TWO-ELEMENT GENERATION OF THE PROJECTIVE UNIMODULAR GROUP[1]

BY

A. A. ALBERT AND JOHN THOMPSON

1. Introduction

Let $\mathfrak{F} = \mathfrak{F}_q$ be the field of $q = p^m$ elements, $\mathfrak{M} = \mathfrak{M}(n, q)$ the multiplicative group of all n-rowed square matrices with elements in $\mathfrak{F}$ and determinant 1, and $\mathfrak{N} = \mathfrak{N}(n, q)$ the subgroup of $\mathfrak{M}$ consisting of its scalar matrices ρI with $\rho^n = 1$. We assume, of course, that $n > 1$. Then $\mathfrak{N}$ is a normal subgroup of $\mathfrak{M}$, and the quotient group

$$\mathfrak{G} = \mathfrak{G}(n, q) = \mathfrak{M}/\mathfrak{N} \tag{1}$$

is a well-known simple group called the *projective unimodular group.*

In 1930 H. R. Brahana[2] gave a list of simple groups of orders less than 1,000,000. An examination of his list reveals the fact that every group there is generated by two elements, one of which has period (group order) two. The purpose of this paper is to prove the corresponding result for a general class of simple groups. We shall derive the following property.[3]

THEOREM. *The projective unimodular group is generated by two elements $A\mathfrak{N}$ and $B\mathfrak{N}$, where the coset $A\mathfrak{N}$ has period two.*

The nature of our proof is such that it is necessary to consider a number of special cases for small matrix orders n. We shall begin with a treatment of the general case $n \geqq 5$, and shall then handle these special cases, the most difficult being the case $n = 2$.

2. The group $\mathfrak{G}$ for $n \geqq 5$

The nonzero elements of $\mathfrak{F}_q$ form a cyclic group $\mathfrak{F}_q^*$ of order $q - 1$, and the set of all elements ρ of $\mathfrak{F}_q^*$, such that $\rho^n = 1$, is a subgroup of $\mathfrak{F}_q^*$ isomorphic to $\mathfrak{N} = \mathfrak{N}(n, q)$. This is a cyclic group generated by an element λ whose period divides both n and $q - 1$, and we observe that, when $n = 2$, the group $\mathfrak{N}$ is the identity group if $p = 2$, and is generated by $-I$ when p is odd.

Our theorem is clearly equivalent to the property that $\mathfrak{M}(n, q)$ is generated by A, B, and λI. We let e_{ij} be the n-rowed square matrix with 1 in its i^{th} row and j^{th} column and zeros elsewhere, and I the n-rowed identity matrix. Then the theory of the reduction of a matrix to diagonal form by elementary

Received April 28, 1958.

[1] This paper was sponsored, in part, by the National Science Foundation.

[2] See the Annals of Mathematics, vol. 31 (1930), pp. 529–549 for this list.

[3] Our theorem was first proved for the case where q is a prime by I. Kaplansky in an unpublished note. It was later proved by L. J. Paige in the cases where $q = 4$ and $q = 8$.

transformations implies that the group $\mathfrak{M}(n, q)$ is generated by the matrices

$$I + xe_{ij} \qquad (i \neq j; i, j = 1, \cdots, n), \tag{2}$$

where x ranges over all nonzero elements of $\mathfrak{F}_q$. Thus our technique will consist of a study of the subgroup $\mathfrak{H}$ of $\mathfrak{M}(n, q)$ generated by A, B, and λI, and a proof of the property that $\mathfrak{H}$ contains all of the matrices in (2).

We note that

$$\begin{gathered}(I + xe_{ij})(I + ye_{ij}) = I + (x + y)e_{ij}, \\ (I + xe_{ij})^{-1} = (I - xe_{ij}),\end{gathered} \tag{3}$$

and that

$$(I + xe_{ij})^t = I + txe_{ij}, \tag{4}$$

for all $i \neq j$, all x and y in $\mathfrak{F}_q$, and all integers t. Also

$$(I + xe_{ij})(I + ye_{rs}) = I + xe_{ij} + ye_{rs} \qquad (i \neq j, j \neq r; r \neq s), \tag{5}$$

and

$$(I + xe_{ij} + ye_{rs})^t = I + txe_{ij} + tye_{rs} \tag{6}$$

for all integers t, and all $i \neq j$, $j \neq r$, $r \neq s$, and $s \neq i$. In particular,

$$(I + xe_{ij} + ye_{rs})^{-1} = I - xe_{ij} - ye_{rs}. \tag{7}$$

Finally, let i, j, k be distinct, let x and y be in $\mathfrak{F}_q$, and let

$$A = I + xe_{ij}, \qquad B = I + ye_{jk}. \tag{8}$$

Then $AB = I + xe_{ij} + ye_{jk} + xye_{ik}$, $A^{-1}B^{-1} = I - xe_{ij} - ye_{jk} + xye_{ik}$, so that the commutator of A and B is

$$ABA^{-1}B^{-1} = I + xye_{ik}. \tag{9}$$

We shall use the convention

$$e_{i,j+n} = e_{i+n,j} = e_{ij} \tag{10}$$

for all $i, j = 1, \cdots, n$, and shall begin with a derivation of the following key lemma.

LEMMA 1. *Let α be a primitive element of $\mathfrak{F}_q$, $n \geqq 5$, and*

$$C = I + \alpha e_{n-1,2} + e_{n1}, \qquad D = (-1)^n(e_{12} - e_{23} + \textstyle\sum_{i=3}^{n} e_{i,i+1}). \tag{11}$$

Then the cosets $C\mathfrak{N}$ and $D\mathfrak{N}$ generate $\mathfrak{G}(n, q)$.

We observe that D is unimodular for all $n \geqq 1$, and that

$$D^{-1} = (-1)^n(e_{21} - e_{32} + \textstyle\sum_{i=3}^{n} e_{i+1,i}). \tag{12}$$

Then a direct computation shows that

$$D^{-1}e_{ij}D = e_{i+1,j+1} \qquad (i \neq 2; j \neq 2; i = j = 2), \tag{13}$$

while

$$D^{-1}e_{2j}D = -e_{3,j+1}, \qquad D^{-1}e_{i2}D = -e_{i+1,3} \quad (i \neq 2; j \neq 2), \tag{14}$$

for all $n > 3$. It follows from (13), (14), and (3) that, if a subgroup $\mathfrak{H}$ of $\mathfrak{M}(n, q)$ contains $I + xe_{ij}$ and $I + ye_{jk}$ with i, j, k distinct, then $\mathfrak{H}$ also contains $I + xye_{ik}$.

We now make the assumption that $n \geqq 5$ and that $\mathfrak{H}_0$ is the subgroup of $\mathfrak{M}(n, q)$ generated by C, D, and the scalar matrices of determinant one. Then $\mathfrak{H}_0$ contains

$$C_1 = D^{-1}CD = I - \alpha e_{n3} + e_{12}, \tag{15}$$

as well as

$$\begin{aligned} CC_1C^{-1}C_1^{-1} &= (I + \alpha e_{n-1,2} + e_{n1})(I - \alpha e_{n3} + e_{12})C^{-1}C_1^{-1} \\ &= [I + (\alpha e_{n-1,2} + e_{n1} - \alpha e_{n3} + e_{12}) + e_{n2}] \\ &\quad \cdot [I - (\alpha e_{n-1,2} + e_{n1} - \alpha e_{n3} + e_{12}) + e_{n2}] = I + 2e_{n2} - e_{n2}. \end{aligned}$$

Thus $\mathfrak{H}_0$ contains

$$E_{n2} = I + e_{n2}. \tag{16}$$

Assume next that $\mathfrak{H}_0$ contains

$$E_{nk} = I + e_{nk} \qquad (2 \leqq k \leqq n - 2). \tag{17}$$

Then $\mathfrak{H}_0$ contains

$$C_{k-1} = D^{1-k}CD^{k-1} = I + \rho e_{k,k+1} + \sigma\alpha e_{k-1,k+2} \qquad (\rho^2 = \sigma^2 = 1), \tag{18}$$

and thus contains

$$\begin{aligned} E_{nk}C_{k-1}E_{nk}^{-1}C_{k-1}^{-1} &= (I + e_{nk})(I + \rho e_{k,k+1} + \sigma\alpha e_{k-1,k+2})E_{nk}^{-1}C_{k-1}^{-1} \\ &= (I + e_{nk} + \rho e_{k,k+1} + \sigma\alpha e_{k-1,k+2} + \rho e_{n,k+1}) \\ &\quad \cdot (I - e_{nk} - \rho e_{k,k+1} - \sigma\alpha e_{k-1,k+2} + \rho e_{n,k+1}) \\ &= I + 2\rho e_{n,k+1} - \rho e_{n,k+1} = I + \rho e_{n,k+1}. \end{aligned}$$

By (3) we see that $\mathfrak{H}_0$ contains $I + e_{n,k+1}$. This completes an inductive proof of the fact that $\mathfrak{H}_0$ contains

$$I + e_{nm} \qquad (m = 2, \cdots, n - 1). \tag{19}$$

But then we apply (13), (14), (3), and (9) to see that $\mathfrak{H}_0$ contains every $I + e_{ij}$ for $i - j \neq 0, n - 1$. It follows that $\mathfrak{H}_0$ contains $I + e_{n2}$, $I + e_{21}$, and (9) implies that $\mathfrak{H}_0$ contains $I + e_{n1}$. We have shown that $\mathfrak{H}_0$ contains

$$I + e_{ij} \qquad (i \neq j; i, j = 1, \cdots, n). \tag{20}$$

We use (15) to see that $\mathfrak{H}_0$ contains

$$(I - e_{12})(I + e_{12} - \alpha e_{n3}) = I - \alpha e_{n3} ;$$

$\mathfrak{H}_0$ contains $I + \alpha e_{n3}$; $\mathfrak{H}_0$ contains $I + \alpha e_{nk}$ by (9) for all $k \neq 3, n$. Since $\mathfrak{H}_0$ has been shown to contain $I + \alpha e_{n3}$, we have proved that $I + \alpha e_{nk}$ is in $\mathfrak{H}_0$ for every $k \neq n$. Using (13), (14), and (9) we see that $I + \alpha e_{ij}$ is in $\mathfrak{H}_0$ for all $i \neq j$.

If $I + xe_{ij}$ and $I + ye_{jk}$ are in $\mathfrak{H}_0$ for x and y in $\mathfrak{F}$, we use (9) to see that $I + xye_{ik}$ is in $\mathfrak{H}_0$. But if i and k are distinct, there is an integer $j \neq i, k$, and the fact that $I + \alpha e_{ij}$ and $I + \alpha e_{jk}$ are in $\mathfrak{H}_0$ implies that $I + \alpha^2 e_{ik}$ is in $\mathfrak{H}_0$ for all $i \neq k$. If $I + \alpha^t e_{ij}$ is in $\mathfrak{H}_0$, then we use (9) with

$$A = I + \alpha^t e_{ij} ,$$

$B = I + \alpha e_{jk}$ to see that $I + \alpha^{t+1} e_{ik}$ is in $\mathfrak{H}_0$. It follows that $I + \alpha^t e_{ij}$ is in $\mathfrak{H}_0$ for every $i \neq j$ and every integer t. Since α is a primitive element of $\mathfrak{F}_q$, it follows that $\mathfrak{H}_0$ contains every $I + xe_{ij}$, $\mathfrak{H}_0 = \mathfrak{M}(n, q)$. This completes a proof of our basic lemma.

Lemma 1 provides a proof of our theorem for $p = 2$ and $n \geqq 5$, since it should be obvious from (6) that C has period p. Assume then that

$$p = 2k + 1. \tag{21}$$

We shall then derive the following result.

LEMMA 2. *Let $p = 2k + 1$, $n \geqq 5$, α be a primitive element of $\mathfrak{F}_q$, and $\delta = -k\alpha$, so that $2\delta = \alpha$. Then the unimodular matrix*

$$A = -(e_{11} + e_{22}) + \sum_{i=3}^{n} e_{ii} + \alpha e_{n-1,2} + e_{n1} \tag{22}$$

has period two,

$$B = (-1)^n(e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + \delta e_{n-1,3} + ke_{n2}) \tag{23}$$

is unimodular, and $\mathfrak{G}(n, q)$ is generated by the cosets $A\mathfrak{N}$ and $B\mathfrak{N}$.

It is trivial to see that A and B are unimodular and that

$$(-1)^n B^{-1} = \delta e_{n2} - ke_{11} + e_{21} - e_{32} + \sum_{i=3}^{n} e_{i+1,i} . \tag{24}$$

Compute

$$\begin{aligned} A_1 = B^{-1}AB &= (e_{21} - e_{32} + \sum_{i=3}^{n} e_{i+1,i} - ke_{11} + \delta e_{n2}) \\ &\quad \cdot (-e_{11} - e_{22} + \sum_{i=3}^{n} e_{ii} + \alpha e_{n-1,2} + e_{n1})(-1)^n B \\ &= [-e_{21} + e_{32} + \sum_{i=3}^{n} e_{i+1,i} + (\alpha - \delta)e_{n2} + (1 + k)e_{11}] \\ &\quad \cdot (e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + \delta e_{n-1,3} + ke_{n2}) \\ &= -e_{22} - e_{33} + \sum_{i=4}^{n} e_{ii} + e_{11} + (2\delta - \alpha)\, e_{n3} + (2k + 1)\, e_{12} . \end{aligned}$$

Since $2k + 1 = p = 0$ in $\mathfrak{F}_q$ and $2\delta = \alpha$, we have

$$A_1 = e_{11} - (e_{22} + e_{33}) + \sum_{i=4}^{n} e_{ii}\,. \tag{25}$$

But then

$$A_1 A = -e_{11} + e_{22} - e_{33} + \sum_{i=4}^{n} e_{ii} + \alpha e_{n-1,2} + e_{n1}\,, \tag{26}$$

and

$$(A_1 A)^2 = I + 2\alpha e_{n-1,2}\,. \tag{27}$$

Assume that $\mathfrak{H}$ is the subgroup of $\mathfrak{M}(n, q)$ generated by our two matrices A and B and the generating matrix λI of $\mathfrak{N}$. Then (4) implies that $\mathfrak{H}$ contains

$$E = I + \alpha e_{n-1,2}\,. \tag{28}$$

Since $\delta = -k\alpha$, we see that $\mathfrak{H}$ contains $E^{-k} = I - k\alpha e_{n-1,2} = I + \delta e_{n-1,2}$ as well as

$$\begin{aligned} E^{-k}B &= (I + \delta e_{n-1,2})B \\ &= B + \delta e_{n-1,2}(e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + \delta e_{n-1,3} + k e_{n2})(-1)^n \\ &= B - (-1)^n \delta e_{n-1,3} = (-1)^n(e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + k e_{n2}). \end{aligned}$$

Define

$$L = (-1)^n(e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + k e_{n2}), \tag{29}$$

and see that L and

$$L^{-1} = (-1)^n(-k e_{11} + e_{21} - e_{32} + \sum_{i=3}^{n} e_{i+1,i}) \tag{30}$$

are in $\mathfrak{H}$. Also

$$\begin{aligned} L^{-1}A_1 L &= (-k e_{11} + e_{21} - e_{32} + \sum_{i=3}^{n} e_{i+1,i}) \\ &\qquad \cdot (e_{11} - e_{22} - e_{33} + \sum_{i=4}^{n} e_{ii})(-1)^n L \\ &= (-k e_{11} + e_{21} + e_{32} - e_{43} + \sum_{i=4}^{n} e_{i+1,i}) \\ &\qquad \cdot (e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + k e_{n2}) \\ &= -k e_{12} + e_{22} - e_{33} - e_{44} + \sum_{i=5}^{n} e_{ii} + e_{11} + k e_{12} \\ &= e_{11} + e_{22} - e_{33} - e_{44} + \sum_{i=5}^{n} e_{ii} = J_4 \end{aligned} \tag{31}$$

is in $\mathfrak{H}$.

We have now seen that $J_3 = A_1$ and J_4 are in $\mathfrak{H}$. Suppose that $\mathfrak{H}$ contains

$$J_j = \sum_{i=1}^{j-2} e_{ii} - (e_{j-1,j-1} + e_{jj}) + \sum_{i=j+1}^{n} e_{ii} \quad (4 \leqq j < n). \tag{32}$$

Then a direct computation shows that $\mathfrak{H}$ contains

$$L^{-1}J_j L = J_{j+1}\,. \tag{33}$$

Hence $\mathfrak{H}$ contains J_j for $j = 3, \cdots, n$. In particular, $\mathfrak{H}$ contains

$$J_n = \sum_{i=1}^{n-2} e_{ii} - (e_{n-1,n-1} + e_{nn}), \tag{34}$$

and also contains

$$J_n A = [I - 2(e_{n-1,n-1} + e_{nn})]A$$
$$= A - 2(e_{n-1,n-1} + e_{nn}) - 2(\alpha e_{n-1,2} + e_{n1}) \tag{35}$$
$$= \sum_{i=3}^{n-2} e_{ii} - (e_{11} + e_{22} + e_{n-1,n-1} + e_{nn} + \alpha e_{n-1,2} + e_{n1}).$$

However,

$$(J_n A)^2 = \sum_{i=3}^{n-2} e_{ii} + (e_{11} + e_{22} + e_{n-1,n-1} + e_{nn} + \alpha e_{n-1,2} + e_{n1})^2 \tag{36}$$
$$= I + 2(\alpha e_{n-1,2} + e_{n1}),$$

and it follows from (6) that the matrix C of Lemma 1 is in $\mathfrak{H}$. Since $E = I + \alpha e_{n-1,2}$ is in $\mathfrak{H}$, so is

$$E^{-1}C = I + e_{n1}, \tag{37}$$

and so is $(E^{-1}C)^{-k} = I - ke_{n1}$. But then

$$(E^{-1}C)^{-k}L = (I - ke_{n1})L$$
$$= L - ke_{n1}(-1)^n(e_{12} - e_{23} + \sum_{i=3}^{n} e_{i,i+1} + ke_{n2}) \tag{38}$$
$$= L - k(-1)^n e_{n2} = D$$

is in $\mathfrak{H}$, where D is the matrix of Lemma 1 By Lemma 1, the group $\mathfrak{H} = \mathfrak{M}(n, q)$ as desired. This completes our proof of the theorem for the general case $n \geqq 5$.

3. The case $n = 4$, $q \neq 9$

We shall assume next that $n = 4$, and redefine C and D by the formulas

$$C = I + \alpha e_{41}, \qquad D = e_{12} - e_{23} + e_{34} + e_{41}, \tag{39}$$

so that

$$D^{-1} = e_{21} - e_{32} + e_{43} + e_{14}. \tag{40}$$

Then we have

$$D^{-1}e_{ij}D = e_{i+1,j+1} \qquad (i \neq 2, j \neq 2; i = j = 2), \tag{41}$$

while

$$D^{-1}e_{2j}D = -e_{3,j+1}, \qquad D^{-1}e_{i2}D = -e_{i+1,3} \qquad (i \neq 2; j \neq 2). \tag{42}$$

As before, we let $\mathfrak{H}_0$ be the subgroup of $\mathfrak{M}(n, q)$ generated by C, D, and the scalar matrix λI, and see that

$$C_1 = D^{-1}CD = I + \alpha e_{12}, \qquad C_2 = D^{-1}CD = I - \alpha e_{23},$$
$$C_3 = D^{-1}C_2 D = I + \alpha e_{34} \tag{43}$$

are all in $\mathfrak{H}_0$. Then (9) implies that if $I + xe_{41}$ and $I + ye_{12}$ are in $\mathfrak{H}_0$, so is $I + xye_{42}$. But then $\mathfrak{H}_0$ contains

$$\begin{aligned} &I + xye_{42}, \qquad D^{-1}(I + xye_{42})D = I - xye_{13}, \\ &D^{-1}(I - xye_{13})D = I - xye_{24}, \qquad D^{-1}(I - xye_{24})D = I + xye_{31}. \end{aligned} \tag{44}$$

If $I + ze_{12}$ is in $\mathfrak{H}_0$, so is

$$(I + ze_{12})(I + xye_{24})(I - ze_{12})(I - xye_{24}) = I + xyze_{14} \tag{45}$$

by (9). As above, $\mathfrak{H}_0$ contains

$$I + (xyz)e_{14}, \quad I + (xyz)e_{21}, \quad I + (xyz)e_{32}, \quad I + (xyz)e_{43}. \tag{46}$$

Finally, if $\mathfrak{H}_0$ contains $I + xye_{42}$ and $I + (abc)e_{21}$, then (9) implies that $\mathfrak{H}_0$ contains $I + (xy)(abc)e_{41}$. Take $\alpha = x = y = a = b = c$ to see that $\mathfrak{H}_0$ contains

$$I + \alpha^4 \alpha e_{41}. \tag{47}$$

We next take $x = \alpha^5$, $y = a = b = c = \alpha$ to see that $\mathfrak{H}_0$ contains $I + \alpha^8 \alpha e_{41}$. But then it should be clear that $\mathfrak{H}_0$ contains $I + \alpha\alpha^{4k} e_{41}$, for all integers k. By (3) we see that $\mathfrak{H}_0$ contains all elements

$$I + \alpha f(\alpha^4) e_{41} \tag{48}$$

for all elements $f(\alpha^4)$ of the field $\mathfrak{F}_p[\alpha^4]$. When $q \neq 9$ it is easy to see that

$$\mathfrak{F}_p(\alpha^4) = \mathfrak{F}_q, \tag{49}$$

and so $\mathfrak{H}_0$ contains

$$I + xe_{41} \tag{50}$$

for all x of $\mathfrak{F}_q$. By (43), (44), (45), (46) we see that $\mathfrak{H}_0$ contains $I + xe_{ij}$ for all $i \neq j$, and so $\mathfrak{H}_0 = \mathfrak{M}(4, q)$.

If $p = 2$, the period of C is two, and our proof of the theorem is complete in that case. Hence take

$$p = 2k + 1, \qquad \alpha = 2\delta, \tag{51}$$

and define

$$\begin{aligned} A &= e_{11} - e_{22} + e_{33} - e_{44} + \alpha e_{41}, \\ B &= e_{12} - e_{23} + e_{34} + e_{41} + \delta e_{42}. \end{aligned} \tag{52}$$

Thus A has period two, and

$$B^{-1} = -\delta e_{11} + e_{14} + e_{21} - e_{32} + e_{43}. \tag{53}$$

Then

$$\begin{aligned} A_1 &= B^{-1}AB \\ &= (-\delta e_{11} + e_{14} + e_{21} - e_{32} + e_{43})\,(e_{11} - e_{22} + e_{33} - e_{44} + \alpha e_{41})B \\ &= [(\alpha - \delta)e_{11} - e_{14} + e_{21} + e_{32} + e_{43}]\,(e_{12} - e_{23} + e_{34} + e_{41} + \delta e_{42}) \\ &= (\alpha - \delta)e_{12} - e_{11} - \delta e_{12} + e_{22} - e_{33} + e_{44}, \end{aligned}$$

and we use (51) to see that

$$J = B^{-1}AB = -e_{11} + e_{22} - e_{33} + e_{44} \tag{54}$$

is in the subgroup $\mathfrak{H}$ of $\mathfrak{M}(n, q)$ generated by A, B, and λI. Also $-JA = I - \alpha e_{41}$ is in $\mathfrak{H}$, and so is

$$(-JA)^{-1} = I + \alpha e_{41} = C. \tag{55}$$

Then $\mathfrak{H}$ contains $C^k = I + k\alpha e_{41} = I - \delta e_{41}$, since

$$2(k\alpha + \delta) = (2k + 1)\alpha = 0.$$

It follows that $C^kB = B - \delta e_{41}(e_{12} - e_{23} + e_{34} + e_{41} + \delta e_{42}) = B - \delta e_{42} = e_{12} - e_{23} + e_{34} + e_{41} = D$. Hence $\mathfrak{H}$ contains both C and D, and $\mathfrak{H} = \mathfrak{M}(n, q)$. We state this result as follows.

LEMMA 3. *The group $\mathfrak{G}(4, q)$ is generated by $C\mathfrak{N}$ and $D\mathfrak{N}$ of (39) if $q \neq 9$. The coset $C\mathfrak{N}$ has period p and so has period two if $p = 2$. If $p \neq 2$, the group $\mathfrak{G}(4, q)$ is generated by $A\mathfrak{N}$ and $B\mathfrak{N}$ when $q \neq 9$, where A and B are given by (52), and A has period two.*

4. The group $\mathfrak{G}(4, 9)$

The field $\mathfrak{F}_9$ is generated over $\mathfrak{F}_3$ by an element α such that

$$\alpha^2 = \alpha + 1. \tag{56}$$

Then

$$\alpha^3 = \beta = 1 - \alpha, \qquad \alpha^4 = \alpha\beta = -1, \tag{57}$$

so that α is a primitive element of $\mathfrak{F}_9$. We shall derive the following result.

LEMMA 4. *Let α be defined by (56). Then $\mathfrak{G}(4, 9)$ is generated by $A\mathfrak{N}$ and $B\mathfrak{N}$, where A and B are given by*

$$\begin{aligned} A &= -e_{11} + e_{22} - e_{33} + e_{44} + \alpha e_{32} + e_{41}, \\ B &= e_{12} - e_{23} + e_{34} + e_{41} + e_{42} + \alpha e_{33}, \end{aligned} \tag{58}$$

and A has period two.

We let $\mathfrak{H}$ be the subgroup of $\mathfrak{M}(4, 9)$ generated by A, B, and $\mathfrak{N}$, and compute

$$B^{-1} = -e_{1'} + e_{21} - e_{32} + e_{43} + e_{14} + \alpha e_{42}. \tag{59}$$

Then a direct computation, for this case of characteristic three, yields

$$J = B^{-1}AB = e_{11} - e_{22} + e_{33} - e_{44}. \tag{60}$$

Also, it is clear that

$$C = -JA = I - \alpha e_{32} + e_{41}. \tag{61}$$

Since C is in $\mathfrak{H}$, so is

$$C^{-1}B = (I + \alpha e_{32} - e_{41})B$$

$$= B + (\alpha e_{32} - e_{41})(e_{12} - e_{23} + e_{34} + e_{41} + e_{42} + \alpha e_{33}) = B - \alpha e_{33} - e_{42},$$

that is, $\mathfrak{H}$ contains

$$D = C^{-1}B = e_{12} - e_{23} + e_{34} + e_{41}. \tag{62}$$

It should now be clear that D^{-1} is given by (40), and that the conjugating relations (41) and (42) hold. Hence $\mathfrak{H}$ contains

$$C_1 = D^{-1}CD = I + \alpha e_{43} + e_{12}, \qquad C_2 = D^{-1}C_1 D = (I + \alpha e_{14} - e_{23}),$$
$$C_3 = D^{-1}C_2 D = I + \alpha e_{21} + e_{34}, \tag{63}$$

as well as

$$C_1 C C_1^{-1} C^{-1} = (I + \alpha e_{43} + e_{12})(I - \alpha e_{32} + e_{41})C_1^{-1}C^{-1}$$
$$= (I + \alpha e_{43} + e_{12} - \alpha e_{32} + e_{41} - \alpha^2 e_{42})$$
$$\cdot (I - \alpha e_{43} - e_{12} + \alpha e_{32} - e_{41} - \alpha^2 e_{42})$$
$$= I - 2\alpha^2 e_{42} + \alpha^2 e_{42} - e_{42} = I - (1 + \alpha^2)e_{42}$$
$$= I - (\alpha + 2)e_{42} = I + \beta e_{42}.$$

By conjugating by D and taking inverses we see that $\mathfrak{H}$ contains

$$L = L_0 = I + \beta e_{42}, \qquad L_1 = I + \beta e_{13},$$
$$L_2 = I + \beta e_{24}, \qquad L_3 = I + \beta e_{31}. \tag{64}$$

As next element we compute the commutator

$$L_1^{-1}C_3 L_1 C_3^{-1} = (I - \beta e_{13})(I + \alpha e_{21} + e_{34})L_1 C_3^{-1}$$
$$= (I + \alpha e_{21} + e_{34} - \beta e_{13} - \beta e_{14})(I - \alpha e_{21} - e_{34} + \beta e_{13} - \beta e_{14})$$
$$= I - 2\beta e_{14} + \alpha\beta e_{23} - \alpha\beta e_{24} + \beta e_{14} = I - \beta e_{14} - e_{23} + e_{24}$$

by (57). Then

$$R = L_1^{-1}C_3 L_1 C_3^{-1} \cdot C_2^{-1} = (I - \beta e_{14} - e_{23} + e_{24})(I - \alpha e_{14} + e_{23})$$
$$= I - \beta e_{14} - e_{23} + e_{24} - \alpha e_{14} + e_{23} = I - (\alpha + \beta)e_{14} + e_{24}$$
$$= I - e_{14} + e_{24}$$

is in $\mathfrak{H}$, and so is

$$JR = (e_{11} - e_{22} + e_{33} - e_{44})(I - e_{14} + e_{24}) = e_{11} - e_{22} + e_{33} - e_{44} - e_{14} - e_{24}.$$

But

$$(65)\quad (JR)^2 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I + 2e_{24}$$

is in $\mathfrak{H}$, and we have shown that $\mathfrak{H}$ contains $I + e_{24}$. Using (41) and (42), and taking inverses when necessary, we see that

$$(66)\qquad I + e_{24}, \quad I + e_{31}, \quad I + e_{42}, \quad I + e_{13}$$

are all in $\mathfrak{H}$. Also $(I - e_{24})R = I - e_{14} + e_{24} - e_{24} = I - e_{14}$ is in $\mathfrak{H}$, and so $\mathfrak{H}$ contains

$$(67)\qquad I + e_{14}, \quad I + e_{21}, \quad I + e_{32}, \quad I + e_{43}.$$

By (9) we see that $\mathfrak{H}$ contains $(I + e_{14})(I + e_{42})(I + e_{14})^{-1}(I + e_{42})^{-1} = I + e_{12}$. Hence $I + e_{12}$, $I + e_{23}$, $I + e_{34}$, $I + e_{41}$, are all in $\mathfrak{H}$, and we have shown that $\mathfrak{H}$ contains $I + e_{ij}$ for all $i \neq j$. Clearly $(I - e_{41})C = I - \alpha e_{32}$ is in $\mathfrak{H}$, and thus $\mathfrak{H}$ contains $I + \alpha e_{32}$, $I + \alpha e_{43}$, $I + \alpha e_{14}$, $I + \alpha e_{21}$. Using (9) we show readily that $\mathfrak{H}$ contains $I + \alpha e_{ij}$, for all $i \neq j$. But (9) implies that if $\mathfrak{H}$ contains $I + \alpha^t e_{ij}$ for all $i \neq j$, then $\mathfrak{H}$ contains

$$(I + \alpha^t e_{ij})(I + \alpha e_{jk})(I + \alpha^t e_{ij})^{-1}(I + \alpha e_{jk})^{-1} = I + \alpha^{t+1} e_{ik}$$

for all i, j, k distinct. It follows immediately that $\mathfrak{H}$ contains $I + xe_{ij}$ for all x in $\mathfrak{F}_9$, and the proof of our lemma is complete.

5. Generation of $\mathfrak{G}(3, q)$

The principal result for the case where $n = 3$ may be stated as follows.

LEMMA 5. *Let $q \neq 4$, let α be a primitive element of $\mathfrak{F}_q$, and let*

$$(68)\qquad C = I + \alpha e_{31}, \quad D = e_{12} + e_{23} + e_{31}.$$

Then $C\mathfrak{N}$ and $D\mathfrak{N}$ generate $\mathfrak{G}(3, q)$, and C has period p. If $p = 2k + 1$, the group $\mathfrak{G}(3, q)$ is generated by $A\mathfrak{N}$ and $B\mathfrak{N}$, where

$$(69)\qquad A = e_{33} - e_{11} - e_{22} - \alpha e_{31}, \quad B = D - k\alpha e_{32},$$

and A has period two.

It is clear that

$$(70)\qquad D^{-1} = e_{13} + e_{21} + e_{32}, \quad D^{-1}e_{ij}D = e_{i+1,j+1} \qquad (i, j = 1, 2, 3).$$

We let $\mathfrak{H}_0$ be the subgroup of $\mathfrak{M}(3, q)$ generated by C, D, and λI, and see that $\mathfrak{H}_0$ contains

$$(71)\qquad C = I + \alpha e_{31}, \quad C_1 = D^{-1}CD = I + \alpha e_{12}, \quad C_2 = D^{-1}C_1D = I + \alpha e_{23}.$$

Assume then that $I + xe_{31}$, $I + ye_{12}$, $I + ze_{32}$ are in $\mathfrak{H}_0$ for x, y, z in $\mathfrak{F}_q$. Then we use (9) to see that $I + xye_{32}$ is in $\mathfrak{H}_0$, and (70) implies that $I + (xy)e_{13}$ is in $\mathfrak{H}_0$. We use (9) again to obtain $I + (xyz)e_{12}$, and see that $I + (xyz)e_{23}$ and $I + (xyz)e_{31}$ are in $\mathfrak{H}_0$. Take $x = y = \alpha$, and use the results just stated to see that $\mathfrak{H}_0$ contains $I + \alpha e_{31}$, $I + \alpha^2 e_{32}$, $I + \alpha^4 e_{31}$. We can then take $x = \alpha^4$, $y = \alpha$, $z = \alpha^2$ and see that $I + \alpha^7 e_{31}$ is in $\mathfrak{H}_0$. Thus the values $x = \alpha^{3k+1}$, $y = \alpha$, $z = \alpha^2$ may be used to complete an inductive argument implying that $I + \alpha^{3t+1} e_{31}$ is in $\mathfrak{H}_0$ for all nonnegative integers t. It follows immediately from (3) that $\mathfrak{H}_0$ contains

$$I + \alpha f(\alpha^3) e_{31} \tag{72}$$

for all elements $f(\alpha^3)$ of $\mathfrak{F}_p(\alpha^3)$. If $\mathfrak{F}_p(\alpha^3)$ is a proper subfield of $\mathfrak{F}_q = \mathfrak{F}_p(\alpha)$ where $p^\nu = q$, then the degree over $\mathfrak{F}_p$ of $\mathfrak{F}_p(\alpha^3)$ must be a proper divisor μ of $\nu = \lambda\mu$.

The period of α is $q - 1$, and the period r of α^3 must divide $p^\mu - 1$. Thus $r = \frac{1}{3}(q - 1)$; $3r = q - 1 = p^\nu - 1$ must divide $3(p^\mu - 1)$. But then $p^{(\lambda-1)\mu} + p^{(\lambda-2)\mu} + \cdots + 1$ divides 3, and this can occur only if $p = 2$, $\mu = 1$, $\lambda = 2$, so that $q = 4$ and $\alpha^3 = 1$.

We have now shown that the assumption that $q \neq 4$ implies that $\mathfrak{H}_0$ contains $I + xe_{31}$ for every x of F_q. By (70) we know that $\mathfrak{H}_0$ contains $I + ye_{32}$ for all y of $\mathfrak{F}_q$, and it follows that $\mathfrak{H}_0$ contains all $I + xe_{ij}$ for x in $\mathfrak{F}_q$ and $i \neq j$, so that $\mathfrak{H}_0 = \mathfrak{M}(3, q)$ as desired.

This completes the proof of the first part of our lemma, and we now assume that $p = 2k + 1$. Compute

$$\begin{aligned} A_1 = B^{-1}AB &= \begin{pmatrix} -\delta & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -\alpha & 0 & 1 \end{pmatrix} B \\ &= \begin{pmatrix} \delta - \alpha & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \delta & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2\delta - \alpha & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \end{aligned} \tag{73}$$

But we have taken $\delta = -k\alpha$, and so $2\delta - \alpha = -(2k + 1)\alpha = 0$,

$$\begin{aligned} A_1 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \\ A_1 A &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -\alpha & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & 0 & -1 \end{pmatrix}, \end{aligned} \tag{74}$$

and

$$(A_1 A)^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2\alpha & 0 & 1 \end{pmatrix}. \tag{75}$$

Hence the subgroup $\mathfrak{H}$ of $\mathfrak{M}(3, q)$ generated by the elements in the cosets $A\mathfrak{N}$ and $B\mathfrak{N}$ contains $I - 2\alpha e_{31}$, and also contains

$$(I - 2\alpha e_{31})^k = I - 2k\alpha e_{31} = I + \alpha e_{31} = C.$$

Also $C^k = I + k\alpha e_{31} = I - \delta e_{31}$ is in $\mathfrak{H}$ and so is

$$C^k B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\delta & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \delta & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = D. \tag{76}$$

By the proof above, $\mathfrak{H} = \mathfrak{M}(3, q)$, and the proof of our lemma is complete.

There remains the case $n = 3$ and $q = 4$. We shall derive the following result.

LEMMA 6. *Let $\alpha \neq 0, 1$ be in $\mathfrak{F}_4$, and let*

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & \alpha \end{pmatrix}. \tag{77}$$

Then A has period two, and the group $\mathfrak{G}(3, 4)$ is generated by $A\mathfrak{N}$ and $B\mathfrak{N}$.

For we see easily that $A^2 = I$ and

$$B^{-1} = \begin{pmatrix} 0 & \alpha & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$B^{-1}AB = \begin{pmatrix} 0 & \alpha & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & 0 & 1 \end{pmatrix} B \tag{78}$$

$$= \begin{pmatrix} 0 & \alpha & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Thus $I + e_{32}$ is in the subgroup $\mathfrak{H}$ of $\mathfrak{M}(3, 4)$ generated by A, B, and αI. Then $\mathfrak{H}$ contains

$$AB^{-1}AB = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & 1 & 1 \end{pmatrix} \tag{79}$$

$$= I + e_{21} + \alpha e_{31} + e_{32}$$

as well as

$$(AB^{-1}AB)^2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = I + e_{31}. \tag{80}$$

We see also that

$$B^{-1}(I + e_{31})B = \begin{pmatrix}0 & \alpha & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}B$$

(81)

$$= \begin{pmatrix}1 & \alpha & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & \alpha\end{pmatrix} = \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = I + e_{12}$$

and

$$B^{-1}(I + e_{12})B = \begin{pmatrix}0 & \alpha & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}B$$

(82)

$$= \begin{pmatrix}0 & \alpha & 1\\ 1 & 1 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & \alpha\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix} = I + e_{23}$$

are in $\mathfrak{H}$. Hence $(I + e_{12})(I + e_{23}) = I + e_{12} + e_{23} + e_{13}$ is in $\mathfrak{H}$, and so is

$$\begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = I + e_{13}\,. \tag{83}$$

But this shows that $(I + e_{23})(I + e_{31}) = I + e_{23} + e_{31} + e_{21}$ is in $\mathfrak{H}$, and so is

$$\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 1\\ 1 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = I + e_{21}\,. \tag{84}$$

Hence $I + e_{ij}$ is in $\mathfrak{H}$ for all $i \neq j$. Moreover

$$(I + e_{21})A = \begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ \alpha & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ \alpha & 0 & 1\end{pmatrix} = I + \alpha e_{31} \tag{85}$$

is in $\mathfrak{H}$. If $I + \alpha e_{ij}$ is in $\mathfrak{H}$, then (9) implies that $I + \alpha e_{ik}$ and $I + \alpha e_{kj}$ are in $\mathfrak{H}$. It follows that $I + \alpha e_{32}$ and $I + \alpha e_{21}$ are in $\mathfrak{H}$, $I + \alpha e_{12}$ is in $\mathfrak{H}$, $I + \alpha e_{13}$ and $I + \alpha e_{23}$ are in $\mathfrak{H}$, and so $I + \alpha e_{ij}$ is in $\mathfrak{H}$ for all $i \neq j$. By (9) we see that if $I + \alpha^t e_{ij}$ is in $\mathfrak{H}$ for all $i \neq j$, then $I + \alpha^{t+1} e_{ik}$ is in $\mathfrak{H}$ for all $i \neq k$. It follows that $\mathfrak{H}$ contains $I + xe_{ij}$ for all $i \neq j$ and all x of $\mathfrak{F}_4$, and the proof of our lemma is complete.

6. Preliminary generation of $\mathfrak{G}(2, q)$

As in the previous cases we assume that α is a primitive element of $\mathfrak{F}_q$, $q = p^m$, so that the period of α is $q - 1$. Write

$$s = (q - 1)/(p - 1) = 1 + p + p^2 + \cdots + p^{m-1}, \qquad u = \alpha^s, \tag{86}$$

so that u is a primitive element of the prime subfield $\mathfrak{F}_p$ of $\mathfrak{F}_q$. When p is odd, we have

$$s \equiv m \pmod 2, \tag{87}$$

and so u is an odd power of α if and only if m is odd. When m is even, all nonzero elements of $\mathfrak{F}_p$ are powers of u and so are even powers of α. We state this elementary property as follows.

LEMMA 7. *If p is odd, there exists an integer u in $\mathfrak{F}_p$ such that $u = \alpha^{2\sigma+1}$ if and only if m is odd.*

Observe now that the matrices

$$B = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} \tag{88}$$

are unimodular. We also observe that $\mathfrak{N}$ is generated by $-I$, and we shall derive the following result.

LEMMA 8. *The matrices B, $-B$, and C generate $\mathfrak{M}(2, q)$.*

For

$$C^{-1} = \begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}, \qquad CB = \begin{pmatrix} 0 & \alpha^{-1} \\ -\alpha & 1 \end{pmatrix}, \tag{89}$$

so that

$$CBC^{-1} = \begin{pmatrix} 0 & \alpha^{-1} \\ -\alpha & 1 \end{pmatrix}\begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha^{-1} & 0 \\ 1 - \alpha^2 & \alpha \end{pmatrix}, \tag{90}$$

from which

$$D = CBC^{-1}B = \begin{pmatrix} \alpha^{-1} & 0 \\ 1 - \alpha^2 & \alpha \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}, \tag{91}$$

where

$$k = \alpha(1 - \alpha^2). \tag{92}$$

Let $\mathfrak{H}_0$ be the subgroup of $\mathfrak{M}(2, q)$ generated by B, $-B$, and C. Then $\mathfrak{H}_0$ contains D and also

$$D_j = B^{-j}DB^j = \begin{pmatrix} 1 & 0 \\ \alpha^{2j}k & 1 \end{pmatrix}, \tag{93}$$

for all integers j. It follows that the matrices

$$D^t = \begin{pmatrix} 1 & 0 \\ kt & 1 \end{pmatrix}, \qquad (D_j)^t = \begin{pmatrix} 1 & 0 \\ \alpha^{2j}tk & 1 \end{pmatrix} \tag{94}$$

are in $\mathfrak{H}_0$ for all integers t and j.

When p is odd and m is odd, we have seen that $\mathfrak{F}_p$ contains an integer $u = \alpha^{2\sigma+1}$. Then there exists an integer j such that one of $\alpha^{2j}k$ and $\alpha^{2j}uk$ is equal to α. But then (93) implies that $\mathfrak{H}_0$ contains $I + \alpha^{2j+1}e_{21}$ for every

j, and (94) implies that $\mathfrak{H}_0$ contains $I + ye_{21}$ for every y of $\mathfrak{F}_q$. Thus $\mathfrak{H}_0$ also contains

$$T = \begin{pmatrix} 1 & 0 \\ -\alpha & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad T^{-1} = -T \tag{95}$$

and

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = I + ye_{12}. \tag{96}$$

It follows that $\mathfrak{H}_0 = \mathfrak{M}(2, q)$ as desired.

When $p = 2$ every nonzero element of $\mathfrak{F}_q$ is an even power of α, and (93) alone implies that $\mathfrak{H}_0$ contains $I + ye_{21}$ for every y of $\mathfrak{F}_q$. As before, we use (95) and (96) to see that $\mathfrak{H}_0 = \mathfrak{M}(2, q)$. There remains the case where p is odd but m is even, so that every $t \neq 0$ in $\mathfrak{F}_p$ is an even power of α.

Assume first that

$$k = \alpha(1 - \alpha)(1 + \alpha) = \alpha^{2\sigma}, \tag{97}$$

for an integral exponent σ. By (93) and (94) we see that $\mathfrak{H}_0$ contains

$$S = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \qquad S_j = B^{-j}SB^j = \begin{pmatrix} 1 & 0 \\ -\alpha^{2j} & 1 \end{pmatrix}, \tag{98}$$

and $\mathfrak{H}_0$ also contains

$$SC = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & \alpha - 1 \end{pmatrix}. \tag{99}$$

Also the matrices

$$S_0 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = S^{-1}, \qquad S_0 C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & \alpha + 1 \end{pmatrix} \tag{100}$$

are both in $\mathfrak{H}_0$. Since -1 is an even power of α and

$$k = \alpha(1 - \alpha)(1 + \alpha)$$

is an even power of α, we know that either $1 - \alpha$ or $1 + \alpha$ must be an even power of α. Hence $\mathfrak{H}_0$ contains a matrix

$$R = \begin{pmatrix} 0 & 1 \\ -1 & \alpha^{2i} \end{pmatrix} \tag{101}$$

for some integer i, and we use (98) to see that $\mathfrak{H}_0$ contains

$$T = \begin{pmatrix} 1 & 0 \\ -\alpha^{2i} & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & \alpha^{2i} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{102}$$

and

$$CT^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}. \tag{103}$$

But then $\mathfrak{H}_0$ contains all of the matrices $B^{-j}(CT^{-1})B^j = I + (\alpha^{2j+1})e_{21}$, and we combine this with the fact that $\mathfrak{H}_0$ contains the $(S_j)^{-1} = I + (\alpha^{2j})e_{21}$ to see that $\mathfrak{H}_0$ contains T and $I + ye_{21}$ for every y of $\mathfrak{F}_q$, so that $\mathfrak{H}_0 = \mathfrak{M}(2, q)$.

The only case not taken care of is that where

$$k = \alpha(1 - \alpha^2) = \alpha^{2\sigma+1}, \qquad 1 - \alpha^2 = \alpha^{2\sigma}.$$

By (93) we know that $\mathfrak{H}_0$ contains

$$E = E_0 = \begin{pmatrix} 1 & 0 \\ -\alpha & 0 \end{pmatrix}, \qquad E_j = B^{-j}EB^j = I - (\alpha^{2j+1})e_{21}, \tag{104}$$

and also contains

$$EC = \begin{pmatrix} 1 & 0 \\ -\alpha & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = T. \tag{105}$$

Also $\mathfrak{H}_0$ contains

$$E_j C = \begin{pmatrix} 1 & 0 \\ -\alpha^{2j+1} & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & k_j \end{pmatrix}, \tag{106}$$

where

$$k_j = \alpha(1 - \alpha^{2j}). \tag{107}$$

If there is an integer i such that $1 - \alpha^{2i}$ is an odd power of α, then

$$k_i = \alpha(1 - \alpha^{2i}) = \alpha^{2\sigma},$$

and $\mathfrak{H}_0$ contains

$$E_i(CT^{-1}) = \begin{pmatrix} 0 & 1 \\ -1 & \alpha^{2\sigma} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha^{2\sigma} & 1 \end{pmatrix}. \tag{108}$$

It is then a simple matter to conclude that $\mathfrak{H}_0 = \mathfrak{M}(2, q)$. However suppose that $1 - \alpha^{2i}$ is an even power of α for every i and thus that $1 + \alpha^{2i}$ is an even power of α. Then

$$\alpha^{2i} + \alpha^{2j} = \alpha^{2i}(1 + \alpha^{2p}) = \alpha^{2i}\alpha^{2\rho} = \alpha^{2(\rho+i)}.$$

It follows that the subset $\mathfrak{L}$ of $\mathfrak{F}_q$ consisting of zero and all even powers of the element α is a proper subfield of $\mathfrak{F}_q$ containing α^2. Hence $\mathfrak{F}_q = \mathfrak{L}(\alpha)$ has degree two over $\mathfrak{L}$, $m = 2\mu$, the period τ of α^2 divides $p^\mu - 1$, and the period of α must divide $2(p^\mu - 1)$. Since α is primitive, we see that

$$p^m - 1 = (p^\mu - 1)(p^\mu + 1)$$

divides $2(p^\mu - 1)$ and $p^\mu + 1$ divides 2, which is impossible since $p > 1$. This completes our proof.

7. The generators of the theorem

We are now ready to construct the generators A and B of our theorem. We use the matrix B of (88), and propose to determine a matrix

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \tag{109}$$

such that

$$a^2 + bc = -1, \tag{110}$$

so that A is unimodular. Note that

$$A^2 = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = -I, \tag{111}$$

so that the coset $A\mathfrak{N}$ has period two as desired. We shall also impose the requirement

$$AB^jA = \begin{pmatrix} 0 & \rho \\ -\rho^{-1} & \sigma \end{pmatrix}, \qquad \sigma \neq 0, \tag{112}$$

for a suitable value of j.

Every nonzero element δ of $\mathfrak{F}_q$ is a power

$$\delta = \alpha^j \tag{113}$$

of α. Then

$$\begin{aligned} D = AB^jA &= \begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}A \\ &= \begin{pmatrix} a\delta & b\delta^{-1} \\ c\delta & -a\delta^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} 0 & \rho \\ -\rho^{-1} & \sigma \end{pmatrix}, \end{aligned} \tag{114}$$

where we are requiring (110) and

$$a^2\delta + bc\delta^{-1} = (a^2\delta^2 + bc)\delta^{-1} = 0. \tag{115}$$

Use (110) to see that (115) becomes

$$d = a\delta, \qquad d^2 - a^2 = 1. \tag{116}$$

We also have

$$\rho = ab(\delta - \delta^{-1}), \qquad \sigma = bc\delta + a^2\delta^{-1}, \tag{117}$$

and the condition $ac(\delta - \delta^{-1}) = -\rho^{-1}$ will follow from the fact that A and B are unimodular.

When $p = 2$, we assume $q > 2$ and (116) is satisfied if

$$a \neq 1, \qquad \delta = 1 + a^{-1} \neq 0, \qquad d = a\delta = a(1 + a^{-1}) = a + 1.$$

Then

$$\begin{aligned} \sigma = bc\delta + a^2\delta^{-1} &= [(1 + a^2)(1 + a^{-2}) + a^2]\delta^{-1} \\ &= (1 + a^2 + a^{-2} + 1 + a^2)\delta^{-1} = a^{-2}\delta^{-1} \neq 0. \end{aligned}$$

Also $\rho = ab(\delta - \delta^{-1}) = ab(\delta^2 - 1)\delta^{-1} = a^{-1}b\delta^{-1} \neq 0$ if $b \neq 0$. We now form

$$B^iD = \begin{pmatrix} \alpha^i & 0 \\ 0 & \alpha^{-i} \end{pmatrix}\begin{pmatrix} 0 & \rho \\ -\rho^{-1} & \sigma \end{pmatrix} = \begin{pmatrix} 0 & \alpha^i\rho \\ -\alpha^{-i}\rho^{-1} & \alpha^{-i}\sigma \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & h \end{pmatrix} \tag{118}$$

if we select $\alpha^i = \rho^{-1}$, $\alpha^{-i} = \rho = a^{-1}b\delta^{-1}$, so that

$$h = \alpha^{-i}\sigma = a^{-3}\delta^{-2}b. \tag{119}$$

We can take

$$b = \alpha a^3\delta^2, \qquad c = (1 + a^2)b^{-1}, \qquad \delta = 1 + a^{-1}, \tag{120}$$

for any $a \neq 0, 1$ and have

$$h = \alpha, \qquad B^iD = C. \tag{121}$$

It follows that the group $\mathfrak{H}$ generated by A, $-A$, B contains C, and so $\mathfrak{H} = \mathfrak{M}(2, q)$. We state this result as follows.

LEMMA 9. *Let $p = 2$, $q > 2$, and take $a \neq 0, 1$, and b and c as in* (120). *Then the matrices A and B of* (109) *and* (88) *generate $\mathfrak{M}(2, q)$ and $A\mathfrak{N}$ has period two.*

The only case that remains is that where p is odd. Then the most general solution of (115) is given by

$$a = (w - w^{-1})/2, \qquad \delta = (w + w^{-1})/(w - w^{-1}), \tag{122}$$

where $w^2 \neq 1, -1$. But then

$$bc = -a^2\delta^2, \qquad bc\delta + a^2\delta^{-1} = \alpha^2\delta^{-1} - a^2\delta^3 = a^2\delta^{-1}(1 - \delta^4),$$

and we require that $\delta^4 \neq 1$,

$$\delta^2 \neq 0, 1, -1, \qquad ab \neq 0. \tag{123}$$

Since $\rho = -ab\delta^{-1}(1 - \delta^2) \neq 0$ if (123) is satisfied, we will have $\rho = \alpha^i$ for some i and will again have (118) where

$$h = \rho\cdot\sigma = -ab\delta^{-1}(1 - \delta^2)a^2\delta^{-1}(1 - \delta^4) = \alpha$$

for

$$b = a^{-3}\delta^2\alpha[(1 - \delta^2)(\delta^4 - 1)]^{-1}, \qquad c = -b^{-1}(1 + a^2). \tag{124}$$

It will then follow that the group $\mathfrak{H}$ generated by A, B, $-B$ contains C and hence is $\mathfrak{M}(2, q)$. The condition $\delta^2 \neq 1, -1$ is equivalent to

$$(w + w^{-1})^2 \neq (w - w^{-1})^2$$

and thus to $w^2 + w^{-2} + 2 \neq w^2 + w^{-2} - 2$, which is always true when p is odd, and to $w^2 + w^{-2} \neq 0$. But the relation $w^2 + w^{-2} = 0$ holds only if $w^4 = -1$. The condition $w^4 = -1$ is not satisfied for $w = \alpha$ unless $q = 9$, $p = 3$. When $q = 3$, we have $\alpha = 2$, $\alpha^2 = 1$, and (122) does not yield a solution since $\alpha = \alpha^{-1}$ and the denominator of δ in (122) vanishes. When $q = 5$, $\alpha = 2$ or 3, and (122) gives $\delta = 0$. Otherwise $\delta^2 \neq 0, 1, -1$, if we take $w = \alpha$. Thus we have derived the following result.

LEMMA 10. *Let p be odd and $q \neq 3, 5, 9$, and define the matrix of* (109) *by* (124) *and*

$$a = (\alpha - \alpha^{-1})/2, \qquad \delta = (\alpha + \alpha^{-1})/(\alpha - \alpha^{-1}). \tag{125}$$

Then the cosets $A\mathfrak{N}$ and $B\mathfrak{N}$ generate $\mathfrak{G}(2, q)$.

$\mathfrak{G}(2, 2) \cong \mathfrak{S}_3$, $\mathfrak{G}(2, 3) \cong \mathfrak{A}_4$, and $\mathfrak{G}(2, 5) \cong \mathfrak{A}_5$, and these three well-known groups possess two generators, one of order 2. $\mathfrak{G}(2, 9)$ has order 360 and is contained in the list of Brahana, so the proof of the theorem is complete.

THE UNIVERSITY OF CHICAGO
CHICAGO, ILLINOIS
THE UNIVERSITY OF CALIFORNIA
LOS ANGELES, CALIFORNIA