ON CHARACTERIZATIONS OF LINEAR GROUPS III

MICHIO SUZUKI

To Professor RICHARD BRAUER on the occasion of his sixtieth birthday

In his address at the International Congress of Mathematicians at Amsterdam [1] Professor R. Brauer proposed a problem of characterizing various groups of even order by the properties of the involutions contained in these groups and he gave characterizations of the general projective linear groups of low dimensions along these lines. The detail of the one-dimensional case has been published in [5], but the two-dimensional case has not appeared yet in detail. His work was followed by Suzuki [7], Feit [6] and Walter [11]. The present paper is a continuation of [7] and discusses a characterization of the two-dimensional projective unitary group over a finite field of characteristic 2. The precise conditions which characterize the group in question will be stated in the first section. The method employed here is similar to the one used in [7]. An application of group characters provides a formula for the order. However a difficulty comes in when one attempts to identify the group. In order to overcome this difficulty we will use a method primarily designed to study a class of doubly transitive permutation groups (cf. [9]). We need also a group theoretical characterization of a class of doubly transitive groups called (ZT)-groups. This is a generalization of a result in [8], and may be of independent interest.

1. Preliminaries. Let F denote the finite field of q elements. In this paper we consider the case when the characteristic of F is 2. We have

$$q = 2^n$$

for some integer n. If E is a quadratic extension of F, the mapping

$$a \to a^q \qquad (a \in E)$$

is an automorphism of E, which generates the Galois group of E/F. Let V

Received September 5, 1961. Reseach supported by NSF.

denote the three-dimensional vector space over E consisting of the triplets (x_1, x_2, x_3) of elements of E. The totality of linear transformations of V which leave the bilinear form

$$B(x, y) = x_1y_3^q + x_2y_2^q + x_3y_1^q$$

invariant forms a unitary group Γ. The two-dimensional projective unitary group $U = U(q)$ over F is the quotient group of Γ by its center. The element

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

is an involution of Γ and it is easy to see that every involution in U is conjugate to the coset of the center containing J. The centralizer $C_\Gamma(J)$ is the totality of matrices

$$\begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & a \end{pmatrix}$$

where $$a, b, c, d, e \in E,\ a^{1+q} = c^{1+q} = 1,$$
$$ae^q + bc^q = ad^q + b^{1+q} + da^q = 0.$$

Hence in U the centralizer of an involution is isomorphic to the group of matrices

$$M(a, b, c; d) = \begin{pmatrix} 1 & 0 & 0 \\ a & d & 0 \\ b & c & 1 \end{pmatrix}$$

where $$a, b, c, d \in E,\ d^{1+q} = 1,$$

(1) $$c^q + ad^q = 0,\ b + b^q = a^{1+q}.$$

We denote by $H = H(q)$ this group of matrices $M(a, b, c; d)$.

The main result of this paper is the following theorem.

THEOREM 1. *Let G be a finite group of even order satisfying the following conditions:*

(1) *the involutions of G form a single conjugate class,*

(2) *if x is an involution in G, its centralizer $C_G(x)$ is isomorphic to $H(q)$, and*

(3) *a Sylow 2-group of G is not a normal subgroup of G.*

If $q>2$, then G is isomorphic to the projective linear group $U(q)$. If $q=2$, G contains an abelian normal subgroup A such that G/A is isomorphic to $H(2)$.

In this last case the structure of A is not uniquely determined.

2. A few properties of the group $H(q)$. By computation we see that

$$M(a, b, c; d)M(a', b', c'; d') = M(a'', b'', c''; d'')$$

where $a'' = a + da'$, $b'' = b + b' + ca'$, $c'' = cd' + c'$ and $d'' = dd'$.

Hence the mapping $M(a, b, c; d) \to d$ is a homomorphism of the group H onto the multiplicative group of non-zero elements of E satisfying $x^{1+q} = 1$. The kernel of this homomorphism is the totality of matrices $M(a, b, c; 1)$, which is obviously a 2-group.

(I) The group $H(q)$ contains a normal 2-group $Q = Q(q)$ such that H/Q is a cyclic group of order $1+q$. The order of Q is q^3.

If $M(a, b, c; d) \in Q$, we have $d = 1$. Hence the conditions (1) become

$$a^q = c \quad \text{and} \quad b + b^q = a^{1+q}. \tag{2}$$

Hence for a given a, there exist exactly q choices for b. The last assertion of (I) follows immediately.

(II) The center of Q consists of elements of order $\leqq 2$ and contains all the involutions of Q. Its order is exactly q.

(III) If the order of an element $x \neq 1$ of H divides $q+1$, then the centralizer $C_H(x)$ is an abelian group of order $q(q+1)$ containing all the involutions of H.

These two properties are proved by easy computations. From the second property it follows that the group Q is a quaternion group of order 8 if $q = 2$.

3. General properties of the group G. Let G be a group satisfying the conditions of Theorem 1. We shall prove a few properties of G in this section. Throughout this and subsequent sections, except § 6, $H = H(q)$ stands for the group defined in the second section. Also the letter $Q = Q(q)$ is reserved for the Sylow 2-group of $H(q)$.

LEMMA 1. *A Sylow 2-group of G is isomorphic to Q.*

Proof. By assumption if x is an involution in the center of a Sylow 2-group S of G, $C_G(x)$ is isomorphic to $H(q)$. From the choice of x, $C_G(x)$ contains S.

Hence S must be isomorphic to Q.

LEMMA 2. *If S and S' are two distinct Sylow 2-groups of G, then $S \cap S' = \{1\}$.*

Proof. Suppose $S \cap S' \neq \{1\}$. Then there is an involution t of G contained in $S \cap S'$. Both S and S' are isomorphic to Q by Lemma 1. According to (II) t belongs to the center of S and at the same time to the center of S'. Hence both S and S' are Sylow 2-groups of $C_G(t)$. By assumption $C_G(t)$ is isomorphic to $H(q)$ which contains only one Sylow 2-group. This contradiction proves Lemma 2.

LEMMA 3. *Two involutions of S are conjugate in $N_G(S)$.*

This is an immediate consequence of Lemma 2 and the first condition on G.

LEMMA 4. *The order of $N_G(S)$ is $q^3(q^2-1)$.*

Proof. Represent $N_G(S)$ as a permutation group on the involutions of S. The subgroup leaving one involution, say t, fixed is $C_G(t)$. Hence the order of $N_G(S)$ is the order of $C_G(t)$ multiplied by the number of involutions in S. The assertion follows from (I) and (II).

LEMMA 5. *If t is an involution of S, then the normalizer of $C_G(t)$ is $N_G(S)$.*

Proof. Since $C_G(t) \cong H$, $C_G(t)$ contains all the involutions of S in its center. Hence every element of $N_G(S)$ transforms $C_G(t)$ into itself. On the other hand the normalizer of $C_G(t)$ is contained in $N_G(S)$ since S is a characteristic subgroup of $C_G(t)$.

4. The case $q=2$. If $q=2$, a Sylow 2-group S of G is a quaternion group. By a theorem of Brauer [4] G is not simple; in fact if N is the maximal normal subgroup of odd order, then G/N contains exactly one involution. This implies that $G = NC_G(t)$. By assumption, $C_G(t)$ is isomorphic to the group $H(2)$. By (III) of §2, $C_G(t)$ contains no non-trivial normal subgroup of odd order. The intersection $N \cap C_G(t)$ is however a normal subgroup of $C_G(t)$ and of odd order. Hence we have $N \cap C_G(t) = \{1\}$. This implies that the element t induces an automorphism of order 2 in N which leaves only the identity element fixed. By a result of Burnside N is an abelian group. Hence G is a solvable group. In this case the structure of N is not uniquely determined. The projective

unitary group $U(2)$ is obtained if N is a non-cyclic group of order 9.

From now on we assume that $q>2$.

5. The centralizer of 2-regular elements. Let S be a Sylow 2-group of G and let t be an involution contained in S. By the second condition on G, $C_G(t)$ is isomorphic to $H(q)$. We are interested in the following set D of elements: D is the totality of 2-regular elements $x \neq 1$ of $C_G(t)$. If $x \in D$, then by (III) $C_G(x) \cap C_G(t)$ is an abelian subgroup of order $q(q+1)$. Let S_0 denote the center of S. Then we have

$$C_G(x) \cap S = S_0.$$

LEMMA 6. *The group S_0 is a Sylow 2-group of $C_G(x)$ for all $x \in D$.*

Proof. S_0 is contained in a Sylow 2-group T of $C_G(x)$ and the group T is contained in a Sylow 2-group R of G. Then R and S are two Sylow 2-groups of G such that $R \cap S \supseteq S_0 \neq \{1\}$. By Lemma 2 we conclude that $R = S$ and hence

$$S_0 \subseteq T \subseteq R \cap C_G(x) = S \cap C_G(x) = S_0.$$

LEMMA 7. *If $x \in D$, $C_G(x)$ satisfies the property that the centralizer of any involution is abelian.*

Proof. Since S_0 is a Sylow 2-group of $C_G(x)$, it suffices to prove the assertion for an involution t of S_0. Then by (III) of the section 2, $C_G(x) \cap C_G(t)$ is an abelian group. It is clear that $C_G(x) \cap C_G(t)$ is the centralizer of t in $C_G(x)$.

On account of Lemma 7 the result of [7] is applicable to $C_G(x)$.

LEMMA 8. *We have one of two cases:*

$C_G(x) \subseteq N_G(S)$ for all $x \in D$, or

$C_G(x) \cong LF(2, q) \times Z$ for all $x \in D$, where Z is a cyclic group of order $q+1$.

Proof. If $x \in D$, the centralizer $C_G(x) = W$ satisfies the condition that the centralizer of any involution of W is an abelian group of order $q(q+1)$. By Lemma 6 the group S_0 is a Sylow 2-group of W and it is an elementary abelian group of order q. The main theorem of [7, *I*] says that we have one of three possibilities: (1) a Sylow 2-group of W is cyclic, (2) a Sylow 2-group of W is normal, or (3) W is direct product of the linear group $LF(2, q)$ and an abelian group X of odd order.

Since we have assumed that $q>2$, S_0 is not cyclic, so the first possibility does not occur. Suppose that for some $x\in D$ we have the third case; i.e. $W=L\times X$ where $L\cong LF(2, q)$. Since the center of $LF(2, q)$ is trivial, X coincides with the center of W. By definition x is contained in the center of W. This implies that $x\in X$. If y is an involution of W, y is contained in L. It follows from the structure of $LF(2, q)$ that the centralizer $C_L(y)$ of y is an abelian group of order q. Hence $C_W(y)=C_L(y)\times X$. We have seen that $C_W(y)$ is an abelian group of order $q(q+1)$. This means that X is an abelian group of order $q+1$. Since $x\in D$, W contains S_0. If t is an involution of S_0, $S_0\times X$ is the centralizer of t in W. The order of X is $q+1$. Hence we conclude that

$$S_0\times X=C_G(x)\cap C_G(t).$$

Since $C_G(t)\cong H(q)$ it follows from the structure of $H(q)$ that X is a cyclic group of order $q+1$ and that any element of D is conjugate to an element of X. Hence for all $x\in D$ we have

$$C_G(x)\cong L\times X.$$

If we have the second possibility for all $x\in D$, then $C_G(x)$ is contained in $N_G(S_0)$. By Lemma 2, $N_G(S_0)$ is a part of $N_G(S)$. This proves the assertion.

6. A characterization of (ZT)-groups. A doubly transitive permutation group G of odd degree d is called a (ZT)-group if no element $\neq 1$ leaves three different letters invariant and G contains no normal subgroup of order d. This class of groups has been studied in detail (cf. [9]) and some group theoretical characterizations have been given [8]. In this paper we need a generalization of a theorem in [8].

THEOREM 2. *Let G be a finite group. Assume that G contains a subgroup H satisfying the following conditions:*

(1) *the subgroup H_0 of H generated by the involutions of H has a non-trivial center,*

(2) *if $x\in H$, $x\neq 1$, then the elements y satisfying*

$$y^{-1}xy=x \text{ or } x^{-1}$$

belong to $N_G(H)$, and

(3) *if $x\in H$ is an involution, $C_G(x)$ is a part of H.*

Then we have one of the following cases: (a) H_0 *is a normal subgroup of* G, (b) *a Sylow 2-group of* G *is either cyclic or a generalized quaternion group or* (c) G *is a* (ZT)*-group.*

For convenience we denote by $C_G^*(x)$ the set of elements $y \in G$ such that $y^{-1}xy = x$ or x^{-1}. Then clearly $C_G^*(x)$ is a subgroup of G containing $C_G(x)$ as a normal subgroup of index 1 or 2. Replacing the conditions (2) and (3) by

$$(2)' \qquad C_G^*(x) \subseteqq H \quad \text{for all} \quad x \neq 1 \text{ of } H,$$

we have proved a similar theorem in [8]. The proof of Theorem 2 is a modification of the proof in [8].

First of all we remark that H contains a Sylow 2-group of G by (3). Hence the index $[N_G(H) : H]$ is odd and every involution of $N_G(H)$ is contained in H. An element of a group is called strongly real if it is a product of two distinct involutions.

LEMMA 9. *If an element* x *of* H *is strongly real, then* x *is a product of two involutions of* H.

Proof. Suppose that x is a product of two involutions u and v. We want to prove that $u \in H$. Since $u^{-1}xu = u^{-1}(uv)u = x^{-1}$, u is contained in $C_G^*(x)$. By (2), $C_G^*(x) \subseteqq N_G(H)$. Hence u is an involution of $N_G(H)$ and so $u \in H$.

It follows from Lemma 9 that each coset of H except H itself contains at most one involution. Assume that H_0 is not normal. Then the argument in [8] shows that G contains only one conjugate class of involutions and that for any involution u of H we have $C_G(u) = H$. Combining with Lemma 9 we conclude that a strongly real element of H is an involution. Furthermore we see that $H = C_G(H_0)$. This implies that two involutions of H are conjugate in $N_G(H)$. Then each coset of H not contained in $N_G(H)$ contains exactly one involution.

LEMMA 10. *If* $x \in N_G(H) - H$ *is strongly real,* $C_G(x) \subseteqq N_G(H)$.

Proof. Suppose not. Then there exist $y \in H$ and an involution u not contained in H such that $xyu = yux$. Then

$$y^{-1}xy = uxu \quad \text{and} \quad x^{-1}y^{-1}xy = x^{-1}uxu.$$

The right side of the last equation belongs to H since $x \in N_G(H)$. By Lemma

9 we have $x^{-1}ux=u$. This means that x is a strongly real element of $C_G(u)$. The group $C_G(u)$ is conjugate to H. Lemma 9 applied to $C_G(u)$ says that x is an involution. This not the case since $x\in N_G(H)$ but is not in H.

LEMMA 11. *If $x\in N_G(H)-H$ is strongly real, then $A=C_G(x)$ satisfies the following properties:*

(i) *A is an abelian group of odd order,*

(ii) *if $y\neq 1$ and $y\in A$, y is strongly real,*

(iii) *if $y\neq 1$ and $y\in A$, then $C_G(y)=A$, and*

(iv) $N_G(A)\cap N_G(H)=A$.

Proof. By assumption x is a product uv of two involutions u and v. Then $u\in C_G^*(x)$ and hence $u\in N_G(A)$. Suppose that an element $w\neq 1$ of A commutes with u. Put $H'=C_G(u)$. Then H' is conjugate to H and H' contains w. Since $w\in A$, x is in the centralizer $C_G(w)$. By the second assumption on H, applied to the conjugate subgroup H', we see that $C_G(w)\subseteqq N_G(H')$. Then x is contained in $N_G(H')$. Since $u\in H'$, we have $x^{-1}u^{-1}xu\in H'$. On the other hand $x^{-1}u^{-1}xu=x^{-1}\cdot x^{-1}=x^{-2}$. Hence x^2 commutes with u. This implies that $x^4=1$. This is impossible as $x\in N_G(H)-H$. Therefore there is no element $\neq 1$ of A which commutes with u. A result of Burnside shows the validity of the properties (i) and (ii). If $y\neq 1$ is an element of A, y is strongly real by (ii). Hence $C_G(y)$ is abelian by (i). This proves the property (iii).

Put $K=N_G(A)\cap N_G(H)$. A is a part of K by Lemma 10. The conditions (i) and (ii) together with Lemma 9 imply that $A\cap H=\{1\}$. It follows from (iii) that the group H_0A is a Frobenius group. If $K\neq A$, KH_0 can not be a Frobenius group. Then K contains an element $z\neq 1$ which commutes with an involution of H_0. This implies that

$$K\cap H\ni z\neq 1.$$

By the isomorphism theorem $K\cap H$ is a normal subgroup of K. Since $A\cap H=\{1\}$, $K\cap H$ is contained in the centralizer of A. This means that

$$K\cap H\subseteqq C_G(A)\cap H=A\cap H=\{1\}.$$

This contradiction proves the last property (iv).

We return to the proof of Theorem 2. We assume that H_0 is not normal in G and that Sylow 2-groups of G are neither cyclic nor generalized quaternion

groups. Then as in [8] we see that $N_G(H) \neq H$. Hence $N_G(H) - H$ contains at least one strongly real element x. By Lemma 11 we see that the transfer theorem of Burnside (in a generalized form) is applicable. We conclude that $N_G(H)$ contains a normal subgroup N such that $N_G(H) = NA$ and $N \cap A = \{1\}$. By Lemma 11 (iii), $N_G(H)$ is a Frobenius group and N is its Frobenius kernel. By a theorem of Thompson [10] N is nilpotent. Since A is of odd order, N is of even order and is a centralizer of an involution. Hence N coincides with H. If $x \neq 1$ is an element of H, $C_G^*(x)$ is contained in $N_G(H)$ by the second assumption of Theorem 2. However $N_G(H)$ is a Frobenius group. Hence $C_G(x)$ is contained in H. Since $N_G(H)/H$ is of odd order, $C_G^*(x)$ is also a part of H. By a theorem of [8] we conclude that G is a (ZT)-group.

7. Further study of the centralizer of the elements in D. The set D of elements has been defined in § 5. We continue the study of the structure of $C_G(x)$ for $x \in D$. Put $M = C_G(x)$.

LEMMA 12. *M is a direct product of two groups L and Z such that $L \cong LF(2, q)$, $q > 2$, and Z is a cyclic group of order $q+1$. M is the normalizer of any subgroup $\neq \{1\}$ of Z.*

Proof. By Lemma 8 we have two possibilities. Suppose that $C_G(x)$ is a part of $N_G(S)$ for all $x \in D$. For an involution t of S put $T = C_G(t)$. Then for any involution u of S we have $C_G(u) = T$ since $T \cong H(q)$. We want to show that the subgroup T satisfies all the assumptions for H of Theorem 2. The involutions of T generate the subgroup S_0 which is elementary abelian. So the first condition is trivially satisfied. Take $x \neq 1$ of T. If the order of x is even, some power of x is an involution u of T. Then $u \in S$ and $C_G^*(x) \subseteq C_G(u) = T$. If the order of x is odd, x belongs to the set D. Hence by assumption $C_G(x)$ is a part of $N_G(S)$, which is by Lemma 5 the normalizer of T. We claim that if $x \in D$, $C_G^*(x) = C_G(x)$. If not, the index $[C_G^*(x) : C_G(x)]$ is 2. Hence $C_G^*(x)$ contains a Sylow 2-group S^* which covers S_0. By Lemma 2 S^* is a part of S. This is impossible since $C_T^*(x) = C_T(x)$. This verifies the second condition. The third one is trivial. By Theorem 2 we have several possibilities.

A Sylow 2-group S of G contains exactly $q-1$ involutions. We have assumed that $q > 2$. This eliminates the second possibility in Theorem 2. If G were a (ZT)-group, the order of its Sylow 2-group would be q or q^2 (cf. [9]).

This is not the case. The remaining possibility is that S_0 is a normal subgroup of G. By Lemma 2 this means that S is a normal subgroup. This case has been excluded. Hence for all $x \in D$, the centralizer $C_G(x)$ is the direct product of two groups L and Z, where L is isomorphic to $LF(2, q)$ and Z is a cyclic group of order $q+1$.

It remains to prove the last assertion. As remarked earlier in the proof of Lemma 8 any element of D in conjugate to an element of Z and conversely an element $\neq 1$ of Z belongs to D. By Lemma 8 the order of $C_G(x)$ is independent of the choice of x. If $M = C_G(x)$ for some $x \in D$, and if $M = L \times Z$, then $x \in Z$ and for any $y \neq 1$ of Z we have $C_G(y) = M$. Consider $N_G(Z_0)$ for a subgroup $Z_0 \neq \{1\}$ of Z. Then $N_G(Z_0) \cap C_G(t)$ for an involution t of S is abelian. Hence $N_G(Z_0)$ satisfies the assumption of the main theorem of [7]. Since $N_G(Z_0) \subseteq M$, $N_G(Z_0)$ is the direct product of the linear group and an abelian group. This implies that $N_G(Z_0) = C_G(Z_0)$. The assertion follows immediately.

8. **The order of G.** By Lemma 12 we see that all the assumptions of the second section of [7, *I*] are satisfied for G. We apply Propositions 5 and 6 of [7, *I*] to obtain the order of G.

It follows from Proposition 6 of [7, *I*] that the order g of G has the form

$$g = q^6 m(q^2-1) f(f+\varepsilon)/(f-a)^2 \qquad (\varepsilon = \pm 1) \tag{3}$$

where f is the degree of an irreducible character X, $m(q^2-1)$ is the order of some subgroup of G and a is the value of X on an involution. From Proposition 5 of [7, *I*] we get a congruence:

$$m \equiv 1 \pmod{2(q-1)}. \tag{4}$$

If $q > 4$, the degree f satisfies $f \equiv \varepsilon \pmod{m(p-1)}$. Hence we have

$$f(f+\varepsilon) \equiv 2 \pmod{m(q-1)}. \tag{5}$$

There are $(q/2)-1$ irreducible characters Y_i of degree $f+\varepsilon$ and the relations

$$X + \varepsilon = Y_i \qquad (i = 1, 2, \ldots \quad (q/2)-1) \tag{6}$$

are valid for all elements of order relatively prime to $q-1$. In particular the relations (6) are true for all elements of order 2 and 4. If we denote the degree of Y_i by f' and the value of Y_i on the involutions by a', the formula (3) can be written as

$$g = q^6 m(q^2-1)ff'/(f'-a')^2. \tag{7}$$

Hence the order formula (3) is symmetrical with respect to f and f'. The congruence (5) is also symmetric. The following lemma is crucial.

LEMMA 13. $f-a=f'-a' \equiv 0 \pmod{q^2}$.

Proof. Consider the group $N=N_G(S)$. The factor group N/S is a group of order q^2-1 by Lemma 4. If t is an involution of S, $C_G(t)$ is of the form SZ where Z is a cyclic group of order $q+1$. If $M=C_G(Z)$, M is the direct product of Z and a group L isomorphic to $LF(2, q)$. If S_0 is the center of S, L contains S_0. From the structure of L we conclude that there is a cyclic group C of order $q-1$ of L which normalizes S_0. Since Sylow 2-groups of G are independent C normalizes S. Therefore the normalizer N of S contains a cyclic group K of order q^2-1. This means that $N=SK$.

We claim that K acts on S/S_0 transitively. Suppose that an element k of K leaves an element of S/S_0 invariant. Then there is a subgroup A of order $2q$ in S such that $k^{-1}Ak=A$. Since S_0 is the center of S and $[A:S_0]=2$, A is abelian. The squares of the elements of A form a characteristic subgroup of order 2. If this group of order 2 is generated by c, then $k^{-1}ck=c$. Hence k is in $C_G(c)$. By assumption $C_G(c)$ is isomorphic to $H(q)$. It is easy to see that no element $\neq 1$ of odd order in $C_G(c)$ commutes with a subgroup of order $2q$. This proves that the group K acts regularly and hence transitively on S/S_0.

It is not difficult to prove that the group N has q^2-1 linear characters, one character of degree q^2-1 and $q+1$ characters of degree $q(q-1)$, which are irreducible. The values of these characters on elements of order 2 and 4 are listed in the table below.

1	1	1
q^2-1	q^2-1	-1
$q(q-1)$	$-q$	0

The first column indicates the degrees, the second the values on the involutions and the last one is the values on the elements of order 4. Note that all the elements of order 4 are conjugate in N.

The character X of degree f decomposes into a sum of irreducible characters

of N. Suppose that this decomposition contains exactly x linear characters, y characters of degree q^2-1 and z characters of degree $q(q-1)$. Then we obtain

$$\begin{aligned} f &= x+(q^2-1)y+q(q-1)z, \\ a &= x+(q^2-1)y-qz, \\ b &= x-y, \end{aligned} \tag{8}$$

where b is the value of X on the elements of order 4. We have immediately

$$f-a=q^2z. \tag{9}$$

This proves Lemma 13. We also remark that the numbers x, y and z in (8) are non-negative integers.

Since the order g of G is divisible by q^3, we see from (7) and Lemma 13 that $ff'\equiv 0 \pmod{q}$. Since $f'=f\pm 1$, q must divide either f or f'. Without loss of generality we may assume that

$$f\equiv 0 \pmod{q}. \tag{10}$$

As remarked earlier, $b-1$ or $b+1$ is the value of some irreducible charater of G. The orthogonality relation of group characters implies that

$$1+b^2+(b\pm 1)^2\leqq q^2,$$

since the order of the centralizer of any element of order 4 is q^2. The formulas (8) and (10) imply that $b\equiv 0 \pmod{q}$. Combined with the above inequality we conclude that

$$b=0. \tag{11}$$

Let 2^m and 2^l be the exact power of 2 dividing $f-a$ and f respectively. Comparing the power of 2 dividing both sides of (7) we get

$$3n=6n+l-2m,$$

where we used the equation $q=2^n$. We want to show that $l=3n$.

By (9) and (10) we may write

$$m=2n+m' \quad \text{and} \quad l=n+l'$$

with non-negative m' and l'. We have $l'=2m'$. Hence the assertion $l=3n$ is equivalent to the relation $m'\geqq n$.

By way of contradiction assume that $m'<n$. The orthogonality relation implies that

$$f+(q-1)a \equiv f-a+aq \equiv 0 \pmod{q^3}.$$

This congruence is obtained by summing X over S and observing the formula (11). The term $f-a$ is divisible by 2^m and $m<3n$. Hence the term aq must be divisible by the same power of 2. This means that $2^{n+m'}$ is the exact power of 2 dividing a. The exact exponent of 2 dividing $(f-a)+a$ is therefore $n+m'$. By definition we have $l=n+m'$ or $l'=m'$. This together with the previously obtained equation $l'=2m'$ implies that $l'=m'=0$.

We write

$$f=qu. \tag{12}$$

The previous discussion proves that u in (12) and z in (9) are odd integers. The order formula (7) is now

$$g=q^3m(q^2-1)u(qu\pm 1)/z^2.$$

Both qu and $qu\pm 1$ are degrees of irreducible characters, so that they divide the group order. Since z^2 is odd we see that z^2 is a divisor of $m(q^2-1)$. On the other hand

$$q^3u(qu\pm 1)/z^2$$

is an integer because it is the index of a subgroup of G. Hence z^2 divides $qu(qu\pm 1)$. Suppose that $q>4$. Then by (5), $qu(qu\pm 1)$ is relatively prime to $m(q-1)$. Hence we conclude that z^2 is a divisor of $q+1$. We have

$$a=qw \text{ with } w=u-qz=qy-z. \tag{13}$$

There are $(q/2)$ irreducible characters of G with values either a or $a\pm 1$ on the involutions. Hence the orthogonality relation implies that

$$(q/2)(|a|-1)^2<q^3(q+1). \tag{14}$$

We write this inequality in the form

$$(u+z-qz-z\pm(1/q))^2<2(q-1). \tag{15}$$

By definition we have $u+z\equiv 0 \pmod{q}$, which implies that

$$u-(q-1)z\equiv 0 \pmod{q}.$$

We have shown that z is a positive integer whose square is a divisor of $q+1$. If $u\neq(q-1)z$, the right side of (15) is larger than $(q-z-(1/q))^2$. Since z^2

divides $q+1$, $z \leqq (q/2)-1$. For $z>(q/2)-1$ would imply

$$q+1 \geqq z^2 > (q-2)^2/4, \text{ or } q<8.$$

We are assuming $q \geqq 8$. The inequality (15) implies

$$(q-z-(1/q))^2 < 2(q+1)$$

or

$$(q-2(z+1))q+(z+(1/q))^2<4.$$

Since the first term is non-negative, we get $z=1$ and $q=4$. This is not the case. Hence $u=(q-1)z$. This is however impossible because of the congruence (5) which is written as

$$qu(qu \pm 1) \equiv 2 \pmod{m(q-1)}.$$

It remains to treat the case $q=4$. We get the inequality (14). Since $q=4$, we obtain a bound for a. We have $|a| \leqq 13$. This gives an upper bound 3 for $|w|$ (see (13)). By definition $u=w+4z$ and z^2 is a divisor of

$$u(4u \pm 1) = (4z+w)(16z+4w \pm 1).$$

In particular z is a divisor of $w(4w \pm 1)$. Since $|w| \leqq 3$, we have a very small number of possibilities for z and hence for u. Only the values 1, 3, 5 are possible for z. The formula (13) gives the corresponding values of w and u. We have the following four possibilities:

z	w	u	$qu \pm 1$
1	-1	3	11, 13
1	3	7	27, 29
3	-3	9	35, 37
5	-1	19	75

It follows from Proposition 5 of [7, I] that the subgroup B of order $(q-1)m$ satisfies the property that $B \cap v^{-1}Bv = \{1\}$ if $v^{-1}Bv \neq B$. Hence the index of $N_G(B)$ is congruent to 1 mod $3m$. The index of $N_G(B)$ is again by Proposition 5 of [7, I] $q^3u(qu \pm 1)/2z^2$. In particular $u(qu \pm 1)$ is prime to 3. This eliminates all the possibilities but one. In the remaining case we have

$$q^3u(qu \pm 1)/2z^2 = 32 \cdot 7 \cdot 29 = 6496.$$

Hence m is a divisor of $2165 = 5 \cdot 433$. The congruence (4) implies that $m \equiv 1 \pmod{10}$. The only possibility is $m=1$. The order of G is $64 \cdot 7 \cdot 29 \cdot 15$ and

the index of $N=N_G(S)$ is $7\cdot 27$. By Lemma 2 the index $[G:N]$ is congruent to 1 modulo 64. This is not the case as $7\cdot 29\equiv 1 \pmod{64}$.

We have shown that $l=3n$. In other words f is divisible by q^3, which is the highest power of 2 dividing the group order g. Hence by a theorem of Brauer-Nesbitt [3] the character X of degree f vanishes on 2-singular elements. In particular we have $a=0$. Put $f=q^3v$. The order formula (3) is now

$$g=q^3(q^2-1)m(q^3v\pm 1)/v.$$

As before $q^3(q^3v\pm 1)/v$ is an integer and v is odd. This means that v is a divisor of $q^3v\pm 1$ and hence $v=1$.

Since the order of M is divisible by $(q+1)^2$ (cf. Lemma 12), $m(q^3\pm 1)$ is a multiple of $q+1$. By (4) m is prime to $q+1$. Hence we have the plus sign. Being the index of $N_G(S)$, $m(q^3+1)$ is congruent to 1 modulo q^3. Hence

$$m\equiv 1 \pmod{q^3}. \tag{16}$$

If $q>4$, q^3 or q^3+1 is congruent to 1 modulo $m(q-1)$. This implies that m is smaller than q^3. The above congruence gives the value $m=1$. If $q=4$, this argument does not apply. However

$$q^3(q^3+1)/2=32\cdot 65=2080$$

is the index of the subgroup $N_G(B)$ and is congruent to 1 modulo $3m$. Hence m is a divisor of 693. No divisor of 693 except 1 satisfies the congruence (16).

We have proved the following proposition.

PROPOSITION. *The order g of G is $q^3(q^2-1)(q^3+1)$.*

COROLLARY. *G is represented as a doubly transitive permutation group of degree q^3+1, in which $N=N_G(S)$ is one of the subgroups leaving one symbol invariant.*

Proof. Represent G as a permutation group Γ on the cosets of N. Since the degree is q^3+1, the Sylow 2-group S of N is regular on the cosets $X\neq N$. For if $1\neq x\in S$ leaves a coset Y invariant, we have $Yx=Y$. If $Y=Ny$, yxy^{-1} belongs to N. Since x is of order a power of 2, yxy^{-1} is contained in S. Then $ySy^{-1}\cap S\neq\{1\}$. By Lemma 2 we have $ySy^{-1}=S$ and $y\in N_G(S)=N$. This proves that Γ is doubly transitive.

9. The structure of $N_G(S)$. In this section we study the structure of the

normalizer $N=N_G(S)$ of a Sylow 2-group S. The group S is by Lemma 1 isomorphic to the group Q of the matrices $M(a, b, c; 1)$ with $c=a^q$ and $b+b^q=a^{1+q}$ (cf. (2) of §2) where a, b, c are elements in the field E of q^2 elements. We take a fixed isomorphism of S onto Q and label the elements of S by the pairs (a, b) of field elements a and b of E. The structure of S is given by the multiplication table for pairs:

$$(a, b)\ (c, d)=(a+c,\ a^q c+b+d). \tag{17}$$

As remarked in the proof of Lemma 13, N contains a cyclic group K of order q^2-1 which acts on S/S_0 regularly. Here we denote by S_0 the center of S. From (17) it follows that S_0 is the totality of pairs $(0, b)$ with $b=b^q$. Hence the mapping $(a, b)\to a$ defines an isomorphism of S/S_0 onto the additive group of E. Since K acts regularly we may identify the group K as the multiplicative group of non-zero elements of E. If $k\in K$, then k is a non-zero element of E and the action of k on S/S_0 is that of left multiplication. Hence we may write

$$k^{-1}(a, b)k=(ka, b^*) \tag{18}$$

where b^* depends on k, a and b. Taking the square of both sides we get

$$k^{-1}(0, c)k=(0, k^{1+q}c). \tag{19}$$

Put $a=1$ in (18). Then b^* is a function of k and b. We write

$$k^{-1}(1, b)k=(k, b^*(k, b)).$$

Multiply (19) to the right. After a simple computation we get

$$b^*(k, b+c)=b^*(k, b)+k^{1+q}c.$$

This implies that $b^*(k, b)+k^{1+q}b$ does not depend on b. We write therefore

$$k^{-1}(1, b)k=(k, k^{1+q}b+\psi(k)), \tag{20}$$

which serves as the defining equation of the function $\psi(k)$. By (2) b satisfies the equation $b+b^q=1$. Hence $\psi(k)$ lies in F since $\psi(k)^q=\psi(k)$. For arbitrary (a, b) with $a\neq 0$, we can find b' such that

$$(a, b)=a^{-1}(1, b')a.$$

It is only necessary to check that the element b' defined by

$$b' = (b + \psi(a))a^{-(1+q)}$$

satisfies the requirements. This is easily done. The formula (18) now becomes

$$k^{-1}(a, b)k = (ka, k^{1+q}b + \psi(k; a)) \tag{21}$$

where $$\psi(k; a) = k^{1+q}\psi(a) + \psi(ak).$$

This function $\psi(k; a)$ satisfies various properties. First of all it is linear with respect to a:

$$\psi(k; a + a') = \psi(k; a) + \psi(k; a') \quad \text{for a fixed } k. \tag{22}$$

This is an easy consequence of the formula (17). Transform (21) by another element l of K. Then we get

$$\psi(kl; a) = l^{1+q}\psi(k; a) + \psi(l; ka). \tag{23}$$

LEMMA 14. *We may assume that* $\psi(k; a) = 0$ *for all* k *and* a.

Proof. Let $K^* = \{k^*\}$ be the cyclic group isomorphic to K. The correspondence $k \to k^*$ is assumed to be an isomorphism. Define a semi-direct product N^* of S and K^* by defining

$$k^{*-1}(a, b)k^* = (ka, k^{1+q}b). \tag{24}$$

We shall prove that the group N^* is isomorphic to N.

Suppose that y is generator of K. If λ is an additive mapping defined on E taking values in F, the function definend by

$$\mu(a) = \lambda(ay) + \lambda(a)y^{1+q}$$

is additive. The mapping $\lambda \to \mu$ of Hom (E^+, F^+) into itself is one-to-one. For if $\lambda(ay) = \lambda(a)y^{1+q}$ for all $a \in E$, then

$$\lambda(ay^m) = \lambda(a)y^{m(1+q)} \quad \text{for all } m.$$

Since y is a generator of E, we have for all $a \in E$

$$\lambda(a) = ca^{1+q} \quad \text{with } c = \lambda(1).$$

Then for any pair a, b of elements of E

$$\lambda(a + b) = c(a + b)^{1+q} = \lambda(a) + \lambda(b) = c(a^{1+q} + b^{1+q}),$$

or $$c(a^q b + ab^q) = 0.$$

This means that $c = 0$ and $\lambda = 0$. Since Hom (E^+, F^+) is finite, the mapping

$\lambda \to \mu$ is onto. Since the function $\psi(y;\ a)$ is additive, there is an additive mapping θ of E into F such that

$$\psi(y;\ a) = \theta(ay) + \theta(a)y^{1+q} \qquad \text{for all } a \in E.$$

We prove that

$$\psi(y^m;\ a) = \theta(ay^m) + \theta(a)y^{m(1+q)} \qquad \text{for all } a \in E.$$

If $m = 1$, this is the defining relation of θ. Assume that $m > 1$. Then by induction

$$\begin{aligned}\theta(ay^m) + \theta(a)y^{m(1+q)} &= \theta(ay \cdot y^{m-1}) + \theta(ay)y^{(m-1)(1+q)} \\ &\quad (\theta(ay) + \theta(a)y^{1+q})y^{(m-1)(1+q)} \\ &= \psi(y^{m-1};\ ay) + \psi(y;\ a)y^{(m-1)(1+q)}.\end{aligned}$$

This is equal to $\psi(y^m;\ a)$ by (23). Hence for any $k \in K$

$$\psi(k;\ a) = \theta(ak) + \theta(a)k^{1+q} \qquad \text{for all } a \in E. \tag{25}$$

Define a mapping σ of S into S by

$$\sigma(a,\ b) = (a,\ b + \theta(a)).$$

Then σ is an automorphism of S. Extend σ to a mapping σ^* of N^* into N by defining $\sigma^*(k^*) = k$ and $\sigma^* | S = \sigma$. Then

$$\begin{aligned}\sigma^*(k^{*-1}(a,\ b)k^*) &= \sigma^*(ka,\ k^{1+q}b) \\ &= (ka,\ k^{1+q}b + \theta(ak)) \\ &= (ka,\ k^{1+q}b + k^{1+q}\theta(a) + \psi(k;\ a)) \\ &= k^{-1}(a,\ b + \theta(a))k \\ &= k^{-1}\sigma(a,\ b)k.\end{aligned}$$

This prove that σ^* is an isomorphism of N^* onto N.

It follows that the structure of N is completely determined by the formulas (17) and (24).

10. Structure equations of G. As before let N denote the normalizer $N_G(S)$ of a Sylow 2-group S. We have shown that N is a semi-direct product of S and a cyclic group K. In the preceding section we proved that for a suitable choice of notation S is the totality of pairs $(a,\ b)$ of elements of E satisfying

$$a^{1+q} = b + b^q$$

and the elements of K are labelled by non-zero elements of E, so that we have formulas (17) and (24). Moreover by Lemma 12 there exsists an involution t of G which normalizes K. The involution t commutes with elements of order $q+1$ but transforms each element of order $q-1$ into its inverse. Therefore we have

$$t^{-1}kt = k^{-q} \quad \text{for } k \in K, \tag{26}$$

If $x \neq 1$ is an element of S, $t^{-1}xt$ is an element outside of N. Being doubly transitive (Corollary to Proposition) G satisfies the property that every elements outside N can be written uniquely as ytz with $y \in N$ and $z \in S$. We define functions f, g and h by

$$t^{-1}xt = g(x)h(x)tf(x) \tag{27}$$

where $g(x)$, $f(x) \in S$ and $h(x) \in K$. The equations in (27) are called the structure equations of G.

LEMMA 15. *The functions f, g and h determine the structure of G uniquely (together with formulas* (17), (24) *and* (26)). *They satisfy the following properties:*

$$f(x)^{-1} = g(x^{-1}),\ g(x)^{-1} = f(x^{-1}) \text{ and } h(x^{-1}) = h(x)^q, \tag{28}$$

$$f(k^{-1}xk) = k^q f(x)k^{-q} \text{ and } h(k^{-1}xk) = k^q h(x)k \quad (k \in K), \tag{29}$$

$$f(f(x)) = x \text{ and } f(g(x)) = h(x)^{-q} f(x)^{-1} h(x)^q, \tag{30}$$

$$f(xy) = h(y)^q f(z) h(y)^{-q} f(y) \tag{31}$$

where x, $y \in S$, $x \neq 1$, $y \neq 1$, $xy \neq 1$ and $z = f(x)g(y)$.

Proof. The first statement is almost obvious. Observe that the elements of $G - N$ can be written uniquely as utv with $u \in N$ and $v \in S$. The formulas (28), (29), (30) and (31) can be proved by using (27).

Since G contains a subgroup isomordhic to $LF(2, q)$, we see that the subgroup S contains an element s such that

$$s^2 = 1 \quad \text{and} \quad t^{-1}st = s^{-1}ts. \tag{32}$$

By suitable choice of the notation we may assume that S is labelled $(0, 1)$. In general if x is labelled as (a, b) and if $f(x)$ is (a', b') we write $(a', b') = f(a, b)$. We want to prove that the functions f, g and h are determined uniquely.

11. The structure equations of the unitary group. In this section we consider the structure equations of the unitary group $U=U(q)$. We have seen that the totality of matrices $M(a, b, c; 1)$ of §2 with (2) forms a Sylow 2-group Q of U. Let $D(k)$ denote the diagonal matrix with k^q, k^{q-1}, k^{-1} in the main diagonal. Then

$$D(k)D(l)=D(kl) \quad \text{and} \quad D(k)^{-1}M(a, b)D(k)=M(ak, k^{1+q}b),$$

where we denote

$$M(a, b)=M(a, b, a^q; 0).$$

Hence the totality R of the matrices $D(k)$ is a cyclic group of order q^2-1 and normalizes Q. If T denotes the matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

T is in the normalizer of R and we have

$$T^{-1}D(k)T=D(k^{-q}). \tag{33}$$

The elements of U corresponding to the matrices $M(a, b)$, $D(k)$ and T generate the whole group U. We have

$$T^{-1}M(0, 1)T=M(0, 1)TM(0, 1). \tag{34}$$

The structure equations of U may be written as

$$TM(a, b)T\equiv M(a', b')D(k)TM(a'', b'')$$

and the congruence is modulo the center of U. It is easy to see that the elements $M(a', b')$, $M(a'', b'')$, $D(k)$ are uniquely determined by a and b. By the formulas (29) and (34), the mapping $M(a, b)\to M(a', b')$, $D(k)$ is determined if we know the images of $M(1, c)$ with $c+c^q=1$. We check

$$TM(1, c)T\equiv M(c^{-1}, c^{-1})D(c^{2-q})TM(c^{-q}, c^{-1}). \tag{35}$$

12. Identification of G. We will compare the structure equations of G to those of U. If we label the element s of S satisfying (32) as (0, 1), we get

$$f(0, 1)=(0, 1) \quad \text{and} \quad h(0, 1)=1. \tag{36}$$

This is in agreement with (34). By the transformation formula (29) we obtain

$f(0, b)$. We have the following formulas:

$$f(0, b) = (0, b^{-1}),\ g(0, b) = (0, b^{-1}) \quad \text{and} \quad h(0, b) = b. \tag{37}$$

Define three functions α, β and γ by

$$f(1, x) = (\alpha(x), \beta(x)) \quad \text{and} \quad h(1, x) = \gamma(x). \tag{38}$$

Then $\alpha(x)$, $\beta(x)$ and $\gamma(x)$ are elements of E and $\alpha(x), \gamma(x) \neq 0$.

Consider any element (a, b) of S. We assume that $a \neq 0$. Then

$$(a, b) = a^{-1}(1, z)a \quad \text{with} \quad a^{1+q}z = b.$$

Hence by (38) and (29) we get

$$f(a, b) = a^q(\alpha(z), \beta(z))a^{-q} = (a^{-q}\alpha(z), a^{-1-q}\beta(z)). \tag{39}$$

Similarly we have the following two formulas:

$$\begin{aligned} &g(a, b) = (a^{-q}\alpha(z^q), a^{-1-q}\beta(z^q)^q), \\ &h(a, b) = a^{1-q}\gamma(z) \qquad (z = a^{-1-q}b). \end{aligned} \tag{40}$$

We have used the fact that $(a, b)^{-1} = (a, b^q)$ (cf. (17)).

Define another function $\delta(x)$ by

$$\delta(x) = \alpha(x)^{-1-q}\beta(x). \tag{41}$$

If $y = \delta(x)$, we have

$$f(\alpha(x), \beta(x)) = (\alpha(x)^{-q}\alpha(y), \alpha(x)^{-1-q}\beta(y)).$$

On the other hand the left side is $ff(1, x)$, which is $(1, x)$ by (30). Hence we have

$$\alpha(y) = \alpha(x)^q \quad \text{and} \quad \beta(y) = x\alpha(x)^{1+q}. \tag{42}$$

This implies in particular that $\delta(y) = x$ or

$$\delta\delta(x) = x. \tag{43}$$

LEMMA 16. *There is an element* $(1, x)$ *such that*

$$\delta(x) = x^q. \tag{44}$$

Proof. Compute $f(g(1, x))$ in two different ways. By (40)

$$g(1, x) = (\alpha(x^q), \beta(x^q)^q).$$

Put $z = \delta(x^q)$. Then by definition (38) we get

$$f(g(1, x)) = (\alpha(x^q)^{-q}\alpha(z^q),\ \alpha(x^q)^{-1-q}\beta(z^q)).$$

On the other hand the formula (30) can be applied. We have

$$f(g(1, x)) = k^{-1}f(1, x)^{-1}k \quad \text{with} \quad k = \gamma(x)^q.$$

Hence $f(g(1, x)) = (\alpha(x)k,\ \beta(x)^q k^{1+q})$. Then we have

$$\alpha(x)k = \alpha(x^q)^{-q}\alpha(z^q) \quad \text{and} \quad \beta(x)^q k^{1+q} = \alpha(x^q)^{-1-q}\beta(z^q).$$

The above equations imply that

$$\delta(z^q) = \alpha(z^q)^{-1-q}\beta(z^q) = \alpha(x)^{-1-q}\beta(x)^q = \delta(x)^q. \tag{45}$$

Consider the set T_0 consisting of all the elements of E satisfying $x + x^q = 1$. The set T_0 contains exactly q elements. We say that two elements a, b of T_0 are equivalent if there are elements $a_0, a_1, \ldots, a_n$ of T_0 such that $a_0 = a$, $a_n = b$ and for any $i (1 \leqq i \leqq n)$ $a_i = a_{i-1}^q$ or $a_i = \delta(a_{i-1})$. Let T_1 be any equivalent class of T_0 in above sense. Let x be an element of T_1. Since $x \neq x^q$, T_1 contains at least two elements. By definition T_1 contains $y = \delta(x)$ and $z = \delta(x^q)$. T_1 also contains y^q and z^q, but by (45) $\delta(z^q) = y^q$. Hence T_1 contains at most 6 elements. Since the set T_0 contains exactly q elements, there must be an equivalent class with fewer than 6 elements. Otherwise q would be a multiple of 6, which is not the case. Then if T_1 is one such class with fewer than 6 elements, x coincides with one of y, z, y^q or z^q. If $x = y$, $\delta(x^q)$ is z and at the same time it is z^q. This is impossible. If $x = z$, $\delta(z) = x^q$ by (43) and x satisfies the requirement. If $x = y^q$, we have $y = \delta(x)$ and $\delta(y) = x = y^q$. If $x = z^q$, we get the contradiction $y = y^q$. In any case there is an element in T_1 satisfying the requirement.

Let x be one of the elements of E satisfying (44). Then $\delta(x) = x^q$ and the formulas (41) and (42) imply that

$$\alpha(x^q) = \alpha(x)^q \quad \text{and} \quad \beta(x^q) = \beta(x)^q. \tag{46}$$

By definition

$$f(1, x+y) = (\alpha(x+y),\ \beta(x+y)),$$

and here y is an arbitrary element of F. Note that $y + y^q = 0$. We compute $f(1, x+y)$ differently. Apply the product formula (31). We have

$$f(1, x)g(0, y) = (\alpha(x),\ \beta(x))(0, y^{-1}) = (\alpha(x),\ \beta(x) + y^{-1}).$$

If $z=\delta(x)+y^{-1}\alpha(x)^{-1-q}=x^q+y^{-1}\alpha(x)^{-1-q}$,

$$f(1,\ x+y)=y(\alpha(x)^{-q}\alpha(z),\ \alpha(x)^{-1-q}\beta(z))y^{-1}(0,\ y^{-1})$$
$$=(y^{-1}\alpha(x)^{-q}\alpha(z),\ y^{-1-q}\alpha(x)^{-1-q}\beta(z)+y^{-1}).$$

Hence we get

$$\alpha(x+y)=y^{-1}\alpha(x)^{-q}\alpha(z) \quad \text{with} \quad z=x^q+y^{-1}\alpha(x)^{-1-q}. \tag{47}$$

For the function g the product formula corresponding to (31) is

$$g(xy)=g(x)h(x)g(z)h(x)^{-1} \quad \text{with} \quad z=f(x)g(y).$$

we have

$$g(1,\ x+y)=(\alpha(x^q+y),\ \beta(x^q+y)^q)$$
$$=(\alpha(x^q),\ \beta(x^q)^q)\gamma(x)(\alpha(x)^{-q}\alpha(z^q),\ \alpha(x)^{-1-q}\beta(z^q)^q)\gamma(x)^{-1}$$
$$=(\alpha(x^q)+\gamma(x)^{-1}\alpha(x)^{-q}\alpha(z^q),\ *).$$

Equating the first entry we obtain

$$\alpha(x^q+y)=\alpha(x^q)+\gamma(x)^{-1}\alpha(x)^{-q}\alpha(z^q) \tag{48}$$

where z is defined as in (47). The two formulas (47) and (48) give the equation

$$y^{-1}\alpha(x^q)^{-q}\alpha(z^q)=\alpha(x^q)+\gamma(x)^{-1}\alpha(x)^{-q}\alpha(z^q).$$

By definition $z^q=x+u$ where $u=y^{-1}\alpha(x)^{-1-q}$. The above equation gives the value $\alpha(x+u)$:

$$\alpha(x+u)=1/(w+u) \quad \text{where} \quad w=\gamma(x)^{-1}\alpha(x)^{-2q}. \tag{49}$$

This formula (49) is true for a fixed x satisfying (46) and for an arbitrary non-zero element u of F. Since

$$\delta(x^q)=x=(x^q)^q$$

by (43), we can apply the preceeding argument to obtain

$$\alpha(x^q+u)=1/(v+u)$$

for an element $u\neq 0$ of F, where $v=\gamma(x^q)^{-1}\alpha(x^q)^{-2q}$. The element of E satisfies the equation $x^q=x+1$. Hence we have $\alpha(x)=1/(v+1)$. Substitute these values in (47). After a simple computation we get

$$yv+(v+1)(v^q+1)=(v^q+1)(w+y).$$

Since this equation is true for any non-zero element y of F, we conclude that

$$v = v^q + 1 \quad \text{and} \quad w = v + 1.$$

Note that we have assumed the inequality $q > 2$, and so there are more than one non-zero elements in F. These equations imply that the formula (49) is true for all $u \in F$ and that $w - x$ is an element of F. Hence we have

$$\alpha(s) = 1/(s^q + c) \tag{50}$$

for all s satisfying $s + s^q = 1$, where c is an element of F independent of s. Then $c^q = c$ and $\alpha(s^q) = \alpha(s)^q$ for all s. Using (42) we get

$$\alpha(\delta(s)) = \alpha(s)^q = \alpha(s^q).$$

This equation implies that

$$\delta(s) = s^q \quad \text{for all } s. \tag{51}$$

Since (51) is true for all s, we have (cf. (49))

$$\gamma(s) = \alpha(s)^{-2q+1} \quad \text{for all } s. \tag{52}$$

It remains to prove that $c = 0$ in (50). If $c = 0$, then $\alpha(s) = s^{-q}$, $\beta(s) = s^{-1}$ and $\gamma(s) = s^{2-q}$. This means that the structure equations of G are identical with the equations (35) of the unitary group. Then G is isomorphic to $U(q)$.

We use the formula (31) again. Compute $f(1, x+y)$ using the fact that $(1, x+y) = (0, y)(1, x)$ for $y \in F$. We have

$$f(0, y)g(1, x) = (0, y^{-1})((x+c)^{-1}, x^q(x+c)^{-1-q}) = ((x+c)^{-1}, y^{-1} + x^q(x+c)^{-1-q}).$$

By (50) and (52), $\gamma(x) = \alpha(x)^{-2q+1} = (x^q + c)^{2q-1}$. If $z = f(0, y)g(1, x)$, then by (39)

$$f(z) = ((x+c)^q(w+c)^{-1}, (x+c)^{1+q}w(w+c)^{-1-q})$$

where $w = x + (x+c)^{1+q}y^{-1}$. By (31) we get

$$f(1, x+y) = (x^q + c)^{2-q} f(z)(x^q + c)^{q-2}((x^q + c)^{-1}, x^q(x^q + c)^{-1-q}).$$

In particular we have by using (17), (24) and (38)

$$(x^q + y)(x^q + y + c)^{-1-q} = x^q(x^q + c)^{-1-q} + (x+c)^{-1}(w+c)^{-q} + w(w+e)^{-1-q}. \tag{53}$$

By definition we have

$$w + c = (x+c)(x^q + y + c)y^{-1}.$$

Multiply $(x+c)^{1+q}(x^q+y+c)^{1+q}$ to the above equation (53). We get

$$(x^q+y)(x+c)^{1+q}=x^q(x^q+y+c)^{1+q}+wy^2+y(x^q+y+c).$$

Since $w=x+(x+c)^{1+q}y^{-1}$, this is reduced to

$$y^2(x^q+x+1)+y(x^q+x+1)x^q+yc=0.$$

The element x satisfies the equation $x^q+x=1$. Hence we have

$$yc=0.$$

Since y was an arbitrary element of F the desired equality $c=0$ is proved.

References

[1] R. Brauer, On the structure of groups of finite order, Proceedings of the International Congress of Mathematicians, vol. **1** (1954), pp. 1-9.

[2] R. Brauer and K. A. Fowler, On groups of even order, Ann. of Math., vol. **62** (1955), pp. 565-583.

[3] R. Brauer and C. Nesbitt, On the modular characters of groups, Ann. of Math., vol. **42** (1941), pp. 556-590.

[4] R. Brauer and M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group, Proc. of the National Acad. Sci. USA, vol. **45** (1959), pp. 1757-1759.

[5] R. Brauer, M. Suzuki and G. E. Wall, A characterization of the one-dimensional unimodular projective groups over finite fields, Illinois Jour. of Math., vol. **2** (1958), pp. 718-745.

[6] W. Feit, A characterization of the simple groups $SL(2, 2^a)$, Amer. Jour. of Math., vol. **82** (1960), pp. 281-300.

[7] M. Suzuki, On characterizations of linear groups, I and II, Trans. Amer. Math. Soc., vol. **92** (1959), pp. 191-219.

[8] M. Suzuki, Finite groups with nilpotent centralizers, Trans. Amer. Math. Soc. vol. **99** (1961), pp. 425-470.

[9] M. Suzuki, On a class of doubly transitive groups, Ann. of Math. vol. **75** (1962), pp. 105-145.

[10] J. G. Thompson, Finite groups with fixed-point-free automorphisms of prime order, Proc. of the National Acad. Sci. USA, vol.**45** (1959), pp. 578-581.

[11] J. H. Walter, On the characterization of linear and projective linear groups, I and II, Trans. Amer. Math. Soc., vol. **100** (1961), pp. 481-529 and vol. **101** (1961), pp. 107-123,

University of Illinois

University of Chicago