SINGER GROUPS, AN APPROACH FROM A GROUP OF MULTIPLIERS OF EVEN ORDER

CHAT YIN HO

(Communicated by Ronald M. Solomon)

Abstract. The order of a Sylow 2-subgroup of a multiplier group of an abelian Singer group is at most half the order of the order of a Sylow 2-subgroup of the automorphism group of the Singer group. We determine the situation when equality occurs. We also study the effect of a nontrivial Sylow 2-subgroup of a multiplier group on the structure of the Singer group.

1. Introduction

A Singer group of a projective plane is a collineation group acting regularly on the points of the plane. An automorphism of a Singer group is a multiplier if it is also a collineation when we identify the points of the plane with the elements of the Singer group. The set of all multipliers is called the multiplier group of the Singer group. The importance of the multiplier group can be seen from Ott’s result [O], which states that a projective plane admitting a finite cyclic Singer group is Desarguesian or the full collineation group is a semidirect product of the Singer group with its multiplier group. A remarkable result of Kantor [K] proves that a flag-transitive projective plane of order \( n \) is Desarguesian, or the plane admits a cyclic Singer group such that \( n^2 + n + 1 \) is a prime and the multiplier group has order \( n + 1 \). Note that \( n + 1 \) is a bound of the order of an abelian multiplier group (see, e.g., [Ho2]).

In 1990 Pott and the author [HoP] proved that if the order of a group of multipliers of a finite cyclic Singer group is divisible by the odd part of the order of the automorphism group of the Singer group, then the order of the plane is 2, 3, 4, or 8. Further, divisibility can be replaced by equality if and only if the order of the plane is 2, 3, or 8.

As in group theory, involutions play a special role. A collineation of order 2 is a quasiperspectivity (see, e.g., [HP]), so the number of fixed points of such a collineation is bigger than the order of the plane. In particular, this number is bigger than 1. Hence the automorphism of an abelian Singer group, which inverts every element of \( S \), is not a multiplier. (In fact, a more general statement is true for difference sets. See, e.g., [B] or [L].) Therefore the order...
of a Sylow 2-subgroup of the multiplier group is at most half the order of a
Sylow 2-subgroup of the automorphism group of an abelian Singer group. In
this paper we use the cyclicity of a Sylow 2-subgroup of a multiplier group [Ho1]
to prove the following, which can be considered as the counterpart in the even
case of the above result.

Theorem 1.1. Let \( s \) be the order of a Sylow 2-subgroup of the automorphism
group of an abelian Singer group. Let \( t \) be the order of a Sylow 2-subgroup of
the multiplier group. Then \( s \geq 2t \), and \( s = 2t \) if and only if one of the following
holds:

1. \( t = 1 \). The Singer group is cyclic of prime order \( p \) such that \( p \equiv 3 \mod 4 \). If the order of the plane \( n \) is even, then \( n = 2 \). If \( n \) is odd,
then \( n \equiv 1 \mod 4 \).

2. \( t = 2 \). The Singer group is cyclic of order 21, and the plane is a
Desarguesian plane of order 4.

Some remarks are in order. Theorem 1.1(2) completely determines the struc-
ture of an abelian Singer group whose multiplier group has a maximally permit-
ted nontrivial Sylow 2-subgroup in the sense that its index in a Sylow 2-subgroup
of the automorphism group of the Singer group is 2. The situation is more com-
plicated when the Sylow 2-subgroup of the multiplier group is trivial; in fact,
there is more than one possible value for \( n \) in Theorem 1.1(1), for example,
\( n = 2, 5, 17 \). A plane of order 2 admitting an abelian Singer group has been
characterized by the fact that 2 divides exactly once the order of the plane (see,
e.g., [L, W]). Theorem 1.1(1) provides a characterization of such a plane using
the multiplier group. Also observe that there is more than one solution for
\( s = 4t \) with \( t \neq 1 \), where \( s \) and \( t \) are defined in Theorem 1.1, for example, a
Desarguesian plane of order \( m^2 \), where \( m \) is 3, 4, 5, 7, or 19. We noted that
the plane of order 3 satisfies \( s = 4 \) and \( t = 1 \).

For a Singer group, the question that its automorphism group has even order
is still unsettled. We prove some results in 2.3 and 2.4. The lack of exis-
tence theorems for multipliers for nonabelian Singer groups presents difficulty
in studying the general case even though we know that a Singer group is always
solvable by the celebrated Feit-Thompson Theorem [FT].

The quadratic form \( v(x) = x^2 + x + 1 \), which is the third cyclotomic poly-
nomial, describes the number of points of a finite projective plane. This number
is \( v(n) \), where \( n \) is the order of the plane. An interesting related problem is
to find \( x \) for which \( v(x) \) and \( v(x - 1) \) are both primes. Note that \( x = 2, 3, \)
and 6 are solutions to the above question. Observe that a projective plane of
order 6 does not exist. This motivates us to study the above question subject to
the condition that \( x \) be the order of a projective plane.

Note that the study of finite projective planes admitting a Singer group is
equivalent to the study of planar difference sets of finite groups (see, e.g., [HP]).
The latter is closely related to the theory of cyclotomy studied in the last chapter
of Disquisitiones Arithmeticae by C. Gauss.

2. Definitions, notation, and preliminary results

In this paper \( \Pi \) is a finite projective plane of order \( n \) and \( S \) is a Singer
group of \( \Pi \). The multiplier group of \( S \) is denoted by \( M \). Our terminology
in group theory is taken from [G], that of projective plane is taken from [HP], and that of difference sets is taken from [B] or [L].

For any prime number \( p \) and any integer \( z \), we write \( z = z_p z_{p'} \), where \( z_p \) is the highest power of \( p \) dividing \( z \). For any real number, let \( v(x) = x^2 + x + 1 \). For the convenience of the reader, we record the following two results.

**Theorem 2.1** (Nagel-Ljunggren [Lj]). For any integer \( a \geq 2 \), the only integers \( x, y \) satisfying the equation \( v(x) = y^a \) are either the trivial solutions (i.e., \( y = 1 \) \{or \( y = -1 \), when \( a \) is even\}, \( x = 0 \), or \( x = -1 \)), or \( a = 3 \), \( y = 7 \), \( x = 18 \) or \( x = -19 \).

**Theorem 2.2** [Ho1, Theorems B and C]. A Sylow 2-subgroup of \( M \) is cyclic. Suppose \( M \) has an involution \( \alpha \). Then \( n \) is a square, \( S = AB \), where \( A = [S, \alpha] = \{s \in S|s^\alpha = s^{-1}\} \) is an abelian normal Hall subgroup of order \( v(\sqrt{n} - 1) \), which is an arc (i.e., no three points of \( A \) are collinear), and \( B = C_S(\alpha) \) is a Hall subgroup of order \( v(\sqrt{n}) \), which is a Baer subplane. Further, \( S = A \times B \) except possibly for \( n = 16 \).

We note that Theorem 2.2 can be used to test the commutativity of \( S \) when its multiplier has a nontrivial Sylow 2-subgroup. For example, using the solvability of \( S \), one can prove that if \( n \) is not divisible by 16, then \( S \) is abelian if and only if \( S \) has a subplane of order \( \sqrt{n} \) which is a coset of an abelian subgroup of \( S \).

We now prove the following result concerning a Sylow 2-subgroup of \( M \).

**Theorem 2.3.** Let \( T \) be a Sylow 2-subgroup of \( M \). Then the following hold:

1. Suppose \( T \neq 1 \). Let \( \alpha \) be an involution of \( T \). Then the kernel of the action of \( T \) on \( C_S(\alpha) \) is \( \langle \alpha \rangle \).
2. \( n = m^{|T|} \) for some integer \( m \). If, in addition, \( S \) is abelian, then \( m \) is not a square.

**Proof.** (1) Let \( K \) be the kernel of the action of \( T \) on \( B := C_S(\alpha) \). Assume \( K \neq \langle \alpha \rangle \). Since \( T \) is cyclic by Theorem 2.2, there is \( \beta \in K \) such that \( \alpha = \beta^2 \). Let \( 1 \neq X \) be a point in \( A := [S, \alpha] \) so \( X \) is incident with a line \( l \) of \( B \), as \( B \) is a Baer subplane by Theorem 2.2. Since \( \alpha \) acts fixed point freely on \( A \), \( |X^{(\beta)}| = 4 \). Now \( X \) is incident with \( l \), and \( l = l^\beta \) implies that the four points \( X^{(\beta)} \) are incident with \( l \). On the other hand, Theorem 2.2 asserts that \( A \) is a characteristic subgroup of \( S \). Therefore \( X \in A \) implies that the four collinear points of \( X^{(\beta)} \) belong to \( A \); however, \( A \) is an arc by Theorem 2.2. This contradiction proves (1).

(2) Let \( |T| = 2^c \). We may assume \( c > 0 \). We use the notation introduced in the proof of (1). By (1), \( T \) induces a group of multipliers of order \( 2^{c-1} \) of the Baer subplane \( B \); thus, a Sylow 2-subgroup of the multiplier group of \( B \) has order \( 2^b \) for some \( b \geq c - 1 \). We now apply induction on the order of a projective plane admitting a Singer group. The order of the Baer subplane \( B \) (with Singer group \( B \)) is \( \sqrt{n} \). Induction implies that \( \sqrt{n} = u^{2^b} \) for some integer \( u \); hence, \( n = m^{2^c} \), where \( m = u^{2^{b-1}} \). Since \( b \geq c - 1 \), \( m \) is an integer as desired.

Suppose \( S \) is abelian. Hall's multiplier theorem (see, e.g., [L]) asserts that any divisor \( l \) of \( n \) is a multiplier (i.e., the automorphism \( z \rightarrow z^l \) is a multiplier). Since \( n^3 \equiv 1 \pmod{v(n)} \), the multiplier \( n \) has order 3. Therefore if
$n = v^{2d}$ for some $d$, then $v^3$ is a multiplier of order $2^d$, so $|T|$ is at least $2^d$. Apply this to the case in which $v = m$ and $d = c$. If $m$ is a square, then $|T| \geq 2^{c+1}$, a contradiction. This contradiction completes the proof of the theorem.

In the rest of this section, let $T$ be a Sylow 2-subgroup of $M$, and let $t = |T|$.

If $t > 1$, let $\alpha$ be the involution of $T$, $A = [S, \alpha]$, and $B = C_S(\alpha)$. Also let $|\text{Aut}(S)|_2 = s$.

The planes of order 16 merit some discussion. For these planes, $|S| = 3 \cdot 7 \cdot 13$. A Hall-$7 \cdot 13$-subgroup $H$ of $S$ is cyclic and normal in $S$; thus, $S/C_S(H)$ is isomorphic to a subgroup of order 1 or 3 in $\text{Aut}(H) \cong Z_6 \times Z_{12}$.

If $S$ is abelian, then $S$ is cyclic and the plane is Desarguesian with $|M| = 12$; thus, $t = 4$ and $s = 2 \cdot 2 \cdot 4 = 2^2t$ in this case.

There are four subgroups of order 3 in $\text{Aut}(H)$, each of which yields a possibility for a nonabelian $S$. In only one of these, the corresponding $B$ is abelian of order 21 as a group. By 2.3, $t \leq 4$. Note that in this case if we write $s = 2^b t$, then $t \leq 2^{b+1}$ for all possibilities of $t$. In all other cases, $B$ is nonabelian, so the multiplier group of $B$ has odd order (see, e.g., [Ho1, 2.2]). By 2.3, $t \leq 2$. Since $s = 2 \cdot 4$, it follows that $2^2t \leq s$.

**Proposition 2.4.** Suppose $s = 2^b t$. Then $t \leq 2^{b+1}$. If $S$ is abelian, then $t \leq 2^b$.

**Proof.** We may assume that $t > 1$. The above discussion on planes of order 16 shows that the proposition holds for $n = 16$.

Assume now $n \neq 16$. By Theorem 2.2, $S = A \times B$, so $\text{Aut}(S) = \text{Aut}(A) \times \text{Aut}(B)$. By 2.3, the restriction of $T$ on $A$ is isomorphic to $T$, and the restriction of $T$ on $B$ has order $t/2$. This implies that $|\text{Aut}(A)|_2 \geq t$ and $|\text{Aut}(B)|_2 \geq t/2$. Hence

$$2^b t = s \geq t \cdot t/2,$$

so $t \leq 2^{b+1}$ as desired.

Suppose $S$ is abelian. Then $B$ is an abelian Singer group; hence the involution of $\text{Aut}(B)$, which inverts every element in $B$, is not a multiplier of $B$. Since the restriction of $T$ to $B$ is a group of multipliers of $B$, $\frac{1}{2}|\text{Aut}(B)|_2 \geq t/2$ in this case. Therefore (2.1) becomes $2^b t \geq t \cdot t/2$; hence $2^b \geq t$. This completes the proof of the proposition.

**Corollary 2.5.** If $s = t \neq 1$, then $t = 2$; $S$ is nonabelian; $A$ is cyclic of prime order $p$ such that $p \equiv 3 \pmod{4}$; and $|\text{Aut}(B)|_2 = 1$.

**Proof.** Apply 2.4 to the case of $b = 0$. We see that $t = 2$ and $S$ is nonabelian under the present assumption, so $s = 2$; therefore $n \neq 16$. By Theorem 2.2, $S = A \times B$. Since the kernel of the restriction of $T$ to $A$ is trivial by 2.3, $|\text{Aut}(A)|_2 \geq 2$. Since $s = 2$ and $s = |\text{Aut}(A)|_2|\text{Aut}(B)|_2$, $|\text{Aut}(A)|_2 = 2$. Two conclusions follow from this and $s = 2$ immediately. The first is $|\text{Aut}(B)|_2 = 1$. The second is that $A$ is cyclic of prime power order as $A$ is abelian by Theorem 2.2. Since $|A| = v(\sqrt{n} - 1)$, $|A|$ is a prime or $|A| = 7^3$ by Theorem 2.1. Suppose $|A| = 7^3$. Then $\sqrt{n} - 1 = 18$. Hence $n = 19^2$, and $|B| = v(19) = 3 \cdot 127$; however, this implies that $|\text{Aut}(B)|_2 \neq 1$, as the Sylow $\{127\}$-subgroup of $B$ is normal in $B$. This contradiction proves that $|A| = p$ is a prime. The fact that $p \equiv 3 \pmod{4}$ follows from $|\text{Aut}(A)|_2 = 2$.\[\text{License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use}\]
3. Proof of Theorem 1.1

We continue to use notation introduced in §2. Further, we assume that $S$ is abelian. Since the involution inverting every element of $S$ is not a multiplier of $S$, $s = 2^t$ with $b \geq 1$. In the rest of this section, we assume $s = 2t$. We now prove Theorem 1.1. By 2.4, $t \leq 2$.

Suppose $t = 1$. Then $s = 2$. This implies that $S$ is a cyclic group of prime order. Since a cyclic plane of order 18 does not exist (see, e.g., [D]), $|S| \neq 7^3$. This implies that $S$ is cyclic of prime order $p$ by 2.1. Since $2 = s = (p-1)/2$, $p \equiv 3 \pmod{4}$. Note that $p-1 = n(n+1)$. Suppose $n$ is even. As $(p-1)/2 = 2$, this implies that $2\|n$, which forces $n = 2$ (see, e.g., [L]). If $n$ is odd, then $2 = (p-1)/2 = (n+1)/2$ implies $n \equiv 1 \pmod{4}$. This establishes (1) of Theorem 1.1.

From now on we assume that $s = 2t$ and $t > 1$. By 2.4 we obtain $t = 2$, so $s = 4$. Since $S$ is abelian, $S = A \times B$. By 2.3 the restriction of $T$ on $A$ is isomorphic to $T$. Since $s = 2t$ and Aut$(B)$ has even order, we see that $|\text{Aut}(A)|_2 = t = 2$. This implies that $A$ is a cyclic group of prime power order. If $|A| = 7^3$, then $\sqrt{n} - 1 = 18$, so $|B| = v(\sqrt{n}) = v(19) = 381 = 3 \cdot 127$. Thus $|\text{Aut}(B)|_2 = 2 \cdot 2 = 4$. So $|\text{Aut}(A)|_2 \cdot |\text{Aut}(B)|_2 = 2 \cdot 4 = s = |\text{Aut}(S)|_2$, which is impossible. This contradiction proves that $|A| \neq 7^3$; therefore, $|A|$, being of the form $v(\sqrt{n} - 1)$, is a prime, say $p$, by Theorem 2.1. As $2 = t = |\text{Aut}(A)|_2$, we have

$$p \equiv 3 \pmod{4}.$$

Next we look at the decomposition of $S = A \times B = P_1 \times \cdots \times P_v$ into a direct product of cyclic groups of prime power order. As $A$ has prime order $p$ and $(|A|, |B|) = 1$, we may assume $P_1 = A$ and $p$ does not divide the order of any one of the subgroups $P_2, \ldots, P_v$. From $s = 4$ we infer that a Sylow 2-subgroup of Aut$(S)$ is either isomorphic to $Z_2 \times Z_2$ or to $Z_4$. This implies that the number $v$ of the direct factors of $S$ is at most 2. Since $|B| > 1$, this forces $v = 2$ and $B$ is a cyclic group of prime power. Since $B$ is a Baer subplane, $\sqrt{n} \neq 18$ as a projective plane of order 18 admitting an abelian Singer group does not exist. Hence $|B| \neq 7^3$. Since $|B| = v(\sqrt{n})$, Theorem 2.1 implies that $|B|$ is a prime, say $q$.

As $2t = s = |\text{Aut}(A)|_2 \cdot |\text{Aut}(B)|_2$ and $|\text{Aut}(A)|_2 = t$, we have $|\text{Aut}(B)|_2 = 2$. This implies that

$$q \equiv 3 \pmod{4}.$$

Suppose $n \equiv 0 \pmod{3}$. Since $S$ is abelian, this implies that 2 does not divide $n$ (see, e.g., [L]). Now $n$ is odd and a square, so $n \equiv 1 \pmod{4}$. Hence $v(n) = n^2 + n + 1 \equiv 3 \pmod{4}$; however, (3.1) and (3.2) imply that $v(n) = pq \equiv 3 \cdot 3 \equiv 1 \pmod{4}$. This contradiction proves $n \not\equiv 0 \pmod{3}$.

Assume now $n \neq 0 \pmod{3}$. Since $n$ is a square, this implies that $v(n) \equiv 0 \pmod{3}$. Thus 3 divides $pq$. Since $q = v(\sqrt{n}) > v(\sqrt{n} - 1) = p$, we have $p = 3$. Hence $\sqrt{n} - 1 = 1$; therefore, $n = 4$. This completes the proof of Theorem 1.1.

Acknowledgment

The author would like to thank Professor W. Feit for his encouraging conversations. The author would also like to express his gratitude to the Department of Mathematics, Yale University, where this article was written.
References


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

E-mail address: cyh@math.ufl.edu