Can. J. Math., Vol. XXV, No. 5, 1973, pp. 1060–1065

A THEOREM ON PERMUTATIONS OF A FINITE FIELD

A. BRUEN AND B. LEVINGER

1. The purpose of this note is to give a new proof of a theorem of L. Carlitz [**2**] and R. McConnel [**5**]. The theorem is as follows:

THEOREM 1. *Let* $F = GF(p^n)$ *be the finite field of order* $q = p^n$ *and let* $K = \{x \in F | x^d = 1\}$ *for some proper divisor* d *of* $q - 1$. *Then, a mapping* f *of* F *into itself satisfies*

$$(x - y)^{-1}(f(x) - f(y)) \in K \tag{1}$$

for $x \neq y$ *in* F, *if and only if* $f(x)$ *is given by*

$$f(x) = a + bx^{p^j} \tag{2}$$

where $a \in F$, $b \in K$, *and* $(q - 1)$ *divides* $d(p^j - 1)$.

The theorem above has been of considerable importance in the study of finite geometries (see [**3**, p. 247; **6**, p. 23]) and a simpler proof seems desirable. This we achieve by purely algebraic means. The key observation is this: *the functions* f *of Theorem* 1 *form a group*. Using this we first show that f must be of the form $f(x) = a + bx^t$. (This is also the first step in McConnel's paper [**5**] although the combinatorial method used there is quite different.) The difficulty then in [**5**] is to show that $t = p^j$. However, we can show this here in a few lines by again using the group property, and so in this fashion the work in [**5**] can be considerably shortened.

Actually, the first part of our proof has been motivated by Wielandt's proof of a theorem of Burnside [**7**, Theorem 7.3] which states that any simply transitive permutation group of prime degree is isomorphic to a subgroup of the affine group $H = \{\alpha | x^\alpha = a + bx\}$ of $GF(p)$. Theorem 1 is a direct consequence of this result when $q = p$ [**1**]. (We are indebted to the referee for pointing out that in this case Theorem 1 also follows from results in a recent book by L. Redei entitled *Lückenhafte Polynome über endlichen Körpern* (Birkhäuser Verlag, Basel and Stuttgart, 1970)). This observation prompted us to attempt to generalize Burnside's theorem to apply to the more general case. We have not been successful in this and it seems likely that there is no obvious generalization of Burnside's theorem which implies Theorem 1 for $n > 1$.

2. We start with some definitions. Let V be the vector space of functions from F to F. Since F is finite of order q, V is exactly the space of polynomials of

Received June 15, 1972 and in revised form, October 13, 1972.

degree $\leqq q - 1$. A convenient basis for V over F is given by the q functions

$$\pi_a(x) = 1 - (x - a)^{q-1}, \quad a \in F. \tag{3}$$

In terms of this basis, any function $f \in V$ has the representation

$$f(x) = \sum_{a \in F} f(a)\pi_a(x). \tag{4}$$

((4) is just the Lagrange interpolation formula.)

If G is a group of permutations of F, we can define an action of G on V by

$$f^g(x) = f(gx), \quad x \in F, \tag{5}$$

for $f \in V$, $g \in G$. (Here gx denotes the image of $x \in F$ under $g \in G$.) A subspace S of V is called a *G-module* if $f^g \in S$ for all $f \in S$, $g \in G$. A key idea is the following: suppose S is a non-trivial G-module ($S \neq F$, V) containing the identity function $\epsilon_1(x) = x$. Then $gx = \epsilon_1{}^g(x)$ is in S, so that the structure of S gives information about the action of G.

We let

$$G = \{ f \in V | (x - y)^{-1}(f(x) - f(y)) \in K \text{ if } x \neq y \} \tag{6}$$

and

$$H = \{ f \in V | f(x) = a + bx, a \in F, b \in K \}. \tag{7}$$

LEMMA 1. *G is a group of permutations of F and $H \subset G$. Further, both H and G are 3/2-transitive on F.*

Proof. It is clear that $H \subset G$, since $(x - y)^{-1}[(a + bx) - (a + by)] = b \in K$. If $g \in G$, then g is a permutation of F, since, for $x \neq y$,

$$(x - y)^{-1}[g(x) - g(y)] \in K$$

so that $g(x) - g(y) \neq 0$. Further, if f, $g \in G$, the quantity

$$(x - y)^{-1}[fg(x) - fg(y)] = (x - y)^{-1}[g(x) - g(y)][g(x) - g(y)]^{-1}[f(g(x)) - f(g(y))]$$

is a product of two elements in K and thus is itself in K. Consequently, $fg \in G$ and G is a group.

Let G_0, H_0 be the stabilizers of 0 in G, H, respectively. If $f \in G_0$, it follows from (6) that $f(x) - f(0) = f(x) = kx \in Kx$. Hence $G_0x \subset Kx$ for any $x \in F$. However, $Kx = \{bx | b \in K\} = \{ f(x) | f \in H_0 \} \subset \{ f(x) | f \in G_0 \} = G_0x$. Thus $G_0x = H_0x = Kx$ and the non-trivial orbits of G_0 and H_0 are the cosets of K in $F\backslash\{0\}$, all of which have the same length.

Remark. A special case of Theorem 1 follows from Lemma 1. For, every 3/2-transitive permutation group is either primitive or a Frobenius group [**8**, Theorem 10.4, p. 25]. If K is contained in a proper subfield F_1 of F, then F_1 is a block of G and G is not primitive. In this case, since $H \subset G$, we have $H = G$.

LEMMA 2 *Let* $\mathrm{Hom}_G(V, V)$ *be the vector space of G-homomorphisms of V into V*

(that is, $\phi \in \mathrm{Hom}_G(V, V)$ if $\phi(f^g) = \phi(f)^g$ for all $f \in V$, $g \in G$). Define the monomials ϕ_k by

$$\phi_k(x) = x^{kd}, \quad k = 0, 1, \ldots, e. \tag{8}$$

Then, if ϕ is in $\mathrm{Hom}_G(V, V)$, $\phi(\pi_0)$ must be a linear combination (over F) of the $e + 1$ monomials in (8). Conversely, given any such linear combination $\sum_{k=0}^{e}\lambda_{kd}x^{kd}$ there then exists a unique element ϕ of $\mathrm{Hom}_G(V, V)$ such that $\phi(\pi_0) = \sum\lambda_{kd}x^{kd}$.

Proof. The idea is to use a kind of counting argument which involves the dimension of $\mathrm{Hom}_G(V, V)$. We know that $\mathrm{Hom}_G(V, V)$ is a vector space over F whose dimension is equal to the number of G_0-orbits in F [7, Lemma 7.1]. As in Lemma 1 this dimension is $e + 1$. Therefore the number of elements in the vector space $\mathrm{Hom}_G(V, V)$ is exactly q^{e+1}, that is, $|\mathrm{Hom}_G(V, V)| = q^{e+1}$ where $|F| = q = p^n$. Now for $a \in F$ define the translation $T_a \in H$ by

$$T_a(x) = x - a. \tag{9}$$

Then $\pi_0{}^{T_a}(x) = \pi_0(x - a) = 1 - (x - a)^{q-1} = \pi_a(x)$. Now from (4) it follows that any $f \in V$ has the form $f = \sum_{a\in F} f(a)\pi_0{}^{T_a}$. Thus for any ϕ in $\mathrm{Hom}_G(V, V)$,

$$\phi(f) = \sum_{a\in F} f(a)\phi(\pi_0{}^{T_a}) = \sum_{a\in F} f(a)\phi(\pi_0)^{T_a},$$

and ϕ *is uniquely determined* by the image of π_0. In particular, the number of elements ϕ in $\mathrm{Hom}_G(V, V)$ is also exactly the number of distinct functions of the form $\phi(\pi_0)$. Therefore if we can show that for $\phi \in \mathrm{Hom}_G(V, V)$, $\phi(\pi_0)$ is some linear combination of the $e + 1$ monomials x^{kd} $(k = 0, 1, \ldots, e)$ we will have proved the first part of the lemma and the second part as well since we showed in the above that $|\mathrm{Hom}_G(V, V)| = q^{e+1}$.

For this purpose, suppose that

$$\phi(\pi_0)(x) = \sum_{i=0}^{q-1} \lambda_i x^i. \tag{10}$$

Let $f \in H_0$ so that $f(x) = bx$. Then $\pi_0{}^f(x) = \pi_0(bx) = \pi_0(x)$, and

$$\phi(\pi_0)(x) = \phi(\pi_0{}^f)(x) = \phi(\pi_0)^f(x) = \sum_{i=0}^{q-1} \lambda_i(bx)^i.$$

Thus $\sum_{i=0}^{q-1}\lambda_i(1 - b^i)x^i = 0$. This means that all q distinct elements of F satisfy a polynomial of degree less than q. Consequently each of the coefficients $\lambda_i(1 - b^i) = 0$ for $i = 0, 1, \ldots, q - 1$. Since b was arbitrary in K this implies $\lambda_i = 0$ unless d divides i. Thus

$$\phi(\pi_0)(x) = \sum_{k=0}^{q-1} \lambda_{kd}x^{kd},$$

and we are done.

COROLLARY. *For each* $k = 0, 1, \ldots, e$, *the subspace of* V *spanned by the polynomials* $(x - a)^{kd}$, $a \in F$, *is a* G*-module.*

Proof. If ϕ is in $\mathrm{Hom}_G(V, V)$ then $\phi(V)$ is a G-module. By the previous lemma, for fixed k, there exists a ϕ in $\mathrm{Hom}_G(V, V)$ with $\phi(\pi_0) = x^{kd}$. Further $\phi(\pi_a)(x) = \phi(\pi_0{}^{T_a})(x) = (\phi(\pi_0))^{T_a}(x) = (x - a)^{kd}$.

LEMMA 3. *Let* $\lambda = \sum_{i=0}^{n-1} \alpha_i p^i$ *where* $0 \leqq \alpha_i < p$, *and*

$$M_\lambda = \{r = \sum_{i=0}^{n-1} \beta_i p^i | 0 \leqq \beta_i \leqq \alpha_i\}. \tag{11}$$

If S_λ *is the subspace of* V *spanned by the polynomials* $(x - a)^\lambda$, $a \in F$, *then* S_λ *has a basis*

$$\{\epsilon_r(x) = x^r | r \in M_\lambda\}. \tag{12}$$

Proof. Since $(x - a)^\lambda = \sum_{r=0}^{\lambda} \binom{\lambda}{r} x^r (-a)^{\lambda - r}$, S_λ is contained in the subspace of V generated by the ϵ_r with $\binom{\lambda}{r} \not\equiv 0$ (in F). This is just the set (12), since $\binom{\lambda}{r}$ is relatively prime to p exactly when $r \in M_\lambda$.

For the converse, we observe that

$$\begin{aligned} \sum_{a \in F} a^{q-1+r-\lambda}(x - a)^\lambda &= \sum_{a \in F} \sum_{k=0}^{\lambda} \binom{\lambda}{k} x^k (-1)^{\lambda - k} a^{q-1+r-k} \\ &= \sum_{k=0}^{\lambda} \binom{\lambda}{k} x^k (-1)^{\lambda - k} \sum_{a \in F} a^{q-1+r-k} \\ &= (-1)^{\lambda - r - 1} \binom{\lambda}{r} x^r \end{aligned}$$

unless $\lambda = q - 1$ and $r = 0$ or $q - 1$. This follows from the well-known fact that $\sum_{a \in F} a^s = -1$, if $s \equiv 0 \bmod (q - 1)$, and $\sum_{a \in F} a^s = 0$, otherwise. Thus $\epsilon_r \in S_\lambda$ whenever $r \in M$ except possibly in the exceptional case where $\lambda = q - 1$. But $\epsilon_{q-1} \in S_{q-1}$, by definition, and

$$\epsilon_0(x) = 1 = \sum_{a \in F} \pi_a(x) = \sum_{a \in F} -(x - a)^{q-1} \in S_{q-1}$$

from (3). This completes the proof.

Since d divides $p^n - 1$, $(d, p) = 1$. Hence, $1, (d - 1) \in M_d$. We have shown that $\phi_1(V) = S_d$ is a G-module. Thus, for any $g \in G$ and $r \in M_d$, $\epsilon_r^g(x) = \epsilon_r(gx) = (gx)^r$ is a polynomial in S_d. We now use this.

LEMMA 4. *Let* $f \in G$. *Then*

$$f(x) = u + vx^t \tag{13}$$

where $u = f(0)$, $v = f(1) - f(0)$, *and* $td \equiv d \bmod (q - 1)$.

https://doi.org/10.4153/CJM-1973-113-4 Published online by Cambridge University Press

Proof. Let $u = f(0)$. Since the translation Tu, (9), is in G, $\psi(x) = Tu(f(x)) = f(x) - u$ is also in G and $\psi(0) = 0$. Since $1, d - 1 \in M_d$, the functions $\epsilon_1{}^{\psi} = \psi$ and $\epsilon_{d-1}{}^{\psi} = \psi^{d-1}$ are in S_d. Now, $\psi \in G_0$ implies $x^{-1}\psi(x) = x^{-1}[\psi(x) - \psi(0)] \in K$ for $x \neq 0$. From the definition of K, it follows that $x^d = \psi(x)^d = \psi(x)\psi(x)^{(d-1)}]$. But x^d can be a product of two polynomials of degree $\leqq d$ only if $\psi(x) = vx^t$ and $\psi(x)^{d-1} = v'x^{d-t}$ where $vv' = 1$ and $0 < t < d$. Then $\psi^d(x) = v^d x^{td} = x^d$, if and only if $td \equiv d \mod (q - 1)$ and $v^d = 1$. Further $v = \psi(1) = f(1) - u = f(1) - f(0)$.

Proof of Theorem 1. We now show that the only possible choices for t in Lemma 4 are $t = p^j$. This will complete the proof of Theorem 1.

Without loss of generality, we may assume that $f \in G$ has the form $f(x) = x^t$. G is a group containing the translations Ta. Thus for any fixed $\alpha \neq 0$, $h(x) = f(T\alpha(x)) = (x - \alpha)^t$ is a function in G. But by Lemma 4, $h(x) = u + vx^{t'} = (x - \alpha)^t$ (where $u = h(0) = (-\alpha)^t$ and $v = h(1) - h(0)$). The equation $(x - \alpha)^t - (u + vx^{t'}) = 0$ of degree $\max(t, t') < q - 1$ is satisfied for each $x \in F$. Thus all coefficients in $(x - \alpha)^t - (u + vx^{t'})$ are 0. This is only possible if $t' = t$, $v = 1$, and $(x - \alpha)^t = x^t + (-\alpha)^t$. Since α was arbitrary, this shows that $f(x + \alpha) = (x + \alpha)^t = x^t + \alpha^t$ for all $\alpha \in F$ which implies that f is an automorphism of F and that $t = p^j$. By Lemma 4, $d(p^j - 1) \equiv 0 \mod (q - 1)$.

3. We have thought about possible generalization of Burnside's theorem which would imply Theorem 1. We were led to conjecture that a 3/2-transitive but not doubly transitive permutation group of degree p^n which contains a regular elementary abelian subgroup T of order p^n is isomorphic to a subgroup of the group $\bar{H} = \{\alpha | x^\alpha = a + bx^{p^j}\}$ of collineations of $GF(p^n)$. However, it is possible to find affine groups which are counterexamples to this conjecture. Our simplest example is a Frobenius group of order $8 \cdot 81$ with Frobenius complement isomorphic to the quaternion group ($q = 3^4$). There exist other examples of Frobenius groups of order $24 \cdot 121$ and $48 \cdot 529$ related to certain near-fields [**4**, p. 391] where the permutation groups are even primitive.

After this work had been completed the writers became aware of a recent publication of H. Wielandt [**9**] in which some of the results in this paper are shown. For example, using the notation there, our Lemma 2 will follow from $H \approx_2 G$ and Theorem 13.3 in Wielandt. However in order to keep the discussion self-contained we have not made use of such results. Also, we do not use Wielandt's classification of groups of degree p^2 (see [**9**, Chapter 4]) from which Theorem 1 can be deduced in the special case when $q = p^2$.

Addendum. A result which is slightly more general than Theorem 1 has also been shown by McConnel in [**5**] (see Theorem 2). Some extensions had been discussed also in another paper by L. Carlitz entitled *Ordered polynomials in a finite field*, Acta. Arith. 7 (1962), 167–172. Extensions of McConnel's results

to more than one variable appear in two further papers by him, namely *Functions over finite fields preserving* mth *powers*, Duke Math. J. *36* (1969), 465–472 and *Functions over finite fields satisfying coordinate* ψ *conditions*, Duke Math. J. *39* (1972), 297–312.

References

1. A. Bruen, *Permutation functions on a finite field*, Can. Math. Bull. *15* (1972), 595–597.
2. L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc. *11* (1960), 456–59.
3. D. A. Foulser, *Replaceable translation nets*, Proc. London Math. Soc. *22* (1971), 235–264.
4. M. Hall, Jr., *The theory of groups* (Macmillan, New York, 1959).
5. R. McConnel, *Pseudo-ordered polynomials over a finite field*, Acta Arith. *8* (1963), 127–151.
6. T. G. Ostrom, *Vector spaces and construction of finite projective planes*, Arch. Math. (Basel) *19* (1968), 1–25.
7. D. S. Passman, *Permutation groups* (Benjamin, New York, 1968).
8. H. W. Wielandt, *Finite permutation groups* (Academic Press, New York, 1964).
9. ——— *Permutation groups through invariant relations and invariant functions*, Lecture notes, Columbus, Ohio State University, 1969.

University of Western Ontario,
London, Ontario;
Colorado State University,
Fort Collins, Colorado