On Multiplier Groups of Finite Cyclic Planes

CHAT Y. HO

Department of Mathematics, University of Florida, Gainesville, Florida 32611

Communicated by Walter Feit

Received December 1, 1987

1. Introduction

A Singer group of a projective plane is a subgroup of collineations acting sharply transitively on the points of the plane. A cyclic plane is a projective plane with a cyclic Singer group. Infinite cyclic planes are non-Desarguesian [K]. On the other hand, all known finite cyclic planes are Desarguesian.

Let \( \Pi \) be a finite cyclic plane and let \( N \) be the normalizer of a Singer group \( S \) in the collineation group \( G \). Then \( N = S \cdot N_X \), where \( N_X \) is the stabilizer of a point \( X \) of \( \Pi \). The group \( M = N/S \cong N_X \) is independent of \( X \) and \( S \). We call \( M \) the multiplier group of \( \Pi \). The importance of \( M \) in the study of finite cyclic planes can be seen from Ott's result [O], which says that either \( \Pi \) is Desarguesian or \( N = G \). In this paper we determine the structure of the Sylow 2-subgroup of \( M \) and study the relationship between \( M \) and \( \Pi \). Hall [H-P, p. 265] proves that three divides \( |M| \). A moment of thought yields that if \( \Pi \) is a Desarguesian plane of order \( p^k \) for some prime \( p \), then \( |M| = 3k \) (in general \( 3k \) divides \( |M| \)). We will show that the converse of this is true for some values of \( k \). The element in Aut(\( S \)), which inverts every element of \( S \), is known to be not in \( M \) ([B, p. 60] or [F, p. 133]). Therefore \( |M| \leq |\text{Aut}(S)|/2 \). Using Galois theory of cyclotomic fields, we classify planes satisfying \( |M| = |\text{Aut}(S)|/2 \) with the help of the Gaussian quadratic sum. Also we are able to give a complete answer to the case \( |M| = |\text{Aut}(S)|/4 \). More precisely, we prove the following.

**Theorem.** Let \( \Pi \) be a finite cyclic plane of order \( n \) with the multiplier group \( M \). Then the following hold.

1. The Sylow 2-subgroup \( T \) of \( M \) is cyclic. If \( |T| = 2^a \) for some integer \( a \geq 0 \), then \( n = m^{2^a} \) for some integer \( m \geq 2 \).
For $k = 3, 5$ or $2^r$ for some integer $x \geq 0$, we have $|M| = 3k$ if and only if $n = p^k$ for some prime $p$.

We have $|M| = |Aut(S)|/2$ if and only if $n = 2$ or 4. Furthermore, $n = 2$ occurs if and only if $|M| = \text{odd}$ in this case.

We have $|M| = |Aut(S)|/4$ if and only if $n = 3$.

Some remarks are in order. Statement (1) improves a result of Ostrom and Wagner on planar 2-subgroups [D, p. 173] for cyclic planes. The cases for the extreme values of $|M|$ are treated in (2) and (3). In particular, (2) gives a characterization of the order of a finite cyclic plane being a prime if and only if its multiplier group has order 3. The study of finite cyclic planes is equivalent to the study of finite cyclic groups with difference sets [HP]. The latter has a close relationship with cyclotomic fields and number theory. Statements (3) and (4) prove that a finite cyclic group with a difference set, whose multiplier group has order at least $|Aut(S)|/4$, has order 7, 21, or 13. We will prove statement (1) in section (1) for $i = 1, \ldots, 4$.

1. Preliminaries and the Proof of (1)

In the rest of this paper, $\Pi$ is a finite cyclic plane of order $n$. The full collineation (resp. multiplier) group of $\Pi$ is $G$ (resp. $M$). Let $S$ be a Singer group of $\Pi$ and let $N = N_G(S)$. For $X \in G$, let $P(X)$ be the set of fixed points of $X$ and Fix($X$) be the fixed-points-lines substructure of $X$. An involution $\sigma$ in $G$ is a Baer involution if $n$ is a square and Fix($\sigma$) is a subplane of order $\sqrt{n}$ (a Baer subplane). Let $A = \text{Aut}(S)$. An integer $t$ is called a multiplier if the automorphism of $S$ (which is also denoted by $t$) $s \rightarrow s'$ is also a collineation of $\Pi$ when we identify the points of $\Pi$ with the elements of $S$. Our terminology in group theory is taken from [G], that of projective planes is taken from [HP], and that of difference sets is taken from [B]. For the convenience of the reader, we record the following two known results.

Theorem 1.1 (Hall [HP, p. 265]). Any divisor of $n$ is a multiplier.

Lemma 1.2 (Ott [O, 1.4]). Suppose $U$ is a subgroup of $N$ such that $|P(U)| \geq 1$. Then $|P(U)| = |C_S(U)|$. If $|C_S(U)| \neq 1$, then $C_S(U)$ is a Singer group of the subplane Fix($U$) (here a triangle is also regarded as a subplane).

The next lemma is an observation about cyclic groups.

Lemma 1.3. We have $S = S_1 \times \cdots \times S_k$, where $S_1, \ldots, S_k$ are cyclic groups of distinct odd prime power orders. Two involutions $\alpha, \beta$ in $A$ are equal if and only if $|C_S(\alpha)| = |C_S(\beta)|$. 481/122/1-17
Proof. The first statement follows from the fact that \( |S| = n^2 + n + 1 \) is odd. The second conclusion holds because an involution in \( A \) either centralizes or inverts \( S_i \) for \( i = 1, \ldots, h \).

Using structures of orbits of points and lines of various subgroups of \( N \) we now prove (1) in the following steps.

(1–1) The Sylow 2-subgroups \( T \) of \( M \) is cyclic and the involution in \( T \) is Baer.

Proof. Let \( \sigma \) be an involution in \( T \). Then there exists \( s \neq 1 \) in \( S \) such that \( \sigma \) inverts \( s \). Suppose \( \sigma \) is a perspectivity. Since \( s \) has odd order, the two involutions \( \sigma, \sigma s \) are conjugate in \( \langle \sigma, s \rangle \). Hence \( \sigma s \) is also a perspectivity. Thus \( \sigma \) and \( \sigma s \) have a common fixed point which is then fixed by \( s = \sigma(\sigma s) \). But \( S \) acts sharply transitively on the points of \( \Pi \). This contradiction proves that \( \sigma \) is not a perspectivity and so it is a Baer involution [HP, p. 91, Theorem 4.3]. By Lemma 1.2 we have \( |C_2(\sigma)| = |P(\sigma)| = n + \sqrt{n + 1} \). Since this last number is independent of \( \sigma \), Lemma 1.3 implies that \( T \) has at most one involution. So \( T \) is cyclic as desired.

(1–2) If \( |T| = 2^a \), then \( n = m^{2b} \) for some integers \( m \geq 2 \) and \( b \geq a \).

Proof. Let \( |T| = 2^a \). We use induction on \( a \). For \( a = 0 \), (1–2) certainly holds. The case \( a = 1 \) follows from (1–1) as the involution in \( T \) is Baer.

Suppose \( a \geq 2 \). Let \( \tau \in T \) such that \( \tau^2 = \sigma \). Let \( \Omega = \text{Fix}(\sigma) \), a Baer subplane. We will prove that \( \tau \) does not induce the identity collineation on \( \Omega \). Let \( P = C_2(\sigma) \) and \( u = |P| \). Then \( u = n + \sqrt{n + 1} \) by Lemma 1.2. So \( S = P \times Q \), where \( |Q| = n - \sqrt{n + 1} \) and \( \sigma \) inverts every element in \( Q \). Let \( Q_1 = Q \langle \sigma \rangle \). There are exactly \( u \) \( Q \)-orbits of points of \( \Pi \) and each such orbit has exactly one point in \( \Omega \). Since \( \Omega = \text{Fix}(\sigma) \), this shows that each \( Q \)-orbit of points is also a \( Q_1 \)-orbit. So the \( Q \)-orbits of points coincide with the \( Q_1 \)-orbits of points. Let \( l \) be a line of \( \Omega \). Then \( l \) carries \( \sqrt{n + 1} \) points of \( \Omega \). Let \( \Gamma \) be the set of \( n - \sqrt{n} \) points of \( l \) outside \( \Omega \). Thus \( \sigma \) acts fixed-point-freely on the points of \( \Gamma \). So \( \Gamma \) is the union of \( (n - \sqrt{n})/2 \langle \sigma \rangle \)-orbits, each of size 2. We claim the following holds.

(A) Any two such \( \langle \sigma \rangle \)-orbits belong to different \( Q_1 \)-orbits.

Deny this. Let \( O_1, \ldots, O_u \) be the \( Q_1 \)-orbits of points such that \( O_i \) contains \( k_i \) subsets of the said \( \langle \sigma \rangle \)-orbits. Thus there exists \( j \) such that \( 1 \leq j \leq u \) and \( k_j > 1 \). Counting the number of points in \( \Gamma \) yields \( n - \sqrt{n} = \sum_{i=1}^n 2k_i \).

Let \( L = \Gamma^2 \). For \( i \leq 1, \ldots, u \), let \( l_i \) be the number of lines in \( L \) passing through a point of \( O_i \). Since \( L \) has the same cardinality as any \( Q_1 \)-orbit of points, \( l_i \) equals to the number of points of \( O_i \) on \( l \). In particular \( l_i \geq 2k_i \), for \( 1 \leq i \leq u \). Counting \( \{ x \cap y | x \neq y \in L \} \) in two ways yields \( |L|(|L| - 1) = \sum_{i=1}^n |O_i|(l_i)(l_i - 1) \). From \( |L| = |O_i| \) and \( l_i \geq 2k_i \) for \( i = 1, \ldots, u \), the last
equation implies \( n - \sqrt{n} \geq \sum_{i=1}^{n} 2k_i(2k_i - 1) \). On the other hand, \( k_j > 1 \). So \( \sum_{i=1}^{n} 2k_i(2k_i - 1) > \sum_{i=1}^{n} u = n - \sqrt{n} \). Therefore we obtain \( n - \sqrt{n} > n - \sqrt{n} \). This contradiction establishes (A).

We now return to prove that \( \tau \) induces a non-identity collineation on \( \Omega \). Deny this. Thus \( \tau \) fixes \( l \). Since \( \sigma - \tau^2 \) acts fixed-point-freely on \( \Gamma \), so does \( \tau \).

Let \( A \) be a \( \langle \tau \rangle \)-orbit in \( \Gamma \). Then \( A \) is the union of two \( \langle \sigma \rangle \)-orbits: \( A_1, A_2 \). Since \( \tau \) fixes every point in \( \Omega \), \( \tau \) leaves invariant each \( Q_1 \)-orbit of points. Hence \( A_1 \) and \( A_2 \) belong to a common \( Q_1 \)-orbit. This contradicts (A).

Therefore \( \tau \) induces a non-identity collineation on \( \Omega \). So the Sylow 2-subgroup of the multiplier group of \( \Omega \) has order divisible by \( 2^a - 1 \). By induction, the order \( \sqrt{n} \) of \( \Omega \) equals to \( m^2 \) for some integers \( m \geq 2 \) and \( c \geq a - 1 \). This implies that \( n = m^{2^{a+1}} \) and establishes (1-2) as \( c + 1 \geq a \).

(1-3) \( \text{If } |T| = 2^a \), then \( n = m^{2^a} \) for some integer \( m \geq 2 \).

Proof. Without loss of generality, we may assume \( a \geq 1 \). By (1-2), \( n = m^{2^a} \) for some integers \( m \geq 2 \) and \( b > a \). By Theorem 1.1, \( m \) is a multiplier. Therefore \( m^3 \) is also a multiplier. Let \( v = n^2 + n + 1 \). Since \( n^3 \equiv 1 \) (mod \( v \)), \( (m^3)^2b \equiv 1 \) (mod \( v \)). From \( (m^3)^{2b-1} < m^{(2b-1)} \cdot 4 = m^{2b+1} = n^2 \), we obtain that \( 1, m^3, ..., (m^3)^{2b-1} \) are all distinct modulo \( v \). Hence the multiplier \( m^3 \) has order \( 2^b \). This implies \( |T| \geq 2^b \), which in turns yields \( a \geq b \). Therefore \( a = b \) and \( n = m^{2^a} \) as desired.

Statement (1) of the theorem follows from (1-1) and (1-3).

2. PROOF OF (2)

Notations are as in Section 1. Also let \( v = n^2 + n + 1 \). The following result is due to Gordon, Mills, and Welch [B, p. 89].

Theorem 2.1. \( \text{If } n = p^k \) for some non-negative integer \( k \) and prime \( p \), then the multiplier group \( M \) consists of all the powers of \( p \) modulo \( v \).

Theorem 2.1 implies that if \( n = p^k \) for some non-negative integer \( k \) and prime \( p \), then \( M \) is a cyclic group of order \( 3k \) generated by \( p \). In particular, this holds for \( k = 3, 5 \) or \( 2^a \). We divide the rest of the proof of (2), which uses Lagrange's theorem and elementary properties of congruences of integers, into the following steps.

(2-1) \( \text{If } |M| = 3 \cdot 2^a \) for some integer \( a \geq 0 \), then \( n = p^{2^a} \).

Proof. By (1-3), we obtain \( n = m^{2^a} \) for some integer \( m \geq 2 \). Hence \( m \) is also a multiplier of \( \Pi \). Let \( p \) be the smallest prime dividing \( m \). If \( m = pq \) with \( q \geq 1 \), then \( p^{2^{a+1}} = (p^{2^a})^2 < v = n^2 + n + 1 \). Thus \( 1, p, ..., p^{2^{a+1}} \) are dis-
tinct modulo \(v\). Therefore the cyclic subgroup of \(M\) generated by the multiplier \(p\) has order bigger than or equal to \(2^s + 1\). This implies \(M = \langle p \rangle\) by Lagrange’s theorem. Since \(n \in M\), \(n \equiv p^b \pmod{v}\) for some \(0 \leq b < v\). From \(1 \equiv n^3 \equiv p^{3b} \pmod{v}\), we conclude that \(b = 2^s\). Since \(n\) and \(p^{2s}\) are both less than \(v\), we obtain \(n = p^{2s}\) as desired.

(2-2) If \(|M| = 9\), then \(n = p^3\) or \(p\) for some prime \(p\).

**Proof.** Let \(p\) be the smallest prime dividing \(n\), and let \(n = pq\). We may assume \(q > 1\). Then \(p^4 < v\). Hence the cyclic subgroup of \(M\) generated by the multiplier \(p\) has order bigger than 5. This implies \(M = \langle p \rangle\) by Lagrange’s theorem. Since \(n \in M\), we obtain \(n \equiv p^b \pmod{v}\) for some \(1 < b \leq 8\). From \(1 \equiv n^3 \pmod{v}\), we get \(b = 3\). Since \(n\) and \(p^3\) are both less than \(v\), so in fact \(n = p^3\) as desired.

(2-3) If \(|M| = 15\), then \(n = p^5\) or \(p\) for some prime \(p\).

**Proof.** Let \(n = pq\), where \(p\) is the smallest prime dividing \(n\). We may assume \(q > 1\). If \(p = q\), then \(n = p^2\). However, this implies that the multiplier \(p^3\) has order 2, which forces \(|M|\) to be even. This contradiction proves that \(q > p\).

Suppose \(p^4 > v\). Since \(v > p^2q^2\), this implies \(p^3 > q^2\). Therefore the following holds.

(B) \(p^2 > q\).

Assume \(p^5 \equiv 1 \pmod{v}\). Then \(p^5 = 1 + kv\). Since \(p^5 \geq v\), so \(k \geq 1\). From \(p^5 < p^2q^2\), we obtain \(k < p\). Now \(1 + kv = p^5 \equiv 0 \pmod{p}\) implies \(1 + k \equiv 0 \pmod{p}\), which forces \(k = p - 1\) as \(1 \leq k < p\). Therefore \(p^5 = 1 + (p - 1)v = p(1 + (p - 1)(pq^2 + q))\). So \(p^5 = p^2q^2 + pq(1 - q) + 1 - q\). This implies \(0 = 1 - q \pmod{p}\). Let \(1 - q = pw\) for some integer \(w\). Substitute this back to the equation of \(p^5\) to get \(p^4 = p^2q^2 + (pq + 1)pw\). Cancelling \(p\) on both sides yields \(p^3 = pq^2 + (pq + 1)w\), which implies that \(0 \equiv w \pmod{p}\). Therefore \(p^2\) divides \(pw = 1 - q\). Thus \(p^2\) divides \(q - 1\). However, this contradicts (B). Hence \(p^5 \equiv 1 \pmod{v}\) when \(p^5 > v\).

Since \(p^4 < v\), we conclude that 1, \(p, \ldots, p^5\) are all distinct modulo \(v\). Therefore \(M = \langle p \rangle\) by Lagrange’s theorem as \(|M| = 15\). Since \(n \in M\), we get \(n \equiv p^b \pmod{v}\) for some \(0 \leq b < 15\). From \(1 \equiv n^3 \pmod{v}\), we obtain \(b = 5\). Hence \(pq = n \equiv p^5 \pmod{v}\). Since \((p, q) = 1\), this implies \(q \equiv p^4 \pmod{v}\). Therefore \(q = p^4\) as both \(q\) and \(p^4\) are less than \(v\). This proves \(n = pq = p^5\) as desired.

(2-4) If \(|M| = 3k\), where \(k = 3\) or 5, then \(n = p^k\), where \(p\) is a prime.
Proof. By (2-3) and (2-4), it suffices to eliminate the case $n = p$, where $p$ is a prime. If $n = p$, then Theorem 2.1 implies that $|M| = 3$. This contradiction establishes (2-4).

Statement (2) follows from (2-1), (2-4), and the remark on Theorem 2.1.

3. Proof of (3)

Notations as in Section 1. Also $v = n^2 + n + 1 = |S|$. Let $\zeta$ be a primitive $v$th root of 1 in the complex number field. We identify $S$ with $\langle \zeta \rangle$ in $Q(\zeta)$, the cyclotomic field obtained by adjoining $\zeta$ to $Q$, the rationals. Next we identify $A = \text{Aut}(S)$ with the Galois group of $Q(\zeta)$ over $Q$.

A subset of $S$ is called a difference set of $S$ if for any element $s \in S$ there exists exactly one pair of elements $a, b$ in this set such that $s = a - b$. By [B, p. 79, Theorem 4.11], there exists a difference set $D$ of $S$ which is left invariant by $M$. Set $\theta = \sum_{d \in D} \zeta^d$. Then $\theta$ belongs to $K$, the fixed subfield of $M$. With the help of the Gaussian quadratic sum we now prove (3) in the following three steps.

(3-1) If $n = 2$ (resp. $n = 4$), then $|M| = |A|/2 = 3$ (resp. 6).

Proof. Since planes of order 2 and 4 are Desarguesian, our conclusion follows from the general fact that for a Desarguesian plane of order $p^k - n$, where $p$ is a prime, the multiplier group has order $3k$.

(3-2) If $|M| = |A|/2$ is odd, then $n = 2$.

Proof. Denote the complex conjugation of $x$ by $\bar{x}$. Since $-1$ is not a multiplier [B, p. 60], we obtain

(C) \( \bar{\theta} \neq \theta \).

Let $g = \sum_{r = 0}^{v - 1} r^2$ be the Gaussian quadratic sum. Then $g$ is an algebraic integer in $Q(\zeta)$. Since $v$ is odd, by Gauss [N, p. 117] we obtain the following.

(D) If $v \equiv \varepsilon \pmod{4}$, where $\varepsilon = 1$ or $-1$, then $g = \sqrt{v}\varepsilon$.

In particular $[Q(g): Q] = 2$. Since $M$ is the unique subgroup of index 2 in $A$ under our assumption, we conclude that $K$ is the unique subfield of $Q(\zeta)$ with degree 2 over $Q$ by the fundamental theorem of Galois theory. Hence $K = Q(g)$. Note that the Galois group of $K$ over $Q$ is generated by the restriction of the complex conjugation.

Suppose $v \equiv 1 \pmod{4}$. Then $K$ is a subfield of the real numbers by (D). Since $\theta \in K$, this implies $\bar{\theta} = \theta$, which contradicts (C). Therefore $v \equiv 3 \pmod{4}$ and $K = Q(\sqrt{-v})$ by (D) again. As $-v \equiv 1 \pmod{4}$, the ring of
algebraic integers of $K$ is $\mathbb{Z} \oplus \mathbb{Z}((-1 + \sqrt{-v})/2)$ [IR, p. 189]. Hence $	heta = x + (y/2)(-1 + \sqrt{-v})$ for some integers $x$ and $y$. Since $\theta \neq \bar{\theta}$ by (C), $y \neq 0$. Also $\theta \bar{\theta} = (x - y/2)^2 + (y^2v)/4$. On the other hand, from the definition of $\theta$ and the difference set $D$, we obtain $\theta \bar{\theta} = n$ as $\sum_{i=0}^{r-1} s_i = 0$. Therefore $4n = 4\theta \bar{\theta} = (2x - y)^2 + y^2v \geq v = n^2 + n + 1$ as $y \neq 0$. Since $n \geq 2$, this last inequality implies $n = 2$. The proof of (3-2) is now completed.

(3-3) If $|M| = |A|/2$, then $n = 2$ or 4.

Proof. By (3-2), we may assume that $|M|$ is even. Since $-1$ is not a multiplier and $|A| = 2|M|$, the elementary abelian 2-subgroup of $A$ has order 4 by (1-1). This together with the fact that each Sylow subgroup of $S$ is cyclic of odd prime power order implies that $S = S_1 \times S_2$ (see Lemma 1.3). Let $\sigma$ be the involution of $M$. By (1-1), $\sigma$ is a Baer involution. By Lemma 1.2, $|C_S(\sigma)| = n + \sqrt{n + 1} \neq 1$. Thus $C_S(\sigma)$ is one of $S_1, S_2$. Without loss of generality we may assume that $C_S(\sigma) = S_1$. Since $S_1$ is cyclic of odd prime power order, $A_1 := \text{Aut}(S_1)$ is cyclic. Hence the only involution of $A_1$ inverts $S_1$. However, $S_1$ acts sharply transitively on the points of $\text{Fix}(\sigma) = \Omega$, so $-1$ is not a multiplier of $\Omega$. This implies that the multiplier group $R$ of $\Omega$ has odd order. Since the only involution in $M$ centralizes $S_1, A_1 \neq M$. From $|A : M| = 2$, this implies that $A = A_1 M$. Hence $|A_1 : A_1 \cap M| = 2$. Hall [B, p. 83] proves that $M$ induces by restriction a subgroup of the multiplier group of $\Omega$. Therefore $A_1 \cap M \leq R$. Thus $A_1 \cap M = R$ as $A_1 > R$. This implies that $|R| = |A_1|/2$. Since $|R|$ is odd, so (3-2) implies that the order $\sqrt{n}$ of $\Omega$ equals 2. Therefore $n = 4$ as desired.

Statement (3) follows from (3-1), (3-2), and (3-3).

4. Proof of (4)

Notations are as in Section 3. The following is a general fact about cyclic groups of odd order.

**Lemma 4.1.** Let $S = S_1 \times \cdots \times S_h$, where $S_i$ is the cyclic Sylow $p_i$-subgroup of $S$ and $A_i = \text{Aut}(S_i)$ for $i = 1, \ldots, h$. For $i = 1, \ldots, h$ if $p_i > 3$, then there exists $\sigma_i \in A_i$ such that $\sigma_i$ is of odd order and $C_S(\sigma_i) = \prod_{j \neq i} S_j$.

We now prove (4) in the following steps.

(4-1) If $|M| = |A|/4$ is odd, then $n = 3$.

**Proof.** There are two cases for $T = A/M$ to be considered.
**Case 1.** \( T \cong Z_2 \times Z_2 \). We will prove that this case cannot occur. By the structure of \( A = \text{Aut}(S) \), the condition stated in case 1 implies that \( S = S_1 \times S_2 \). Let \( p_1 < p_2 \). So \( 3 < p_2 \). By Lemma 4.1 there exists \( \sigma_2 \in A_2 \) of odd order such that \( C_S(\sigma) = S_1 \). Since \( \sigma_2 \) has odd order, \( \sigma_2 \notin M \). By Lemma 1.2, \( S_1 \) acts as a Singer group on the subplane \( \Pi_2 = \text{Fix}(\sigma_2) \).

Suppose \( |S_1| > 3 \). Then \( \Pi_2 \) is a proper subplane whose multiplier group \( M_2 \) contains \( A_1 \cap M \). Since \(-1\) is not a multiplier of \( \Pi_2 \) and \( |A_1| = 2 \) odd, so \( |A_1| = 2 |M_1| \). By (3-2), the order of \( \Pi_2 \) is 2. Hence \( |S_1| = 7 \), which forces \( p_1 = |S_1| = 7 \). Applying Lemma 4.1 to \( p_1 \) yields \( \sigma_1 \in A_1 \) such that \( \sigma_1 \) has odd order and \( C_S(\sigma_1) = S_2 \). Interchanging the indices 1 and 2 in the above argument, we obtain, as \( p_2 > 3 \), that \( p_2 - |S_2| - 7 \). This contradiction proves that \( |S_1| = 3 \).

Suppose \( |S_2| > p_2 \). Then there exists \( r \in A_2 \) of odd order such that \( |S_2| : C_{S_2}(r) = p_2 \). Let \( W = C_{S_2}(r) \). Thus \( C_S(r) = S_1 \times W \) has order bigger than 3. By Lemma 1.2, \( S_1 \times W \) is a Singer group on the proper subplane \( A = \text{Fix}(r) \). Now \( \text{Aut}(S_1 \times W) = A_1 \times (A_2 / \langle r \rangle) \), which shows that the multiplier group of \( A \) has odd order \( |\text{Aut}(S_1 \times W)| \), where \( e = 2 \) or 4. Therefore the order \( w \) of \( A \) is 2 when \( e = 2 \) by (3-2) or 3 when \( e = 4 \) by induction. This implies that \( |S_1 \times W| = 7 \) or 13 according to \( w = 2 \) or 3. But \( |S_1| = 3 \). This contradiction proves that case 1 cannot occur.

**Case 2.** \( T \) is cyclic of order 4. This implies that \( S \) is a p-group for some prime \( p \). First we show that \( |S| = p \). Deny this. Then there exists \( \sigma \in A \) of odd order such that \( V = C_S(\sigma) \) has index \( p \) in \( S \). If \( |V| = 3 \), then \( |S| = 9 = n^2 + n + 1 \), which is impossible. Hence \( |V| > 3 \). By Lemma 1.2, \( V \) acts as a Singer group on the proper subplane \( \text{Fix}(\sigma) \). Since \( \text{Aut}(V) = A \langle \sigma \rangle \), we get that the multiplier group of \( \text{Fix}(\sigma) \) has odd order \( |\text{Aut}(V)|/4 \). By induction, the order of \( \text{Fix}(\sigma) \) is 3. Hence \( |V| = 13 \) and so \( |S| = 169 \), which is impossible [B, p. 88]. Therefore \( |S| = p \) as desired. Hence \( A \) is cyclic.

By [B, p. 79], \( M \) fixes a line \( l \) of \( \Pi \). We claim the following holds.

(E) Any subgroup of \( M \) fixing at least four points on \( l \) is the identity subgroup.

Let \( H = \langle h \rangle \) be one such subgroup. By Lemma 1.2, \( \text{Fix}(H) \) is a proper subplane. Since \( |S| = p \) is a prime, there are \( p \) conjugates of \( H \) in \( \{ H^s | s \in S \} \). As \( \Pi \) has \( p \) points, the set \( \{ P(H^s) | s \in S \} \) cannot be disjoint. Thus there exists \( x \in S \) such that \( P(H) \cap P(H^x) \neq \emptyset \). Therefore \( h^{-1}h^x \) fixes a point. But \( 1 \neq [h, x] \in S \), which acts sharply transitively on the points of \( \Pi \). This contradiction establishes (E).

From \( |S| = p \) is a prime, we get \( |A| = p - 1 = n(n + 1) \). Let \( O \) be an orbit of points of \( M \) on \( l \). Suppose \( |O| > 3 \). By (E), \( M \) acts fixed-point-freely on \( O \) as \( M \) is cyclic. Hence \( n(n + 1)/4 = |M| \) divides \( |O| \leq n + 1 \). This implies that \( n \leq 4 \). Since \( n = 2 \) or 4 cannot occur, we have \( n = 3 \) and (4-1) is
established in this case. Therefore we may assume that each $M$-orbit of points on $l$ has size 3 or 1 as $|M|$ is odd. If there are two orbits of size 3, then the kernel $H$ of the action of $M$ on each one of these orbits coincide as $M$ is cyclic. Therefore $H = 1$ by (E) and $M$ acts fixed-point-freely on an orbit of size 3. Thus $n(n+1)/4$ divides 3, which forces $n = 3$. However, this contradicts the fact there are two $M$-orbits of size 3 on $l$. Since $S$ is a Singer group, no element of $M$ can fix all points on $l$. Therefore there is exactly one $M$-orbit of points $R$ of size 3 on $l$. If there are at least two more points on $l$, then (E) implies that $M$ acts fixed-point-freely on $R$. Again we obtain $n = 3$. But we have at least $5 = |R| + 2$ point on $l$ under the present assumption. This contradiction proves that there is exactly one more point on $l$ besides the three points in $R$. Therefore $n + 1 = 4$ and $n = 3$ as desired. The proof of (4-1) is now complete.

(4-2) If $|M| = |A|/4$, then $n = 3$.

Proof. By (4-1), we may assume that $|M|$ is even. By (1), the involution $\sigma$ in $M$ is a Baer involution. From Lemma 1.2, $C = C_S(\sigma)$ is a Singer group on the Baer subplane $\Omega = \text{Fix}(\sigma)$. Since $|S|$ is odd $S = C \times [S, \sigma]$, where $|[S, \sigma]| = n - \sqrt{n+1}$, which is prime to $|C|$. Let $X = \text{Aut}(C)$ and $Y = \text{Aut}([S, \sigma])$. Then $|A| = |X|/|Y|$. Let $C = \langle \gamma \rangle \leq S = \langle \zeta \rangle$. Then $Q(\gamma)$ is a Galois extension subfield of $Q(\zeta)$ over $Q$. Hence every Galois automorphism of $Q(\gamma)$ can be extended to a Galois automorphism of $Q(\zeta)$. This shows that an odd-order automorphism of $C$ is the restriction of an element in $M$ as $M$ contains all odd-order automorphism of $S$. Therefore all odd-order automorphisms in $X$ belong to the multiplier group $J$ of $\Omega$. In the proof of (1–2) we see that for $\tau \in M$ with $\tau^2 = \sigma$, the restriction of $\tau$ on $\Omega$ is not the identity collineation. From this and the fact that $-1$ is not a multiplier of $\Omega$, we obtain $|J| = |X|/e$, where $e = 2$ or 4. If $e = 4$, then induction implies that the order $\sqrt{n}$ of $\Omega$ equals 3. Hence $n = 9$. But $|M| = 6 \neq |A|/4$ in this case. Therefore $e = 2$. By (2) we obtain $\sqrt{n} = 2$ or 4. The case $n = 4$ cannot occur as $|M| \neq |A|/4$. So $n = 16$. Since cyclic planes of order 16 are Desarguesian [D, p. 209, 5], we obtain $|M| = 3 \cdot 4$. But $|S| = 3 \cdot 7 \cdot 13$ and so $|A| = 2 \cdot 6 \cdot 12 \neq 4|M|$. This final contradiction establishes (4–2) and completes the proof of the theorem.

REFERENCES


