining $(i-2r)$ spots. Thus

$$\begin{aligned}\operatorname{card}(\bar{W} \cap \mathscr{W}_{i-r}) &= \operatorname{card}(\bar{W}_r \cap \mathscr{W}_{i-r}) \\ &= (i-r)/j = \frac{i-r}{j}\binom{r}{i-(i-r)} = \frac{k}{j}\binom{r}{i-k}.\end{aligned}$$

Case 2. $i - r + 1 \leqq k \leqq i$. We must use $(i-k)$ factors of AB to obtain i letters in all. The $\dfrac{i-r}{j}$ distinct *c.p.*'s in $\mathscr{W}_r$, affording r possible positions for the $(i-k)$ factors of AB, may each be formed in $\binom{r}{i-k}$ ways, so

$$\operatorname{card}(\bar{W} \cap \mathscr{W}_k) = \frac{i-r}{j}\binom{r}{i-k}.$$

Similarly, each of the $\dfrac{r}{j}$ distinct *c.p.*'s in $\bar{W}_{r-1}$ may be formed in $\binom{r-1}{i-k}$ ways, so $\operatorname{card}(\bar{W}_{r-1} \cap \mathscr{W}_k) = \dfrac{r}{j}\binom{r-1}{i-k}$.

For the moment set $(i-k) = m$. Then

$$\begin{aligned}\operatorname{card}(\bar{W} \cap \mathscr{W}_k) &= \operatorname{card}(\bar{W}_r \cap \mathscr{W}_k) + \operatorname{card}(\bar{W}_{r-1} \cap \mathscr{W}_k) \\ &= \frac{i-r}{j}\binom{r}{m} + \frac{r}{j}\binom{r-1}{m} \\ &= \frac{1}{j}\left(\frac{(i-r)r!}{m!(r-m)!} + \frac{r(r-1)!}{m!(r-1-m)!}\right) \\ &= \frac{1}{j}\cdot\frac{r!}{m!(r-m)!}(i-r+r-m) \\ &= \frac{1}{j}\binom{r}{m}(i-m) = \frac{i-(i-k)}{j}\binom{r}{m} \\ &= \frac{k\binom{r}{i-k}}{j}.\end{aligned}$$

LEMMA 9. *Let* $a_0, a_1, \ldots, a_r$ $(r < p/2)$ *be numbers such that*

$$a_k + a_{k+1} \equiv 0, \bmod p^2.$$

Then $\sum_{m=0}^{r} a_m \binom{r}{m} \equiv 0, \bmod p^2.$

Proof. We show by induction that for $1 \leqq k \leqq r$,

$$\sum_{m=0}^{k} a_m \binom{r}{m} \equiv \frac{(r-1)(r-2)\ldots(r-k)}{k!} a_k, \bmod p^2.$$

Base. $a_0 \binom{r}{0} + a_1 \binom{r}{1} \equiv a_0 + r a_1$

$$\equiv a_0 + a_1 + (r-1)a_1 \equiv (r-1)a_1 \bmod p^2.$$

Inductive step. Suppose for some $1 \leqq k < r$,

$$\sum_{m=0}^{k} a_m \binom{r}{m} \equiv \frac{(r-1)(r-2)\ldots(r-k)}{k!} a_k \bmod p^2. \quad \text{Then}$$

$$\sum_{m=0}^{k+1} a_m \binom{r}{m} \equiv \frac{(r-1)(r-2)\ldots(r-k)}{k!} a_k + a_{k+1} \binom{r}{k+1}$$

$$\equiv \frac{(r-1)\ldots(r-k)}{k!} a_k + \frac{r(r-1)\ldots(r-k)}{(k+1)!} a_{k+1}$$

$$\equiv \frac{(r-1)\ldots(r-k)}{k!} \left[\frac{(k+1)a_k + r a_{k+1}}{k+1} \right]$$

$$\equiv \frac{(r-1)\ldots(r-k)}{k!} \left[\frac{(k+1)(a_k + a_{k+1}) + (r-(k+1))a_{k+1}}{k+1} \right]$$

$$\equiv \frac{(r-1)\ldots(r-k)}{(k+1)!} (r-(k+1)) a_{k+1}, \bmod p^2$$

The induction is therefore completed and we may use it for $k = r$, obtaining immediately that $\sum_{m=0}^{r} a_m \binom{r}{m} \equiv 0 \bmod p^2$.

THEOREM 10. *If W is a mixed word of E, then card $(\bar{W}) \equiv 0 \bmod p^2$.*

Proof. Let us say that W begins with an A, and has i letters, r diphthongs, and $l = (i/j)$ distinct *c.p.*'s. Note that $j < i \leq p$ for a mixed word W. By lemma 8,

$$\text{card}\,(\bar{W} \cap \mathscr{W}_k) = \frac{k\binom{r}{i-k}}{j} \quad \text{when } k = (i-r), \ldots, i,$$

and otherwise is zero. So

$$\operatorname{card}(\bar{W}) = \sum_{k=i-r}^{i} \binom{p}{k} \operatorname{card}(\bar{W} \cap \mathscr{W}_k) = \frac{1}{j} \sum_{k=i-r}^{i} k \binom{p}{k} \binom{r}{i-k}.$$

But for $1 \leqq k < p$,

$$\begin{aligned} & k\binom{p}{k} + (k+1)\binom{p}{k+1} \\ &= \frac{k \cdot p!}{k!(p-k)!} + \frac{(k+1)p!}{(k+1)!(p-(k+1))!} \\ &= p!\left[\frac{k + (p-k)}{k!(p-k)!}\right] \\ &= p\binom{p}{k} \equiv 0 \bmod p^2 \end{aligned}$$

Letting

$$m = r - (i-k) \quad \text{and} \quad a_m = k\binom{p}{k}$$

we have

$$\begin{aligned} \operatorname{card}(\bar{W}) &= \frac{1}{j} \sum_{k=i-r}^{i} k \binom{p}{k} \binom{r}{i-k} \\ &= \frac{1}{j} \sum_{m} a_m \binom{r}{m}, \text{ summation on } m = r - (i - (i-r)) \text{ to } m = r - (i-i) \\ &= \frac{1}{j} \sum_{m=0}^{r} a_m \binom{r}{m} \equiv 0 \bmod p^2 \end{aligned}$$

by lemma 9.

COROLLARY 11. $\phi(E) = \phi\left(\sum_{k=1}^{p} \binom{p}{k} A^k\right) + \phi\left(\sum_{k=1}^{p} \binom{p}{k} B^k\right)$.

Proof. Recall that the characteristic of $\mathfrak{W}_2(\kappa)$ is p^2. By lemma 7,

$$\phi(E) = \sum_{\bar{W} \subseteq \mathscr{W}} \operatorname{card}\ (\bar{W})\, \phi(W) \in \mathfrak{W}_2(\kappa)$$

where $\mathscr{W}$ is the set of all words (including repetitions) in E. By theorem 10, $\operatorname{card}(\bar{W}) \equiv 0 \bmod p^2$ whenever W is a mixed word, so $\operatorname{card}(\bar{W}) = 0$ in $\mathfrak{W}_2(\kappa)$ for

every mixed word W. The non-mixed words of E are A^k and B^k for $k = 1, \ldots, p$, which have only one distinct *c.p.*, and $\binom{p}{k}$ copies in $\mathscr{W}$; that is,

$$\operatorname{card}(\overline{A^k}) = \operatorname{card}(\overline{B^k}) = \binom{p}{k}$$

Thus $\phi(E) \equiv \phi\left(\sum_{k=1}^{p} \binom{p}{k} A^k\right) + \phi\left(\sum_{k=q}^{p} \binom{p}{k} B^k\right)$.

THEOREM 12. *For $u, v \in \mathscr{U}$, $R\theta(uv) = R\theta(u) + R\theta(v)$.*

Proof. Let $u = A + I$, $v = B + I$; then $A, B \in \mathscr{U}'$, and

$$\begin{aligned} p\theta(uv) &= \phi\left(\sum_{k=1}^{p} \binom{p}{k} (A + B + AB)^k\right. \\ &= \phi(E) = \phi\left(\sum_{k=1}^{p} \binom{p}{k} A^k\right) + \phi\left(\sum_{k=1}^{p} \binom{p}{k} B^k\right) \\ &= p\theta(u) + p\theta(v) \\ &= p(\theta(u) + \theta(v)). \end{aligned}$$

Now for $y = (y_0, y_1)$, $z = (z_0, z_1)$ in $\mathfrak{W}_2(\kappa)$,

$$\begin{aligned} py = pz &\Leftrightarrow (0,1)(y_0, y_1) = (0,1)(z_0, z_1) \\ &\Leftrightarrow (0, y_0^p) = (0, z_0^p) \Leftrightarrow y_0 = z_0, \end{aligned}$$

since κ is a field of characteristic p. That is $py = pz \Leftrightarrow R(y) = R(z)$. We thus have $R\theta(uv) = R(\theta(u) + \theta(v)) = R\theta(u) + R\theta(v)$.

PART IV

In this section we construct a solvable algebraic group G in characteristic $p > 0$, having a unipotent automorphism σ, and two σ-stable maximal tori *not* conjugate by a σ-fixed point:

Take $\mathfrak{G}$, $\mathfrak{T}$, $\mathfrak{U}$, σ, θ, as in Part I. Let $U = \{u \in \mathfrak{U} \mid \theta(u) = 0\}$. Then by Theorems 3 and 12, θ is a rational representation on $\mathfrak{U}$, so U is an algebraic group. When κ is algebraically closed, as we assume, $\dim U > 0$.

LEMMA 13. *U is σ-stable.*

Proof. For $u \in \mathfrak{U}$, $\rho(u)$ *is in* $\mathscr{U}$. $\rho(\sigma(u)) = \hat{\sigma}(\rho(u))$, and by Cor. 2, $\theta(\sigma(u)) = R\hat{\theta}\rho(\sigma(u)) = R\hat{\theta}\hat{\sigma}(\rho(u))$. But for $v \in \mathscr{U}$, $\hat{\phi}(\hat{\sigma}(v)) = \sum_{i=1}^{p} \hat{\sigma}^i(\hat{\sigma}(v)) = \sum_{i=1}^{p} \hat{\sigma}^i(v) = \hat{\phi}(v)$;

so

$$p\hat{\theta}(\hat{\sigma}(v)) = \hat{\phi}((\hat{\sigma}(v))^p) = \hat{\phi}(\hat{\sigma}(v^p)) = \hat{\phi}(v^p) = p\hat{\theta}(v).$$

As in the proof of Theorem 12, this implies that $R\hat{\theta}(\hat{\sigma}(v)) = R\hat{\theta}(v)$. Thus:

$$\theta(\sigma(u)) = R\hat{\theta}(\hat{\sigma}(\rho(u))) = R\hat{\theta}(\rho(u)) = R\hat{\theta}\rho(u) = \theta(u).$$

In particular, $\theta(u) = 0 \Rightarrow \theta(\sigma(u)) = 0$, so U is σ-stable.

Set $T = \mathfrak{T}$. Then:

LEMMA 14. *U is T-stable.*

Proof. Observe that $\rho(T)$ is diagonal and consists of "blocks" such that for $S \in \rho(T)$, if S_i denotes the i^{th} block of $\rho(T)$, then $(S_i)_{1,1} = (S_i)_{p+1,p+1}$. Moreover S^{-1} exists and is simply $\rho(t^{-1})$, where $S = \rho(t) \in \rho(T)$. Hence

$$(SvS^{-1})_{1,p+1} = S_{1,1}(S^{-1})_{p+1,p+1}v_{1,p+1} = v_{1,p+1},$$

for all $S \in \rho(T)$, $v \in \mathscr{U}$, and thus

$$\hat{\phi}(SvS^{-1}) = \sum_{i=1}^{p} [\hat{\sigma}^i(SvS^{-1})]_{1,p+1} = \sum_{i=1}^{p} \hat{\sigma}^i(v)_{1,p+1} = \hat{\phi}(v),$$

for all $v \in \mathscr{U}$. So $p\hat{\theta}(SvS^{-1}) = \hat{\phi}((SvS^{-1})^p) = \hat{\phi}(Sv^pS^{-1}) = \hat{\phi}(v^p) = p\hat{\theta}(v)$. Observing also that for $t \in T$, $u \in U$,

$$[\rho(t)\rho(u)\rho(t)^{-1}]_{i,j} = \rho(t)_{i,i}\rho(t^{-1})_{j,j}\rho(u)_{i,j}$$

$= (t_{i,i}, 0)(t_{j,j}^{-1}, 0)(u_{i,j}, 0) = (t_{i,i}t_{j,j}^{-1}u_{i,j}, 0) = ((tut^{-1})_{i,j}, 0)$, we see that

$$\rho(tut^{-1}) = \rho(t)\rho(u)\rho(t)^{-1}.$$

It follows that

$$\theta(tut^{-1}) = R\hat{\theta}\rho(tut^{-1}) = R\hat{\theta}(\rho(t)\rho(u)\rho(t)^{-1}) = R\hat{\theta}(\rho(u)) = \theta(u),$$

as in the proof of Lemma 13, so U is T-stable.

Hence, $G = T \cdot U$ is a σ-stable solvable algebraic group with σ-stable maximal torus T. Its σ-fixed points are those of its matrices M for which $M_1 = M_2 = \ldots = M_p$. The cartan subgroup $C(T) = T \times C_u$ consists of those of its matrices X for which $(X_i)_{kj} = 0$ when $k \neq j$ and $(k,j) \neq (1,p+1)$. The condition $\theta(X) = 0$ on C_u amounts to $\theta(X) = \sum_{i=1}^{p} (X_i)_{1,p+1} = 0$.

Therefore, if U has a matrix X such that $X^{-1} \cdot \sigma(X) \in C_u$ and

$$X^{-1} \cdot \sigma(X) \notin \{c^{-1} \cdot \sigma(c) \mid c \in C_u\},$$

then XTX^{-1} is a σ-stable maximal torus of G which is *not* conjugate to T by a σ-fixed point of G. We now exhibit such an element X.

Let $X \in U$ be given by $(X_i)_{k,j} = a \neq 0$ for $k < j$ and $(k,j) \neq (1,p+1)$, $i = 1,\ldots,p$.

Note that $X = A \cdot Y$ where

$$A_1 = A_2 = \ldots = A_p = \begin{bmatrix} 1 & a & a & \cdot & \cdot & & a & a & 0 \\ & 1 & a & a & \cdot & \cdot & \cdot & a & a \\ & & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & a \\ & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & & \cdot & \cdot & \cdot & a \\ & & & & & & \cdot & a & a \\ & & & & & & & 1 & a \\ & & & & & & & & 1 \end{bmatrix}$$

(i.e., $(A_i)_{kj} = a$, $k < j$, $(k,j) \neq (1,p+1)$, and $(A_i)_{1,p+1} = 0$) and

$$Y_i = \begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & 0 & X_i \\ & 1 & 0 & 0 & \cdot & \cdot & 0 \\ & & 1 & 0 & 0 & \cdot & \cdot \\ & & & \cdot & \cdot & \cdot & \cdot \\ & & 0 & & \cdot & \cdot & 0 \\ & & & & & \cdot & 0 \\ & & & & & & 1 \end{bmatrix}$$

where $x_i = (X_i)_{1,p+1}$

Although A and Y are not in U, they are in $\mathfrak{U}$, so θ is defined on them separately, and $\theta(X) = \theta(AY) = \theta(A) + \theta(Y)$. $\theta(Y)$ amounts to $\sum_{i=1}^{p} x_i$; and as A is σ-fixed, $\theta(A)$ amounts to:

$$\sum_{k=1}^{p-1} \left(\binom{p}{k} \Big/ p \right) \left[\sum_{i=1}^{p} (\sigma^i(A^k))_{1,p+1} \right] + (A^p)_{1,p+1}$$

$$= \sum_{k=1}^{p-1} \binom{p}{k} (A^k)_{1,p+1} + (A^p)_{1,p+1} = a^p$$

Therefore the condition $\theta(X) = 0$ amounts to $\sum_{i=1}^{p} x_i = -a^p$. We may note here

that Y (hence X) cannot then be σ-fixed. For if it were, $\sum_{i=1}^{p} x_i = \sum_{i=1}^{p} [\sigma^i(Y)]_{1,p+1}$ would be $px_1 = 0$.

Now $X^{-1} \cdot \sigma(X) = Y^{-1}A^{-1}\sigma(A)\sigma(Y) = Y^{-1}\sigma(Y)$, which is given by

$$[Y^{-1}\sigma(Y)]_i = \begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & 0 & 0 & (x_{i+1} - x_i) \\ & 1 & 0 & 0 & \cdot & \cdot & 0 & 0 \\ & & 1 & 0 & 0 & \cdot & \cdot & 0 \\ & & & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & \cdot & \cdot & \cdot & \cdot \\ & & 0 & & & \cdot & \cdot & 0 \\ & & & & & & 1 & 0 \\ & & & & & & & 1 \end{bmatrix}$$

for $i = 1, \ldots, p-1$. The p^{th} block is similar, with corner entry $(x_1 - x_p)$. Thus $X^{-1}\sigma(X)$ is in C_u.

Suppose, though, that $\exists\, Z \in C_u$ such that $X^{-1} \cdot \sigma(X) = Z^{-1} \cdot \sigma(Z)$. Let $(Z_i)_{1,p+1} = z_i$, $i = 1, \ldots, p$. Then

$$\begin{aligned} ([Z^{-1} \cdot \sigma(Z)]_i)_{1,p+1} &= z_{i+1} - z_i,\ i = 1, \ldots, p-1 \\ &= z_1 - z_p,\ i = 1 \end{aligned}$$

Therefore:

$$\begin{aligned} z_2 - z_1 &= x_2 - x_1 \\ z_3 - z_2 &= x_3 - x_2 \\ &\vdots \qquad\quad \vdots \\ z_k - z_{k-1} &= x_k - x_{k-1} \\ &\vdots \qquad\quad \vdots \\ z_p - z_{p-1} &= x_p - x_{p-1} \end{aligned}$$

Adding the first $(k-1)$ equations above we obtain $z_k - z_1 = x_k - x_1$, for $k = 2, \ldots, p$. Hence,

$$\sum_{k=1}^{p} z_k = \sum_{k=1}^{p} (z_k - z_1) = \sum_{k=1}^{p} (x_k - x_1) = \sum_{k=1}^{p} x_k$$

But the conditions $\theta(Z) = 0$, $\theta(X) = 0$ dictate that

$$0 = \sum_{k=1}^{p} z_k = \sum_{k=1}^{p} x_k = -a^p \neq 0.$$

Hence there can be no such $Z \in C_u$; whence the σ-stable maximal torus XTX^{-1} cannot be conjugate to T by a σ-fixed point of G.

Note. The work represented by the paper was undertaken and completed at Purdue University, West Lafayette, Indiana.

REFERENCES

1. S. J. Gottlieb, *Automorphisms of Algebraic Groups with Stable Maximal Tori.* Doctoral Dissertation, Rutgers University, 1973.
2. ———, *Algebraic Automorphisms of Algebraic Groups with Stable Maximal Tori,* Pacific J. Math. (2) 72 (1977), 461–470.
3. N. Jacobson, *Lectures in Abstract Algebra,* Volume III. D. Van Nostrand Co. Inc., Princeton, N.J., 1964.

Bell Telephone Laboratories
Whippany, New Jersey 07981.