PERMUTATIONS IN A FINITE FIELD

L. CARLITZ

A polynomial $f(x)$ with coefficients $\in GF(q)$ is called a permutation polynomial if the numbers $f(\alpha)$, where $\alpha \in GF(q)$, are a permutation of the α's. (For references see [2, Chap. 18].) In a letter to the writer, E. G. Straus has inquired whether all permutation polynomials can be generated by means of the special types

$$\alpha x + \beta, \quad x^{q-2} \qquad (\alpha, \beta \in GF(q), \alpha \neq 0). \tag{1}$$

For $q=5$, this was proved to be true by Betti; for $q=7$ the corresponding result was verified by Dickson [1, p. 119].

In this note we show very simply that this result holds for all q. Since the totality of permutation polynomials evidently furnishes a representation of the symmetric group on q letters, it will suffice to show that every transposition (0α) can be generated by means of the special polynomials (1); here α denotes a fixed nonzero number $\in GF(q)$. We consider the following polynomial

$$g(x) = -\alpha^2\left(\left((x-\alpha)^{q-2} + \frac{1}{\alpha}\right)^{q-2} - \alpha\right)^{q-2}. \tag{2}$$

Then in the first place we easily verify that $g(0)=\alpha$ and $g(\alpha)=0$. Secondly if $\beta \neq 0$, $\beta \neq \alpha$, then

$$\begin{aligned} g(\beta) &= -\alpha^2\left(\left(\frac{1}{\beta-\alpha} + \frac{1}{\alpha}\right)^{q-2} - \alpha\right)^{q-2} \\ &= -\alpha^2\left(-\frac{\alpha^2}{\beta}\right)^{q-2} = \beta, \end{aligned}$$

so that β is carried into itself. This shows that the polynomial (2) does indeed effect the transposition (0α), and therefore our result follows.

We may state the following

THEOREM. *Every permutation on the numbers of $GF(q)$ can be derived from* (1).

REFERENCES

1. L. E. Dickson, ***The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group***, Ann. of Math. vol. 11 (1896–97) pp. 65–120.

2. ———, *History of the theory of numbers*, vol. 3, Washington, 1923.

DUKE UNIVERSITY

Received by the editors December 6, 1952.