Conspectus materiae tomi XLI, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange

Address of the Editorial Board and of the exchange

Die Adresse der Schriftleitung und des Austausches

Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-03221-9 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

Matrix field extensions

by

JACOB T. B. BEARD, Jr.,* (Cookeville, Tenn.) and
ROBERT M. MCCONNEL (Knoxville, Tenn.)

1. Introduction and notation. Let R denote either the ring Zm of integers modulo m, or the Galois field $\mathrm{GF}(q)$, $q = p^d$, $d \geq 1$, and let $(R)_n$ denote the ring of all $n \times n$ matrices over R under the usual matrix addition and multiplication. Subrings M of $(R)_n$ which are fields are called subfields of $(R)_n$, and have been characterized in [1], [2], [6], and enumerated in [3], [6]. The set $\mathscr{R}_n$ of all subfields of $(R)_n$ is non-empty except when $R = Zm$ and no prime divides m exactly once. Additional results in [1], [2], [3], [6] establish that, under set inclusion, the partially ordered set $\mathscr{R}_n$ is the union of algebraically disjoint complete inf semi-lattices ([3]; Theorem 29) such that if $M \in \mathscr{R}_n$ and M has identity I, then M is contained in the unique semi-lattice whose minimum element has identity I. When $R = Zm$ or $R = \mathrm{GF}(p)$, it has been shown [3], [6] that the similarity classes of $\mathscr{R}_n$ (under the action of conjugation by the group G of non-singular matrices in $(R)_n$) are precisely the sets of subfields of $(R)_n$ having common rank and order. In the case $R = \mathrm{GF}(p^d)$, $d > 1$, our attention focuses on the set $\bar{\mathscr{R}}_n$ of all subfields M of $(R)_n$ such that the canonical projection of a normal form of M ([4], p. 332) contains the set $S_r(R)$ of $r \times r$ scalar matrices over R for $r = \operatorname{rank} M$. Recall that a matrix field M' of $(R)_n$ is a normal form of M provided M is similar over R to M' and each matrix in M' has the form $1^\circ\text{-sum}\ (A;\ n-r, 0) = \operatorname{diag}[O_{n-r}, A]$, where $r = \operatorname{rank} M$ and O_{n-r} denotes the zero matrix of order $n-r$. In this case we write $M' = 1^\circ\text{-sum}\ (M'', n-r, 0)$ and the matrix field M'' of $(R)_r$ is the canonical projection of M'. Again, the similarity classes of $\bar{\mathscr{R}}_n$ are sets of subfields of $(R)_n$ having common rank and order, and we note $\mathscr{R}_n = \bar{\mathscr{R}}_n$ when $d = 1$. Our current results permit the enumeration of maximal chains in $\mathscr{R}_n$ ($\bar{\mathscr{R}}_n$ if $d > 1$) which are rooted at an arbitrarily given element $M \in \mathscr{R}_n$ by using the number $E(q, n, l, m, r)$,

* This author was partially supported by a Summer Research Stipend from The University of Texas at Arlington.

calculated in Section 2, of distinct extension fields M' in $(R)_n$ having order q^m of an arbitrary matrix field M having order q^l and rank r. The analogous number $E(M, q, n, l, m, r)$ in the case $d > 1$ and $M \in \mathscr{R}_n - \overline{\mathscr{R}}_n$ is discussed briefly in Section 5. While determining $E(q, n, l, m, r)$ and considering $E(M, q, n, l, m, r)$, we observe a simplification for the explicit expression given in [3] for the number $N(q, n, m, r)$ of distinct subfields of $(\mathrm{GF}(q))_n$ of order p^m and rank r (Section 4). Other results (Section 3) include a constructive matrix representation for the Galois group of M' over M and the enumeration of all non-singular matrices P and similarity transformations φ_P which induce M-automorphisms of M'. In Section 6 we sharpen a previous result ([4], Theorem 10) and obtain the number of restricted solutions $(g(x), B)_A$ of the equation $A = g(B)$ for $g(x) \in \mathrm{GF}[q, x]$ and $A, B \in (\mathrm{GF}(q))_n$.

Our language and notation is that of [1]–[4], [6]. Briefly, if $M \in \mathscr{R}_n$ and M has multiplicative identity I, then rank M is defined as rank I, and we recall that the rank of each non-zero matrix in M is that of I. The set of all $n \times n$ scalar matrices aI_n, $a \in R$, with I_n the identity of $(R)_n$, is denoted by $S_n(R)$. The ring extension of $S_n(R)$ in $(R)_n$ obtained by adjoining $A \in (R)_n$ is denoted by $S_n(R)[A]$, and we recall that $(R)_n$ is algebraic over R. Finally, for each non-singular matrix $P \in (R)_n$, the similarity transformation φ_P on $(R)_n$ is defined by: $\varphi_P(A) = PAP^{-1}$ for all $A \in (R)_n$.

We emphasize that the identity I of a subfield M of $(R)_n$ need not be the identity I_n of $(R)_n$. (See [12] for an example of a ring R such that $(R)_n$ contains a subfield and $(R)_n$ has no identity.)

2. The number $E(q, n, l, m, r)$. Let $F = \mathrm{GF}(q)$, $q = p^d$, $d \geqslant 1$, and let $\mathscr{F}_n$ denote the set of all subfields of the algebra $(F)_n$. Let $\overline{\mathscr{F}}_n$ denote the set of all subfields M of $(F)_n$ such that $S_n(F) \subseteq M$ or, in case rank $M = r < n$, M contains a subfield which is similar over F to the subfield 1°-sum $(S_r(F);\ n-r, 0)$. As shown in [1], [2], for $M \in \overline{\mathscr{F}}_n$, M has order q^l for some l dividing the rank r of M. Certainly any field extension $M' \in \mathscr{F}_n$ of $M \in \overline{\mathscr{F}}_n$ satisfies $M' \in \overline{\mathscr{F}}_n$ and has order q^m where $l|m$. Thus the number $E(q, n, l, m, r)$ of field extensions M' of such an M in $(F)_n$ having order q^m is positive if and only if $l|m$ and $m|r$. (To see the sufficiency of the condition $l|m$ and $m|r$, see the proof technique used in [1], Theorem 9 or [5], Section 5.) If $M_1, M_2 \in \overline{\mathscr{F}}_n$ have the same order and rank, then M_1 and M_2 are similar over F ([3], Sections 4–6). It will follow, from two observations, that $E(q, n, l, m, r)$ is independent of the field M and, instead, is a function of only q, n, l, m, r as displayed. First, no two distinct fields $M_1, M_2 \in \mathscr{F}_n$ of the same order have a common extension field $M' \in \mathscr{F}_n$, otherwise M' would not contain a unique subfield of order $|M_1| = |M_2|$. Second, for $M_1, M_2 \in \overline{\mathscr{F}}_n$ of equal rank and order, let M_1, M_2 have $E_1 = E_1(q, n, l, m, r)$, $E_2 = E_2(q, n, l, m, r)$ distinct field extensions in $\mathscr{F}_n$ of order q^m respectively. Let $P \in (F)_n$ be any matrix, as guaranteed above, such that $PM_1P^{-1} = M_2$. If M_1' and M_1'' are counted by E_1, then $PM_1'P^{-1}$ and $PM_1''P^{-1}$ are counted by E_2. Since the similarity transformation φ_P on $(F)_n$ induces a bijection on $\mathscr{F}_n$ which maps $\overline{\mathscr{F}}_n$ to itself, then $E_1 \neq E_2$ is impossible. This argument that $E(q, n, l, m, r)$ is independent of the field $M \in \overline{\mathscr{F}}_n$ of order q^l and rank r has established

$$E(q, n, l, m, r) = \frac{\overline{N}(q, n, m, r)}{\overline{N}(q, n, l, r)}, \tag{2.1}$$

where $\overline{N}(q, n, m, r)$ is the number of matrix fields $M \in \overline{\mathscr{F}}_n$ of order q^m and rank r. From [3], Theorem 18, and (2.1) we conclude

$$E(q, n, l, m, r) = \frac{\dfrac{g(d, n)}{mg(d, n-r)g(dm, r/m)}}{\dfrac{g(d, n)}{lg(d, n-r)g(dl, r/l)}} = \frac{lg(dl, r/l)}{mg(dm, r/m)}.$$

THEOREM 1. *Let* $F = \mathrm{GF}(q)$, $q = p^d$, $d \geqslant 1$. *Let M be a subfield of $(F)_n$ of order q^l and rank r such that M contains $S_n(F)$ or a subfield similar over F to 1°-sum $(S_r(F);\ n-r, 0)$. The number $E(q, n, l, m, r)$ of distinct extension fields of M in $(F)_n$ of order q^m is given by*

$$E(q, n, l, m, r) = \frac{lg(dl, r/l)}{mg(dm, r/m)} \tag{2.2}$$

whenever $l|m|r$, where $g(s, t) = \prod_{j=0}^{t-1} (p^{st} - p^{sj})$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$. *Otherwise,* $E(q, n, l, m, r) = 0$.

Tight bounds on $E(q, n, l, m, r)$ can be obtained from (2.2) by straightforward manipulations of $g(dl, r/l)/g(dm, r/m)$. Letting $[x]$ and $\{x\}$ denote respectively the greatest and least integer functions of x, one has

$$\left\{\frac{l}{m} q^{r^2(m-l)/2lm}\right\} \leqslant E(q, n, l, m, r) \leqslant \left[\frac{(q^r-1)^{r/l}}{(q^m-1)^{r/m}} \frac{l}{m} q^{r^2(m-l)/2lm}\right]. \tag{2.3}$$

In the case of an arbitrary modulus $m_0 > 1$, let

$$m_0 = m_1 m_2 \ldots m_s, \tag{2.4}$$

where $m_i = p_i^{\alpha(i)}$, $\alpha(i) > 0$, and the primes p_i are distinct. Following [6], we consider the matrix ring $(Zm_0)_n$ over the integers modulo m_0 as

$$(Zm_0)_n = (Zm_1)_n \oplus \ldots \oplus (Zm_s)_n. \tag{2.5}$$

The subfields of $(Zm_0)_n$ are precisely those subrings M of $(Zm_0)_n$ such that M is a subfield of an ideal $(Zp)_n$ of $(Zm_0)_n$ for some prime $p\| m_0$ ([6], Theorem 7). Thus for every subfield M of $(Zm_0)_n$, there exists a prime $p\|m_0$ such that $S_n(Zp)\subseteq M$ or, when rank $M=r<n$, M contains a subfield similar over Zm_0 to 1°-sum $(S_r(Zp);\ n-r,0)$. Moreover, any two subfields of $(Zm_0)_n$ having the same order and rank are similar over Zm_0 ([6], Theorem 17). Thus the techniques used previously in this section remain valid. The number $N(p,n,m,r)$ of distinct subfields of $(Zm_0)_n$ having order p^m and rank r is positive if and only if $p\|m_0$ and $m|r$, and takes the value ([6], Theorem 10)

$$N(p,n,m,r)=\frac{1}{m}\,\frac{g(1,n)}{g(1,n-r)g(m,r/m)}. \tag{2.6}$$

The appropriate analog of (2.1) yields

THEOREM 2. *Let $m_0>1$ have factorization (2.4) and let M be a subfield of $(Zm_0)_n$ having order p^l and rank r. Then $p\|m_0$. The number $E(p,n,l,m,r)$ of distinct extension fields of M in $(Zm_0)_n$ having order p^m is given by*

$$E(p,n,l,m,r)=\frac{lg(l,r/l)}{mg(m,r/m)} \tag{2.7}$$

whenever $l|m|r$, where $g(s,t)=\prod_{j=0}^{t-1}(p^{st}-p^{sj})$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$. Otherwise, $E(p,n,l,m,r)=0$.

3. Matrix Galois groups. Again, let $F=\mathrm{GF}(q)$, $\mathscr{F}_n$, and $\overline{\mathscr{F}}_n$ be as in Section 2, and let $\mathscr{F}_n(m,r)$ ($\overline{\mathscr{F}}_n(m,r)$) denote the set of all matrix fields in $\mathscr{F}_n$ ($\overline{\mathscr{F}}_n$) having order q^m and rank r. Then $\overline{\mathscr{F}}_n$ is stable under the action of G on $(F)_n$ so that G acts of $\overline{\mathscr{F}}_n$, and the sets $\overline{\mathscr{F}}_n(m,r)$ are the similarity (conjugacy) classes of the action, with G acting transitively on each $\overline{\mathscr{F}}_n(m,r)$. Let $M\in\overline{\mathscr{F}}_n(m,r)$ and let $N_G(M)$ denote the normalizer of M in G: $N_G(M)=\{P\in G:\ PMP^{-1}=M\}$. Then the cardinality $|\overline{\mathscr{F}}_n(m,r)|$ of $\overline{\mathscr{F}}_n(m,r)$ is given by $|\overline{\mathscr{F}}_n(m,r)|=[G:N_G(M)]$, so that from $\overline{N}(q,n,m,r)=|\overline{\mathscr{F}}_n(m,r)|$ we have

$$\frac{g(d,n)}{mg(d,n-r)g(dm,r/m)}=\frac{g(d,n)}{|N_G(M)|},$$

$$|N_G(M)|=mg(d,n-r)g(dm,r/m). \tag{3.1}$$

Let $C_G(M)$ denote the centralizer of M in G:

$$C_G(M)=\{P\in G:\ PAP^{-1}=A \text{ for all } A\in M\}.$$

The argument which established ([3], (3.3), (6.1)) now yields

$$|C_G(M)|=g(d,n-r)g(dm,r/m). \tag{3.2}$$

In keeping with the standard terminology, we say that the similarity transformation φ_P on $(F)_n$ induces an automorphism of M if and only if $P\in N_G(M)$, and φ_P is an M-automorphism of $(F)_n$ if and only if $P\in C_G(M)$. If $L\in\mathscr{F}_n(l,r)$ and L is a subfield of M, let $G(M/L)$ denote the Galois group of M over L. In particular, for $M\in\overline{\mathscr{F}}_n(m,r)$, let $M_q\in\overline{\mathscr{F}}_n(1,r)$ denote the subfield of M having order q.

THEOREM 3. *Let $F=\mathrm{GF}(q)$, $q=p^d$, $d\geqslant 1$, and let $M\in\overline{\mathscr{F}}_n(m,r)$. Then $G(M/M_q)\cong N_G(M)/C_G(M)$. Moreover, for each M_q-automorphism $a\in G(M/M_q)$ of M, there exist $g(d,n-r)g(dm,r/m)$ distinct non-singular matrices $P\in(F)_n$ such that $\varphi_P|_M=a$, where $g(s,0)=1$ and $g(s,t)$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$. The number of distinct M_q-automorphisms φ_P of $(F)_n$ such that $\varphi_P|_M$ is an arbitrary fixed M_q-automorphism of M is $g(d,n-r)g(dm,r/m)/g(d,1)$.*

Proof. We claim that $\gamma(P)=\varphi_P|_M$ for each $P\in N_G(M)$ defines an endomorphism γ: $N_G(M)\to G(M/M_q)$. The only concern is that φ_P must fix M_q element-wise, as it clearly does in the case $r=n$ since $M_q=S_n(F)$. Thus suppose $r<n$, and let $P_1MP_1^{-1}=M'=1^\circ\text{-sum}(M'';\ n-r,0)$ where $M''\in\mathscr{F}_r(m,r)$, so that $M'_q=1^\circ\text{-sum}(S_r(F);\ n-r,0)$. For the time being, let $Q\in N_G(M')$ be arbitrary. Then $Q\in N_G(M'_q)$. Let $\mathrm{diag}[O_{n-r},\ aI_r]$, $\mathrm{diag}[O_{n-r},\ bI_r]\in M'_q$ such that $Q\,\mathrm{diag}[O_{n-r},\ aI_r]Q^{-1}=\mathrm{diag}[O_{n-r},bI_r]$. For the appropriate partition of Q we then have

$$\begin{bmatrix}Q_1 & Q_2\\ Q_3 & Q_4\end{bmatrix}\begin{bmatrix}0 & 0\\ 0 & aI_r\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & bI_r\end{bmatrix}\begin{bmatrix}Q_1 & Q_2\\ Q_3 & Q_4\end{bmatrix},$$

$$\begin{bmatrix}0 & aQ_2\\ 0 & aQ_4\end{bmatrix}=\begin{bmatrix}0 & 0\\ bQ_3 & bQ_4\end{bmatrix}.$$

Thus $Q_2=Q_3=0$, and Q_1, Q_4 have full rank. Hence $a=b$, and φ_Q fixes M'_q element-wise. Now take $Q=P_1PP_1^{-1}$. Then $Q\in N_G(M')$ since $P_1N_G(M)P_1^{-1}=N_G(P_1MP_1^{-1})$. On writing $P=P_1^{-1}(P_1PP_1^{-1})P_1$, it is evident that φ_P fixes M_q element-wise, and the claim is established. Moreover, $\ker\gamma=C_G(M)$, thus $N_G(M)/C_G(M)$ is embeddable in $G(M/M_q)$. Since $|N_G(M)/C_G(M)|\cong m$ by (3.1) and (3.2), and $|G(M/M_q)|=m$, then $G(M/M_q)=N_G(M)/C_G(M)$. The penultimate claim of the theorem follows from (3.2). The final result follows from the former since $G/C(G)\cong\mathrm{Inn}((F)_n)$ and $|C(G)|=q-1=g(d,1)$.

As an illustration of Theorem 3, consider $M\in\overline{\mathscr{F}}_n(n,n)$ so that M is a largest maximal subfield of $(F)_n$. Then $M_q=S_n(F)$ and, for each $a\in G(M/M_q)$, there exist q^n-1 distinct non-singular matrices $P\in(F)_n$ such that the restrictions of φ_P to M are M_q-automorphisms of M, determining $1+q+\ldots+q^{n-1}$ distinct similarity transformations of $(F)_n$ whose restrictions to M are α.

The Galois group $G(M/M_q)$ can be embedded in $(F)_n$ as follows. Let $M \in \overline{\mathscr{F}}_n(m, r)$. By [2], Theorems 6, 8, 9, we can find a matrix $P_1 \in (F)_n$ such that

$$(3.3)\qquad P_1MP_1^{-1} = 1^\circ\text{-sum}\big(k\text{-sum}(S_m(F)[C]);\ n-r,\ 0\big),$$

where $r = km$, and such that C is the companion matrix of a polynomial $f(x) \in F[x]$ which is primitive of the second kind ([3], proof of Theorem 2, [5], [7], [8], [9], [13]). Let $A \in M$ such that

$$(3.4)\qquad P_1AP_1^{-1} = 1^\circ\text{-sum}\big(k\text{-sum}(C);\ n-r,\ 0\big) = C_1.$$

Hence $C_G(P_1MP_1^{-1})$ is the set of all diagonal block matrices $\operatorname{diag}|B_1, B_2|$ $\in (F)_n$ such that $B_2 \in \big(S_m(F)[C]\big)_k$ is non-singular and $B_1 \in (F)_{n-r}$ is non-singular. Moreover, the argument used to obtain (3.2) establishes

$$(3.5)\qquad C_G(M) = P_1^{-1}C_G(P_1MP_1^{-1})P_1.$$

Since C^q is a root of $f(x)$ and $f(x)$ is prime in $F[x]$, it follows that C is similar over F to C^q, and hence C_1, as defined in (3.4), is similar over F to C_1^q. Compute C^q and $P \in (F)_m$ so that $PCP^{-1} = C^q$. Let $P_2 = \operatorname{diag}|I_{n-r}$, $k\text{-sum}(P)|$, so that

$$P_2C_1P_2^{-1} = C_1^q \quad\text{and}\quad P_2 \in C_G(P_1M_qP_1^{-1}).$$

Then $P_2P_1AP_1^{-1}P_2^{-1} = C_1^q$, so that from (3.3) and (3.4) we have

$$(3.6)\qquad (P_1^{-1}P_2P_1)A(P_1^{-1}P_2P_1)^{-1} = P_1^{-1}C_1^qP_1 = A^q.$$

Take $Q = P_1^{-1}P_2P_1$, so that from (3.6) we have

$$QAQ^{-1} = A^q,$$
$$Q^2AQ^{-2} = Q(QAQ^{-1})Q^{-1} = QA^qQ^{-1} = (QAQ^{-1})^q = (A^q)^q = A^{q^2},$$

and by induction,

$$Q^jAQ^{-j} = A^{q^j}, \quad 0 \leqslant j \leqslant m-1.$$

Since $f(x)$ is primitive of the second kind, $A^{q^i} \neq A^{q^j}$, $0 \leqslant i < j \leqslant m-1$. Hence the coset $QC_G(M)$ is a cyclic generator of $N_G(M)/C_G(M)$, and the similarity transformations φ_{Q^j} on $(F)_n$, $0 \leqslant j \leqslant m-1$, induce all of the M_q-automorphisms of M.

Let $L \in \overline{\mathscr{F}}_n(l, r)$ with L an intermediate field between M_q and M, and represent $G(M/M_q)$ as $G(M/M_q) = \{Q^j\colon 0 \leqslant j \leqslant m-1\}$. Then

$$G(M/L) = \{Q^{jl}\colon 0 \leqslant j \leqslant (m-1)/l\}, \qquad G(L/M_q) = \{Q^{jm/l}\colon 0 \leqslant j \leqslant l-1\}$$

follow from basic Galois theory and the representation chosen for $G(M/M_q)$.

Rather than belabor the point, we merely observe that the obvious analogs of the results of this section hold for $(Zm_0)_n$ and follow from (2.5) and [6], Theorem 7.

4. The number $N(q, n, m, r)$. As in [3], let $N(q, n, m, r)$ denote the number of subfields of $(F)_n$ of order p^m and rank r, $F = \mathrm{GF}(q)$, $q = p^d$, $d \geqslant 1$. The expressions given in [3], (7.7), (8.2), for $N(q, n, m, r)$ can be simplified considerably, using the techniques of [2], Theorem 6, and [3], Section 8, with one additional observation. Let $M \in \mathscr{F}_n(m, r)$, so that M is similar over F to the matrix field $M' = 1^\circ\text{-sum}\big(S_r(F_p)[A]$; $n-r, 0\big)$. Note that M' contains the matrix $A' = 1^\circ\text{-sum}(A;\ n-r, 0)$. Then A' has minimal polynomial $f(x) = xg(x)$ over $F_p = \mathrm{GF}(p)$ where $\big(x, g(x)\big) = 1$, $g(x) \in F_p[x]$ is prime of degree m. Now use the additional information that $f(x)$ factors in $F[x]$ as

$$(4.1)\qquad f(x) = xP_1(x)\ldots P_s(x) = P_0(x)P_1(x)\ldots P_s(x)$$

where the primes $P_i(x) \in F[x]$ are distinct, $s = (m, d)$, and for $i > 0$ $P_i(x)$ has degree m/s ([10], p. 33). Following Hodges [11], A (and hence M) uniquely determines a partition $\pi = \pi(n)$ of n (independent of A, M, and the particular prime $g(x) \in F_p[x]$ of degree m) of the form

$$(4.2)\qquad \pi(n)\colon n = k_0 + \sum_{i=1}^{s} \frac{m}{s}k_i, \qquad k_i \geqslant 0,$$

where $xI - A$ has k_i elementary divisors $P_i(x)$. The expressions $a(\pi)$ and $b(\pi)$ defined by Hodges ([11], p. 292) and used in [3], Sections 7, 8, are seen to have the value zero. Thus Theorem 20 and Theorem 25 of [3] simplify to the following result.

THEOREM 4. *Let $F = \mathrm{GF}(q)$, $q = p^d$, $d \geqslant 1$, and let $N(q, n, m, r)$ be the number of distinct subfields of $(F)_n$ having order p^m and rank $r \leqslant n$. Then $N(q, n, m, r) = 0$ if no prime polynomial $g(x) \neq x$ of degree m in $F_p[x]$ is r-admissible for F. Whenever $F_p[x]$ contains a prime polynomial $g(x) \neq x$ of degree m which is r-admissible for F,*

$$(4.3)\qquad N(q, n, m, r) = \frac{1}{m}g(d, n)\sum_{\pi}\prod_{i=0}^{s} g(dm, k_i)^{-1},$$

where $xg(x)$ has factorization (4.1); the summation is over all partitions π of n obtained by taking $k_0 = n-r$ in (4.2) and k_i a non-negative integer for $i > 0$; $g(s, 0) = 1$ and $g(s, t)$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$.

The number $N(q, n)$ of distinct subfields given by [3], Theorem 26, is then

$$N(q, n) = \sum_{r=1}^{n} \sum_{m=1}^{rd} N(q, n, m, r), \tag{4.4}$$

where $N(q, n, m, r)$ is given in (4.3).

5. Remarks on $E(M, q, n, l, m, r)$. Let $M_1, M_2 \in \mathscr{F}_n(l, r)$. The argument used in Section 2 establishes that if M_1 is similar over F to M_2, then M_1 and M_2 have the same number of extension fields in $(F)_n$ of order p^m. Though M_1 and M_2 have the same partition π of n as given in (4.2) whenever M_1 is similar to M_2 over F, M_1 can have dis-similar extension fields in $(F)_n$ having the same order, call them M_1' and M_1'' (e.g. see [3], Example 1). In general, the partitions π' and π'' determined by M_1' and M_1'' apparently can be equal or different, and certainly $\pi \neq \pi', \pi''$. It is easily seen that if two similar fields M_1, M_2 have dis-similar extension fields $M_1' \supset M_1$ and $M_2' \supset M_2$ in $(F)_n$ of the same order, then M_1 (and dually M_2) has dis-similar extension fields in $(F)_n$ of the same order. Thus the enumeration technique of [3], [11], and Section 4, based on the partitions π of n, does not permit the explicit calculation of the number $E(M, q, n, l, m, r)$ of field extensions of order p^m in $(F)_n$ of a subfield M of $(F)_n$ having order p^l and rank r, nor would an enumeration technique based on the similarity classes of $\mathscr{F}_n$.

6. A related result. Let $F = \mathrm{GF}(q)$, $q = p^d$, $d \geqslant 1$, and suppose $A \in (F)_n$ has characteristic polynomial $f^k(x)$ and minimal polynomial $f(x)$ which is prime in $F[x]$. In [4], Theorem 10, it was stated (without proof) that for each integer $m \mid k$ and each prime $h(x) \in F[x]$ of degree mn/k, there exist at least mn/k matrices $B_i \in (F)_n$ having characteristic polynomial $h^{k/m}(x)$, minimal polynomial $h(x)$, and satisfying $A = g_i(B_i)$ for unique $g_i(x) \in F[x]$ of degrees $r_i < mn/k$. We show that the number of matrices B_i satisfying the conditions is precisely $E(q, n, n/k, mn/k, n)\, mn/k$.

Let A satisfy the hypothesis so that $M = S_n(F)[A] \in \overline{\mathscr{F}}_n(n/k, n)$. Suppose $m \mid k$ and $h(x) \in F[x]$ is prime of degree mn/k. Using the construction technique in the proof of [1], Theorem 9, [5], Section 5, let $M' = S_n(F)[B] \in \overline{\mathscr{F}}_n(mn/k, n)$ be an extension of M. Then M' contains mn/k distinct roots $B_i \in (F)_n$ of $h(x)$, each having characteristic polynomial $h^{k/m}(x)$, and minimal polynomial $h(x)$ over F. Clearly, for each i there exists a unique $g_i(x) \in F[x]$ of degree $r_i < mn/k$ such that $g_i(B_i) = A$. Since the same is true of each extension M' of M in $(F)_n$ having order $q^{mn/k}$ and each such M' lies in $\overline{\mathscr{F}}_n(mn/k, n)$, and since any matrix $B_i \in (F)_n$ satisfying the conditions lies in such an extension M' of M, we are done.

References

[1] J. T. B. Beard, Jr., *Matrix fields over prime fields*, Duke Math. J. 39 (1972), pp. 313–321.

[2] — *Matrix fields over finite extensions of prime fields*, ibid. 39 (1972), pp. 475–484.

[3] — *The number of matrix fields over* GF(*q*), Acta Arith. 25 (1974), pp. 315–329.

[4] — *A rational canonical form of matrix fields*, ibid. 25 (1974), pp. 331–335.

[5] — *Computing in* GF(*q*), Math. Comp. 28 (1974), pp. 1159–1166.

[6] J. T. B. Beard, Jr., and R. M. McConnel, *Matrix fields over the integers modulo m*, Linear Algebra and Appl. 14 (1976), pp. 95–105.

[7] J. T. B. Beard, Jr., and K. I. West, *Some primitive polynomials of the third kind*, Math. Comp. 28 (1974), pp. 1166–1167.

[8] L. Carlitz, *Primitive roots in a finite field*, Trans. Amer. Math. Soc. 73 (1952), pp. 373–382.

[9] H. Davenport, *Bases for finite fields*, J. London Math. Soc. 43 (1968), pp. 21–39; ibid., 44 (1969), pp. 378.

[10] L. E. Dickson, *Linear groups*, Leipzig 1901.

[11] J. H. Hodges, *Scalar polynomial equations for matrices over a finite field*, Duke Math. J. 25 (1958), pp. 291–296.

[12] T. J. Laffey and D. L. McQuillan, *A note on subfields of matrix rings*, Linear Algebra and Appl. 16 (1977), pp. 1–3.

[13] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), pp. 243–274.

TENNESSEE TECHNOLOGICAL UNIVERSITY
Cookeville, Tennessee, U.S.A.
UNIVERSITY OF TENNESSEE
Knoxville, Tennessee, U.S.A.

Received on 12. 3. 1979
and in revised form on 28. 7. 1980 (1142)