TRANSLATES OF SUBGROUPS OF THE MULTIPLICATIVE GROUP OF A FINITE FIELD

BY

P. J. CAMERON, J. I. HALL, J. H. VAN LINT, T. A. SPRINGER AND H. C. A. VAN TILBORG

To H. Freudenthal on the occasion of his seventieth birthday

(Communicated at the meeting of February 22, 1975)

ABSTRACT

Let k be a finite field, $\xi \in k$, G a subgroup of $k^\times$. We classify the triples (k, ξ, G) for which the set $\xi + G$ intersects less than 3 cosets of G in $k^\times$.

1. INTRODUCTION

The following problem is a generalization of a special case, which arose in connection with the construction of certain combinatorial configurations in statistical analysis. The special case was proposed as a problem to one of the authors by E. Seiden. Let p be a prime, $q = p^\alpha$, and denote by k the finite field $GF(q)$. Let $q-1 = dr$ and let G be the subgroup of order r of the multiplicative group $k^\times$. We denote by t a generator of G. If ξ is an element of k we consider

$$\xi + G := \{\xi + g \mid g \in G\}.$$

The set $\xi + G$ may contain 0. In the present situation this does not interest us. We are interested in finding out whether $\xi + G$ has a nonempty intersection with more than 2 distinct cosets of G (including G itself) in $k^\times$. Obviously, this can only be the case if $r > 2$ and $d > 2$. Also, it is clearly necessary that $\xi \neq 0$. From now on we assume that $\xi \neq 0, r > 2, d > 2$. We remark that the number of cosets of G which have a nonempty intersection with $\xi + G$ depends only on the coset to which ξ belongs. We shall study the cases $r = 3$ and $r = 4$ in the next two sections. There, the obvious exceptions to our requirement appear in a natural way. In section 4 we shall show that besides these obvious exceptions there is only one other one.

2. *The case $r = 3$.* If $r = 3$ and $-\xi \in G$, then the set $\xi + G$ contains 0 and two other elements. Therefore it cannot have a nonempty intersection with 3 distinct cosets of G. Suppose $-\xi \notin G$ and assume that $\xi + 1$, $\xi + t$, and $\xi + t^2$ are not in different cosets of G. This implies that $(\xi + 1)^3$, $(\xi + t)^3$, and $(\xi + t^2)^3$ are not all different. Since $t^3 = 1$ and $r = 3$ imply $p \neq 3$, one

immediately finds that $\xi \in G$. Indeed, if $\xi \in G$, then $\xi + G$ intersects the two cosets $2G$ and $-G$.

3. *The case $r=4$.* It is not difficult to include the case $r=4$ in the treatment of the general case in the next section. Since a separate treatment gives the reader a little more insight in the problem, we discuss the case $r=4$ in the same way as we did $r=3$. We now have $p \neq 2$, $G=\{1, t, -1, -t\}$. If $\xi+G$ intersects at most two cosets of G, we must have one of the cases

a) $(\xi+1)^4=(\xi-1)^4$,

b) $(\xi+t)^4=(\xi-t)^4$,

c) $(\xi+1)^4=(\xi+t)^4$, $(\xi-1)^4=(\xi-t)^4$

(for a suitable choice of the generator t). In case a) we find $\xi^2=-1$, while in case b) we find $\xi^2=1$, so $\xi \in G$ in either case. If $\xi \in G$, then $\{(\xi+g)^4 | g \in G\}=\{0, 16, -4\}$. Hence $\xi+G$ intersects two cosets of G, unless $p=5$, in which case $\xi+G$ intersects only one coset of G. Indeed, if $p=5$, then G is the multiplicative subgroup of the prime field of k. In fact, we see that for any r, if G is the multiplicative subgroup of a subfield of k and if $\xi \in G$, then $\xi+G$ is the set $\{0\} \cup G \backslash \{\xi\}$.

If we are in case c) we find that

$$2\xi^2+3(t+1)\xi+2t=2\xi^2-3(t+1)\xi+2t=0.$$

This leads to a contradiction, unless $p=3$. Indeed, if $p=3$, then G is the subgroup of index 2 in the multiplicative group of $GF(3^2)$. In this case $k=GF(3^{2\beta})$. For any $\xi \in GF(3^2)$, the set $\xi+G$ intersects at most 2 cosets of G in $k^\times$.

Again, we learn from this example to expect an exception in the general case. If G is the subgroup of index 2 in the multiplicative group of a subfield k_1 of k and $\xi \in k_1$, then $\xi+G$ cannot have a nonempty intersection with more than 2 cosets of G.

4. *The case $r \geqslant 5$.* Let $r \geqslant 5$, $\xi \neq 0$, and assume that $\xi+G$ has a nonempty intersection with at most 2 cosets of G. Then there are 2 elements ϱ and σ in k such that for every $g \in G$ either $\xi+g=0$ or $(\xi+g)^r=\varrho$ or $(\xi+g)^r=\sigma$. This implies that there exists a polynomial

$$f(x)=\sum_{i=0}^{r+1} a_i x^i$$

with coefficients in k, such that

$$\{(\xi+x)^r-\varrho\}\{(\xi+x)^r-\sigma\}(\xi+x)=(x^r-1)f(x). \tag{4.1}$$

On the right hand side of (4.1) the coefficients of x^{r-i} and x^{2r-i} have sum 0 (for $1 \leqslant i \leqslant r-2$). Writing the left hand side as

$$(\xi+x)^{2r+1}-(\varrho+\sigma)(\xi+x)^{r+1}+\varrho\sigma(\xi+x)$$

and computing the same sum we find

$$(4.2)\qquad \binom{2r+1}{i+1}+\xi^r\binom{2r+1}{r-i}-(\varrho+\sigma)\binom{r+1}{i+1}=0,\quad (1\leqslant i\leqslant r-2).$$

We take a linear combination of equation (4.2) with successive values of i in such a way that the term with ϱ and σ is eliminated. Using the fact that $r\not\equiv 0 \pmod p$ this yields

$$(4.3)\qquad \binom{2r+1}{i+1}-\xi^r\binom{2r+1}{r-i-1}=0,\quad (1\leqslant i\leqslant r-3).$$

Again, we take a linear combination for 2 successive values of i in (4.3) and eliminate the term involving ξ^r. The result is

$$(4.4)\qquad 2(r+1)^2\binom{2r+1}{i+1}=0,\quad (1\leqslant i\leqslant r-4).$$

(i) $p=2$.

Since (4.4) is of no use to us if $p=2$ we consider $p=2$ separately. Assume $p=2$. Let $r+1=2^a m$, m odd. Substitute $i=1$ in (4.3). It follows that $\xi^r=1$, i.e. $\xi\in G$, and

$$\binom{2r+1}{r-2}=1.$$

If $m=1$ then G is the multiplicative group of a subfield of k. We knew that this was one of the possible solutions. In the following we shall use a theorem due to M. E. Lucas (cf. L. E. Dickson [1]).

Theorem. *Let p be a prime. If $m\in\Omega$, we write*

$$m=\sum_{i\geqslant 0} a_i(m)p^i$$

with $0\leqslant a_i(m)<p$. *Then*

$$\binom{m}{n}\equiv\prod_{i\geqslant 0}\binom{a_i(m)}{a_i(n)}\pmod p,$$

where $\binom{k}{l}=0$ *if* $l>k$.

We now continue the treatment of the case $p=2$ and assume that $m>1$. By Lucas' theorem

$$\binom{2r+1}{r-2}=1 \text{ iff } r+1=2^l,\ 2^l-1, \text{ or } 2^l-2.$$

Since $m\neq 1$, we must have $r+1=2^l-2$. If $l\geqslant 4$, we can substitute $i=3$ in (4.3). This yields $\xi^r=0$, a contradiction. It remains to check the case $r=5$,

$p=2$, $\xi \in G$. This proves to be a solution. Now G is the subgroup of index 3 in the multiplicative group of $GF(2^4)$. If $\xi \in G$, then $\xi+G$ contains 0 and two elements from each of the cosets of G different from G. This is easily checked by considering the representation of $GF(2^4)$ as $GF(2)[\alpha]$, where $\alpha^4+\alpha+1=0$. The property we have studied plays a role in proving that the Ramsey number $N(3, 3, 3; 3)$ is >16 (cf. R. E. Greenwood and A. M. Gleason [2]). In this proof the pairs of elements of $GF(2^4)$ are partitioned into 3 classes according to the coset of G containing their difference. Then no class contains a triangle.

(ii) $p>2$.

Now, we find from (4.4) with $i=1$ that $p|(r+1)$ or $p|(2r+1)$. When investigating these possibilities, we write $r+1=p^a m$, $(p \nmid m)$, respectively $2r+1=p^a m$ $(p \nmid m)$. We use the following identities for binomial coefficients in these cases. Again these follow directly from Lucas' theorem. If $r+1=p^a m$ then

$$\binom{r+1}{i}=\begin{cases}0 & \text{if } 1 \leqslant i<p^a,\\ m & \text{if } i=p^a,\end{cases} \tag{4.5}$$

$$\binom{2r+1}{i}=\begin{cases}(-1)^i & \text{if } 1 \leqslant i<p^a,\\ 2m-1 & \text{if } i=p^a.\end{cases} \tag{4.6}$$

If $2r+1=p^a m$ then

$$\binom{2r+1}{i}=\begin{cases}0 & \text{for } 1 \leqslant i<p^a,\\ m & \text{for } i=p^a.\end{cases} \tag{4.7}$$

Let $r+1=p^a m$. If $m>1$ we can substitute $i=p^a-2$ and $i=p^a-1$ in (4.3). This yields, using (4.6),

$$\xi^r\binom{2r+1}{r-p^a+1}=1,\ \xi^r\binom{2r+1}{r-p^a}=2m-1.$$

Hence

$$m \equiv 0 \pmod p,$$

a contradiction.

Hence we have $r+1=p^a$. Using (4.6) we find from (4.3), by substituting $i=1$, that $\xi^r=1$, i.e. $\xi \in G$ and G is the multiplicative group of a subfield of k.

This was a solution which we expected.

Now consider the case that $2r+1=p^a m$. If $m>1$ then, since m must be odd, $m \geqslant 3$ and if $p=3$ then $m \geqslant 5$. Therefore

$$p^a-1 \leqslant r-3=\tfrac{1}{2}(p^a m-1)-3.$$

Then we can substitute $i = p^a - 2$ in (4.3). From (4.7) we then find

$$\binom{2r+1}{r-p^a+1} = 0,$$

hence

$$\binom{2r+1}{r-p^a} = 0,$$

and then substitution of $i = p^a - 1$ in (4.3) yields $m \equiv 0 \pmod p$. Hence $m = 1$. Therefore $2r+1 = p^a$, i.e. G is the subgroup of order 2 in the multiplicative group of a subfield k_1 of k. Using (4.2) with $i = 1$ and (4.7) we find that $\varrho + \sigma = 0$. Then (4.1) becomes

$$\xi^{2r+1} + x^{2r+1} + \varrho\sigma(\xi + x) = (x^r - 1)f(x).$$

So $\varrho\sigma = -1$, whence $\{\varrho, \sigma\} = \{1, -1\}$ and $\xi \in k_1$. Again, this is the solution we expected. Summarizing, we have proved the following theorem.

THEOREM. *Let p be a prime, $k = GF(p^\alpha)$, $p^\alpha - 1 = rd$ where $r \geqslant 3$ and $d \geqslant 3$, $\xi \in k$, ($\xi \neq 0$) and let G be the subgroup of order r in $k^\times$. Then the set*

$$\xi + G = \{\xi + g | g \in G\}$$

has a nonempty intersection with at least 3 cosets of G in $k^\times$ unless

i) *G is the multiplicative group of a subfield of k and $\xi \in G$,*
ii) *p is odd, G is the subgroup of index 2 in the multiplicative group of a subfield k_1 of k and $\xi \in k_1$,*
iii) *$r = 3$ and $\xi \in G$ or $-\xi \in G$,*
iv) *$r = 4$* and *$\xi \in G$,*
v) *$r = 5$, $p = 2$, $\xi \in G$.*

London University
Technological University, Eindhoven
University of Utrecht

REFERENCES

1. DICKSON, L. E., Theory of Numbers, Vol. I, p. 271, Chelsea 1952.
2. GREENWOOD, R. E. and A. M. GLEASON, Combinatorial Relations and Chromatic Graphs, Can. J. Math. 7, 1–7 (1955).