

Linear permutation polynomials with coefficients in a subfield

by

J. V. BRAWLEY (Clemson, S. C.), L. CARLITZ* (Durham N. C.),
and THERESA VAUGHAN (Durham, N. C.)

To Professor Carl Ludwig Siegel

1. Introduction. Let $\text{GF}(q^n)$ denote the finite field of order q^n , where $q = p^r$ for some $r > 0$ and some prime p , and let $\text{GF}(q^m)$ be a subfield of $\text{GF}(q^n)$ so that $n = ms$ for some integer s , $1 \leq s \leq n$. If f is any function from $\text{GF}(q^n)$ to $\text{GF}(q^n)$ it is well-known that f has a unique polynomial representation

$$(1.1) \quad f(x) = \sum_{i=0}^{q^n-1} a_i x^i,$$

where the coefficients $a_i \in \text{GF}(q^n)$. In case f is a permutation of $\text{GF}(q^n)$ the corresponding polynomial $f(x)$ is called a permutation polynomial. The set of all such permutation polynomials under composition modulo $x^{q^n} - x$ forms a group which is isomorphic to the symmetric group S_{q^n} . Those permutation polynomials of the form (1.1) whose coefficients a_i are in $\text{GF}(q^m)$ constitute a subgroup, the structure of which has been determined by Carlitz and Hayes [2] as a semi-direct product of certain symmetric groups and cyclic groups. In this paper we consider an analogous situation for polynomials of the form

$$(1.2) \quad f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$$

with coefficients a_i in $\text{GF}(q^m)$. Such polynomials (which represent a subalgebra of the algebra of linear transformations of $\text{GF}(q^n)$ over $\text{GF}(q)$) are generalizations of the Ore polynomials [6], [7], where the coefficients a_i are assumed to lie in $\text{GF}(q)$. The set of all Ore polynomials under the modulo $x^{q^n} - x$ operations of addition and composition of functions, and scalar multiplication by elements of $\text{GF}(q)$, forms a commutative algebra over $\text{GF}(q)$ which is isomorphic to $\text{GF}(q)[x]/(x^n - 1)$ (see [7]).

* Supported in part by NSF grant GP-17031.



In order to generalize Ore's work, put

$$(1.3) \quad R_m = \left\{ f(x) = \sum_{i=0}^{m-1} a_i x^{q^i}; a_i \in \text{GF}(p^m) \right\}.$$

Then R_m under the above mentioned operations is an algebra over $\text{GF}(q)$. The case $m = 1$ is that treated by Ore. In § 2 of the present paper we show that R_n is isomorphic to the ring of $n \times n$ matrices over $\text{GF}(q)$ from which it follows that the group of units of R_n , the so-called Betti–Mathieu group, is isomorphic to the general linear group $\text{GL}(n, q)$. (See [1], [3].) In § 3 we prove that R_m is isomorphic to the ring of $m \times m$ matrices with entries from the residue class ring $\text{GF}(q)[x]/(x^s - 1)$. This includes Ore's result as well as that given in § 2 as special cases. Using this isomorphism it is easy to describe the group of units of R_m as a direct product of subgroups in contrast to the Carlitz–Hayes result. This description and several interesting combinatorial results are contained in § 4.

2. Preliminaries. The ring of polynomials with coefficients in $\text{GF}(q)$ will be denoted by $\text{GF}(q)[x]$. If $f(x) \in \text{GF}(q)[x]$, the principal ideal generated by $f(x)$ is denoted by $(f(x))$, and the residue class ring consisting of the elements of $\text{GF}(q)[x]$ reduced modulo $f(x)$ is written $\text{GF}(q)[x]/(f(x))$. Also if S is any ring with identity and k is any positive integer, the ring of $k \times k$ matrices with elements from S will be written as $(S)_k$, and $\text{GL}(k, S)$ will denote the group of nonsingular $k \times k$ matrices over S . In case $S = \text{GF}(q^n)$ the notation $\text{GL}(k, q^n)$ is used for $\text{GL}(k, S)$.

Consider the finite field $\text{GF}(q^n)$ as a vector space of dimension n over $\text{GF}(q)$. Let L be the algebra of linear transformations of $\text{GF}(q^n)$ over $\text{GF}(q)$. The set R_n of all polynomials of the form

$$(2.1) \quad f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$$

with the coefficients $a_i \in \text{GF}(q^n)$, equipped with the modulo $x^n - x$ operations of addition and composition of functions and scalar multiplication by elements of $\text{GF}(q)$, is an algebra over $\text{GF}(q)$, which is in fact isomorphic to the algebra L .

THEOREM 2.1. *The algebras R_n and L are isomorphic.*

Proof. For each $f(x) \in R_n$ let f be the function from $\text{GF}(q^n)$ to $\text{GF}(q^n)$ defined by substitution and let ψ denote the mapping that takes $f(x)$ to f . Then for each $f(x) \in R_n$ $\psi(f(x)) \in L$ as $(\xi + \eta)^{q^i} = \xi^{q^i} + \eta^{q^i}$ and $(\lambda \xi)^{q^i} = \lambda^{q^i} \xi^{q^i} = \lambda \xi^{q^i}$ for all integers $i > 0$ and $\xi, \eta \in \text{GF}(q^n)$, $\lambda \in \text{GF}(q)$, i.e., $\psi: R_n \rightarrow L$. Moreover, it is immediate that

$$\begin{aligned} \psi(f(x) + g(x)) &= f + g, \\ \psi(\lambda f(x)) &= \lambda f, \end{aligned}$$

and

$$\psi(f(g(x))) = f \circ g,$$

so that ψ is an algebra homomorphism. ψ is one-one by the remark in the first paragraph of § 1, and since $|R_n| = (q^n)^n = q^{n^2} = |L|$, the proof is complete.

It follows immediately that

COROLLARY 2.2. *The algebra R_n is isomorphic to $(\text{GF}(q))_n$.*

The Betti–Mathieu group is by definition the group of units of R_n ; hence we have reproved (see [1], [3])

COROLLARY 2.3. *The Betti–Mathieu group is isomorphic to $\text{GL}(n, q)$.*

3. The algebra R_m . If $n = ms$, where m and s are positive integers, we define the algebra R_m to be the set of all polynomials of the form

$$(3.1) \quad f(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$$

with coefficients $a_i \in \text{GF}(q^m) \subseteq \text{GF}(q^n)$, equipped with addition and composition of functions and scalar multiplication by elements of $\text{GF}(q)$. When $m = n$, the algebra R_n is, as we have seen, isomorphic to the algebra of all linear transformations of $\text{GF}(q^n)$ over $\text{GF}(q)$. When $m = 1$, the algebra R_1 is the algebra of polynomials studied by Ore in [6], [7] who has shown that R_1 is isomorphic to the residue class ring $\text{GF}(q)[x]/(x^n - 1)$. The next theorem is a generalization of these results.

THEOREM 3.1. *If $n = ms$, where m and s are positive integers, then the algebra R_m is isomorphic to the algebra $(\text{GF}(q)[x]/(x^s - 1))_m$, of $m \times m$ matrices with elements from the residue class ring $\text{GF}(q)[x]/(x^s - 1)$.*

Proof. For convenience, let $S_m = (\text{GF}(q)[x]/(x^s - 1))_m$. Fix any ordered basis $B = \{\beta_1, \beta_2, \dots, \beta_m\}$ for $\text{GF}(q^m)$ over $\text{GF}(q)$. If $f(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ with coefficients a_i in $\text{GF}(q^m)$, let $[f]_B$ denote the matrix in $(\text{GF}(q))_m$ which represents the linear transformation $f(x)$ in the ordered basis B .

We first note that any element of R_m , say

$$(3.2) \quad g(x) = \sum_{i=0}^{m-1} a_i x^{q^i}; \quad a_i \in \text{GF}(q^m)$$

may be rewritten as

$$(3.3) \quad g(x) = \sum_{i=0}^{s-1} \sum_{k=0}^{m-1} a_{im+k} x^{q^{im+k}}.$$

If we let $g_i(x) = \sum_{k=0}^{m-1} a_{im+k} x^{q^k}$ for $i = 0, 1, \dots, s-1$, then we may write

$$(3.4) \quad g(x) = \sum_{i=0}^{s-1} g_i(x^{q^{im}}).$$

On the other hand, any element F of S_m has the form $F = (f_{ij}(x))$ (for $i, j = 0, 1, \dots, m-1$), where each $f_{ij}(x)$ is a polynomial over $\text{GF}(q)$ of degree less than s , and we may rewrite the matrix F as follows:

$$(3.5) \quad F = F_0 + F_1x + F_2x^2 + \dots + F_{s-1}x^{s-1}$$

where each F_k ($k = 0, 1, \dots, s-1$) is an $m \times m$ matrix over $\text{GF}(q)$, and the (i, j) th entry of F_k is the coefficient of x^k in the polynomial $f_{ij}(x)$.

Now for each F_k , there exists a polynomial

$$(3.6) \quad g_k(x) = \sum_{i=0}^{m-1} b_{ik}x^{qi}$$

such that F_k is the matrix representing $g_k(x)$ in the ordered basis B , that is, $F_k = [g_k]_B$.

It is now fairly obvious how to define an isomorphism between S_m and R_m . If F is given by (3.5) and the corresponding $g_k(x)$ are given by (3.6), define a mapping $\varphi: S_m \rightarrow R_m$ by

$$(3.7) \quad \varphi(F_k x^k) = g_k(x^{q^k m})$$

where it is understood that map φ is to be extended linearly to all of S_m . It is clear that this is indeed a map from S_m to R_m , since every element of R_m may be written in the form (3.4). Evidently addition and scalar multiplication by elements of $\text{GF}(q)$ are preserved, and it follows from Theorem 2.1 that φ is bijective. It remains only to show that the map φ preserves composition. Suppose that $G = [g]_B$ and $H = [h]_B$ are any two matrices in $(\text{GF}(q))_m$. Then if i and k are positive integers less than s , and $i+k \equiv j \pmod{s}$, we have

$$(3.8) \quad \varphi(Gx^i) \circ \varphi(Hx^k) = g(x^{q^i m}) \circ h(x^{q^k m}) = g(h(x^{q^{k+m} m})) = g(h(x^{q^j m}))$$

since the coefficients of $h(x)$ are elements of $\text{GF}(q^m)$. Since $Gx^i Hx^k = GHx^j$, and $\varphi(GHx^j) = g(h(x^{q^j m}))$, it follows that

$$(3.9) \quad \varphi(Gx^i) \circ \varphi(Hx^k) = \varphi(GHx^j)$$

and so φ preserves composition. Thus φ is an isomorphism. This completes the proof.

4. The group of units of R_m and related results. In order to characterize the group of units of R_m we will use the following known facts.

LEMMA 4.1. *If S is a commutative ring with 1 which has the direct sum decomposition $S = \bigoplus_{i=1}^t S_i$, then $(S)_m = \bigoplus_{i=1}^t (S_i)_m$ and moreover $\text{GL}(m, S) = \bigoplus_{i=1}^t \text{GL}(m, S_i)$ so that*

$$(4.1) \quad |\text{GL}(m, S)| = \prod_{i=1}^t |\text{GL}(m, S_i)|.$$

LEMMA 4.2. *If $S = \text{GF}(q)[x]/(P(x)^e)$ where $P(x)$ is an irreducible in $\text{GF}(q)[x]$ of degree d , then*

$$(4.2) \quad |\text{GL}(m, S)| = q^{edm^2} \prod_{i=1}^m (1 - q^{-id}).$$

The proof of Lemma 4.1 is easy. As for Lemma 4.2, one can use the formula of McDonald [5] once it is noted that S is a finite local ring. Basically, the proof uses the correspondence theorem for rings together with the facts that (i) $M = P(x) \cdot S$ is the unique maximal ideal of S , (ii) $S/M = \text{GF}(q^d)$ and (iii) $A \in (S)_m$ is nonsingular iff $\mu(A) = (\mu(a_{ij})) \in (S/M)_m$ is nonsingular where $\mu: S \rightarrow S/M$ is the natural homomorphism.

THEOREM 4.3. *Let $S = \text{GF}(q)[x]/(x^s - 1)$, and suppose that*

$$(4.3) \quad x^s - 1 = P_1(x)^{e_1} P_2(x)^{e_2} \dots P_t(x)^{e_t}$$

where the $P_j(x)$ are distinct irreducible elements of $\text{GF}(q)[x]$, and the degree of $P_j(x)$ is d_j for $j = 1, 2, \dots, t$. Set $S_j = \text{GF}(q)[x]/(P_j(x)^{e_j})$. Then $\text{GL}(m, S)$ is isomorphic to the direct product of the set $\{\text{GL}(m, S_j): j = 1, 2, \dots, t\}$ and moreover

$$(4.4) \quad |\text{GL}(m, S)| = q^{m^2 s} \prod_{j=1}^t \prod_{i=1}^m (1 - q^{-id_j}).$$

Proof. It is only necessary to note that $S = S_1 \oplus S_2 \oplus \dots \oplus S_t$. Then by Lemma 4.1, $\text{GL}(m, S)$ is isomorphic to the direct product of the set $\{\text{GL}(m, S_j): j = 1, 2, \dots, t\}$. To get the equality (4.4), use Lemma 4.2:

$$|\text{GL}(m, S_j)| = q^{e_j d_j m^2} \prod_{i=1}^m (1 - q^{-id_j}),$$

and from Lemma 4.1,

$$\begin{aligned} |\text{GL}(m, S)| &= \prod_{j=1}^t |\text{GL}(m, S_j)| = \prod_{j=1}^t q^{e_j d_j m^2} \prod_{i=1}^m (1 - q^{-id_j}) \\ &= q^{sm^2} \prod_{j=1}^t \prod_{i=1}^m (1 - q^{-id_j}). \end{aligned}$$

COROLLARY 4.4. *If $R_m = \left\{ \sum_{i=0}^{n-1} a_i x^{qi} : a_i \in \text{GF}(q^m) \right\}$, then the group of units of R_m is isomorphic to the direct product of the set $\{\text{GL}(m, S_j): j = 1, 2, \dots, t\}$ of Theorem 4.3, and the order of the group of units of R_m is given by (4.4).*

COROLLARY 4.5. *Under the hypothesis of Theorem 4.3, if also $(s, q) = 1$, then the group of units of R_m is isomorphic to a direct product of general linear groups.*



Proof. If $(s, q) = 1$, then each exponent e_k appearing in the factorization (4.3) of $x^s - 1$ is equal to one, and each S_j is isomorphic to the field $\text{GF}(q^{d_j})$. Then $\text{GL}(m, S_j) = \text{GL}(m, q^{d_j})$ is a general linear group.

It should be noted that (4.4) can be derived directly from the result of Farahat [4] which gives the order of any finite ring S with 1 in terms of $|\text{rad} S|$ and the structure of $S/\text{rad} S$ as assured by the Wedderburn-Artin Theorem. This involves however computing $|\text{rad} S|$ and knowing exactly how $S/\text{rad} S$ decomposes into a direct sum of matrix rings over finite fields.

As final items we consider several interesting combinatorial questions. Suppose we are given the polynomial

$$(4.5) \quad f(x) = \sum_{i=1}^{m-1} b_i x^{a^i}; \quad b_i \in \text{GF}(q^m),$$

so that $f(x)$ acting on $\text{GF}(q^m)$ as a vector space over $\text{GF}(q)$ is a linear transformation f . The questions are (i) How many $\varphi(x) \in R_n$ when acting on $\text{GF}(q^m)$ equal f and (ii) How many of these $\varphi(x)$ are in the group of units of R_n ; i.e., are permutations of $\text{GF}(q^n)$. The answers to these questions are the content of our last theorem.

THEOREM 4.6. *The number of polynomials*

$$(4.6) \quad \varphi(x) = \sum_{i=1}^{n-1} a_i x^{a^i}; \quad a_i \in \text{GF}(q^n),$$

whose restriction to $\text{GF}(q^m)$ define the same functions as (4.5) is $q^{m(n-m)}$. Of these, the number which are in the group of units of R_n is zero if $f(x)$ is not one-one on $\text{GF}(q^m)$ and is $q^{m(n-m)} |\text{GL}(n-m, q)|$ if $f(x)$ is one-one on $\text{GF}(q^m)$, where $|\text{GL}(t, q)|$ is the well-known number $\prod_{i=0}^{t-1} (q^t - q^i)$. Thus, in particular, the number of such extensions of $f(x)$ is independent of the function $f(x)$.

Proof. Any $\varphi(x)$ of the form (4.6) may be rewritten as

$$\varphi(x) = \sum_{i=0}^{m-1} \sum_{j=1}^{s-1} a_{i+mj} x^{a^{i+mj}}$$

If $\xi \in \text{GF}(q^m)$ then

$$\xi^{a^{i+mj}} = \xi^{a^i} \xi^{a^{mj}} = \xi^{a^i},$$

so that

$$\varphi(\xi) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{s-1} a_{i+mj} \right) \xi^{a^i}.$$

Hence

$$\varphi(\xi) = f(\xi) \quad \text{for all } \xi \in \text{GF}(q^m)$$

if and only if

$$\sum_{j=0}^{s-1} a_{i+mj} = b_i \quad (i = 0, 1, \dots, m-1).$$

The number of solutions $(a_0, a_1, \dots, a_{n-1})$ to this system of linear equations is independent of the particular b_i 's and is $q^{n(s-1)m} = q^{n(n-m)}$ which completes the first part of the theorem.

As for the second part, clearly if $f(x)$ is not one-one on $\text{GF}(q^m)$ none of the $\varphi(x)$ maps on R_n whose restriction to $\text{GF}(q^m)$ equals $f(x)$ can be one-one; thus, assume $f(x)$ is one-one on $\text{GF}(q^m)$. Any linear map is completely determined by its action on a basis. Thus if $f(x)$ is given linear and one-one on $\text{GF}(q^m)$, then the number of ways to extend $f(x)$ to a one-one linear map on $\text{GF}(q^n)$ is precisely the number of distinct ordered linearly independent sequences of $n-m$ elements of $\text{GF}(q^n)$ which are bases for complementary subspaces of $\text{GF}(q^m)$. By a standard argument, this number is given by

$$\begin{aligned} & (q^n - q^m)(q^n - q^{m+1}) \dots (q^n - q^{n-1}) \\ &= q^n (q^{n-m} - 1) q^m (q^{n-m} - q) \dots q^m (q^{n-m} - q^{n-m-1}) \\ &= q^{m(n-m)} \prod_{j=0}^{n-m-1} (q^{n-m} - q^j) = q^{m(n-m)} |\text{GL}(n-m, q)|. \end{aligned}$$

This completes the proof.

References

- [1] L. Carlitz, *A note on the Betti-Mathieu group*, Portugal. Math. 22 (1963), pp. 121-125.
- [2] — and D. Hayes, *Permutations with coefficients in a subfield*, Acta Arith. 21 (1972), pp. 31-35.
- [3] L. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, New York 1958.
- [4] H. K. Farahat, *The multiplicative groups of a ring*, Math. Zeitschr. 87 (1965), pp. 378-384.
- [5] B. R. McDonald, *Involuntary matrices over finite local rings*, Canadian J. Math. 24 (1972), pp. 369-378.
- [6] O. Ore, *On a special class of polynomials*, Amer. Math. Soc. Trans. 35 (1933), pp. 559-584.
- [7] — *Contributions to the theory of finite fields*, Amer. Math. Soc. Trans. 36 (1934), pp. 243-274.

Received on 17. 9. 1972