Canad. Math. Bull. Vol. **15** (4), 1972

MATHEMATICAL NOTES

Manuscripts for this Department should be sent to R. D. Bercov and A. Meir, Editors-in-Chief, Canadian Mathematical Bulletin, Department of Mathematics, University of Alberta, Edmonton 7, Alberta.

PERMUTATION FUNCTIONS ON A FINITE FIELD

BY
AIDEN BRUEN

1. **Summary.** Using a well-known theorem of Burnside on permutation groups of prime degree we offer new and simplified proofs of Theorems A, B, B′ below for the case $q=p$ a prime.

2. **Background.** In [1] Carlitz proved the following interesting result, which has been of considerable importance in the theory of finite planes (see [3, p. 23]).

THEOREM A (Carlitz). *Let F_q denote the finite field of order q, where $q=p^n$ is odd. Let f be a function from F_q to F_q satisfying the following conditions.*

(i) $f(0)=0, f(1)=1$

(ii) $a\neq b \Rightarrow (f(b)-f(a))(b-a)^{-1}=s$, *where s is some nonzero square in F_q and a, b are in F_q.*

Then it follows that $f(x)=x^{p^j}$ for some j in the range $0\leq j<n$.

This result has been generalized in [2] as follows.

THEOREM B (McConnel). *Let F_q be the finite field of order $q=p^n$. Let $d\neq 1$ be any proper divisor of $q-1$ and set $q-1=md$. For x in F_q put $\psi_d(x)=x^m$. Suppose f is any function from F_q to F_q satisfying the following conditions.*

(i) $f(0)=0, f(1)=1$

(ii) $\psi_d(f(b)-f(a))=\psi_d(b-a)$ *for all a, b in F_q.*

Then it follows that $f(x)=x^{p^j}$ for some j in the range $0\leq j<n$.

We note that by putting $d=2$ Theorem A follows from Theorem B. Also, condition (ii) implies that f is actually a *permutation function* on F_q.

Using the notation there, one can show that Theorem B is equivalent to the more pleasant-sounding.

THEOREM B′. *Let f be a function from F_q to F_q such that $f(0)=0, f(1)=1$. Assume also that $a\neq b\Rightarrow (f(b)-f(a))(b-a)^{-1}\in G$ where G is some given proper subgroup of the multiplicative group F_q^* of F_q. Then $f(x)=x^{p^j}$ with $0\leq j<n$.*

9—(12 pp.)

Proof. The multiplicative group F_q^* of F_q is cyclic, with generator w say. Let f satisfy the hypotheses of Theorem B. Now let $G=\{x \in F_q^* \mid x^m=1\}$. Then G is a proper (cyclic) subgroup of F_q^* of order m, with generator w^d, where $q-1=md$. Thus the hypotheses in B' are satisfied. The converse follows from the fact that if G is a finite group of order m, then x in G implies $x^m=1$.

We proceed to show Theorem B′ for the case $q=p$ a prime. The heart of the matter lies in the following simple observation.

THEOREM 1. *Let S denote the class of all functions f from F_q to F_q satisfying the following condition. $a\neq b \Rightarrow (f(b)-f(a))(b-a)^{-1} \in X$ for all $a\neq b$ in F_q, with X being some given proper subgroup of $F_q^*=F_q-\{0\}$. Then, under composition of functions, the set S forms a group.*

Proof. S is finite. Thus it suffices to show that f, g in S implies fg is in S, where fg denotes the composition of f, g. Let a, b be in F_q with $a\neq b$. Then it follows that $g(b)\neq g(a)$. Put $u=g(b)$, $v=g(a)$. Now

$$\begin{aligned}\frac{fg(b)-fg(a)}{b-a} &= \frac{f(g(b))-f(g(a))}{g(b)-g(a)}\cdot\frac{g(b)-g(a)}{b-a}\\ &= \frac{f(u)-f(v)}{u-v}\cdot\frac{g(b)-g(a)}{b-a}\end{aligned}$$

The product of 2 elements of X is in X and the result is immediate.

We can now regard S as a permutation group on F_q. With the notation of theorem 1 we obtain

LEMMA 2. *S is transitive, but not doubly transitive, on the elements of F_q.*

Proof. S contains the translations $x\to x+d$ with d in F_q, since $1 \in X$. Thus S is transitive on F_q. Let $t\neq 0$ be any element of F_q not in the proper subgroup X. Then there is no function f in S such that $f(0)=0$ and $f(1)=t$ say. Thus S is not doubly transitive on F_q.

Let us now specialize to the case $q=p$ a prime. In [4, p. 53] the author discusses the proof of a result of Burnside [4, Theorem 7.3] concerning finite permutation groups of prime degree. An examination of the proof of that result will easily reveal.

THEOREM 3. *Let S be a transitive group of permutation functions on F_p, the field of order p, with p a prime. Assume that S contains the mapping $x\to x-1$ and assume also that S is not doubly transitive on the elements of F_p. Then every function f in S is given by $f(x)=cx+d$, for suitable c, d in F_p.*

https://doi.org/10.4153/CMB-1972-103-3 Published online by Cambridge University Press

Now we can easily prove Theorem B, that is, Theorem B′, for the case $q=p$. We use the notation of Theorem B′. Suppose f is a function on F_q to F_q such that $a\neq b\Rightarrow(f(b)-f(a))(b-a)^{-1}\in G$. Then f must be contained in the group S of Theorem 1. Now S contains all translations $x\to x+d$. Using Lemma 2 and Theorem 3 we get then that $f(x)=cx+d$. Since also $f(0)=0, f(1)=1$ the result follows.

It is not inconceivable that Theorem B′ in full can be proved by using information on permutation groups of degree p^n. The author is investigating this possibility.

References

1. L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc. **11** (1960), 456–459.

2. R. McConnel, *Pseudo ordered polynomials over a finite field*, Acta Arith. **8** (1963), 127–151.

3. T. G. Ostrom, *Vector spaces and construction of finite projective planes*, Arch. Math. **19** (1968), 1–25.

4. D. S. Passman, *Permutation groups*. Benjamin, New York, 1968.

Colorado State University,
Fort Collins, Colorado

University of Western Ontario,
London, Ontario

https://doi.org/10.4153/CMB-1972-103-3 Published online by Cambridge University Press