Can. J. Math., Vol. XXIV, No. 3, 1972, pp. 369–378

INVOLUTORY MATRICES OVER FINITE LOCAL RINGS

B. R. McDONALD

1. Introduction. A square matrix A over a commutative ring R is said to be involutory if $A^2 = I$ (identity matrix). It has been recognized for some time that involutory matrices have important applications in algebraic cryptography and the special cases where R is either a finite field or a quotient ring of the rational integers have been extensively researched. However, there has been no detailed attempt to extend the theory to all finite commutative rings. In this paper we illustrate in detail the theory of involutory matrices over finite commutative rings with 1 having odd characteristic. The method is a careful analysis of finite local rings of odd prime power characteristic. The techniques might be also used in the examination of involutory matrices over local rings of characteristic 2^λ; however, as illustrated by finite fields of characteristic 2 and $Z/2^\lambda Z$ (Z the rational integers), the arguments are basically different. The reader will note the methods are not limited to only questions on involutory matrices.

Acknowledgement. The author would like to express his appreciation to Joel Brawley and John Fulton for communications on several occasions.

2. Preliminaries and notation. Let S denote a finite commutative ring with identity. Since S is Artinian there exists a ring direct sum decomposition of S, $S = \oplus \sum_{i=1}^{t} R_i$, into finite local rings R_i where t is unique and the R_i are unique up to ring isomorphism (for example, see [**1**, Theorem 8.7, p. 90]. If $(S)_n$ and $\mathrm{GL}_n(S)$ denote the ring of n by n matrices over S and the invertible n by n matrices over S, respectively, then the above decomposition induces naturally

$$(S)_n = \oplus \sum_{i=1}^{t} (R_i)_n \text{ and } \mathrm{GL}_n(S) = \oplus \sum_{i=1}^{t} \mathrm{GL}_n(R_i).$$

Thus, for most questions we may reduce the study of matrices over finite commutative rings to matrices over finite local rings. Observe that if A in $(S)_n$ has the decomposition $A = A_1 \oplus \ldots \oplus A_t$, then A is involutory if and only if each A_i is involutory. Thus, we restrict our attention to $(R)_n$ where R is a finite local ring.

We now introduce conventions and notation which will be utilized throughout the paper. We let R denote a finite local ring with maximal ideal M and finite residue field $K = R/M$. The maximal ideal is nilpotent and we let β

Received December 15, 1970 and in revised form, March 21, 1972.

denote the least positive integer satisfying $M^\beta = 0$; i.e., β is the degree of nilpotency of M. For simplicity we refer to β as the *nilpotency of* R.

The characteristic of R, $\chi(R)$, is a power of a prime $\chi(R) = p^\lambda$ ($\lambda \geqq 1$). Indeed R contains a copy of Z/Zp^λ. The case where $\chi(R) = 2^\lambda$ causes considerable difficulty (for example, see [**10**] for finite fields of characteristic 2 and [**3**] for $Z/Z2^\lambda$). For this reason we assume throughout that $\chi(R) = p^\lambda$ where p is an *odd* prime.

If T is a finite set we denote the cardinality of T by $|T|$ and the set of n by n matrices with elements in T by $(T)_n$.

It is important to observe that we have the following natural sequence of ring morphisms σ_i, $2 \leqq i \leqq \beta$,

$$R = R/M^\beta \xrightarrow{\sigma_\beta} R/M^{\beta-1} \to \ldots \to R/M^i \xrightarrow{\sigma_i} R/M^{i-1} \to \ldots \to R/M^2 \xrightarrow{\sigma_2} R/M = K$$

where $\ker(\sigma_i) = M^{i-1}/M^i$. Let $\sigma_1 : K \to 0$ and take $M^0 = R$; thus $\ker(\sigma_1) = M^0/M^1$. We denote R/M^i by $R^{(i)}$ for $1 \leqq i \leqq \beta$. Also for each i we have a natural ring morphism $\mu_i : R^{(i)} \to K$ with $\ker(\mu_i) = M/M^i$.

For simplicity of notation we will suppress the subscript i on σ_i and μ_i using only σ and μ. Further, the morphism $\sigma : R^{(i)} \to R^{(i-1)}$ (respectively, $\mu : R^{(i)} \to K$) induces natural morphisms $(R^{(i)})_n \to (R^{(i-1)})_n$ (respectively, $(R^{(i)})_n \to (K)_n$) and $\mathrm{GL}_n(R^{(i)}) \to \mathrm{GL}_n(R^{(i-1)})$ (respectively, $\mathrm{GL}_n(R^{(i)}) \to \mathrm{GL}_n(K)$). These morphisms will also be denoted by σ (respectively, μ).

Let ϕ_i denote the cardinality of M^{i-1}/M^i for $1 \leqq i \leqq \beta$. We call $\{\phi_1, \ldots, \phi_\beta\}$ the *invariants* of R. Observe

$$|R| = \prod_{i=1}^{\beta} \phi_i.$$

THEOREM 2.1. *Let R be a finite local ring. Then*

$$|\mathrm{GL}_n(R)| = |R|^{n^2} \prod_{i=0}^{n-1} (1 - \phi_1^{i-n}).$$

We take $|\mathrm{GL}_0(R)| = 1$.

Proof. Observe $\mu : \mathrm{GL}_n(R) \to \mathrm{GL}_n(K)$ is surjective. Thus

$$|\mathrm{GL}_n(R)| = |\ker(\mu)|\,|\mathrm{GL}_n(K)|.$$

But

$$|\mathrm{GL}_n(K)| = |K|^{n^2} \prod_{i=0}^{n-1} (1 - \phi_1^{i-n})$$

where $\phi_1 = |K|$ and $|\ker(\mu)| = |M|^{n^2}$. Since $|R| = |M||K|$ the result follows.

We remark that the characteristic of R does not enter into the proof. Thus the above is valid for all finite local rings. Indeed, R does not even need to be commutative.

To conclude this section we single-out two items which will be used repeatedly. First, for $\sigma : R^{(i)} \to R^{(i-1)}$ the kernel of σ is the ideal M^{i-1}/M^i in $R^{(i)}$; hence $(M^{i-1}/M^i)_n$ is a two-sided ideal in $(R^{(i)})_n$. Further, since the

product of any two elements in M^{i-1}/M^i is in M^i/M^i and is thus zero, we have that the product of any two matrices in $(M^{i-1}/M^i)_n$ is the zero matrix. Second, $(R^{(i-1)})_n$ is the image of $(R^{(i)})_n$ under σ. Thus if $\bar{A}$ is in $(R^{(i-1)})_n$ then we may write a preimage A under σ as

$$A = \bar{A} + N$$

where N may be chosen arbitrarily in $(M^{i-1}/M^i)_n$. Indeed, without loss we may think of $\bar{A}$ as also an element of $(R^{(i)})_n$ (if we are careful with multiplication). This is often implicitly done in classical number theory—the element p is in Z/Zp^k and in Z/Zp^{k+1} but in the former ring $p^k = 0$ while in the latter ring $p^k \neq 0$.

3. Involutory matrices—canonical sets under similarity. Again we repeat that R denotes a finite local ring with $\chi(R) = p^\lambda$ (p odd prime).

Hodges [**9**] determined a canonical set under similarity for the n by n involutory matrices over a finite field of odd characteristic. Hodges further determined the number of such matrices. Brawley [**2**] extended the canonical set to Z/Zp^β (p odd prime) and enumerated the matrices for this case. The even characteristic is discussed in [**10**] (for finite fields) and in [**3**] (for $Z/2^\beta Z$). We now establish the Brawley-Hodges canonical form for finite local rings of odd prime power characteristic.

THEOREM 3.1. *Let R be a finite local ring and A be in $\mathrm{GL}_n(R)$. Then $A^2 = I$ if and only if there exists a Q in $\mathrm{GL}_n(R)$ and a unique t, $0 \leqq t \leqq n$, with*

$$QAQ^{-1} = J_t$$

where $J_t = \mathrm{diag}(I_t, -I_{n-t})$ (I_s denotes an s by s identity matrix).

Proof. Let V be a free R-module of R-dimension n. The matrix A determines naturally an R-linear morphism $\alpha : V \to V$ with $\alpha^2 = i_V$. Let

$$N(\alpha) = \{x \text{ in } V | \alpha(x) = x\} \quad \text{and} \quad P(\alpha) = \{x \text{ in } V | \alpha(x) = -x\}.$$

Clearly $N(\alpha) \cap P(\alpha) = 0$. If x is in V, expressing x as

$$x = \tfrac{1}{2}(x - \alpha(x)) + \tfrac{1}{2}(\alpha(x) + x)$$

(note: 2 is a unit in R) shows that $V = N(\alpha) + P(\alpha)$. Thus $V = N(\alpha) \oplus P(\alpha)$ and since V is R-free we have that $N(\alpha)$ and $P(\alpha)$ are projective R-modules. But projective modules over local rings are free. Thus if $\{v_1, \ldots, v_t\}$ and $\{w_1, \ldots, w_{n-t}\}$ are free R-bases for $N(\alpha)$ and $P(\alpha)$, respectively, then their union is a free basis for V. The matrix of α relative to this basis is J_t. It remains only to check uniqueness. Here recall that if W is a free R-module then $\{w_1, \ldots, w_s\}$ is a free R-basis of W if and only if their images form a K-basis for W/MW. This reduces the problem to the field case where uniqueness is well known.

The above proof replaces the matrix theoretic approach of Hodges and Brawley and is easier. Note that the proof is also valid for non-commutative local rings.

We now enumerate the n by n involutory matrices in $\mathrm{GL}_n(R)$.

Let $S(n, t, R)$ denote the number of distinct n by n matrices in $(R)_n$ similar to J_t. This number is determined by letting $\mathrm{GL}_n(R)$ act as a transformation group on $(R)_n$ by conjugation, i.e., let

$$\mathrm{GL}_n(R) \times (R)_n \to (R)_n$$

by

$$\langle G, A \rangle \to GAG^{-1}.$$

Then $S(n, t, R)$ is the cardinality of the orbit of J_t and is $[\mathrm{GL}_n(R) : I(J_t)]$, the index of the stabilizer $I(J_t)$ of J_t in $\mathrm{GL}_n(R)$. Thus, we need only compute $|I(J_t)|$. But this is easily seen to be $|\mathrm{GL}_t(R)||\mathrm{GL}_{n-t}(R)|$. Hence

$$S(n, t, R) = \frac{|\mathrm{GL}_n(R)|}{|\mathrm{GL}_t(R)|\,|\mathrm{GL}_{n-t}(R)|}$$

$$= |R|^{2t(n-t)} \frac{g_n}{g_t g_{n-t}}$$

where

$$g_s = \prod_{i=0}^{s-1} (1 - \phi_1{}^{i-s})$$

(Recall $\phi_1 = |R/M|$ and $g_0 = 1$.) Consequently, the number N of involutory matrices in $\mathrm{GL}_n(R)$ is

$$N = \sum_{t=0}^{n} S(n, t, R) = g_n \sum_{t=0}^{n} \left(|R|^{2t(n-t)} \frac{1}{g_t g_{n-t}} \right).$$

We now give the extension of another well-known result on involutory matrices over finite fields and Z/Zp^β. It was first proven by Levine and Nahikian [**10**] for fields of odd prime characteristic and later by Brawley [**4**] for quotient rings of rational integers. If an n by n matrix A is involutory and $QAQ^{-1} = J_t$ (J_t defined in Theorem 3.1) then the integer $s = n - t$ is called the *signature* of A. We take $s = 0$ if and only if $A = I_n$.

THEOREM 3.2. *Let R be a finite local ring and A in $\mathrm{GL}_n(R)$. Then A is involutory of signature t if and only if A has the form $I_n - 2QP$ where Q and P^T are n by s matrices over R and $PQ = I_s$.*

Proof. Using (3.1) the proof is easily adapted from [**10**] and [**4**].

In Theorem 3.2 two matrix pairs $\langle Q, P \rangle$ and $\langle Q', P' \rangle$ may yield the same involutory matrix. We now utilize Brawley's technique [**4**] to account for this duplicity. As utilized above, if P is a matrix over R we say the *rank* of P is the rank of μP as a matrix over $\mu R = K$.

If P is an s by n matrix over R, the *Q-set* (P) of P is

$$(P) = \{Q | Q \text{ is } n \text{ by } s, \operatorname{rank}(Q) = s \text{ and } PQ = I_s\}.$$

The *P-class* $[P]$ of P is the corresponding set of involutory matrices

$$[P] = \{I_n - 2QP | Q \text{ is in } (P)\}.$$

We now state two results for finite local rings of odd prime power characteristic which were initially observed by Brawley for finite fields and Z/Zp^{β}. The proofs given by Brawley (see [**4**, Theorems 3 and 4, pp. 474–475]) suffice also for this setting.

THEOREM 3.3. *If P is an s by n matrix of rank s $(s > 0)$ over R, then the map*

$$Q \to I_n - 2QP$$

determines a bijection between (P) and $[P]$.

THEOREM 3.4. *Let P and P' be s by n matrices of rank s over R. Then $[P] = [P']$ if and only if there exists an invertible matrix B in $\mathrm{GL}_s(R)$ with $P = BP'$. Further, the classes $[P]$ and $[P']$ are either identical or disjoint.*

LEMMA 3.5. *Let R be a finite local ring. If P is an s by n $(s \leqq n)$ matrix over R with rank s and $\sigma(n, s)$ denotes the number of n by s matrices X satisfying*

$$PX = I_s,$$

then

$$\sigma(n, s) = |R|^{s(n-s)}.$$

Prior to the proof we make several remarks concerning matrices under equivalence transformations. Yohe ([**11**]; in particular, [**11**, Theorem III, p. 344]) has shown that in general a matrix P over a Noetherian local ring R can be brought to diagonal form under equivalence; i.e., TPU = diagonal matrix where T and U are invertible, if and only if the maximal ideal of R is principal. However, it is easy to convince oneself that if P is s by n *and* of rank s, then there exist invertible T (s by s) and U (n by n) such that

$$TPU = [I_s, 0].$$

Important to this is the observation that under the map $\mu : R \to K$ a preimage of a non-zero element of K is a unit of R.

Proof. Consider $PX = I_s$ where P is s by n and of rank s and X is n by s. By the above comment there exist T (s by s) and U (n by n) such that

$$TPU = [I_s, 0].$$

Thus, letting $\bar{Y} = U^{-1}X$ the above equation is equivalent to

$$[I_s, 0]\bar{Y} = T.$$

Partitioning $\bar{Y} = [\bar{Y}_1, \bar{Y}_2]^T$ where $\bar{Y}_1$ is s by s and $\bar{Y}_2$ is $n - s$ by s we see that

$\bar{Y}_1 = T$ and $\bar{Y}_2$ is arbitrary. Consequently, there exist $|R|^{s(n-s)}$ choices for $\bar{Y}$ and hence for X.

COROLLARY 3.6. *If P is an s by n matrix of rank s over R, then*

$$|P| = |R|^{s(n-s)}.$$

4. Symmetric involutory matrices. In this section we examine symmetric involutory matrices over finite local rings. The work in this area was pioneered for finite fields and for Z/Zp^{λ} by Fulton [**7**]. Note that for any commutative ring R and matrix A in $(R)_n$, any two of the following imply the third.

(a) A is involutory.
(b) A is symmetric.
(c) A is orthogonal.

We continue the assumption that R has odd prime power characteristic.

LEMMA 4.1. *Let R be a finite local ring. Let α_1, α_2, χ be units of R. Then there exist elements ξ and η (of which at least one is a unit) with*

$$\alpha_1\xi^2 + \alpha_2\eta^2 = \chi.$$

Proof. The proof is by induction on the nilpotency β of R. If $\beta = 1$ then R is a finite field and this is handled by Dickson [**6**, p. 46]. Thus assume the result is true for $R^{(i-1)}$ where $\beta > i \geqq 1$. Consider $R^{(i)}$ and $\sigma : R^{(i)} \to R^{(i-1)}$.

We may suppose there exist ξ_{i-1} and η_{i-1} in $R^{(i)}$ (one of which is a unit) such that

$$\alpha_1\xi^2{}_{i-1} + \alpha_2\eta^2{}_{i-1} = \chi + m$$

where m is in M^{i-1}/M^i. Let

$$\xi_i(\delta) = \xi_{i-1} + \delta m$$
$$\eta_i(\beta) = \eta_{i-1} + \beta m.$$

Since a unit plus a nilpotent is a unit, one of $\xi_i(\delta)$ or $\eta_i(\beta)$ is a unit for every choice of δ and β in $R^{(i)}$. Consider

$$\alpha_1\xi_i{}^2(\delta) + \alpha_2\eta_i{}^2(\beta) = \chi + 2\xi_{i-1}\delta m + 2\eta_{i-1}\beta m + m.$$

We want to choose δ or β so that

$$2\xi_{i-1}\delta m + 2\eta_{i-1}\beta m + m = 0$$

in $R^{(i)}$. This is possible since either $2\xi_{i-1}\delta$ or $2\eta_{i-1}\beta$ is a unit.

THEOREM 4.2. *Let R be a finite local ring. A matrix A in $(R)_n$ is involutory symmetric of signature s if and only if*

$$A = I_n - 2P^T D_\epsilon P$$

where

(1) P *is* s *by* n.
(2) $D_\epsilon = \operatorname{diag}(I_{s-1}, \epsilon)$ *where* $\epsilon = 1$ *or* ϵ *is an arbitrary non-square unit of* R.
(3) $PP^T = D_\epsilon^{-1}$.

Proof. Suppose $A = I_n - 2P^T D_\epsilon P$ where P and D_ϵ satisfy (1), (2), and (3). Set $Q = P^T D_\epsilon$. Then by Theorem 3.2 A is involutory of signature s. Clearly A is symmetric.

Assume A is involutory symmetric of signature s in $(R)_n$. Then by Theorem 3.2, $A = I - 2QP$. Since A is symmetric $QP = P^T Q^T$ and $Q = P^T Q^T Q$. Thus $N = Q^T Q$ is an s by s invertible symmetric matrix and

$$A = I - 2P^T NP.$$

The technique described by Dickson [**6**, p. 158] can be modified for a finite local ring. Thus there exists an s by s invertible matrix B with

$$B^T NB = \operatorname{diag}[I_r, \epsilon I_{s-r}]$$

for some r in $\{0, 1, 2, \ldots, s\}$ where ϵ is a non-square unit or $\epsilon = 1$ (in this case $r = s$). Now, if $r - s > 1$, following Fulton, let

$$C = \operatorname{diag}\left[I_r, \begin{bmatrix} \alpha & -\delta \\ \delta & \alpha \end{bmatrix}, I_{s-r-2} \right]$$

where by Lemma 4.1, $\alpha^2 + \delta^2 = \epsilon$. Then

$$C^T B^T NBC = \operatorname{diag}[I_r, \epsilon^2 I_2, \epsilon I_{s-r-2}].$$

Repeating the argument we eventually determine an invertible F with

$$F^T NF = \operatorname{diag}[I_{s-1}, \epsilon]$$

where $\epsilon = 1$ or ϵ is a non-square unit.

In enumerating the symmetric involutory matrices we will proceed by induction on the nilpotency of R. The count when R has nilpotency 1, i.e., R is a finite field of odd prime characteristic, is given by Fulton. We need the following lemma.

LEMMA 4.3. *The element* ϵ *of* $R^{(i)}$ *is a non-square unit if and only if* $\sigma\epsilon$ *is a non-square unit of* $R^{(i-1)}$.

Proof. Certainly if $\sigma\epsilon$ is a non-square unit then ϵ is a non-square unit.

Conversely, suppose ϵ is a non-square unit and $\sigma\epsilon = \alpha^2$. Then $\epsilon = \alpha^2 + m$ where m is in M^{i-1}/M^i. We now show that an element x may be chosen so that $\alpha^2 + m = (\alpha + x)^2$ thus contradicting choice of ϵ. If $\alpha^2 + m = (\alpha + x)^2$ the element x must satisfy $x^2 + 2\alpha x = m$. If we select x in M^{i-1}/M^i this reduces to $2\alpha x = m$ or $x = (2\alpha)^{-1} m$ since 2α is a unit.

Prior to the next result we need some observations on the $\ker(\sigma)$ for $\sigma : R^{(i)} \to R^{(i-1)}$. The $\ker(\sigma) = M^{i-1}/M^i$. Since, as an R-module, M^{i-1}/M^i has an R-annihilator M then M^{i-1}/M^i is naturally a $K = R/M$ vector space

of finite dimension. Thus, we may select and fix once and for all a K-basis $\alpha_1, \ldots, \alpha_t$ in M^{i-1}/M^i and for each element m of M^{i-1}/M^i may be expressed uniquely as $m = \sum k_i\alpha_i$ where the k_i are considered in K. For simplicity we suppress reference to the basis and write $m = \langle k_1, \ldots, k_t\rangle$. Further, if r is in $R^{(i)}$ then $r = \bar{r} + m$ where m is in M/M^i. Then

$$rm = \langle \bar{r}k_1, \ldots, \bar{r}k_t\rangle$$

since $m\alpha_i = 0$.

The above is motivated by the following observation. The kernel of the natural map $Z/Zp^n \to Z/Zp^{n-1}$ is $Zp^{n-1}/Zp^n = \{ap^{n-1} | a \text{ in } Z/Zp\}$ which is a Z/Zp-vector space of dimension 1. Further, to say $ap^{n-1} \equiv bp^{n-1} \pmod{p^n}$ implies $a \equiv b \pmod{p}$ means that the two Z/Zp-vectors are equal if and only if their Z/Zp-scalars are equal.

The above comments extend naturally to the matrix ring. Thus if N is in $(M^{i-1}/M^i)_n$ then

$$N = \langle \bar{N}_1, \ldots, \bar{N}_t\rangle$$

where $\bar{N}_i$ is considered in $(K)_n$. We employ bar notation to indicate elements considered in or over K.

For $1 \leqq i \leqq \beta$ let

$$\psi_i = \dim_k(M^{i-1}/M^i).$$

Note for i, $\phi_1\psi_i = \phi_i$.

We now consider solutions of $YY^T = D_\epsilon^{-1}$ in $(R)_n$ where ϵ is a non-square unit of R.

LEMMA 4.4. *Let ϵ be a non-square unit of $R^{(i)}$. Let $\sigma\epsilon = \rho$. Let $D_\epsilon^{-1} = \operatorname{diag}[I_{s-1}, \epsilon^{-1}]$. Then the s by n matrix P in $(R^{(i)})_n$ is a solution to $YY^T = D_\epsilon^{-1}$ if and only if $P = P_1 + A$ and*

$$P_1P_1^T = D_\rho^{-1} + N$$

where

$$A = \langle \bar{A}_1, \ldots, \bar{A}_{\psi_i}\rangle$$
$$N = \langle \bar{N}_1, \ldots, \bar{N}_{\psi_i}\rangle$$

are matrices over M^{i-1}/M^i satisfying

$$\bar{A}_jP_1^T + P_1\bar{A}_j^T = \bar{S}_j - \bar{N}_j \quad (1 \leqq j \leqq \psi_i)$$

where $\bar{S}_j$ is given by

$$D_\epsilon^{-1} = D_\rho^{-1} + S, S = \langle \bar{S}_1, \ldots, \bar{S}_{\psi_i}\rangle.$$

Proof. Let the s by n matrix P over $R^{(i)}$ satisfy $YY^T = D_\epsilon^{-1}$. Then $\sigma P = P_1$; i.e., $P = P_1 + A$, A in $(M^{i-1}/M^i)_n$, and $P_1P_1^T = D_\rho^{-1}$ in $(R^{(i-1)})_n$. Thus $P_1P_1^T = D_\rho^{-1} + N$ for N in $\ker(\sigma)$. Then

$$D_\rho^{-1} + S = D_\epsilon^{-1} = (P_1 + A)(P_1 + A)^T = D_\rho^{-1} + N + AP_1^T + P_1A^T.$$

Therefore

$$\bar{S}_j = \bar{N}_j + \bar{A}_j P_1^T + P_1 \bar{A}_j^T$$

for $1 \leqq j \leqq \psi_i$.

Conversely, if $P = P_1 + A$ with A described above, then

$$PP^T = P_1 P_1^T + AP_1^T + P_1 A^T = D_\rho^{-1} + N + (S - N) = D_\epsilon^{-1}.$$

We note that the above holds also if $\epsilon = 1$.

Let $N(i, \beta)$ denote the number of distinct solutions over $(R^{(i)})_n$ of the matrix equation $YY^T = D_\beta^{-1}$. For a given P_1 and $S - N$ over $(R^{(i)})_n$ and $(M^{i-1}/M^i)_n$, respectively, let $T(i, j)$ denote the number of distinct solutions X in $(K)_n$

$$X\bar{P}_1^T + \bar{P}_1 X^T = \bar{S}_j - \bar{N}_j.$$

By the above lemma,

$$N(i, \epsilon) = N(i - 1, \epsilon) \prod_{j=1}^{\psi_i} T(i, j).$$

Hodges [**8**] determines $T(i, j)$ and $N(1, \epsilon)$ has been found by Carlitz [**5**].

However, as noted by Fulton, a pair of distinct s by n solutions to $YY^T = D_\epsilon^{-1}$ do not necessarily determine distinct involutory symmetric matrices in $(R^{(i)})_n$. Duplications arise from the automorphisms of D_ϵ^{-1}. For if P satisfies $YY^T = D_\epsilon^{-1}$, then so does $B^{-1}P$ where B is any automorph of D_ϵ^{-1} and

$$(B^{-1}P)^T D_\epsilon (B^{-1}P) = P^T (B^{-1})^T D_\epsilon B^{-1} P = P^T D_\epsilon P.$$

Conversely, if the symmetric involutory matrices $I_n - 2P_1^T D_\epsilon P_1$ and $I_n - 2P^T D_\epsilon P$ are equal, then $P_1^T D_\epsilon P_1 = P^T D_\epsilon P$ and

$$D_\epsilon = (PP_1^*)^T D_\epsilon (PP_1^*) = B^T D_\epsilon B$$

where P_1^* is a right inverse of P_1 and $B = PP_1^*$.

Hence it is necessary to determine distinct automorphs of D_ϵ^{-1}.

THEOREM 4.5. *For D_ϵ^{-1} in $(R^{(i)})_n$ let*

$$D_\epsilon^{-1} = D_\rho^{-1} + S$$

where $\sigma\epsilon = \rho$ and S is in $(M^{i-1}/M^i)_n$. Then $B^T D_\epsilon^{-1} B = D_\epsilon^{-1}$ if and only if $B = B_1 + P$ and $B_1^T D_\rho^{-1} B_1 = D_\rho^{-1} + Q$ where P and Q are in $(M^{i-1}/M^i)_n$ and where, further, if

$$P = \langle \bar{P}_1, \ldots, \bar{P}_{\psi_i} \rangle,$$
$$S = \langle \bar{S}_1, \ldots, \bar{S}_{\psi_i} \rangle,$$
$$N = \langle \bar{N}_1, \ldots, \bar{N}_{\psi_i} \rangle,$$

then $\bar{P}_j$ is a solution Y to

$$(*) \qquad Y^T D_\rho^{-1} \bar{B}_1 + \bar{B}_1^T D_\rho^{-1} Y = \bar{S}_j - \bar{L}_j - \bar{B}_1^T \bar{S}_j \bar{B}_1$$

for $1 \leqq j \leqq \psi_i$ in $(K)_n$.

https://doi.org/10.4153/CJM-1972-030-x Published online by Cambridge University Press

The proof is similar to the proof of the preceding theorem.

Hodges [8] has determined the number $S(i, j)$ of solutions of (*). Then for $(R^{(i)})_n$ let

$$T(i) = \prod_{j=1}^{\psi_i} S(i, j).$$

Carlitz [5] has obtained the number of distinct solutions X to $X^T D_\delta^{-1} X$ in $(K)_n$ where $\mu\epsilon = \delta$. If $Q(1, \epsilon)$ denotes this number then the number $Q(\beta, \epsilon)$ of distinct solutions in $(R)_n$ of $B^T D_\epsilon^{-1} B = D_\epsilon^{-1}$ is

$$Q(\beta, \epsilon) = Q(1, \epsilon) \prod_{i=1}^{\beta} T(i)$$

(where β = nilpotency of R). Hence,

THEOREM 4.6. *The number $S(R, n, s)$ of distinct symmetric n by n matrices of signature s over R is*

$$S(R, n, s) = \frac{N(\beta, 1)}{Q(\beta, 1)} + \frac{N(\beta, \epsilon)}{Q(\beta, \epsilon)}$$

where β is the nilpotency of R and ϵ is a non-square unit of R.

REFERENCES

1. M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra* (Addison-Wesley, Reading, Mass., 1969).
2. J. Brawley, Jr., *Similar involutory matrices* (mod p^m), Amer. Math. Monthly *73* (1966), 499–501.
3. ——— *Similar involutory matrices modulo R*, Duke Math. J. *34* (1967), 649–666.
4. ——— *Certain sets of involutory matrices and their groups*, Duke Math. J. *36* (1969), 473–478.
5. L. Carlitz, *Representations by quadratic forms in a finite field*, Duke Math. J. *21* (1954), 123–137.
6. L. E. Dickson, *Linear groups with an exposition of Galois field theory* (Dover, New York, 1958).
7. J. D. Fulton, *Symmetric involutory matrices over finite fields and modular rings of integers*, Duke Math. J. *36* (1969), 401–408.
8. J. H. Hodges, *Some matrix equations over a finite field*, Ann. Mat. Pura. Appl. *44* (1957), 245–250.
9. ——— *The matrix equation $X^2 - I = 0$ over a finite field*, Amer. Math. Monthly 65 (1958), 518–520.
10. J. Levine, and H. M. Nahikian. *On the construction of involutory matrices*, Amer. Math. Monthly *69* (1962), 267–272.
11. C. R. Yohe, *Triangle and diagonal forms for matrices over commutative Noetherian rings*, J. of Algebra *6* (1967), 335–368.

The University of Oklahoma,
Norman, Oklahoma