ON CHARACTERIZATIONS OF LINEAR GROUPS, II(1)

BY

MICHIO SUZUKI

The main object of this paper is to characterize the linear fractional group G_0 in 2 variables over a finite field F of characteristic 2 by the properties of involutions in it. Here by an involution we shall mean an element of order 2. G_0 is isomorphic with the factor group of Γ, the totality of 3×3 nonsingular matrices over F, modulo its center Δ. It is easily seen that any involution of Γ is conjugate to the involution I:

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

Let Ω be the totality of 3×3 nonsingular matrices commuting with I. Then Ω is a group of order $q^3(q-1)^2$ consisting of triangular matrices with the bottom main diagonal element equal to the top one. Hence in G_0 the centralizer N_0 of an involution has order $q^3(q-1)$ and is isomorphic with the factor group Ω/Δ of Ω modulo the center of Γ. Our main theorem is the converse to this statement.

THEOREM. *Let G be a finite group of even order and τ be an involution of G. If the centralizer of τ is isomorphic with Ω/Δ and if every involution of G is conjugate to τ, then G is isomorphic with G_0, the linear fractional group of 2 variables, with one exception. The exceptional case occurs when F has only two elements and in this case we have $G\cong LF(3, 2)$ or $G\cong A_6$.*

A similar characterization of the linear fractional group in 2 variables over a field of odd characteristic has been obtained by R. Brauer in the case that the ground field has q elements with $q\equiv -1 \pmod 4$ (cf. [2; 2*]).

1. In this section we shall consider the group Ω/Δ and derive several properties of this group which will be used in the subsequent argument.

Throughout this section N_0 stands for the group Ω/Δ. It is clear that N_0 is isomorphic with the totality of 3×3 matrices of the form

$$M(\alpha, \beta, \gamma; \delta) = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & \delta & 0 \\ \beta & \gamma & 1 \end{pmatrix}$$

Received by the editors February 10, 1958.

(1) The investigation has been done at Harvard University with support from the National Science Foundation: NSF Grant, G 2268.

where α, β, γ and $\delta \neq 0$ are elements of a finite field F of characteristic 2. We take N_0 as the totality of $M(\alpha, \beta, \gamma; \delta)$. Let q be the number of elements contained in F so that $q = 2^\mu$.

The matrix multiplication may be written as

$$M(\alpha, \beta, \gamma; \delta)M(\alpha', \beta', \gamma'; \delta') = M(\alpha'', \beta'', \gamma''; \delta'')$$

where

$$\alpha'' = \alpha + \delta\alpha', \qquad \beta'' = \beta + \gamma\alpha' + \beta', \qquad \gamma'' = \gamma\delta' + \gamma' \quad \text{and} \quad \delta'' = \delta\delta'.$$

Hence the mapping ϕ of N_0 defined by $\phi(M(\alpha, \beta, \gamma; \delta)) = \delta$ is a homomorphism of N_0 onto the multiplicative group of nonzero elements of F. The kernel of ϕ is the totality of $M(\alpha, \beta, \gamma; 1)$ and is of course a 2-group of order q^3. Thus we have the following proposition.

(I) N_0 contains a normal subgroup Q of order q^3 and the factor group N_0/Q is a cyclic group of order $q-1$.

Furthermore from the matrix multiplication we conclude the following propositions, which may be proved by computation.

(II) $M(\alpha, \beta, \gamma; 1)^2 = M(0, \alpha\gamma, 0; 1)$. In particular $M(\alpha, \beta, \gamma; 1)$ is an involution if $\alpha\gamma = 0$; otherwise the order is 4.

(III) The center C of Q is of order q consisting of elements $M(0, \beta, 0; 1)$, and C is the center of N_0.

(IV) The centralizer of each element $\neq 1$ of N_0 with an order a divisor of $q-1$ is an abelian group of order $q(q-1)$.

(V) The centralizer of each element of order 4 in N_0 is an abelian group of order q^2.

Let P be the subgroup of Q consisting of matrices $M(\alpha, \beta, 0; 1)$ and L be the subgroup corresponding to the totality of matrices $M(0, \beta, \gamma; 1)$.

(VI) Both P and L are abelian groups of order q^2 consisting of elements of order $\leqq 2$. They are normal in Q.

(VII) Every involution of N_0 is contained in either P or L and the intersection of P and L is the center C.

These two propositions are obvious from the property (II) and the definition of P and L.

(VIII) Involutions of P not contained in C are conjugate to each other in N_0. The same property holds for L.

Proof. We have $M(0, 0, \lambda; \delta^{-1})^{-1} = M(0, 0, \delta\lambda; \delta)$ and

$$M(0, 0, \lambda; \delta^{-1})M(\alpha, \beta, 0; 1)M(0, 0, \delta\lambda; \delta) = M(\delta^{-1}\alpha, \lambda\alpha + \beta, 0; 1).$$

Hence if $M(\alpha, \beta, 0; 1)$ is not in C then $\alpha \neq 0$ and we may take λ and δ in such a way that $\delta = \alpha$ and $\lambda\alpha + \beta = 0$. Hence every involution of P not contained in C is conjugate to $M(1, 0, 0; 1)$ and this is the statement (VIII).

Since $Q = P \cup L$, Q/C is a direct product of P/C and L/C.

(IX) The factor group Q/C is an abelian group of order q^2 and of type $(2, \cdots, 2)$.

Finally we shall prove the following proposition.

(X) The commutator subgroup of N_0 is Q if $q>2$.

Since N_0/Q is a cyclic group the commutator subgroup N_0' of N_0 is a part of Q. Since $M(\alpha-1, \beta, 0; 1)M(1, 0, 0; 1) = M(\alpha, \beta, 0; 1)$, we see that if $\alpha \neq 1$ and 0, $M(\alpha, \beta, 0; 1)$ is a commutator in N_0 (cf. the computation in (VIII)). If $q>2$, the field F contains an element α which is neither 0 nor 1. Then $M(\alpha, \beta, 0; 1)$ is an involution of P which is not in C and is a commutator. Hence by (VIII) every involution of P not contained in C is a commutator. Thus the commutator subgroup N_0' contains P. Similarly L is a part of N_0' and hence $Q = P \cup L \subseteq N_0'$.

2. Let G be a finite group of even order, and τ be an involution of G. In the rest of this paper we assume the two conditions (A) and (B):

(A) the centralizer N_0 of τ in G is isomorphic with Ω/Δ;

(B) every involution of G is conjugate to τ in G.

We shall use the same notations introduced in the first section; i.e. C stands for the center of N_0, Q the 2-Sylow subgroup of N_0 and P or L is the subgroup of Q as defined in the §1.

PROPOSITION 1. *Q is a 2-Sylow subgroup of G.*

Proof. By way of contradiction suppose that Q is a proper subgroup of a 2-Sylow subgroup Q^* of G. We can take a subgroup Q' of Q^* such that $[Q': Q] = 2$. By a property of 2-groups Q is a normal subgroup of Q'. Since C is the center of Q, it is a characteristic subgroup of Q. Hence C is a normal subgroup of Q'. Again by a property of 2-groups we see that C contains a central element $\tau' \neq 1$ of Q'. By the assumption (B) τ' is conjugate to τ in G and hence the centralizer of τ' is isomorphic with N_0. Since τ' is in the center of Q' we conclude that a 2-Sylow subgroup of the normalizer of τ' has a greater order than Q. This is impossible.

PROPOSITION 2. *P is never conjugate to L in G.*

Proof. By way of contradiction suppose that there is an element $\pi \in G$ such that $\pi P \pi^{-1} = L$. Then $\pi Q \pi^{-1}$ and Q are 2-Sylow subgroups of the normalizer of L by (VI) and Proposition 1. Hence there is an element ρ such that $\rho L \rho^{-1} = L$ and $\rho\pi Q \pi^{-1}\rho^{-1} = Q$. Put $\sigma = \rho\pi$. We have $\sigma P \sigma^{-1} = \rho\pi P \pi^{-1}\rho^{-1} = \rho L \rho^{-1} = L$ and $\sigma Q \sigma^{-1} = Q$. Hence $\sigma L \sigma^{-1}$ is a subgroup of Q consisting of elements of order $\leqq 2$. By the property (VII) of the first section $\sigma L \sigma^{-1} = P$. Hence some power σ_1 of σ has an order a power of 2 and still exchanges P and L. Q and σ_1 generate a 2-group. By Proposition 1 Q is a 2-Sylow subgroup of G and hence Q contains σ_1. Since both P and L are normal subgroups of Q by (VI) of §1, we get a contradiction.

3. If $q=2$, the group N_0 is a dihedral group of order 8. Hence N_0 contains an element π of order 4 such that $\tau = \pi^2$. Since N_0 is the centralizer of τ in G, the centralizer of π in G is a part of N_0 and hence coincides with the cyclic

group generated by π. The structure of a finite group possessing such a property is known (cf. [7]). From the results of [7] we conclude that G is isomorphic with either $LF(2, 7) \cong LF(3, 2)$ or $LF(2, 9) \cong A_6$, the alternating group on six letters. In fact a direct proof of this result can be carried through by using a method similar to the one in [7] and it is much easier. We shall however not enter in this special case. Hereafter we assume in addition to the assumptions (A) and (B) the following one:

(C) q is greater than 2.

4. Let M be the normalizer of the subgroup P in G. We want to prove the following proposition in this section.

PROPOSITION 3. *The factor group M/P is isomorphic with the general linear group consisting of all the 2×2 nonsingular matrices over F.*

First of all we consider the normalizer of Q in G.

PROPOSITION 4. *Let N be the normalizer of a 2-Sylow subgroup Q of G. Then $[N: N_0] = q-1$.*

Proof. If τ' is an involution of C, τ' is conjugate to τ in G. By a lemma of Burnside [4, §123] τ' is conjugate to τ in N. Hence $[N: N_0] \geqq q-1$. On the other hand if σ and σ' are two elements of N which transform τ into τ', then σ and σ' are in the same coset modulo N_0. Hence $[N: N_0] \leqq q-1$, whence the equality follows.

PROPOSITION 5. *If Q and Q' are two different 2-Sylow subgroups of G containing P, then we have $Q \cap Q' = P$.*

Proof. By way of contradiction suppose that the intersection $D = Q \cap Q'$ contains P as a proper subgroup. Then $L_0 = D \cap L$ contains C properly. Since Q/C is abelian by (IX) of the first section L_0 is a normal subgroup of D. Since every involution of D is either in P or L_0, $C = L_0 \cap P$ is a characteristic subgroup of D. This implies that C is a normal subgroup of Q'. By a property of 2-groups C contains a central element τ' of Q'. Hence the centralizer of τ' contains Q'. On the other hand the centralizer of τ' is N_0 which contains Q as a normal subgroup. We have therefore $Q = Q'$.

We now prove Proposition 3. The group Q/P is a 2-Sylow subgroup of M/P. By the assumption (C) q is greater than 2. Hence Q/P is not cyclic by (IX) of §1. We shall show that Q/P is not a normal subgroup of M/P. By the assumption (B) a central involution τ of Q is conjugate to an involution τ_1 of P is not contained in C. The centralizer of τ_1 contains a normal subgroup Q_1 of order q^3. Q_1 is a 2-Sylow subgroup of G containing P. Since τ_1 is not in the center of Q by (III) of the first section Q_1 is different from Q. Hence Q_1/P is another 2-Sylow subgroup of M/P, which shows the non-normality of Q/P. Next we shall prove that the centralizer of any involution in M/P is abelian. Take any involution τ' of Q/P and consider the centralizer

of τ' in M/P. This centralizer has the form U/P where U is a subgroup of G. If $\sigma \in U$, Q/P and $\sigma Q\sigma^{-1}/P$ are two 2-Sylow subgroups of M/P containing τ'. Hence $Q \cap \sigma Q\sigma^{-1} \supset P$. By Proposition 5 we have $Q = \sigma Q\sigma^{-1}$; i.e. U is contained in the normalizer N of Q. By the splitting theorem of Schur [9, p. 125] U contains a subgroup V such that $U = QV$ and $Q \cap V = e$. V is then a group of odd order. Let T/P be the subgroup generated by τ'. V is considered as an operator domain acting on T. $T_1 = T \cap L$ is abelian group of type $(2, \cdots, 2)$ and contains all the involutions of T not in P. Hence T_1 is left invariant by V. The group T_1 is completely decomposable as a V-module. Since C is an invariant subgroup of T_1, T_1 contains a subgroup T_2 such that $T_1 = T_2C$, $T_2 \cap C = e$ and T_2 is V-invariant. The isomorphism theorem yields $T_2 \cong T_1/C \cong T/P$. Hence T_2 is a group of order 2 generated by an involution τ_2. Since T_2 is V-invariant, τ_2 commutes with every element of V. Thus V is a subgroup of odd order contained in the centralizer N_2 of τ_2. By assumptions (A) and (B) V is a cyclic group. The center C_2 of N_2 is an abelian group of order q contained in L (cf. (III) and (VII)). Since $C_2 \cap C = e$, we have $L = C_2 \cup C$. The subgroup $V \cup C_2$ is an abelian group by (IV) of the first section. We have $P \cup (V \cup C_2) = P \cup C_2 \cup V = P \cup L \cup V = Q \cup V = U$. By the isomorphism theorem we assert that $U/P \cong (C_2 \cup V)/(C_2 \cup V) \cap P$, and U/P is abelian. Thus we have shown the commutativity of the centralizer of any involution in M/P.

By the main theorem of [8] M/P is a direct product of a linear fractional group $LF(2, 2^r)$ and an abelian group A of odd order. Since Q/P is a 2-Sylow subgroup the linear group which is a direct factor must be $LF(2, q)$. The centralizers of involutions are direct products of 2-Sylow subgroups and A. In our case $U/P \cong (Q/P) \times (VP/P)$. Hence $A \cong V$. The normalizer of a 2-Sylow subgroup of M/P has the form N/P, where N is the normalizer of a 2-Sylow subgroup of G. Hence by the Proposition 4 it has an order $q(q-1)^2$. On the other hand this normalizer is a direct product of VP/P and a subgroup of order $q(q-1)$. Hence the order of V is $q-1$. Since V is cyclic M/P is isomorphic with the general linear group consisting of all the 2×2 non-singular matrices over F.

5. The object of this section is to determine the order of G using the result of §2 of [8].

Let V be the subgroup of order $q-1$ defined in the previous section. Put $W = PV$. From the result of the preceding section W/P is the center of M/P. In particular W is a normal subgroup of M. Let H be the normalizer of V in M. If $\rho \in M$, $\rho V\rho^{-1}$ is a subgroup of W. Since $W = PV$ and P is a normal subgroup, we may apply Theorem 26 of [9, p. 126] to see that $\rho V\rho^{-1}$ and V are conjugate in W; there is an element π of W such that $\pi\rho V\rho^{-1}\pi = V$. Thus $\pi\rho \in H$; in other words $M = WH$. Since $H \supseteq V$, $M = WH = PVH = PH$. We shall show that $H \cap P = e$. If $H \cap P \neq e$, $H \cap P$ contains an involution τ_1 which commutes with every element of V. Then the central-

izer N_1 of τ_1 in G contains V. Hence N_1 contains $P \cup V = W$. On the other hand P is a normal subgroup of N_1 and hence $N_1 \subseteq M$. Since W is a normal subgroup of M, W is also a normal subgroup of N_1. Since $N_1 = Q_1 W$ with the 2-Sylow subgroup Q, of N_1, the factor group N_1/W is an abelian group, which contradicts (X) of the first section. Hence by the isomorphism theorem $H \cong M/P \cong LF(2, q) \times V$.

We want to apply Propositions 5 and 6 of [8] to M and V. The second assumption in these propositions is satisfied because of our assumptions (A) and (B). The third one follows trivially since the order of V is $q-1$. As for the first condition we need only to show that H is the normalizer of any subgroup $V_0 \neq e$ of V. First of all we prove the following proposition.

PROPOSITION 6. *If X is a 2-Sylow subgroup of H, X is a 2-Sylow subgroup of the centralizer of V_0.*

Proof. Let τ be an involution contained in X. By the assumptions (A) and (B) of the second section of this paper the centralizer of τ in G is isomorphic with N_0. X is contained in a 2-Sylow subgroup Y of the centralizer of V_0. Since $V_0 \neq e$, Y does not contain elements of order 4 by (V) of the first section. Hence Y consists of elements of order $\leqq 2$ and is abelian. Therefore Y and V_0 are contained in the centralizer of τ. By (IV) the order of Y is not greater than q; i.e. $X = Y$.

PROPOSITION 7. *The normalizer of V_0 in G coincides with the centralizer of V_0.*

Proof. Suppose that two elements σ and σ' of V_0 are conjugate: $\sigma' = \pi\sigma\pi^{-1}$. Consider a 2-Sylow subgroup X of H. X is by Proposition 6 a 2-Sylow subgroup of the centralizer of σ and at the same time of σ'. Hence X and $\pi X \pi^{-1}$ are two 2-Sylow subgroups of the centralizer of σ'. There is an element ρ such that $\rho\sigma' = \sigma'\rho$ and $X = \rho\pi X \pi^{-1}\rho^{-1}$. If τ is an involution of X, τ is conjugate to $\rho\pi\tau\pi^{-1}\rho^{-1}$ in H which is a part of the centralizer of σ'. Hence there is an element ρ' such that $\rho'\sigma' = \sigma'\rho'$ and $\tau = \rho'\rho\pi\tau\pi^{-1}\rho^{-1}\rho'^{-1}$. This means that σ and σ' are conjugate in the centralizer of τ. By the structure of N_0 this happens only if $\sigma = \sigma'$. Thus our assertion has been proved.

Let H' be the normalizer of V_0 in G. By Proposition 7 H' is the centralizer of V_0. Let τ be any involution of H'. By Proposition 6 τ is conjugate in H' to an element of H. Hence we assume τ is an element of H. Let A be the centralizer of τ in H'. Thus A is the intersection of the centralizers of τ and $1 \neq \sigma \in V_0$. By the property (IV) (together with assumptions (A) and (B)) we conclude that A is an abelian group of order $q(q-1)$. Again by the main theorem of [8] H' is a direct product of a linear group and an abelian group. The linear group in the direct factor must be $LF(2, q)$, while the abelian part has order $q-1$. Comparing the orders we get $H' = H$.

We have proved that every assumption of Proposition 6 of [8] is satisfied.

From this proposition we conclude that G has irreducible characters X and Y_i $(i=1, 2, \cdots, t=q/2)$ satisfying relations $X(\sigma)+\epsilon=Y_i(\sigma)$ $(\epsilon=\pm 1)$ for all elements σ of an order relatively prime to $q+1$, and the order g of G is

$$g = n^2m(q+1)f(f+\epsilon)/h(f-a)^2$$

where n is the order of the centralizer of an involution τ in G, $hm(q+1)$ is the order of some subgroup, m is an integer, $m\equiv 1 \pmod{2h}$, f is the degree of X, h is the order of V and $a=X(\tau)$. Moreover we have $t=q/2>1$ and hence $f\equiv\epsilon \pmod{m(q+1)}$. The congruence for m is a consequence of (iii) in Proposition 5 of [8]. In our case $n=q^3(q-1)$ and $h=q-1$. Thus

$$g = q^6(q-1)(q+1)mf(f+\epsilon)/(f-a)^2.$$

A 2-Sylow subgroup Q has an order q^3 and P is a subgroup of order q^2 consisting of elements of order $\leqq 2$. It follows that g is divisible by q^3 and $f\equiv a \pmod{q^2}$. The last congruence is proved by summing X over P. Hence the denominator in the expression of g is divisible by q^4. Hence $f(f+\epsilon)$ must be a multiple of q. Therefore q divides $f+\epsilon$ or f. We distinguish two cases accordingly.

CASE I. q is a divisor of $f+\epsilon$. This case is proved to be impossible. Let 2^λ and 2^ν be the highest power of 2 dividing $f+\epsilon$ and $f-a$ respectively. Put $f+\epsilon=2^\lambda u$ and $f-a=2^\nu v$. We have $\nu\geqq 2\mu$ since $f\equiv a \pmod{q^2}$, and $\lambda\geqq\mu$ by assumption, where $2^\mu=q$. We may write $\lambda=\mu+\lambda'$ and $\nu=2\mu+\nu'$ $(\lambda', \nu'\geqq 0)$. Counting the exponent of 2 dividing the order formula we get

$$3\mu = 6\mu+\lambda-2\nu = 6\mu+\mu+\lambda'-4\mu-2\nu' = 3\mu+\lambda'-2\nu'.$$

Suppose $\nu\leqq\lambda$. Then $2\mu+\nu'\leqq\mu+\lambda'=\mu+2\nu'$ or $\mu\leqq\nu'$. Hence we have $\lambda, \nu\geqq 3\mu$. Since $f+\epsilon$ is the degree of Y_i, we have $\lambda\leqq 3\mu$. Hence $\lambda=\nu=3\mu$, $f+\epsilon=q^3u$ and $f-a=q^3v$. The character Y_i is of the highest kind (cf. [3]) so that it vanishes on 2-singular elements: $Y_i(\tau)=a+\epsilon=0$. Hence $f+\epsilon=f-a=q^3u$. The order formula now reads $g=q^3(q-1)(q+1)m(q^3u-\epsilon)/u$. Since $(q^2-1)m$ is an order of a subgroup, $q^3(q^3u-\epsilon)/u$ is an integer. Since u is odd we must have $u=1$. Since g is divisible by $(q-1)^2$ and $m\equiv 1 \pmod{q-1}$, we conclude that $q^3-\epsilon$ is divisible by $q-1$. Since $q-1\geqq 3$, ϵ must be 1. From the congruence $f\equiv\epsilon \pmod{q+1}$ we get $q^3\equiv 2 \pmod{q+1}$, or $3\equiv 0 \pmod{q+1}$. This is impossible since we have assumed $q>2$.

Next assume that $\nu>\lambda$. Let π be an element of order 4 of Q. Then the centralizer of π in G has an order q^2. Hence every element of order 4 of N is conjugate to π in N. Let $b=X(\pi)$. The orthogonality relation yields that $f+(2q^2-q-1)a+q(q-1)^2b\equiv 0 \pmod{q^3}$. Since $f\equiv a \pmod{q^2}$ we get $a\equiv b \pmod{q}$. This congruence is valid in any case. In Case I we have $f+\epsilon\equiv 0 \pmod{q}$. Hence $a+\epsilon=f+\epsilon-(f-a)\equiv 0 \pmod{q}$. On the other hand $Y_i(\pi)=b+\epsilon\equiv a+\epsilon\equiv 0 \pmod{q}$. The orthogonality relation yields that $q^2=\sum_\mu |X_\mu(\pi)|^2$ where the summation ranges over all the irreducible char-

acters of G. Hence $q^2=1+b^2+(b+\epsilon)^2(q/2)+\cdots$. In particular $(b+\epsilon)^2<q^2$. Since $b+\epsilon\equiv 0 \pmod q$ we get $b+\epsilon=0$. Summing Y_i over Q we get $f+\epsilon+(2q^2-q-1)(a+\epsilon)\equiv 0 \pmod{q^3}$, or $f-a+(a+\epsilon)q(2q-1)\equiv 0 \pmod{q^3}$. Our assumption was $\nu>\lambda$. By definition 2^λ is the highest power of 2 dividing $f+\epsilon$ and 2^ν is the highest power of 2 dividing $f-a$. Since $\nu>\lambda$, 2^λ is the highest power of 2 dividing $a+\epsilon$. Hence $\lambda+\mu$ is the exact exponent of 2 dividing $(a+\epsilon)q(2q-1)$. Since we have assumed $\nu>\lambda$, ν is smaller than 3μ. Hence we have $\nu=\lambda+\mu$ and $\nu'=0$. We conclude therefore $f+\epsilon=qu$ and $f-a=q^2v$. Then $a+\epsilon=qw$ where $w=u-qv$.

From the orthogonality relation it follows that $\sum_\mu |X_\mu(\tau)|^2=q^3(q-1)$ where the summation ranges over all the irreducible characters of G. Since $Y_i(\tau)=a+\epsilon=qw$ we have $q^2w^2(q/2)<q^3(q-1)$ or $w^2<2(q-1)$. From the order formula $g=q^6(q-1)(q+1)mfqu/q^4v^2=q^3(q-1)(q+1)mfu/v^2$. As before $fu\equiv 0 \pmod{q-1}$. Since $f=qu-\epsilon$, f and u have no common divisor. We may write $q-1=st$, $(s,t)=1$, so that $f=sf'$ and $u=tu'$. Since $(q^2-1)m$ is the order of a subgroup v^2 is a divisor of fu. Let $v=v_1v_2$, $v_1^2|f$ and $v_2^2|u$. Then v_1 and v_2 are relatively prime. Moreover v_1 is relatively prime to $m(q+1)$ since $f\equiv\epsilon \pmod{m(q+1)}$. The degree f of X is a divisor of g and therefore we conclude that v_1^2 is a divisor of $q-1$. Since $(f,u)=1$, v_1^2 is a divisor of s. Similarly v_2 is prime to $m(q+1)$. Hence v_2^2 is a divisor of t. Altogether we conclude that v^2 is a divisor of $q-1$. The congruence $f-a+(a+\epsilon)q(2q-1)\equiv 0 \pmod{q^3}$ implies that $q^2v+q(u-qv)q(2q-1)\equiv 0 \pmod{q^3}$ or $v\equiv u \pmod q$. Thus we have three relations for u and v: $u\equiv v \pmod q$, $v^2|q-1$ and $(u-qv)^2<2(q-1)$. If $q>8$, we get $v\leqq(q-1)/2$ and $|u-qv|\leqq(q-1)/2$. Hence $u=(1+q)v$. If $q=4$ or 8, then $v=1$ and we get the same conclusion. This is however impossible because $f+\epsilon=qu=q(1+q)v\equiv 2\epsilon \pmod{m(1+q)}$, or $2\epsilon\equiv 0 \pmod{1+q}$. Thus we have shown the impossibility of Case I.

Case II. q is a divisor of f. We write as $f=2^\lambda u$ and $f-a=2^\nu v$ with odd integers u and v. By assumption $\lambda=\mu+\lambda'$ and $\nu=2\mu+\nu'$ with non-negative integers λ' znd ν'. Counting the exponent of 2 dividing both sides of the order formula we get $\lambda'=2\nu'$. Suppose $\lambda<\nu$. Then $\nu'<\mu$ and $3\mu>\nu$. Use the same argument as before. This time we get $X(\pi)=b=0$. The highest exponent of 2 dividing a is λ. Hence as before $\lambda+\mu=\nu$ and $\nu'=0$. Thus $f=qu$, $f-a=q^2v$ and $a=q(u-qv)$. Using the orthogonality relation we get $(u-qv)^2<2(q-1)$. This inequality may be proved as follows. Let $w=u-qv$. Then $a=qw$. Hence $a^2+(a+\epsilon)^2(q/2)<q^3(q-1)$; or $2qw^2+(qw-1)^2<2q^2(q-1)$. If $w^2\geqq 2(q-1)$, then $2qw^2-2qw+1<0$ which is impossible for integral values of w. The congruence $u\equiv v \pmod q$ follows by summing X over Q. By the same argument as in Case I we see that v^2 is a divisor of $q-1$. Hence $u=(q+1)v$ as before, which is again impossible.

Thus we must have $\lambda\geqq\nu$. Hence $\lambda\geqq 3\mu$. Since f is a degree of X, $\lambda\leqq 3\mu$ and hence we get $\lambda=3\mu$ and $\nu'=\mu$. We have now $f=q^3u$. X is therefore of the

highest kind and hence vanishes on 2-singular elements. In particular $X(\tau) = a = 0$. The order formula now reads $g = q^3(q-1)(q+1)m(q^3u+\epsilon)/u$. As before u is a divisor of $q^3u+\epsilon$ and hence $u=1$. Since $q^3+\epsilon$ is a multiple of $q-1$, ϵ must be -1. The congruence $f \equiv -1 \pmod{m(q+1)}$ implies that m is a divisor of q^2-q+1. On the other hand $m \equiv 1 \pmod{2(q-1)}$. We have therefore $q^2-q+1 = m\{l(q-1)+1\} = \{2k(q-1)+1\}\{l(q-1)+1\}$ or $q = 2kl(q-1) + 2k + l$. Hence $kl = 0$. We have either $k=0$ or $l=0$. This means that either $m=1$ or $m = q^2-q+1$. We have shown the validity of the following:

PROPOSITION 8. *Let M be the normalizer of P (cf. Proposition 3). Then the index of M is either q^2+q+1 or q^4+q^2+1.*

6. In this section we consider the case $[G: M] = q^4+q^2+1$, i.e. the case $m = q^2-q+1$. This case turns out to be impossible. In order to prove the impossibility we shall return to the situation of the §2 of [8].

As shown in §2 of [8] the normalizer R of a subgroup R_0 of order $q+1$ of H is of order $2(q-1)m(q+1)$. We may assume that $R \supseteq V$, the subgroup of order $q-1$ defined in the §4. R contains a normal subgroup R_1 of order $2m(q+1)$ and R_1 has a normal subgroup R_2 of index 2. R_2 is an abelian group. Every element $\neq 1$ of V induces an automorphism of R_2/R_0 which leaves only the identity fixed. Hence every element $\neq 1$ of R_2/R_0 has exactly $q-1$ elements which are conjugate under the action of V on R_2/R_0. Hence every characteristic subgroup of R_2/R_0 has an order congruent to 1 modulo $q-1$. Since $m = q^2-q+1 < q^2$, we conclude that R_2/R_0 is characteristically simple. This implies that m is a power of a prime number p: $m = p^n$. Suppose $n>1$. Then $p^n-1 = (p-1)(p^{n-1}+\cdots+1) = q(q-1)$. If $p \equiv 1 \pmod q$, $p^n-1 \geqq p^2-1 = (p-1)(p+1) \geqq q(q+2) > q(q-1)$; a contradiction. Hence $p^{n-1}+\cdots+1 \equiv n \equiv 0 \pmod 2$. Then $p^n-1 = (r-1)(r+1) = q(q-1)$. We get $r \geqq q \geqq r+1$ which is clearly impossible. Thus $n=1$ and $m = q^2-q+1 = p$ is a prime number.

Let π be an element of order p. From the result in [8, §2] it follows that the centralizer of π is R_2. Hence p divides the order g to the first power only. We may therefore apply the results of R. Brauer [1].

In [8, §2], we have shown G has irreducible characters Φ_{ik}, Ξ_k, H_k and Θ_j ($i = 1, 2, \cdots, t = q/2$; $k = 1, 2, \cdots, q-1$; $j = 1, 2, \cdots, s$; $s = (m-1)(q+1)/2(q-1) = q(q+1)/2$) and all the rest of characters of G vanish on p-singular elements. So they constitute the totality of irreducible characters in the p-blocks of positive defect. By Theorem 8 of [1] G has exactly $2(q-1)+t(q-1)+s$ characters of degree not divisible by p. Hence we conclude that all the characters Φ_{ik}, Ξ_k, H_k and Θ_j are actually different. In particular Ξ_k and H_k appear only in ψ_{ik}^* in the notation of [8, §2]. Hence we have $\Xi_k(\sigma) = \epsilon_k'$ and $\mathrm{H}_k(\sigma) = \epsilon_k''$ for $1 \neq \sigma \in R_2$. The formula for the coefficient $A(\sigma)$ of $\langle \rho\sigma \rangle$ in the expansion of $\langle \tau \rangle^2$ in the group ring is now

$$A(\sigma) = ((q^2+q+1)m(q+1)/q^3)\sum_{k=1}^{q-1}\{\Xi_k(\tau)^2/\Xi_k(1))\epsilon_k' + (\mathrm{H}_k(\tau)^2/\mathrm{H}_k(1))\epsilon_k'' - (\Phi_{ik}(\tau)^2/\Phi_{ik}(1))\epsilon_k\}\omega_k(\sigma)$$

where $\rho \neq 1$, $\rho \in R_0$, $\sigma \in V$ and $\omega_k(\sigma)$ are the irreducible characters of V. Hence using the orthogonality relation and the value of g we conclude that $(q^3-1)(\Xi_k(\tau)\mathrm{H}_k(1) - \Xi_k(1)\mathrm{H}_k(\tau))^2 = q^3\Xi_k(1)\mathrm{H}_k(1)\Phi_{ik}(1)$. Let $f_1 = \Xi_k(1)$, $f_2 = \mathrm{H}_k(1)$, $a_1 = \Xi_k(\tau)$ and $a_2 = \mathrm{H}_k(\tau)$. Then $\Phi_{ik}(1) = \epsilon(\epsilon_1 f_1 + \epsilon_2 f_2)$ where $\epsilon = \epsilon_k$, $\epsilon_1 = \epsilon_k'$ and $\epsilon_2 = \epsilon_k''$. We have the relation

$$(*) \qquad (q^3-1)(a_2f_1 - a_1f_2)^2 = q^3f_1f_2(\epsilon_2f_1 + \epsilon_1f_2).$$

As before we have $f_i \equiv a_i \pmod{q^2}$. If $b_1(b_2)$ is the value of Ξ_k (or H_k) on elements of order 4, $b_i \equiv a_i \pmod q$ and $|b_i| < q$. Summing Ξ_k (or H_k) over R_1 we get $f_i + \epsilon_i(q^3+1-1) + a_i(q^3+1) \equiv 0 \pmod{2(q^3+1)}$. Set

$$f_i + \epsilon_i q^3 + a_i(q^3+1) = 2k_i(q^3+1).$$

Then $2k_i \equiv f_i + a_i \equiv 2a_i \pmod{q^2}$. Hence $f_i = \epsilon_i + (q^3+1)(a_i - \epsilon_i + l_iq^2)$. In order to simplify the notations we shall drop the suffix i for a while. If l is negative, then $a - \epsilon + lq^2$ is negative (since $|a| < q^2-1$), which is impossible. If $l > 1$, $a - \epsilon + lq^2 > q^2$. Hence $f^2 > (q^3+1)^2q^4 > q^3(q-1)(q^3+1)(q^3-1) = g$ which is impossible. If $l = 1$, then $f = \epsilon + (q^3+1)(q^2+a-\epsilon)$, $f \equiv q^2+a \pmod{q^3}$ and $a \leqq 0$. By summing Ξ_k (or H_k) over Q we get

$$f + (2q^2 - q - 1)a + (q^3 - 2q^2 + q)b \equiv 0 \pmod{q^3},$$

or $f - a + (2q-1)q(a-b) \equiv 0 \pmod{q^3}$. Hence $a \equiv b+q \pmod{q^2}$. Since $|b| < q$, we get $b+q > 0$ and hence $a = b+q-q^2$. The degree f is now written as $f = \epsilon + (q^3+1)(q+b-\epsilon) = (q^3+1)(q+b) - \epsilon q^3$. f is a divisor of g. From the form of f we see that $(f, q^3+1) = 1$ and $f \equiv b \pmod q$. If $f \equiv 0 \pmod q$, we get $b \equiv 0 \pmod q$ and hence $b = 0$. Then $f = q + q^3(q-\epsilon)$ is a divisor of $q(q-1)(q^3-1)$. Since $f \equiv 1+1-\epsilon \pmod{q-1}$, either f is relatively prime to $q-1$ or $(f, q-1) = 3$. Hence $1 + q^2(q-\epsilon) \leqq 3(q^2+q+1)$ or $q - \epsilon < 5$. Hence $q = 4$ and $\epsilon = 1$. The value of f is $4 \cdot 49$ which is not a divisor of g. Hence $f \not\equiv 0 \pmod q$. Let $b = 2^\lambda c$, $c \not\equiv 0 \pmod 2$. Then $2^\lambda < q = 2^\mu$. Let $q+b = x$. f is a divisor of $2^\lambda(q-1)(q^3-1)$. We have therefore $fh = 2^\lambda(q-1)(q^3-1)$ with some integer h. Reducing modulo $2^\lambda q$ we get $h(q+b) \equiv 2^\lambda \pmod{2^\lambda q}$. Hence $h(2^{\mu-\lambda}+c) \equiv 1 \pmod q$. Hence we get $(1+kq)f = (1+kq)\{(q^3+1)x - \epsilon q^3\} = x(q-1)(q^3-1)$. Here k is a non-negative integer and $1 + kq = h(2^{\mu-\lambda}+c)$. If $k = 0$, we have $(q^3+1)x - \epsilon q^3 = x(q-1)(q^3-1)$. Hence $2q^3+1 \geqq (q-1)(q^3-1)$, or $4 > q$ which is not the case. Hence $k > 0$. If $\epsilon = -1$, we get $1 + kq > q-1$ and $(q^3+1)x + q^3 > x(q^3-1)$ which contradict the above equality. Hence $\epsilon = 1$. Expanding both sides we get

$$q^3x + x - q^3 + q^4kx + qkx - q^4k = q^4x - q^3x - qx + x;$$

$q^3(k-1)(x-1) + q^2(2x-1) + (k+1)x = q^3$. Hence either $k = 1$ or $x = 1$. If

$k=1$, $1+q$ is a divisor of $x(q-1)(q^3-1)$. Since $(q+1, q-1)=(q+1, q^2+q+1)=1$, $1+q$ is a divisor of x. Now $1+q$ divides $b-1=x-q-1$. Since $|b|<q$, $b=1$ and $x=1+q$. Hence $q^2(2q+1)+2(q+1)=q^3$ which implies that q is a divisor of 2. This is not the case. If $x=1$, the degree $f=(q^3+1)-q^3=1$. This implies that $a=\pm 1=1-q^2$ which is impossible. Thus in any case the assumption $l=1$ leads to a contradiction. The only possible degree is of the form $f=\epsilon+(q^3+1)(a-\epsilon)=a+q^3(a-\epsilon)$.

Consider the relation (*). We have here $f_i=a_i+q^3(a_i-\epsilon_i)$ $(i=1, 2)$. Hence $a_2f_1-a_1f_2=q^3(a_1\epsilon_2-a_2\epsilon_1)$. Let 2^{λ_i} $(i=1, 2)$ be the highest power of 2 dividing a_i. Assume that $2^{\lambda_i}<q^3$ for $i=1, 2$. If $\lambda_1>\lambda_2$, $a_1\epsilon_2-a_2\epsilon_1$ and $\epsilon_2a_1+\epsilon_1a_2$ are divisible exactly by 2^{λ_2}. Hence the exponent of 2 dividing the left hand side of (*) is exactly $6\mu+2\lambda_2$, while the right side is divisible by only $3\mu+\lambda_1+2\lambda_2<6\mu+2\lambda_2$. We get a similar contradiction in case of $\lambda_1<\lambda_2$. Suppose $\lambda_1=\lambda_2$. Let 2^{λ_3} and 2^{λ_4} be the exact powers of 2 dividing $\epsilon_1a_2+\epsilon_2a_1$ and $\epsilon_1a_2-\epsilon_2a_1$ respectively. Both λ_3 and λ_4 are greater than λ_1 but one of them is equal to λ_1+1. If $\lambda_3=\lambda_1+1$, then $\lambda_4>\lambda_3$. Considering the exponents of 2 dividing both sides of (*) we get $3\mu+\lambda_1+\lambda_2+\lambda_3=6\mu+2\lambda_4>6\mu+2\lambda_3$, or $\lambda_1>3\mu+1$ which is impossible. If $\lambda_4=\lambda_1+1$, then the exponent of 2 dividing $\epsilon_2f_1+\epsilon_1f_2$ is $3\mu+2$. This is impossible since $\epsilon_2f_1+\epsilon_1f_2$ is a degree of an irreducible character. Thus at least one of λ_i, say λ_1, must be greater than 3μ; in other words $a_1\equiv 0 \pmod{q^3}$. Since $|a_1|<q^2$ we have $a_1=0$. Then the degree f_1 is $-\epsilon_1q^3$. Hence $f_1=q^3$ and $\epsilon_1=-1$. The relation (*) is now

$$(q^3-1)a_2^2=f_2(\epsilon_2q^3-f_2).$$

Since $\epsilon_2q^3-f_2>0$, we have $\epsilon_2=1$ and $f_2<q^3$. Hence $f_2=a_2+q^3(a_2-1)=a_2(q^3+1)-q^3<q^3$, which implies that $a_2=1$ and $f_2=1$.

Our result may be summarized as follows: In suitable notations the Ξ_k are linear and $\Xi_k(\tau)=1$, $\epsilon_k'=1$, and the H_k are of degree q^3 and $\epsilon_k''=-1$. Hence the degree of Φ_{ik} is q^3-1 and $\Phi_{ik}(\tau)=-1$, $\epsilon_k=-1$. For the element σ of order 4 we have $\Xi_k(\sigma)=1$ and $\Phi_{ik}(\sigma)=-1$. From the values of characters we see that Ξ_k and H_k belong to the first p-block B of G. B contains $q/2$ more characters which are p-conjugate to each other (cf. [1]). If Θ is one of the characters in the exceptional family of B, Θ must be one of the Θ_j in our notation. We have a relation $\pm\Theta+\sum\delta_k\Xi_k+\sum\delta_k'\mathrm{H}_k=0$ valid for all p-regular elements. Here δ_k and δ_k' are ± 1 and they are determined by the conditions $\Xi_k(1)\equiv\delta_k$ and $\mathrm{H}_k(1)\equiv\delta_k'$ (mod p). Since $p=q^2-q+1$, we have $\delta_k=1$ and all the $\delta_k'=-1$. Hence in particular for the element σ of order 4 we get $\pm\Theta(\sigma)=q-1$. This is however impossible because $q^2=\sum|X_\mu(\sigma)|^2\geqq\sum_j|\Theta_j(\sigma)|^2=q(q-1)^2/2$. Hence

PROPOSITION 9. *The value of m must be* 1.

7. From Proposition 9 we conclude the following proposition.

PROPOSITION 10. *Let G be a finite group satisfying conditions* (A), (B) *and* (C). *Then the order of G is $g=q^3(q-1)(q+1)(q^3-1)$. G contains a subgroup M of index q^2+q+1 which is the normalizer of an elementary abelian group P of order q^2.*

Let $\mathfrak{P}$ be the set of all conjugate subgroups of P. Since M is the normalizer of P, $\mathfrak{P}$ has exactly $1+q+q^2$ elements. We have the following proposition.

PROPOSITION 11. *If P_1 and P_2 are two different elements of $\mathfrak{P}$ then $P_1 \cap P_2 = e$.*

Proof. Suppose $P_1 \cap P_2 = D \neq e$. There is an involution $\tau \in D$. The centralizer of τ contains a normal subgroup Q_0 of order q^3 which contains P_1 and P_2. By Proposition 2 two different elementary abelian subgroups of order q^2 of Q_0 are not conjugate in G. This is a contradiction.

PROPOSITION 12. *G is represented faithfully as a permutation group $\Gamma(P)$ on the set $\mathfrak{P}$. This permutation group $\Gamma(P)$ is doubly transitive.*

Proof. As is well known in the theory of transitive representations of groups $\Gamma = \Gamma(P)$ is isomorphic with the coset representation of G on the cosets of M. The kernel of Γ is therefore the largest normal subgroup of G contained in M. Consider a normal subgroup X of M. If $X \cap P = e$, X is contained in the centralizer of P. On the other hand the centralizer of P coincides with P itself. Hence $X = e$. Hence if $X \neq e$, X must contain an involution τ of P. If X is the kernel of Γ, X contains all involutions of G by the assumption (B). Since M is the normalizer of P, M contains all involutions of G. This is impossible since M contains at most $(q^3-q^2)(q+1)+(q^2-1)=(q^2-1)(q^2+1)$ involutions, while G has exactly $(q^2-1)(q^2+q+1)$ involutions. Hence the kernel of Γ consists of the identity only: in other words Γ is faithful.

We consider the normalizer N of Q. It is not too difficult to show that N has $(q-1)^2$ linear characters, $2(q-1)$ characters of degree $q-1$, one with degree $(q-1)^2$ and $q-1$ characters of degree $q(q-1)$. The faithful irreducible representations are of degree $q(q-1)$. As a matrix representation Γ has degree q^2+q+1. Γ certainly contains the principal character of G. Since Γ is faithful the decomposition of Γ on N contains at least one faithful character of N. Hence Γ has an irreducible component X of degree $\geqq q(q-1)$. Suppose $\Gamma \neq 1+X$; then Γ contains another character Y of degree $\leqq 2q$. The restriction Y' of Y to N does not contain any character of degree $q(q-1)$, since $q(q-1) > 2q$. This means that the representation with the character Y represents every element of C by the unit matrix. Let G_1 be the kernel of this representation. Then G_1 is a proper normal subgroup of G containing all the involutions of G. Hence in particular G_1 contains a 2-Sylow subgroup Q of G. By a well-known argument we conclude that $G = G_1 N$ where N is the normalizer of Q. By the isomorphism theorem we see that $G/G_1 \cong N/N \cap G_1$. Since $N \cap G_1$ contains Q, G/G_1 is abelian. Therefore the degree of Y is one. Since Y is a com-

ponent of Γ, the restriction Y'' to M contains the principal character of M. Hence Y'' is the principal character. This implies that $G_1 \supseteq M$. Since $N \subseteq M$, we conclude that $G = G_1N = G_1M = G_1$ which is a contradiction since G_1 is a proper subgroup. Hence $\Gamma = 1 + X$ and this is equivalent to the double transitivity (cf. [4, §207]).

A similar proposition holds if we replace P by L.

PROPOSITION 13. *The normalizer of L in G has an index q^2+q+1. G is represented as a doubly transitive permutation group on the set of all conjugate subgroups of L and this representation is faithful.*

Our assumptions are symmetric with respect to P and L. So we get this proposition by the same argument as in case of P just replacing P by L.

8. As before let Q be a 2-Sylow subgroup and P and L be two elementary abelian subgroups of order q^2 (cf. §1). P is not conjugate to L (Proposition 2). Let $\mathfrak{P}$ ($\mathfrak{L}$) be the set of all conjugate subgroups of P (L). Hereafter we shall call an element of $\mathfrak{P}$ a *point* and an element of $\mathfrak{L}$ a *line*. We want to define an incidence relation between points and lines so that $(\mathfrak{P}, \mathfrak{L})$ forms a projective plane. Let P_1 be a point and L_1 a line. We shall say that P_1 is on L_1 or L_1 passes through P_1 if and only if $P_1 \cap L_1 \neq e$. From this definition it follows easily that our incidence relation is symmetric with respect to points and lines. Hence we have a duality.

PROPOSITION 14. *The set $\mathcal{P} = (\mathfrak{P}, \mathfrak{L})$ with the incidence relation defined above forms a projective plane.*

Proof. We want to show that two lines have one and only one point in common. Let P be a point. Then the normalizer M of P in G has $1+q$ 2-Sylow subgroups. Take two different 2-Sylow subgroups Q and Q'. Q contains another elementary abelian subgroup L of order q^2. Similarly Q' contains L'. These subgroups L and L' are lines. It is clear that both $L \cap P$ and $L' \cap P$ have orders q and hence $\neq e$. By the definition of incidence P is a common point of two lines L and L'. Suppose that P' is a common point of L and L'. Then we can take involutions τ and τ' of $L \cap P'$ and $L' \cap P'$ respectively. The centralizer of τ contains L and P' and hence L and P' are in the same Sylow subgroup Q_1 of G. Similarly L' and P' are in the same Sylow subgroup Q_1' of G. There is an element σ of G such that $\sigma P \sigma^{-1} = P'$, $\sigma Q \sigma^{-1} = Q_1$ and $\sigma Q' \sigma^{-1} = Q_1'$. (Note that the group M is triply transitive as a permutation group of the 2-Sylow subgroups of M.) Hence $\sigma L \sigma^{-1} = L$ and $\sigma L' \sigma^{-1} = L'$. This means that P and P' are conjugate in the subgroup M_0 consisting of elements which leave L and L' invariant. Using properties of the linear group M/P we know that M_0 is a subgroup of order $q^2(q-1)^2$ and contains P as a normal subgroup. This means $P = P'$. Hence P is the only common point of L and L'. In general if we take two arbitrary lines L_1 and L_2, G contains an element ρ such that $\rho L \rho^{-1} = L_1$ and $\rho L' \rho^{-1} = L_2$ by Proposition 13. Clearly

$\rho P\rho^{-1}$ is the only common point of L_1 and L_2 and our assertion is proved.

From the duality we conclude that two different points determine a unique line passing through both points. From the above consideration a line contains exactly $1+q$ points. Since $1+q+q^2$ is the total number of points, we see that there exist four points no three of which are collinear. Hence $\mathfrak{P}$ forms a projective plane.

PROPOSITION 15. *G is a subgroup of the collineation group of P.*

This proposition is clear from the definitions of points, lines and the incidence relation.

PROPOSITION 16. *P is Desarguesian.*

Proof. We shall apply a theorem of Gleason [5] which says that a projective plane is Desarguesian if for any point P and for any line L passing through P there is a collineation $\neq 1$ which leaves every point on L and every line passing through P fixed. Let P be any point. Then every line L' passing through P is contained in a 2-Sylow subgroup of the normalizer M of P. Hence every element of P leaves every such line invariant. By the duality every element of L leaves every point on L fixed. Hence every element of $L\cap P$ leaves all points of L as well as all lines through P invariant. If P is on L then $L\cap P$ contains a collineation $\neq 1$ by definition. Hence our projective plane $\mathfrak{P}$ satisfies the assumption of Gleason's theorem (loc. cit.) and hence $\mathfrak{P}$ is Desarguesian.

From a property of Desarguesian planes the ground field F of $\mathfrak{P}$ has exactly q elements: $F=GF(q)$. If $q=2^\mu$, the order of the group G^* of all the collineations of $\mathfrak{P}$ is $\mu q^3(q^2-1)(q^3-1)$. G^* contains a normal subgroup G_0 of index μ consisting of all the linear transformations. By Proposition 15 G^* contains a subgroup isomorphic with G. Hence we may consider G itself as a subgroup of G^*. Let $G_1=G\cap G_0$. Then the index $[G_0: G_1]$ is not larger than μ. The only subgroup of G_0 with index $<q$ is G_0 itself or the normal subgroup of index 3 (if $q\equiv 1 \pmod 3$). This may be proved by using the fact G_0 has at most 3 characters of degree $<q$ (cf. the table of characters for G_0 obtained by Steinberg [6]). Suppose $G_1\neq G_0$. Then $[G_0: G_1]=3$. Since G has the same order as G_0 by Proposition 10, we have $[G: G_1]=3$. $G_0^*=GG_0$ is a subgroup of G^* generated by G_0 and a semi-linear transformation σ_0 such that $\sigma_0(\lambda, \mu, \nu)=(\lambda^\sigma, \mu^\sigma, \nu^\sigma)$ where σ is an automorphism of F over F' and $[F: F']=3$. G_1 is the subgroup of G_0 consisting of linear transformations with determinant 1. If C is the center of a 2-Sylow subgroup Q of G, C is a subgroup of G_1 and the centralizer of C in G_1 is of order $q^3(q-1)/3$. Hence the centralizer of C in G contains an element ρ such that $\rho(\lambda, \mu, \nu)=(\lambda^\sigma, \mu^\sigma, \nu^\sigma)A$ where A is a 3×3 matrix with coefficients in F. Since ρ commutes with every involution in C we have $I(\alpha^\sigma)A=AI(\alpha)$ for any $\alpha\in F$, where $I(\alpha)=M(0, \alpha, 0; 1)$ in the notation of the first section. This is however impossible. Hence G_1 must coin-

cide with G_0. Therefore we have $G \supseteq G_0$. By Proposition 10, G has the same order as G_0 and hence we conclude $G = G_0$. Thus we have shown the following final proposition.

PROPOSITION 17. *Let G be a finite group satisfying the conditions* (A), (B) *and* (C). *Then G is isomorphic with the group of all linear fractional transformations of 2 variables over the finite field F of q elements.*

Together with the result of [7] (cf. §3) we get the main theorem stated in the introduction.

BIBLIOGRAPHY

1. R. Brauer, *On groups whose order contains a prime number to the first power* I, Amer. J. Math. vol. 64 (1942) pp. 401–420.

2. ———, *Characterization of some type of finite groups*, Lecture at the University of Tokyo: noted by K. Sekino, Sûgaku vol. 7 (1956) pp. 245–246.

2*. ———, *On the structure of groups of finite order*, Proceedings of the International Congress of Mathematicians vol. 1, 1954, pp. 1–9.

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

4. W. Burnside, *The theory of groups of finite order*, Cambridge, 1911.

5. A. M. Gleason, *Finite Fano planes*, Amer. J. Math. vol. 78 (1956) pp. 797–807.

6. R. Steinberg, *The representations of $GL(3, q)$, $GL(4, q)$, $PGL(3, q)$ and $PGL(4, q)$*, Canad. J. Math. vol. 3 (1951) pp. 225–235.

7. M. Suzuki, *On finite groups containing an element of order 4 which commutes only with its powers*, Illinois J. Math. vol. 3 (1959) pp. 255–271.

8. ———, *On characterizations of linear groups*, I, Trans. Amer. Math. Soc. vol. 92 (1959) pp. 191–204.

9. H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig-Berlin, 1937.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.
UNIVERSITY OF ILLINOIS,
URBANA, ILL.