Conspectus materiae tomi XXV, fasciculi 4

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 статьей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

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

ACTA ARITHMETICA
XXV (1974)

The number of matrix fields over GF(q)*

by

J. T. B. BEARD, JR., (Arlington, Tex.)

1. Introduction and notation. Let F be a field, and let $(F)_n$ denote the algebra of all $n \times n$ matrices over F under normal matrix addition and multiplication. If a subring M of $(F)_n$ is itself a field, we call M a *matrix field*. Although it is non-standard, we also refer to M as a subfield of the ring $(F)_n$. In [1], [2] we have characterized all subfields of $(F)_n$ whenever F is a finite extension of its prime subfield. The primary purpose of this paper is to determine the number $N(q, n)$ of distinct subfields of $(F)_n$ whenever $F = \mathrm{GF}(q)$ is the Galois field of order $q = p^d$ for some prime p and positive integer d. In the process we discover further results on the structure of the set $\mathscr{F}_n$ of all subfields of $(F)_n$, as well as some rather nice divisibilities between certain integers. We will first obtain $N(p, n)$, and then generalize the techniques used therein to obtain $N(q, n)$. In finding $N(q, n)$, we rely heavily on a result of Hodges [5]. Our language and notation is that of [1] and [2].

Until further notice, we let $F = \mathrm{GF}(p)$ unless indicated otherwise. It is easily established that $N(p, n) > 0$ for all primes p and all integers $n \geqslant 1$, and that every subfield of $(F)_n$ has order p^m for some positive integer $m \leqslant n$. We remember that if a subfield M of $(F)_n$ has rank r, then each non-zero matrix in M has rank r, and $r > 0$. In computing $N(p, n)$ we find it convenient to consider the number $N(p, n, m, r)$ of distinct subfields of $(\mathrm{GF}(p))_n$ having order p^m and rank r. Clearly,

$$N(p, n) = \sum_{r=1}^{n} \sum_{m=1}^{n} N(p, n, m, r). \tag{1.1}$$

From our characterization of the subfields of $(F)_n$, Theorem 2 and Theorem 3 of [1], we immediately have

---

* These results are contained in the author's doctoral dissertation, written under the direction of Professor Robert M. McConnel, to whom the author wishes to express his sincere gratitude.

THEOREM 1. *$N(p, n, m, r) \neq 0$ if and only if $m|r$.*

Hence (1.2) above becomes

$$N(p, n) = \sum_{r=1}^{n} \sum_{m|r} N(p, n, m, r). \tag{1.2}$$

2. The number $N(p, n, m, n)$. In order to indicate the proof technique clearly, we first determine $N(p, n, m, n)$ for arbitrary divisors m of n, and then consider $N(p, n, m, r)$ for arbitrary divisors m of r where $r < n$. Accordingly, we obtain

THEOREM 2. *The number of distinct subfields of $(\mathrm{GF}(p))_n$ having order p^m and rank n is given by*

$$N(p, n, m, n) = \frac{1}{m} \frac{g(1, n)}{g(m, n/m)} \tag{2.1}$$

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

Proof. Let m be an arbitrary positive divisor of n. Let $g(x)$ be an arbitrary prime polynomial of degree m in $F[x]$, where $F = \mathrm{GF}(p)$. Let A be an arbitrary root in $(F)_n$ of $g(x)$. Then the minimal polynomial $h(x)$ of A over F divides $g(x)$ in $F[x]$. Thus $h(x) = g(x)$ as $g(x)$ is prime in $F[x]$, and hence $g(x)$ is the only non-trivial similarity invariant of A. Hence A is similar over F to the matrix $k\text{-sum}\big(C(g(x))\big)$, where $n = mk$. Since any matrix in $(F)_n$ which is similar over F to $k\text{-sum}\big(C(g(x))\big)$ is a root of $g(x)$, then the number of distinct roots in $(F)_n$ of $g(x)$ is precisely the number of matrices in $(F)_n$ which are similar over F to $k\text{-sum}\big(C(g(x))\big)$. The multiplicative group G of all non-singular matrices in $(F)_n$ operates in the set $(F)_n$ under conjugation, and it follows by a well-known result ([4], p. 61) that the number of distinct matrices in $(F)_n$ which are similar over F to $k\text{-sum}\big(C(g(x))\big)$ (and hence the number of distinct roots in $(F)_n$ of $g(x)$) is precisely the index in G of the stabilizer of the matrix $k\text{-sum}\big(C(g(x))\big)$. Let $C(g(x), k)$ denote the order of the stabilizer of $k\text{-sum}\big(C(g(x))\big)$; i.e., $C(g(x), k)$ is the number of non-singular matrices in $(F)_n$ which commute with $k\text{-sum}\big(C(g(x))\big)$. Letting $D(g(x), n)$ denote the number of distinct roots in $(F)_n$ of $g(x)$, we have

$$D(g(x), n) = \frac{g(1, n)}{C(g(x), k)}. \tag{2.2}$$

We note that the number $g(s, t)$ is well-known, appearing in [5] for example. The number $C(g(x), k)$ is a special case of a result of Dickson ([3], p. 235), and is easily calculated using Hodges' formulation [5] of this result. However, we use our own results [1] to calculate $C(g(x), k)$. To do so, we consider $(F)_n$ as $((F)_m)_k$, and remember that these are isomorphic

in a "nice" way. It is well-known that the only matrices in $(F)_m$ which commute with $C(g(x))$ are precisely the matrices in $S_m(F)\big[C(g(x))\big]$. Thus $C(g(x), k)$ is the number of non-singular matrices of order k over $S_m(F)\big[C(g(x))\big]$ which commute with $k\text{-sum}\big(C(g(x))\big)$. Since the matrix $k\text{-sum}\big(C(g(x))\big)$ is central in the ring $\big(S_m(F)\big[C(g(x))\big]\big)_k$, then $C(g(x), k)$ is precisely the number of non-singular matrices contained in

$$\big(S_m(F)\big[C(g(x))\big]\big)_k.$$

By Theorem 2 of [1], $S_m(F)\big[C(g(x))\big]$ is a field of order p^m, so that $C(g(x), k) = g(m, k) = g(m, n/m)$ and (2.2) becomes

$$D(g(x), n) = \frac{g(1, n)}{g(m, n/m)}. \tag{2.3}$$

Notice that the number $D(g(x), n)$ is independent of the prime polynomial $g(x)$ of degree m in $F[x]$. We now characterize the distinct subfields of $(F)_n$ having order p^m and rank n.

LEMMA 3. *Let $F = \mathrm{GF}(p)$, and let $M_1, M_2 \in \mathscr{F}_n$ have order p^m and rank n. Then $M_1 \neq M_2$ if and only if $M_1 \cap M_2$ contains no root in $(F)_n$ of any prime polynomial of degree m in $F[x]$.*

Proof. We prove both directions by contraposition. Let $M_1, M_2 \in \mathscr{F}_n$ have order p^m and rank n. Then $I_n \in M_1 \cap M_2$, and since $S_n(F)$ is the ring generated by I_n, we have $S_n(F) \subseteq M_1 \cap M_2$. For the necessity, assume some prime polynomial $g(x) \in F[x]$ of degree m has a root $A \in M_1 \cap M_2$. Then A is a root of the prime polynomial $g(X) \in S_n(F)[X]$ of degree m and $M_1 = S_n(F)[A] = M_2$.

To show the sufficiency, assume $M_1 = M_2$. By Theorem 2 of [1], M_1 contains a matrix A which is similar over F to $k\text{-sum}\big(C(g(x))\big)$, where $g(x) \in F[x]$ is prime and has degree m. Thus A is a root of $g(x)$, $A \in M_1 = M_1 \cap M_2$, and the lemma is proved.

We have already shown that if $g(x)$ is any prime polynomial of degree m in $F[x]$, and A is any root in $(F)_n$ of $g(x)$, then A is similar over F to $k\text{-sum}\big(C(g(x))\big)$. Hence by Theorem 2 of [1], $S_n(F)[A]$ is a subfield of $(F)_n$ having order p^m and rank n. Since $S_n(F) \subseteq S_n(F)[A]$, then the minimal polynomial of A over $S_n(F)$ is $g(X) \in S_n(F)[X]$. Since $S_n(F)[A]$ is a normal field extension of $S_n(F)$, then $g(X)$ has m distinct roots in $S_n(F)[A]$. Hence $S_n(F)[A]$ contains precisely m distinct roots in $(F)_n$ of $g(x)$. Furthermore, if $h(x)$ is any prime polynomial of degree m in $F[x]$, then $S_n(F)[A]$ contains precisely m distinct roots of $h(x)$. For if $h(x)$ is such a polynomial, it has a root B in $(F)_n$ by (2.3). Then $S_n(F)[B]$ is a field of order p^m and rank n. Thus choosing any isomorphism

$$\varphi\colon S_n(F)[B] \to S_n(F)[A],$$

we have $h(\varphi(B)) = O_n$, since φ is the identity map on $S_n(F)$. By Lemma 3, we thus have

LEMMA 4. *Let $F = \mathrm{GF}(p)$, and let m, n be positive integers. If $g(x)$ is any prime polynomial of degree m in $F[x]$, then $m|D(g(x), n)$. Moreover, there are precisely $\frac{1}{m} D(g(x), n)$ distinct matrix fields in the subset $\{S_n(F)[A]: A \in (F)_n$ is a root of $g(x)\}$ of $\mathscr{F}_n$.*

To see that Lemma 4 holds even if $m \nmid n$, observe that $g(x)$ has no roots in $(F)_n$ in that case. Continuing, we have a pigeon-hole process within grasp. Let $l = \frac{1}{m} D(g(x), n)$. By Lemma 4, there are precisely l distinct subfields $M_1, \ldots, M_l$ of $(F)_n$ of the form $M_i = S_n(F)[A_i]$ where A_i is a root in $(F)_n$ of $g(x)$; and furthermore, each M_i has order p^m and rank n. Let M be any subfield of $(F)_n$ having order p^m and rank n. Then M contains a root $B \in (F)_n$ of some prime polynomial $h(x)$ of degree m in $F[x]$. Since each M_i contains m distinct roots of $h(x)$; and since $h(x)$ has precisely $D(g(x), n)$ distinct roots in $(F)_n$; then by Lemma 4, $B \in M_j$ for some $j, 1 \leqslant j \leqslant l$. Hence by Lemma 3 $M = S_n(F)[B] = M_j$. Thus $N(p, n, m, n) = l$ and the theorem is proved.

Excepting $g(x) = x$, $D(g(x), n)$ should be viewed as denoting the number of distinct roots in $(F)_n$ of $g(x)$, $g(x)$ prime in $F[x]$, which have rank n. Notice that if F is an arbitrary field, and if $A \in (F)_n$ is a root of a prime polynomial $g(x) \in F[x]$, then A has rank n if and only if $g(x) \neq x$. This follows because A is similar over F to k-sum$\big(C(g(x))\big)$ for some k dividing n, and each diagonal block of k-sum$\big(C(g(x))\big)$ is non-singular since $g(x)$ has a non-zero constant term.

3. The number $N(p, n, m, r)$. We now find $N(p, n, m, r)$, where $1 \leqslant r < n$. To do so, we generalize the techniques of the previous section and keep in mind the results given in Theorem 3 of [1].

THEOREM 5. *The number of distinct subfields of $(\mathrm{GF}(p))_n$ having order p^m and rank $r < n$ is given by*

$$N(p, n, m, r) = \frac{1}{m} \frac{g(1, n)}{g(1, n-r)\, g(m, r/m)} \tag{3.1}$$

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

Proof. Let $F = \mathrm{GF}(p)$. Fix r, where $1 \leqslant r < n$, and fix m as any positive divisor of r. Let $g(x) \neq x$ be an arbitrary prime polynomial of degree m in $F[x]$, and let $f(x) = xg(x)$. Let $A \in (F)_n$ be any root of $f(x)$ having rank r, and let A have minimal polynomial $h(x)$ over F. Then $h(x)$ divides $f(x)$ in $F[x]$. Since A has rank $r > 0$, then $h(x) \neq x$, and as $r < n$, then $h(x) \neq g(x)$. Hence $h(x) = f(x)$. Let $r = mk$. Since $\big(x, g(x)\big)$

$= 1$, then $C(f(x))$ is similar over F to the matrix diag$\big|C(x), C(g(x))\big|$ ([6], p. 154). Since $r < n$, we conclude that A is similar over F to the matrix

$$A' = \mathrm{diag}\big|C(x), \ldots, C(x), C(g(x)), \ldots, C(g(x))\big|,$$

where $C(x)$ appears on the diagonal of A' precisely $n-r$ times, and $C(g(x))$ appears on the diagonal of A' precisely k times. Thus by definition (see [1]),

$$A' = 1^\circ\text{-sum}\Big(k\text{-sum}\big(C(g(x))\big); n-r, 0\Big).$$

Since any matrix in $(F)_n$ which is similar over F to A' is a root of $f(x)$ and has rank r, then the number of roots in $(F)_n$ of $f(x)$ having rank r is precisely the number of matrices in $(F)_n$ which are similar over F to A'. As before, we denote this number by $D(f(x), r)$ and have

$$D(xg(x), r) = \frac{g(1, n)}{C(g(x), k, n-r)}, \tag{3.2}$$

where $C(g(x), k, n-r)$ is the number of non-singular matrices in $(F)_n$ which commute with A'. By an argument similar to that used in obtaining (2.3), we find that

$$\begin{aligned} C(g(x), k, n-r) &= g(1, n-r)\, C(g(x), k) \\ &= g(1, n-r)\, g(m, k) = g(1, n-r)\, g(m, r/m). \end{aligned}$$

Thus (3.2) becomes

$$D(xg(x), r) = \frac{g(1, n)}{g(1, n-r)\, g(m, r/m)}. \tag{3.3}$$

As before, we now characterize the distinct subfields of $(F)_n$ having order p^m and rank r. We need the following two results.

LEMMA 6. *Let $F = \mathrm{GF}(p)$. Let M_1, M_2 be subfields of $(F)_n$ of order p^m and having a common identity I of rank $r < n$. Then $M_1 \neq M_2$ if and only if $M_1 \cap M_2$ contains no non-zero root in $(F)_n$ of a polynomial $xg(x) \in F[x]$, where $g(x)$ is any prime polynomial of degree m.*

Proof. Let M_1 and M_2 be subfields of $(F)_n$ of order p^m and having a common identity I of rank $r < n$. Choose any non-singular matrix $P \in (F)_n$ such that PIP^{-1} is the partial identity matrix $C_r = 1^\circ\text{-sum}(I_r; n-r, 0)$. Then

$$1^\circ\text{-sum}\big(S_r(F); n-r, 0\big) \subseteq PM_1P^{-1} \cap PM_2P^{-1},$$

since C_r generates the ring 1°-sum$\big(S_r(F); n-r, 0\big)$. Suppose some non-zero matrix $B \in M_1 \cap M_2$ is a root of a polynomial $xg(x) \in F[x]$, where $\deg g(x) = m$ and $g(x)$ is prime in $F[x]$. Then $PBP^{-1} \in PM_1P^{-1} \cap PM_2P^{-1}$. Further-

more, $PBP^{-1} = 1^\circ\text{-sum}(B'; n-r, 0)$ for some $B' \epsilon (F)_r$ having rank r, and B' is similar over F to $k\text{-sum}\big(C(g(x))\big)$ where $r = mk$. Hence B' has minimal polynomial $g(x)$ over F and

$$PM_1P^{-1} = 1^\circ\text{-sum}\big(k\text{-sum}\big(S_r(F)[B']; n-r, 0\big)\big) = PM_2P^{-1}.$$

Conjugating by P^{-1}, we have $M_1 = M_2$.

Conversely, suppose $M_1 = M_2 = M$. Then by Theorem 3 in [1], M is similar over F to $1^\circ\text{-sum}\big(S_r(F)[B]; n-r, 0\big)$, where $B = k\text{-sum}\big(C(g(x))\big)$ for some prime polynomial $g(x) \neq x \epsilon F[x]$ of degree m. It is clear that the minimal polynomial of the matrix $1^\circ\text{-sum}(B; n-r, 0)$ over the field $1^\circ\text{-sum}\big(S_r(F); n-r, 0\big)$ is then $g(X) \epsilon 1^\circ\text{-sum}\big(S_r(F); n-r, 0\big)[X]$ since $B \epsilon (F)_r$. Hence $1^\circ\text{-sum}(B; n-r, 0)$ is a root of $xg(x)$. Thus M contains a non-zero root of $xg(x)$, and the lemma is proved.

Standard (matrix) algebraic techniques yield

LEMMA 7. *Let F be an arbitrary field, and let $M_1, M_2 \epsilon \mathscr{F}_n$. Then M_1 and M_2 have distinct identities if and only if $M_1 \cap M_2 = (O_n)$.*

From Lemma 3, Lemma 6, and Lemma 7, we immediately have

THEOREM 8. *Let $F = \mathrm{GF}(p)$. Let $M_1, M_2 \epsilon \mathscr{F}_n$ have order p^m and rank r. Then M_1 and M_2 are distinct if and only if $M_1 \cap M_2$ contains no non-zero root in $(F)_n$ of any polynomial $x^s g(x) \epsilon F[x]$, where $g(x)$ is prime of degree m, $s = 0$ if $r = n$, and $s = 1$ for $r < n$.*

We continue with the proof of Theorem 5. Let $f(x)$ be any polynomial in $F[x]$ having the form $f(x) = xg(x)$, where $g(x)$ is prime, $\deg g(x) = m$, and $g(x) \neq x$. Then $f(x)$ has $D\big(f(x), r\big)$ roots A in $(F)_n$ having rank r. As argued earlier, A is similar over F to the matrix $A'' = 1^\circ\text{-sum}\Big(k\text{-sum}\big(C(g(x))\big); n-r, 0\Big)$. Let $P \epsilon (F)_n$ be any non-singular matrix such that $PAP^{-1} = A''$, and let $M' = k\text{-sum}\big(S_m(F)\,|C(g(x))|\big)$. Then

$$M = P^{-1}(1^\circ\text{-sum}(M'; n-r, 0))P$$

is a subfield of $(F)_n$ having order p^m and rank r, and $A \epsilon M$. Let $A' = k\text{-sum}\big(C(g(x))\big)$, so that

$$PMP^{-1} = 1^\circ\text{-sum}(M'; n-r, 0)$$

and

$$PAP^{-1} = 1^\circ\text{-sum}(A'; n-r, 0).$$

Since A is a root of $f(x)$, then A' is a root in $(F)_r$ of $f(x)$. Since A' has rank $r > 0$, then A' is not a root of the polynomial x. Hence A' is a root in $(F)_r$ of $g(x)$, since $A' \epsilon M'$ and M' is a field. As argued in Section 2, M' contains precisely m distinct roots in $(F)_r$ of any prime polynomial $d(x) \epsilon F[x]$ having degree m. Let $B' \epsilon M'$ be a root of such a polynomial $d(x) \neq x$, and consider the matrix $PBP^{-1} \epsilon (F)_n$ as defined by

$$PBP^{-1} = 1^\circ\text{-sum}(B'; n-r, 0).$$

If $d(x)$ has constant term a, and if $h(x) = xd(x)$, then

$$h(PBP^{-1}) = PBP^{-1}d(PBP^{-1}) = \mathrm{diag}\,|O_{n-r}, B'| \cdot \mathrm{diag}\,|aI_{n-r}, O_r|,$$

and hence PBP^{-1} is a root in PMP^{-1} of $h(x)$. Thus B is a root in M of $h(x)$. Furthermore, B has rank r since B' necessarily has rank r. Since the roots in M' of $d(x)$ are distinct, then M contains precisely m distinct non-zero roots of $h(x)$ and each of them has rank r. In particular, if $d(x) \neq x$ is any prime polynomial in $F[x]$ having degree m, then any matrix field $M \epsilon \mathscr{F}_n$ which contains a root A of $xg(x)$ having rank r contains precisely m distinct roots in $(F)_n$ of $xd(x)$ which have rank r. Since any root $A \epsilon (F)_n$ of $xg(x)$ having rank r lies in a subfield M of $(F)_n$, then from Theorem 8 we find there exist precisely $\frac{1}{m} D\big(xg(x), r\big)$ distinct subfields of $(F)_n$ which contain roots of rank r in $(F)_n$ of $xg(x)$. Let $l = \frac{1}{m} D\big(xg(x), r\big)$, and let $M_1, \ldots, M_l$ denote these distinct subfields. Then each M_i has order p^m and rank r. Let M be an arbitrary subfield of $(F)_n$ having order p^m and rank r. Then by Theorem 3 in [1], M is similar over F to a matrix field $1^\circ\text{-sum}(M'; n-r, 0)$ where $M' \epsilon \mathscr{F}_r$ has rank r. Furthermore, any matrix B in M is similar over F to a matrix $1^\circ\text{-sum}(B'; n-r, 0)$ where $B' \epsilon M'$ has rank r if and only if $B \neq O_n$. Let B' have minimal polynomial $d(x)$ over F. Then $d(x)$ is prime in $F[x]$ since $S_r(F) \subseteq M'$, and B is a root in $(F)_n$ of $xd(x)$. Moreover, B has rank r if and only if $d(x) \neq x$. In particular, we can choose a non-zero matrix $B' \epsilon M'$ whose minimal polynomial $d(x)$ over F has degree m. Hence B has rank r and is a root in $(F)_n$ of $xd(x)$. Since each M_i contains precisely m distinct roots in $(F)_n$ of $xd(x)$ having rank r; and since $xd(x)$ has exactly $D\big(xg(x), r\big)$ distinct roots in $(F)_n$ having rank r; then $B \epsilon M_j$ for some j, $1 \leqslant j \leqslant l$. Thus by Theorem 8 we have $M = M_j$. Hence $N(p, n, m, r) = l$ and we are done.

Set $g(s, 0) = 1$. On combining the results of Theorem 2 and Theorem 5, we have

THEOREM 9. *Let $F = \mathrm{GF}(p)$. The number of distinct subfields of $(F)_n$ having order p^m and rank r is given by*

$$N(p, n, m, r) = \frac{1}{m} \frac{g(1, n)}{g(1, n-r)g(m, r/m)} \tag{3.4}$$

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

4. The number $N(p, n)$ and further results. From Theorem 9 and (1.2) we have

THEOREM 10. *Let $F = \mathrm{GF}(p)$. The number $N(p, n)$ of distinct subfields of $(F)_n$ is given by*

$$N(p,n) = \sum_{r=1}^{n} \sum_{m|r} \frac{1}{m} \frac{g(1,n)}{g(1,n-r)g(m,r/m)} \tag{4.1}$$

where $g(s,t) = \prod_{r=0}^{t-1} (p^{st} - p^{sr})$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$ and $g(s,0) = 1$.

In the course of proving Theorem 2 and Theorem 5 we have proved

THEOREM 11. *Let $F = \mathrm{GF}(p)$. Then any subfields of $(F)_n$ having the same order and rank are similar over F.*

Letting $\tau(r)$ denote as usual the number of positive divisors of r, we have

THEOREM 12. *Let $F = \mathrm{GF}(p)$. The number of similarity classes of $\mathscr{F}_n$ is $\sum_{r=1}^{n} \tau(r)$.*

Composing the results given in Theorem 7 in [1], Theorem 8 in [1], Theorem 11, and (3.4) of Theorem 9, we obtain the following analog of the Sylow Theorems.

THEOREM 13. *Let $F = \mathrm{GF}(p)$. Then the following are true.*

(i) *Any subfield of $(F)_n$ having rank r is contained in a maximal subfield of $(F)_n$ having order p^r.*

(ii) *Any maximal subfields of $(F)_n$ having the same order are similar over F.*

(iii) *The number of (maximal) subfields of $(F)_n$ of any given order divides the order of the multiplicative group of non-singular matrices in $(F)_n$.*

Immediately from (3.4) we obtain two interesting but considerably weaker results.

THEOREM 14. *Given any prime p and any integer $n \geqslant 1$, then $n | g(1,n)$, where $g(1,n) = \prod_{r=0}^{n-1} (p^n - p^r)$ is the number of non-singular matrices of order n over $\mathrm{GF}(p)$.*

THEOREM 15. *For each prime p and all integers $n > 1$,*

$$n \Big| \prod_{r=1}^{n-1} (p^n - p^r).$$

5. Preliminary remarks concerning $N(q,n)$. In the remainder of the paper we let $F = \mathrm{GF}(q)$, where $q = p^d$. To find $N(q,n)$, we generalize the techniques of the previous sections. The importance of the set of "scalar matrices" contained in a given matrix field is seen once again (see [2]) on comparing $N(q,n)$ to the number $\bar{N}(q,n)$ of distinct subfields of $(F)_n$ which themselves contain either $S_n(F)$ or a subfield which is similar over F to $1^\circ\text{-sum}\big(S_r(F); n-r, 0\big)$ for some $r < n$. We obtain $\bar{N}(q,n)$ first, by a trivial extension of our previous techniques, after determining the number $\bar{N}(q,n,m,r)$ of distinct subfields of $(F)_n$ which are counted by $\bar{N}(q,n)$, have order q^m, and have rank r. These results are given in Section 6. In Section 7 we determine the number $N(q,n,m,n)$ of distinct subfields of $(F)_n$ having order p^m and rank n. In Section 8 we determine the number $N(q,n,m,r)$ of distinct subfields of $(F)_n$ having order p^m and rank r for $r < n$. Our formula for $N(q,n)$ will be given in Section 9 along with additional results.

We conclude this section by observing that under the weaker hypothesis that $F = \mathrm{GF}(q)$, then Theorem 11 and (i) and (ii) of Theorem 13 are false. Regarding Theorem 11, we consider

EXAMPLE 1. Let $F = \mathrm{GF}(4)$, with $F^* = (a)$, so that $F = \{0, 1, a, a^2\}$. Let $C_1, C_2 \in (F)_4$ be given by

$$C_1 = \left|\begin{array}{cc:cc} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right| \quad \text{and} \quad C_2 = \left|\begin{array}{c:c:c:c} a & 0 & 0 & 0 \\ \hdashline 0 & a & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right|,$$

and consider $M_1, M_2 \in \mathscr{F}_4$ where

$$M_1 = S_4\big(\mathrm{GF}(2)\big)[C_1] \quad \text{and} \quad M_2 = S_4\big(\mathrm{GF}(2)\big)[C_2].$$

Then $F \cong M_1 \cong M_2$, and both M_1 and M_2 have rank 4. It is easily verified that C_1 is the rational canonical form over F for C_1^2, and that C_2 is not similar over F to either C_1 or C_1^2. Hence M_1 and M_2 are not similar over F.

Regarding parts (i) and (ii) of Theorem 13, we consider

EXAMPLE 2. Let $F = \mathrm{GF}(4)$, and let $M_1 = S_2\big(\mathrm{GF}(2)\big)[C]$, where

$$C = \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix}.$$

Then $M_1 \in \mathscr{F}_2$, and M_1 has order 4 and rank 2. We show that M_1 is maximal in $\mathscr{F}_2$, and hence has no extensions in $\mathscr{F}_2$ of order 16. Any matrix in $(F)_2$ which commutes with C has the form

$$\begin{vmatrix} x & y \\ y & x+y \end{vmatrix}.$$

By direct examination, we see that any non-trivial ring extension R of M_1 by such a matrix contains a non-zero singular matrix, and hence R is not a field since R has identity I_2. Hence M_1 is maximal in $\mathscr{F}_2$.

Let $M_2 = \{\text{diag}|x, 0|: x \epsilon F\}$. Then M_1 and M_2 are isomorphic maximal subfields of $(F)_2$. They are not similar over F since M_2 has rank 1.

6. The number $\overline{N}(q, n)$. Let M be a subfield of $(F)_n$ which is counted by $\overline{N}(q, n)$. Then M satisfies the hypotheses of Theorem 8 in [2] or Theorem 9 in [2]. It follows easily that M has order q^m for some $m \geqslant 1$. Also, M is similar over F to either

$$k\text{-sum}\big(S_m(F)\big[C\big(f(x)\big)\big]\big) \quad \text{or} \quad 1^\circ\text{-sum}\Big(k\text{-sum}\big(S_m(F)\big[C\big(f(x)\big)\big]\big); n-r, 0\Big)$$

as M has rank $r = n$ or $r < n$, for some prime polynomial $f(x)$ of degree m in $F[x]$ where $r = mk$. Thus we have defined $\overline{N}(q, n, m, r)$ appropriately, and moreover, the arguments given in Sections 1–3 remain valid in determining $\overline{N}(q, n)$. Accordingly, we have the following results.

THEOREM 16. *$\overline{N}(q, n, m, r) > 0$ if and only if $m|r$.*

THEOREM 17. *Let $F = \text{GF}(q)$, and let M_1, $M_2 \epsilon \mathscr{F}_n$ be counted by $\overline{N}(q, n)$. If M_1 and M_2 have order q^m and rank r, then $M_1 = M_2$ if and only if $M_1 \cap M_2$ contains a non-zero root in $(F)_n$ of some polynomial $x^s g(x) \epsilon F[x]$, where $g(x)$ is a prime of degree m, $s = 0$ if $r = n$, and $s = 1$ if $r < n$.*

THEOREM 18. *Let $F = \text{GF}(q)$, where $q = p^d$. The number of distinct subfields of $(F)_n$ which are counted by $\overline{N}(q, n)$, have order q^m, and rank r, is given by*

$$\overline{N}(q, n, m, r) = \frac{1}{m} \frac{g(d, n)}{g(d, n-r)g(dm, r/m)} \tag{6.1}$$

whenever $m|r$, where $g(s, 0) = 1$, and $g(s, t) = \prod_{r=0}^{t-1} (p^{st} - p^{sr})$ is the number of non-singular matrices of order t over $\text{GF}(p^s)$.

THEOREM 19. *Let $F = \text{GF}(q)$, where $q = p^d$. Then*

$$\overline{N}(q, n) = \sum_{r=1}^{n} \sum_{m|r} \frac{1}{m} \frac{g(d, n)}{g(d, n-r)g(dm, r/m)}, \tag{6.2}$$

where $g(s, 0) = 1$, and $g(s, t) = \prod_{r=0}^{t-1} (p^{st} - p^{sr})$ is the number of non-singular matrices of order t over $\text{GF}(p^s)$.

7. The number $N(q, n, m, n)$. It is clear that each subfield of $(F)_n$ has order p^m for some $m \geqslant 1$, and from our characterization in [2] that $N(q, n, m, r) = 0$ whenever $m > rd$. We proceed as indicated by

$$N(q, n) = \sum_{r=1}^{n} \sum_{m=1}^{rd} N(q, n, m, r), \tag{7.1}$$

and obtain $N(q, n, m, n)$ in this section. We first observe that an arbitrary polynomial which is prime in $F[x]$ and has degree $m \leqslant nd$ need not have

a root in $(F)_n$. For example, let $F = \text{GF}(4)$, $n = 4$, and $f(x) = x^3 + x + 1$. Since $f(x)$ clearly has no roots in F, then $f(x)$ has no roots in $(F)_4$, since $f(x)$ itself is the only choice of non-trivial similarity invariant for such a root in $(F)_4$. We thus state

DEFINITION. Let F be an arbitrary field. A polynomial $f(x) \epsilon F[x]$ is called *n-admissible for F* if and only if $f(x)$ has a root in $(F)_n$.

The difficulties of determining whether or not a given polynomial $f(x) \epsilon \text{GF}[q, x]$ is n-admissible for $\text{GF}(q)$ are shown very clearly by Hodges' work [5]. In essence, a monic polynomial $f(x) \epsilon \text{GF}[q, x]$ is n-admissible for $\text{GF}(q)$ if and only if the degrees and multiplicities of its prime factors in $\text{GF}[q, x]$ induce at least one special partition of n. For our purposes, the following synopsis of Hodges' main result is sufficient.

FACT 1 (Hodges). *Let $f = f(x) \epsilon \text{GF}[q, x]$ be monic, where $q = p^d$, and suppose*

$$f = P_1^{h(1)} P_2^{h(2)} \dots P_w^{h(w)}, \tag{7.2}$$

where $P_i \epsilon \text{GF}[q, x]$ is prime of degree d_i and $h(i) \geqslant 1$ for $1 \leqslant i \leqslant w$, and $P_i \neq P_j$ for $i \neq j$. For each partition π of n defined by an equation of the form

$$n = \sum_{i=1}^{w} d_i \sum_{j=1}^{h(i)} j k_{ij} \tag{7.3}$$

where $k_{ij} \geqslant 0$, let

$$b_i(\pi) = \sum_{u=1}^{h(i)} \Big[k_{iu}^2 (u-1) + 2u k_{iu} \sum_{v=u+1}^{h(i)} k_{iv}\Big], \tag{7.4}$$

and let

$$a(\pi) = \sum_{i=1}^{w} d_i b_i(\pi). \tag{7.5}$$

Then the number of distinct roots in $\big(\text{GF}(q)\big)_n$ of f is given by

$$E(f, n) = g(d, n) \sum_{\pi} q^{-a(\pi)} \prod_{i=1}^{w} \prod_{j=1}^{h(i)} g(d_i d, k_{ij})^{-1}, \tag{7.6}$$

where the summation is over all partitions π of n defined by (7.3); the k_{ij} are non-negative integers defined by (7.3); $b_i(\pi)$ is defined by (7.4); $a(\pi)$ is defined by (7.5); and

$$g(s, t) = \prod_{r=0}^{t-1} (p^{st} - p^{sr})$$

is the number of non-singular matrices of order t over $\text{GF}(p^s)$.

Thus a polynomial $f(x) \epsilon \mathrm{GF}[q, x]$ is n-admissible for $\mathrm{GF}(q)$ if and only if $E(f, n) \neq 0$. We are able to obtain

THEOREM 20. *Let $F = \mathrm{GF}(q)$, where $q = p^d$, and let $N(q, n, m, n)$ be the number of distinct subfields of $(F)_n$ having order p^m and rank n. Then $N(q, n, m, n) = 0$ if and only if $F_p[x]$ contains no prime polynomial of degree m which is n-admissible for F. Otherwise,*

$$N(q, n, m, n) = \frac{1}{m} E(g, n), \tag{7.7}$$

where $g(x)$ is any arbitrary polynomial of degree m over F_p which is prime in $F_p[x]$ and which is n-admissible for F, and $E(g, n)$ is given by (7.6).

Proof. We proceed as indicated by Section 2, except relative to Theorem 6 in [2]. As in the proof of the latter ([2], p. 480) for A and $h(x)$, we note that $(F)_n$ is an algebraic algebra over F_p.

It is clear that (7.7) holds for $m = 1$. Accordingly, let $m > 1$, and let $g(x) \epsilon F_p[x]$ be any polynomial of degree m which is prime in $F_p[x]$ and is n-admissible for F. Then $g(x) \neq x$. Let $A \epsilon (F)_n$ be an arbitrary root of $g(x)$. Then the minimal polynomial $h(x)$ of A over F_p divides $g(x)$ in F_p, and hence $h(x) = g(x)$. Since $g(x) \neq x$ is prime in $F_p[x]$, then $g(x)$ has a non-zero constant term. Since the similarity invariants of A each divide $g(x)$ in $F[x]$, then each similarity invariant of A has a non-zero constant term. Hence A has rank n. Let

$$C = \mathrm{diag}\big|C\big(f_1(x)\big), \ldots, C\big(f_k(x)\big)\big|$$

be the rational canonical form for A over F. Then as argued above, $g(x)$ is the minimal polynomial over F_n of $C\big(f_i(x)\big)$ for $1 \leqslant i \leqslant k$. Hence $S_n(F_p)[C]$ is a subfield of $(F)_n$ having order p^m and rank n, and $S_n(F_p)[A]$ is also. As before, let $D\big(g(x), n\big)$ denote the number of distinct roots in $(F)_n$ of $g(x)$ which have rank n. Since in this case each root in $(F)_n$ of $g(x)$ has rank n, then $D\big(g(x), n\big)$ is given by (7.6) as derived in Fact 1. A minor change in the proof of Lemma 3 yields

LEMMA 21. *Let $F = \mathrm{GF}(q)$, where $q = p^d$. If M_1 and M_2 are subfields of $(F)_n$ having order p^m and rank n, then $M_1 = M_2$ if and only if $M_1 \cap M_2$ contains a non-zero root in $(F)_n$ of some prime polynomial in $F_p[x]$ having degree m.*

We have already shown that each root $A \epsilon (F)_n$ of $g(x)$ lies in a subfield $M = S_n(F_p)[A]$ of $(F)_n$ having order p^m and rank n. Since M is a normal extension of $S_n(F_p)$, then M contains m distinct roots in $(F)_n$ of $g(x)$. Hence by Lemma 21, $m \mid D\big(g(x), n\big)$, and letting $l = \frac{1}{m} D\big(g(x), n\big)$, then there are precisely l distinct subfields $M_1, \ldots, M_l$ of $(F)_n$ of the form

$M_i = S_n(F_p)[A_i]$ where A_i is a root in $(F)_n$ of $g(x)$. Let $h(x)$ be any polynomial of degree m over F_p which is prime in $F_p[x]$ and which is n-admissible for F. Let B be any root in $(F)_n$ of $h(x)$. Then $S_n(F_p)[B]$ is a subfield of $(F)_n$ having order p^m and rank n. Hence for any i, $1 \leqslant i \leqslant l$, choose any isomorphism $\varphi\colon S_n(F_p)[B] \to M_i$. Then $h\big(\varphi(B)\big) = O_n$, and hence each M_i contains m distinct roots in $(F)_n$ of $h(x)$. Now, let M be an arbitrary subfield of $(F)_n$ having order p^m and rank n. Then as argued in proving Theorem 6 in [2], $M = S_n(F_p)[B]$ where $B \epsilon (F)_n$ has minimal polynomial $h(x)$ over F_p for some prime polynomial $h(x) \epsilon F_p[x]$ of degree m. Hence M contains a root in $(F)_n$ of $g(x)$, and $M = M_j$ for some j, $1 \leqslant j \leqslant l$. The initial claim of the theorem is now obvious, and we are done.

8. The number $N(q, n, m, r)$. Our technique for finding $N(q, n, m, r)$ where $1 \leqslant r < n$ parallels that of Section 3, except for slight modifications as indicated by Theorem 6 in [2]. Accordingly, we fix r, where $1 \leqslant r < n$. Let m be any fixed positive integer such that there exists a prime polynomial $g(x) \neq x$ of degree m which is prime in $F_p[x]$ and which is r-admissible for F. Let $f(x) = xg(x)$. Then $f(x)$ is n-admissible for F and has roots in $(F)_n$ having rank r. Let $A \epsilon (F)_n$ be any root of $f(x)$ having rank r, and let A have minimal polynomial $h(x)$ over F_p. Then $h(x)$ divides $f(x)$ in $F_p[x]$. Since $r > 0$, then $h(x) \neq x$, and since $r < n$, then $h(x) \neq g(x)$. Thus $h(x) = f(x)$. Let $s(x)$ be the minimal polynomial of A over F. Then $s(x) \mid f(x)$ in $F[x]$. Since $x \nmid g(x)$, then we can factor $s(x)$ as $s(x) = xt_k(x)$ or $s(x) = t_k(x)$ where $t_k(x) \epsilon F[x]$ satisfies $\big(x, t_k(x)\big) = 1$. If $s(x) = t_k(x)$, then the rational canonical form for A over F is non-singular, which contradicts A having rank $r < n$. Thus $s(x) = xt_k(x)$. Hence A is similar over F to a matrix of the form

$$\begin{aligned} A' &= \mathrm{diag}\big|C(x), \ldots, C(x), C\big(t_1(x)\big), \ldots, C\big(t_k(x)\big)\big| \\ &= 1^\circ\text{-sum}\big(\mathrm{diag}\big|C\big(t_1(x)\big), \ldots, C\big(t_k(x)\big)\big|; n-r, 0\big), \end{aligned} \tag{8.1}$$

where each $C\big(t_i(x)\big)$ has minimal polynomial $g(x)$ over F_p and is non-singular. Let

$$C = \mathrm{diag}\big|C\big(t_1(x)\big), \ldots, C\big(t_k(x)\big)\big|.$$

Then C has rank r, and $S_r(F_p)[C]$ is a subfield of $(F)_r$ having order p^m and rank r. Thus on conjugating $1^\circ\text{-sum}\big(S_r(F_p)[C]; n-r, 0\big)$ by an appropriate matrix, we obtain a subfield of $(F)_n$ which contains A, has order p^m, and has rank r. Again, let $D\big(xg(x), r\big)$ denote the number of distinct roots in $(F)_n$ of $xg(x)$ which have rank r. Since the rank of a root $A \epsilon (F)_n$ of $xg(x)$ is determined by the multiplicity of the elementary divisor x of A, then $D\big(xg(x), r\big)$ can be computed using Hodges' result as given in Fact 1. Indeed, the argument which establishes that A is similar over F to the matrix A' as given in (8.1) leads to a proof of

THEOREM 22. *Let $f = f(x) \in \mathrm{GF}[q, x]$ have factorization* (7.2), *where $P_1^{h(1)} = x$. Then the number of distinct roots in $(\mathrm{GF}(q))_n$ of $f(x)$ which have rank r is given by* (7.6), *where the summation is over all partitions π of n obtained by taking $k_{11} = n - r$ and k_{ij} a non-negative integer for $i > 1$ in* (7.3); *$b_i(\pi)$ is defined by* (7.4); *and $a(\pi)$ is defined by* (7.5).

We continue, and characterize the distinct subfields of $(F)_n$ having order p^m and rank r. Appealing to Theorem 6 in [2] rather than Theorem 3 in [1], only slight modifications in the proof of Lemma 6 yield

LEMMA 23. *Let $F = \mathrm{GF}(q)$, where $q = p^d$. Let M_1, M_2 be subfields of $(F)_n$ of order p^m and having a common identity of rank $r < n$. Then $M_1 = M_2$ if and only if $M_1 \cap M_2$ contains a non-zero root in $(F)_n$ of some polynomial $xg(x) \in F_p[x]$, where $g(x) \neq x$ is prime in $F_p[x]$ and has degree m.*

From Lemma 21, Lemma 23, and Lemma 7, we obtain the following generalization of Theorem 8.

THEOREM 24. *Let $F = \mathrm{GF}(q)$, where $q = p^d$. Let $M_1, M_2 \in \mathscr{F}_n$ have order p^m and rank r. Then M_1 and M_2 are distinct if and only if $M_1 \cap M_2$ contains no non-zero root in $(F)_n$ of a polynomial $x^s g(x) \in F[x]$, where $g(x) \neq x$ has degree m and is prime in $F_p[x]$; $s = 0$ if $r = n$; and $s = 1$ for $r < n$.*

We have accumulated the following facts. For any fixed r, $1 \leqslant r < n$; and for any m such that there exists a polynomial $g(x) \neq x$ of degree m over F_p which is prime in $F_p[x]$ and is r-admissible for F; then each root $A \in (F)_n$ of $xg(x)$ having rank r lies in a subfield M of $(F)_n$ having order p^m and rank r. A similar argument to those given earlier establishes that if $h(x) \neq x$ is any polynomial of degree m which is prime in $F_p[x]$ and which is r-admissible for F, then each such subfield M of $(F)_n$ contains precisely m distinct roots of $xh(x)$ having rank r; and if M' is an arbitrary subfield of $(F)_n$ having order p^m and rank r, then M' contains a root of $xg(x)$ having rank r. Hence by Theorem 24 and Theorem 22 we have

THEOREM 25. *Let $F = \mathrm{GF}(q)$, where $q = p^d$, and let $N(q, n, m, r)$ be the number of distinct subfields of $(F)_n$ having order p^m and rank $r < n$. Then $N(q, n, m, r) = 0$ if and only if no prime polynomial $g(x) \neq x$ of degree m in $F_p[x]$ is r-admissible for F. Otherwise,*

$$(8.2) \qquad N(q, n, m, r) = \frac{1}{m} g(d, n) \sum_{\pi} q^{-a(\pi)} \prod_{i=1}^{w} \prod_{j=1}^{h(i)} g(d_i d, k_{ij})^{-1},$$

for any prime polynomial $g(x) \in F_p[x]$ of degree m which is r-admissible for F; where $xg(x)$ has factorization (6.5) *with $P_1^{h(1)} = x$; the summation is over all partitions π of n obtained by taking $k_{11} = n - r$ in* (7.3) *and k_{ij} a non-negative integer for $i > 1$; $b_i(\pi)$ is defined by* (7.4); *$a(\pi)$ is defined by* (7.5); *and $g(s, t) = \prod_{r=0}^{t-1} (p^{st} - p^{sr})$ is the number of non-singular matrices of order t over $\mathrm{GF}(p^s)$.*

9. The number $N(q, n)$ and further results. In summary, we have

THEOREM 26. *Let $F = \mathrm{GF}(q)$, where $q = p^d$. Then*

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

where $N(q, n, m, r)$ is given by (7.7) *if $r = n$, and by* (8.2) *if $r < n$.*

From (6.1) we obtain the following generalizations of Theorem 14 and Theorem 15.

THEOREM 27. *Given any prime p and any integers $n, d \geqslant 1$, then $n \mid g(d, n)$ where $g(d, n) = \prod_{r=0}^{n-1} (p^{dn} - p^{dr})$ is the number of non-singular matrices of order n over $\mathrm{GF}(p^d)$.*

THEOREM 28. *Given any prime p and any integers $d \geqslant 1$ and $n > 1$, then*

$$n \mid \prod_{r=1}^{n-1} (p^{dn} - p^{dr}).$$

As an easily argued consequence of Lemma 7, we conclude with

THEOREM 29. *Let F be an arbitrary field, and let $M_1, M_2 \in \mathscr{F}_n$. Then $M_1 \cap M_2 \in \mathscr{F}_n$ if and only if $M_1 \cap M_2 \neq (O_n)$.*

References

[1] J. T. B. Beard, jr., *Matrix fields over prime fields*, Duke Math. J. 39 (1972), pp. 313–322.

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

[3] L. E. Dickson, *Linear Groups*, Leipzig 1901.

[4] P. Dubreil and M. L. Dubreil-Jacotin, *Lectures on Modern Algebra*, New York 1967.

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

[6] S. Perlis, *Theory of Matrices*, Pa., 1952.

UNIVERSITY OF TEXAS AT ARLINGTON
Arlington, Texas

Received on 30. 5. 1972 (292)