REFERENCES

1. H. Bachmann, *Transfinite Zahlen*, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.), vol. 1, Springer-Verlag, Berlin, 1955. vii+204 pp.

2. G. Birkhoff, *Lattice theory*, revised edition xiii+283 pp., Amer. Math. Soc., Providence, R. I., 1948.

3. G. Grätzer and E. T. Schmidt, *Two notes on lattice congruences*, Ann. Univ. Sci. Budapest. Eötvös. Sect. Math. 1 (1958), 83–87.

UNIVERSITY OF CALIFORNIA, BERKELEY

A NOTE ON FINITE FIELDS[1]

L. CARLITZ

1. Let q be a power of an odd prime and let $F=GF(q^n)$ denote the finite field of order q^n. Let F^* denote the multiplicative group of the nonzero elements of F and let Z be the subgroup of F^* of order $(q^n-1)/(q-1)$. It will be assumed that

$$\left(q-1, \frac{q^n-1}{q-1}\right) = 1. \tag{1}$$

Then every nonzero element ξ of F has a representation

$$\xi = \alpha\zeta \qquad (\alpha \in GF(q),\ \zeta \in Z), \tag{2}$$

and the representation is unique. For $\zeta \in Z$, $\zeta \neq 1$, put

$$1 - \zeta = \tau(\zeta)\sigma(\zeta), \tag{3}$$

where $\tau(\zeta) \in GF(q)$, $\sigma(\zeta) \in Z$.

Put $Z_1 = Z - \{1\}$. In a letter to the writer, J. G. Thompson has raised the question whether the mapping $\zeta \to \sigma(\zeta)$ defined by (3) can be a permutation of Z_1. We shall show that the answer is negative.

Indeed let us assume that the mapping $\zeta \to \sigma(\zeta)$, is a permutation of Z_1. In view of (1) the mapping $\zeta \to \zeta^{q-1}$ is a permutation of Z_1 and consequently if we put

$$\zeta_1 = (1-\zeta)^{q-1} = (\sigma(\zeta))^{q-1},$$

then $\zeta \to \zeta_1$ is a permutation of Z_1. We recall that

Received by the editors June 29, 1961.

[1] Supported in part by National Science Foundation grant G 16485.

$$\sum_{\zeta \in Z} \zeta^r = 0 \qquad \left(1 \leqq r < \frac{q^n - 1}{q - 1}\right),$$

so that

(4) $$\sum_{\zeta \in Z_1} \zeta^r = -1 \qquad (1 \leqq r \leqq q - 1).$$

Since

$$\zeta_1 = (1 - \zeta)^{q-1} = 1 + \zeta + \cdots + \zeta^{q-1}$$

it follows that

(5) $$\sum_{\zeta_1 \in Z_1} \zeta_1 = \sum_{\zeta \in Z_1} 1 + \sum_{\zeta \in Z_1} \zeta + \cdots + \sum_{\zeta \in Z_1} \zeta^{q-1}.$$

But

$$\sum_{\zeta \in Z_1} 1 = \frac{q^n - 1}{q - 1} - 1 = 0 \qquad (\text{in } F),$$

so that (5) becomes

$$-1 = -(q - 1) = 1,$$

a contradiction since q is odd.

We may accordingly state

THEOREM 1. *The mapping $\zeta \to \sigma(\zeta)$ defined by* (3) *is not a permutation of Z_1.*

In view of Theorem 1, there exist two distinct elements ξ, η in Z_1 such that

(6) $$1 - \xi = \alpha\zeta, \qquad 1 - \eta = \beta\zeta,$$

where $\alpha, \beta \in GF(q)$, $\zeta \in Z_1$; clearly $\alpha \neq \beta$. Thus (6) implies

(7) $$1 - \eta = \lambda(1 - \xi),$$

where $\lambda = \beta/\alpha$ is a number of $GF(q)$ distinct from 1. Conversely if (7) holds and we put $1 - \xi = \alpha\zeta$, where $\alpha \in GF(q)$, $\zeta \in Z_1$ then it follows that

$$1 - \eta = \lambda\alpha\zeta = \beta\zeta.$$

Thus (6) and (7) are equivalent. We remark also that if the pair (ξ, η) satisfy (7), then the same is true of $(\xi^q, \eta^q), \cdots, (\xi^{q^{n-1}}, {}^q\eta^{n-1})$, so that solutions of (7) with λ fixed occur in sets of d, where d is some divisor of n.

2. To generalize Theorem 1, we may consider the finite field

$GF(p^n)$ where p is a prime, $p^n-1=rs$, $(r, s)=1$, $r<s$ and $r\not\equiv 1 \pmod p$. Let F^* denote the the multiplicative group of the nonzero elements of $GF(p^n)$ and let Y, Z denote the subgroups of F^* of order r and s respectively. Since $(r, s)=1$, the intersection of Y and Z consists of the identity element only. Thus every element ξ of F^* has a unique representation

$$\xi = \eta\zeta \qquad (\eta \in Y, \zeta \in Z). \tag{8}$$

For $\zeta\in Z$, $\zeta\neq 1$, put

$$1 - \zeta = \tau(\zeta)\sigma(\zeta), \tag{9}$$

where $\tau(\zeta)\in Y$, $\sigma(\zeta)\in Z$.

Put $Z_1=Z-\{1\}$. We shall show that the mapping $\zeta\to\sigma(\zeta)$ is not a permutation of Z_1. For if we assume that $\zeta\to\sigma(\zeta)$ is a permutation of Z_1, then since $(r, s)=1$ it follows that

$$\zeta \to \zeta_1 = (1 - \zeta)^r \tag{10}$$

is also a permutation of Z_1. Now

$$S_t = \sum_{\zeta\in Z} \zeta^t = 0 \qquad (1 \leqq t \leqq s - 1). \tag{11}$$

Indeed if ζ_1 denotes a generator of Z, then

$$\zeta_1^t S_t = \sum_{\zeta\in Z} (\zeta_1\zeta)^t = \sum_{\zeta\in Z} \zeta^t = S_t.$$

Since $\zeta_1^t\neq 1$, (11) follows at once.

Next expanding $(1-\zeta)^r$ we get

$$\zeta_1 = \sum_{t=0}^{r} (-1)^t \binom{r}{t} \zeta^t.$$

Summing over all $\zeta\in Z_1$ we get

$$\sum_{\zeta_1\in Z_1} \zeta_1 = \sum_{t=0}^{r} (-1)^t \binom{r}{t} \sum_{\zeta\in Z_1} \zeta^t. \tag{12}$$

We now make use of (11) and in addition recall that $r<s$. Then (12) reduces to

$$-1 = (s-1) - \sum_{t=1}^{r} (-1)^t \binom{r}{t} = s - (1-1)^r.$$

Since $r\not\equiv 1 \pmod p$, we have a contradiction. This proves

THEOREM 2. *Let* $p^n-1=rs$, *where* $(r, s)=1$, $r<s$, $r\not\equiv 1 \pmod p$.

Then the mapping $\zeta \to \sigma(\zeta)$ *defined by* (9) *is not a permutation of* Z_1.

As a consequence of Theorem 2 there exist two distinct elements ζ_1, ζ_2 in Z_1 such that

$$(13) \qquad 1 - \zeta_1 = \eta_1\zeta, \qquad 1 - \zeta_2 = \eta_2\zeta,$$

where $\eta_1, \eta_2 \in Y$, $\zeta \in Z_1$; clearly $\eta_1 \neq \eta_2$. Clearly (13) implies

$$(14) \qquad 1 - \zeta_2 = \eta(1 - \zeta_1),$$

where η is a number of Y distinct from 1. Conversely if (14) holds and we put $1-\xi_1=\eta_1\zeta$, where $\eta_1 \in Y$, $\zeta \in Z_1$, then $1-\xi_2=\eta\eta_1\zeta=\eta_2\zeta$ with $\eta_2 \in Y$. Thus (13) and (14) are equivalent.

In the next place if ζ is any element of Z then $\zeta = \alpha^r$ for some α in F^*. Thus (14) becomes

$$(15) \qquad 1 - \alpha_2^r = \eta(1 - \alpha_1^r).$$

In this equation we think of η as fixed and α_1, α_2 as the unknowns.

Davenport and Hasse [1, p. 173] have discussed equations of the form (15). If N is the total number of solutions of (15) then, specializing their result, we have $(q = p^n)$

$$|N - q| \leqq r(r - 1)q^{1/2}.$$

In particular if $r = o(q^{1/4})$ then N is of order $q^{1/2}$.

Reference

1. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1935), 151–182.

Duke University