ACTA ARITHMETICA
XXI (1972)

Permutations with coefficients in a subfield

by

L. Carlitz and D. R. Hayes (Durham, N.C.)*

To the memory of Wacław Sierpiński

1. Introduction. Each permutation of the finite field $GF(q^n)$ is the function associated to a unique polynomial over $GF(q^n)$ of degree less than q^n. The smallest subfield of $GF(q^n)$ which contains all the coefficients of this polynomial will be referred to as the *coefficient field* of f. It is clear that the permutations with coefficient field contained in $GF(q)$ form a subgroup $A(q^n)$ of the group of all permutations of $GF(q^n)$. The principal aim of this paper is the determination of the structure of $A(q^n)$. We find that $A(q^n)$ can be built-up out of symmetric groups and cyclic groups using the semidirect product. We denote the symmetric group on m letters by S_m and the cyclic group of order r by C_r.

The group $A(q^n)$ contains the subgroup $B(q^n)$ generated by the linear permutations $x \to ax+b$ with $a, b \in GF(q)$ and the permutation * defined by

$$x^* = \begin{cases} 0 & \text{if} \quad x = 0, \\ 1/x & \text{if} \quad x \neq 0. \end{cases}$$

Note that $x^* = x^{q^n-2}$ on $GF(q^n)$. It is known [1] that * and the linear permutations generate the full symmetric group when $n = 1$. In fact, the transposition (ab) is given by the permutation

$$(1) \qquad x \to a+(b-a)\big[1-\big(1+(b-a)(x-b)^*\big)^*\big]^*.$$

We show that $B(q^n) \neq A(q^n)$ for $n > 1$ except in the one case $q = 2$ and $n = 2$. In fact, except for this special case, for $n > 1$ $B(q^n) = S_q \times L_q$, where L_q is the group of linear fractional transformations over $GF(q)$. Thus, $B(q^n)$ is actually independent of n for $n > 1$!

* Supported in part by NSF grants GP-17071 and GP-21085.

2. The group $A(q^n)$. Denote the Frobenius automorphism $x \to x^q$ by φ.

LEMMA 1. *The group $A(q^n)$ is the group of all permutations f of $\mathrm{GF}(q^n)$ such that $f\varphi = \varphi f$.*

Proof. It is clear that each permutation in $A(q^n)$ commutes with φ. Conversely, if

$$f(x) = \sum_{\nu=0}^{q^n-1} a_\nu x^\nu$$

commutes with φ, then $f(x^q) = (f(x))^q$ for all $x \in \mathrm{GF}(q^n)$. If $y = x^q$, this means that

$$f(y) = \sum_{\nu=0}^{q^n-1} (a_\nu - a_\nu^q) y^\nu = 0$$

for all $y \in \mathrm{GF}(q^n)$. Since $\deg f < q^n$, we must have $a_\nu = a_\nu^q$ and hence $a_\nu \in \mathrm{GF}(q)$ for $\nu = 0, 1, \ldots, q^n - 1$. Hence, the coefficient field of f is contained in $\mathrm{GF}(q)$, and the proof is complete.

We can now determine the orbits of the action of $A(q^n)$ on $\mathrm{GF}(q^n)$. For each divisor d of n, put

$$K_d = \{a \in \mathrm{GF}(q^n) |\ \deg a = d \text{ over } \mathrm{GF}(q)\}.$$

LEMMA 2. *If $a \in \mathrm{GF}(q^n)$ has degree d over $\mathrm{GF}(q)$, then the orbit of a under $A(q^n)$ is K_d.*

Proof. The commutation $f\varphi = \varphi f$ for $f \in A(q^n)$ implies that each subfield of $\mathrm{GF}(q^n)$ containing $\mathrm{GF}(q)$ is setwise invariant under the action of $A(q^n)$. Since K_d is the complement in $\mathrm{GF}(q^d)$ of the union of those of its proper subfields which contain $\mathrm{GF}(q)$, K_d must also be invariant under the action of $A(q^n)$. Therefore, $\mathrm{Orb}(\alpha) \subset K_d$. To prove the reverse inclusion, we have to exhibit for every $\beta \in K_d$ a permutation $f \in A(q^n)$ such that $f(\alpha) = \beta$. If β is one of the field conjugates $\varphi^s(\alpha)$ of α over $\mathrm{GF}(q)$, then we take $f = \varphi^s$. Otherwise, put

$$f(x) = \begin{cases} x & \text{if } x \text{ is not a field conjugate of } \alpha \text{ or } \beta \text{ over } \mathrm{GF}(q), \\ \varphi^s(\beta) & \text{if } x = \varphi^s(\alpha) \text{ for some integer } s, \\ \varphi^s(\alpha) & \text{if } x = \varphi^s(\beta) \text{ for some integer } s. \end{cases}$$

Then f is well-defined because $\varphi^s(\alpha) = \varphi^t(\alpha)$ means that d divides $s - t$ and this means that $\varphi^s(\beta) = \varphi^t(\beta)$ as $\deg \beta = d$. One verifies immediately that f is a permutation with $f(\alpha) = \beta$ and that $f\varphi = \varphi f$. Therefore, $f \in A(q^n)$ by Lemma 1, and so $\beta \in \mathrm{Orb}(\alpha)$. This shows $K_d \subset \mathrm{Orb}(\alpha)$ and completes the proof.

For every divisor d of n, let $A_d(q^n)$ be the group of all permutations g on K_d such that $g\varphi = \varphi g$. Restriction to K_d yields a homomorphisms $\mathrm{res}_d\colon A(q^n) \to A_d(q^n)$ as one easily checks. Putting these homomorphisms together, we get a homomorphism

$$\mathrm{res}\colon A(q^n) \to \bigtimes_{d|n} A_d(q^n)$$

into the direct product of the $A_d(q^n)$.

THEOREM 1. *The homomorphism* res *defined above is an isomorphism.*

Proof. We construct the inverse homomorphism inf as follows: Given $g = (g_d)_{d|n}$ in the product group, let $\inf(g) = f$ where $f(x) = g_d(x)$ when $\deg x = d$. Then $f\varphi = \varphi f$ since $g_d\varphi = \varphi g_d$ for all $d|n$. Therefore, $f \in A(q^n)$ by Lemma 1. That inf is inverse to res is immediate. This completes the proof.

In order to complete our study of $A(q^n)$, we must determine the structure of the groups $A_d(q^n)$. The set K_d is the set of zeros of the irreducible polynomials of degree d over $\mathrm{GF}(q)$. Therefore, $\# K_d = d\pi(d)$, where $\pi(d) = \pi_q(d)$ is the number of monic irreducibles of degree d over $\mathrm{GF}(q)$. Let $C_d = \boldsymbol{Z}/d\boldsymbol{Z}$ be the standard cyclic group of order d, and let the symmetric group $S_{\pi(d)}$ act on the $\pi(d)$-fold product $C_d^\pi(d)$ by permuting the co-ordinates in the obvious way. This gives a homomorphism $\psi\colon S_{\pi(d)} \to \mathrm{Aut}(C_d^{\pi(d)})$.

THEOREM 2. *The group $A_d(q^n)$ is naturally isomorphic to the semidirect product*

$$C_d^{\pi(d)} \mathop{\times}_{\psi} S_{\pi(d)}$$

where $S_{\pi(d)}$ acts on $C_d^{\pi(d)}$ via ψ.

Proof. Partition K_d into classes of conjugate elements over $\mathrm{GF}(q)$ and chose arbitrarily a set Γ of representative elements, one from each conjugacy class. Given $\alpha \in \Gamma$, let H_α denote the set of elements which are conjugates of α. Thus, $H_\alpha = \{\varphi^s(\alpha) |\ s = 0, 1, \ldots, d-1\}$. If $g \in A_d(q^n)$, then since $g\varphi = \varphi g$, g must map the elements of H_α onto another set of conjugate elements. Thus, g induces a permutation $\tau(g)$ on the set of conjugacy classes of elements of degree d over $\mathrm{GF}(q)$. Now there are $\pi(d)$ such conjugacy classes, and so we get a map $\tau\colon A_d(q^n) \to S_{\pi(d)}$ which is easily seen to be a group homomorphism.

Our choice of Γ enables us to construct a homomorphism $\sigma\colon S_{\pi(d)} \to A_d(q^n)$ such that $\tau\sigma = I$, where I is the identity map on $S_{\pi(d)}$. Among other things, the existence of such a "section" σ proves that τ is surjective. We proceed as follows: Given $t \in S_{\pi(d)}$, let $\sigma(t) = g$ where for all $\alpha \in \Gamma$, $g(\alpha)$ is that element of $t(H_\alpha)$ which belongs to Γ and

$$g(\varphi^s(\alpha)) = \varphi^s(g(\alpha)) \quad \text{for} \quad s = 1, 2, \ldots, d-1.$$

A little thought should convince the reader that g is indeed a permutation of K_d with $g\varphi = \varphi g$ and that $\tau\sigma = I$. We can now write the split exact sequence

$$(2) \qquad 1 \to \mathrm{Ker}(\tau) \to A_d(q^n) \underset{\tau}{\overset{\sigma}{\leftrightarrows}} S_{\pi(d)} \to 1.$$

Now, any $g \in \mathrm{Ker}(\tau)$ maps H_a into itself. Since $g\varphi = \varphi g$, the restriction of g to H_a is an element of the cyclic group C_d^a of order d generated by the restriction φ_a of φ itself to H_a. Therefore, the process of restriction to H_a induces a homomorphism res_a: $\mathrm{Ker}(\tau) \to C_d^a$ for every $a \in \Gamma$. Putting these homomorphisms together and arguing as in the proof of Theorem 1, we get an *isomorphism* res: $\mathrm{Ker}(\tau) \to \bigtimes_{a\in\Gamma} C_d^a$ onto the direct product of the C_d^a. In particular, $\mathrm{Ker}(\tau)$ is an *abelian group*. Returning to the exact sequence (2), we see that $A_d(q^n)$ is indeed the semidirect product of the $\pi(d)$-fold product of cyclic groups of order d with $S_{\pi(d)}$, and it remains only to investigate how $S_{\pi(d)}$ acts on $\mathrm{Ker}(\tau)$.

Identify each C_d^a with the standard cyclic group $C_d = \mathbf{Z}/d\mathbf{Z}$ by requiring that φ_a correspond to $1 \bmod d$. Then $g \in \mathrm{Ker}(\tau)$ is identified via res with the $\pi(d)$-tuple $(s_a)_{a\in\Gamma} \bmod d$, where each s_a is determined by $g(a) = \varphi_a^{s_a}(a)$. The action of $t \in S_{\pi(d)}$ on $\mathrm{Ker}(\tau)$ is given by the inner automorphism through $\sigma(\tau)$. This translates into an action on $\pi(d)$-tuples mod d as follows: Suppose g is identified with (s_a), and suppose $t \in S_{\pi(d)}$ is given. Then for all $a \in \Gamma$,

$$\big(\sigma(t)\, g\, \sigma(t)^{-1}\big)(a) = \sigma(t)\big(g(\beta)\big) = \sigma(t)\big(\varphi^{s_\beta}(\beta)\big) = \varphi^{s_\beta}\big(\sigma(t)(\beta)\big) = \varphi^{s_\beta}(a)$$

where $\beta \in \Gamma$ is determined by $t(H_\beta) = H_a$. Thus, t acts on the $\pi(d)$-tuple (s_a) by replacing each coordinate s_a by s_β where $t(\beta) = a$. But this is just the Ψ-action. The proof is complete.

COROLLARY. *The order of* $A(q^n)$ *is* $\prod_{d|n} (\pi(d))! \cdot d^{\pi(d)}$.

3. The group $B(q^n)$. Let M be the subgroup of $B(q^n)$ consisting of those permutations g such that $g(x) = x$ for $x \in \mathrm{GF}(q^n) \setminus \mathrm{GF}(q)$; and let N be the subgroup of $B(q^n)$ consisting of those permutations g such that $g(x) = x$ for $x \in \mathrm{GF}(q)$. Since each element of M commutes with every element of N, multiplication gives a group homomorphism μ: $M \times N \to B(q^n)$. The kernel of μ is clearly trivial, and so μ is injective.

LEMMA 3. *Suppose g is a permutation of* $\mathrm{GF}(q)$. *Then the permutation* g^e *of* $\mathrm{GF}(q^n)$ *defined by*

$$g^e(x) = \begin{cases} x & \text{for} \quad x \notin \mathrm{GF}(q), \\ g(x) & \text{for} \quad x \in \mathrm{GF}(q) \end{cases}$$

belongs to $B(q^n)$.

Proof. Write g as a product of transpositions (ab) on $\mathrm{GF}(q)$. Then, by definition, g^e is the product of the same transpositions viewed as transpositions on $\mathrm{GF}(q^n)$. Now (1) shows that each such transposition belongs to $B(q^n)$. Therefore, g^e belongs to $B(q^n)$, and the proof is complete.

COROLLARY. *The subgroup M is isomorphic to S_q, and $\mu: M \times N \to B(q^n)$ is an isomorphism.*

Proof. By the above lemma, $g \to g^e$ is an isomorphism from S_q to M. Obviously, every permutation f of $\mathrm{GF}(q^n)$ can be written in the form $f = g^e h$ where g is a permutation of $\mathrm{GF}(q)$ and $h(x) = x$ for $x \in \mathrm{GF}(q)$. If $f \in B(q^n)$, then so is h as $g^e \in B(q^n)$ by the lemma. Therefore, μ is surjective. Since μ is obviously injective, μ is an isomorphism, and the proof is complete.

Since $0 \notin \mathrm{GF}(q^n) \setminus \mathrm{GF}(q)$, the definition of $B(q^n)$ shows that every $h \in N$ can be written in the form $x \to (ax+b)/(cx+d)$ where $ad \neq bc$. Therefore, we have a homomorphism δ: $L_q \to N$, where L_q is the group of linear fractional transformations with coefficients in $\mathrm{GF}(q)$.

THEOREM 3. *If $n > 1$ and $q \neq 2$, the homomorphism δ is an isomorphism. Therefore, $B(q^n)$ is isomorphic to $S_q \times L_q$.*

Proof. Since δ is obviously surjective, we have to look at its kernel. Now $(ax+b)/(cx+d) = x$ implies $cx^2 + (d-a)x - b = 0$ for all $x \in \mathrm{GF}(q^n) \setminus \mathrm{GF}(q)$. Since $n > 1$ and $q \neq 2$ there are more than two such x and so we must have $c = 0$, $b = 0$ and $d = a$. In other words, $(ax+b)/(cx+d)$ is the identity element of L_q. Therefore, δ is injective and hence is an isomorphism. This completes the proof.

THEOREM 4. *If $n > 1$ and $q \neq 2$, then $B(q^n) \neq A(q^n)$.*

Proof. We show that in fact φ does not belong to $B(q^n)$. Assume otherwise. Then $\varphi \in N$, and therefore $x^q = (ax+b)/(cx+d)$ for all $x \in \mathrm{GF}(q^n) \setminus \mathrm{GF}(q)$. Multiplying both sides by $cx+d$, we see that the polynomial $cx^{q+1} + dx^q - ax - b$ has at least $q^n - q$ roots. Now $q^n - q > q+1$ if $n > 1$ and $q > 2$ as one easily checks. Therefore, $c = d = a = b = 0$, which is absurd. The proof is complete.

It is not difficult to verify that, for $q = 2$ and $n = 2$, $A(q^n)$ and $B(q^n)$ are actually equal.

Reference

[1] L. Carlitz, *Permutations in a finite field*, Proc. Amer. Math. Soc. 4 (1953), p. 538.

DUKE UNIVERSITY
THE UNIVERSITY OF MASSACHUSETTS

Received on 19. 4. 1971 (160)