PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 109, Number 3, July 1990

MULTIPLIER GROUPS OF PLANAR DIFFERENCE SETS AND A THEOREM OF KANTOR

CHAT YIN HO AND ALEXANDER POTT

(Communicated by Warren J. Wong)

ABSTRACT. A recent result of W. Kantor followed by a work of W. Feit has rekindled interest in the longstanding conjecture of finite cyclic planes. In this paper we prove that the order of the multiplier group equals the odd part of the order of the automorphism group of a Singer group if and only if the order of the plane is 2, 3, or 8. This yields another proof for Feit's result mentioned above.

1. INTRODUCTION

Let G be a finite group of order v written multiplicatively. A subset D of G is a planar difference set if each nonidentity element of G can be expressed as xy^{-1} for $x, y \in D$ exactly once. The study of finite cyclic planes is equivalent to the study of finite cyclic groups with planar difference sets. (See, for example, [B] or [HP].) The latter leads to the study of multipliers. Let Π be a finite cyclic plane and let N be the normalizer of a Singer group S (i.e. S is a cyclic collineation group of Π which acts sharply transitively on the points of Π) in the full collineation group. Then $N = S \cdot N_X$, where N_X is the stabilizer of a point X of Π in N. The group $N/S \cong N_X$ is independent of X and S. This is the multiplier group of Π, which can be identified as $\mathrm{Aut}(S) \cap \mathrm{Aut}(\Pi)$. The importance of the multiplier group can be seen from Ott's result of 1975 [O], which states that a finite cyclic plane is Desarguesian or a Singer group is normal in the full collineation group. In this paper we prove the following.

Theorem 1.1. *If the order of a group of multipliers of a finite cyclic plane is divisible by the odd part of the order of the automorphism group of a Singer group, then the order of the plane is* 2, 3, 4, *or* 8. *In particular, the order of the multiplier group equals the odd part of the order of the automorphism group of a Singer group if and only if the order of the plane is* 2, 3, *or* 8.

Received by the editors August 29, 1989 and, in revised form, October 10, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 51E15, 20B25, 05B10, 11T15.
The second author thanks the Deutsche Forschungsgemeinschaft for its financial support and the University of Florida for its hospitality during the time of this research.

0002-9939/90 $1.00 + $.25 per page

A flag is an incident point-line pair. It is conjectured that every finite projective plane which admits a flag transitive collineation group must be Desarguesian. Evidence for this conjecture was obtained by W. Kantor who uses the classification of finite simple groups and detailed knowledge of their maximal subgroups of odd index to prove the following important result in 1987 [K].

Theorem 1.2 (Kantor). *Let Π be a projective plane of order n admitting a flag transitive collineation group G. Then Π is Desarguesian or G is a Frobenius group of order $(n^2+n+1)(n+1)$ and n^2+n+1 is a prime.*

Using planar different sets and number theory, W. Feit gave an elegant proof of the following result in 1988 [F].

Theorem 1.3 (Feit). *Let Π be a flat transitive projective plane of order n which is not Desarguesian. Then $p = n^2+n+1$ is a prime, $n \equiv 0 \pmod 8$, n is not a power of 2 and $d^{n+1} \equiv 1 \pmod p$ for every divisor d of n.*

We could obtain Theorem 1.3 from Theorem 1.1 as follows. If n is a power of 2, then the multiplier group has order $n+1$, which equals the odd part of the order $n(n+1)$ of the automorphism group of a Singer group. By Theorem 1.1, this implies $n = 2$, or 8 and the plane is Desarguesian. Hence n cannot be a power of 2 when Π is not Desarguesian. It is well known that if $2^a | n$, but $2^{a+1} \nmid n$ for $a = 1$, or 2, then $n = 2^a$. (See, for example, [JV].) Finally, the order of the multiplier group being $n+1$ implies that $d^{n+1} \equiv 1 \pmod p$ for every divisor d of n by Hall's multiplier theorem (Theorem 2.1 below).

2. Preliminary results

In this section, Π is a finite cyclic plane of order n. Let S be a Singer group of Π, and let N be the normalizer of S in the full collineation group of Π. For any collineation group H, let $P(H)$ be the set of fixed points of H and $\mathrm{Fix}(H)$ be the fixed-points-lines substructure of H. An integer t is called a multiplier if the automorphism of S: $s \to s^t$ is also a collineation of Π when we identify the points of Π 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 readers, we record the following known results.

Theorem 2.1 (Hall [HP]). *Any divisor of n is a multiplier.*

Theorem 2.2 (Gordon, Mills, and Welch [B]). *If $n = p^k$ for some nonnegative integer k and prime p, then the multiplier group consists of all the powers of p modulo n^2+n+1.*

Lemma 2.3 (Ott [O]). *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 $\mathrm{Fix}(U)$. (Here a triangle is also regarded as a subplane.)*

For brevity, we write difference sets for planar difference sets. The order of a difference set D is defined to be $|D| - 1$.

Lemma 2.4. *Let D be a difference set of order n of a cyclic group $G = G_1 \times \cdots \times G_h$, where G_i is the Sylow p_i-subgroup of G for $i = 1, \ldots, h$. Assume M is a group of multipliers of G. If M fixes D and $G_2 \times \cdots \times G_h \subseteq C_G(M)$, then the following holds.*

(1) *There exists a shift $R = Dg$ of D such that R is fixed by M, and R contains a generator of G.*
(2) $|M| \leq n + 1$.

Proof. By the definition of a difference set, we see that $D \not\subseteq H$, for any proper subgroup H of G. Let $\overline{G} = G/\Phi(G)$, where $\Phi(G)$ is the Frattini subgroup of G. Then $\overline{G} \cong Z_{p_1} \times \cdots \times Z_{p_h}$. As no proper subgroup can contain D, $\overline{D}$ will contain an element $x = (x_1, \ldots, x_h)$, such that $x_1 \neq 1$. Let $d \in D$ such that $\overline{d} = x$. Multiplying d by a suitable element $g \in G_2 \times \cdots G_h$, we may assume $\overline{dg} = (y_1, \ldots, y_h)$ with $y_1 \neq 1 \neq \cdots \neq y_h$. Thus $G = \langle dg \rangle$. Since $g \in C_G(M)$ and M fixes D, we obtain that M fixes Dg. This proves (1).

Next we prove (2). By (1) we may assume that there is a difference set R of G invariant under M and containing a generator d of G. If $d^\alpha = d^\beta$, for $\alpha, \beta \in M$, then $\alpha = \beta$ as $\langle d \rangle = G$. Hence $|M| = |\{d^\alpha : \alpha \in M\}| \leq |R| = n + 1$ as required.

Corollary 2.5. *Let D be a difference set of order n of a cyclic group G. Suppose $|G| = 3^i \cdot p^s$, $i \in \{0, 1\}$, and p is a prime different from 3. Assume M is a group of multipliers of G, and $|M|$ is odd. If M fixes D, then the following holds.*

(1) *There is a shift Dg of D such that Dg contains a generator of G, and Dg is fixed by M.*
(2) $|M| \leq n + 1$.

Proof. Since $|M|$ is odd, our condition on $|G|$ forces that $C_G(M)$ contains the Sylow 3-subgroup of G. This establishes (1) and (2) by applying Lemma 2.4.

We remark that $D = \{3, 6, 12, 7, 14\}$ is a difference set of Z_{21} (written additively). The multiplier group M generated by the multiplier: $x \to 2x$ has order 6 and D is the only shift of D fixing by M. Both conclusions (1) and (2) of Corollary 2.5 fail in this example.

3. Proof of Theorem 1.1

We continue to use the notations in the first paragraph of the last section. Further, for any positive integer z we use $z_{2'}$ to denote the odd part of z (i.e. $z = 2^k(z_{2'})$ and $z_{2'}$ is odd). If the order n of the plane is 2, 3, 4, or 8, then the plane is Desarguesian and the full multiplier group has order 3, 3, 6, or 9, respectively, which is divisible by the odd part of the order of the automorphism group of a Singer group, respectively.

Let $v = n^2 + n + 1$. Let M be a group of multipliers of Π which satisfies the conditions of Theorem 1.1. There is a difference set D invariant under M. (See, for example, [HP].) We divide the rest of the proof of Theorem 1.1 into the following three steps.

Lemma 3.1.

(1) *If* $|M|$ *is even, then* $n = 4$.
(2) *If* $v = p$ *or* $3p$ *for some prime* $p \neq 3$ *and* $|\mathrm{Aut}(S)|_{2'}$ *divides* $|M|$, *then* $n = 2, 3, 4,$ *or* 8.

Proof. Suppose $|M|$ is even. Then M has only one involution α, which is a Baer involution [Ho]. As $|\mathrm{Aut}(S)|_{2'}$ divides $|M|$, M induces on the Baer subplane $C_S(\alpha)$ a group of multipliers whose order is divisible by $|\mathrm{Aut}(C_S(\alpha))|_{2'}$. By induction, $\sqrt{n} \in \{2, 3, 4, 8\}$. Hence $n \in \{4, 9, 16, 64\}$. Only $n = 4$ survives the condition that $|\phi(v)|_{2'}$ divides $|M|$, where $\phi(v)$ denotes the Euler function. This proves (1).

In proving (2), we may assume, by (1), that $|M|$ is odd. Thus, without loss of generality, we may assume $|M| = |\mathrm{Aut}(S)|_{2'}$.

First we treat the case in which v is a prime. Hence $|\mathrm{Aut}(S)| = v - 1 = n(n+1)$ in this case. Further $C_S(m) = 1$ for any $1 \neq m \in M$. Thus a nontrivial element in M fixes one point only. Since M fixes a line, this implies that $|M| \leq n + 1$.

Suppose n is even. Since $n + 1$ is odd, we obtain $|M| \geq n + 1$. So $|M| = n + 1$. This forces $n = 2^k$ for some nonnegative integer k. By Theorem 2.2, we obtain $3k = |M| = 2^k + 1$. Hence $k = 1$, or 3, and so $n = 2$, or 8 as required.

If n is odd, then $|M| \geq n$. Since $|M| \leq n + 1$, this implies that $n + 1 = 2^k$ for some nonnegative integer k and $|M| = n$. Since 3 divides $|M|$ by Theorem 2.1, $2^k - 1 = n = |M| \equiv 0 \pmod 3$. Hence k is even. Let $k = 2a$. Then $n = 2^{2a} - 1 = (2^a + 1)(2^a - 1)$. By Theorem 2.1, $x \to tx$ for $t \in \{1, 3, 2^a + 1, 2^a - 1\}$ are multipliers for S (written additively at this moment). By Corollary 2.5, there is a difference set R of S such that R is M invariant and R contains a generator c of S. Thus $\{c, 3c, (2^a + 1)c, (2^a - 1)c\} \subseteq R$. So $3c - c = (2^a + 1)c - (2^a - 1)c$. This contradicts the fact that every nontrivial element has only one representation as a difference of two elements in the difference set R unless $a = 1$. Therefore $a = 1$ and $n = 3$ as desired.

Next we treat the case in which $v = 3p$ for some prime p different from 3. Thus $\mathrm{Aut}(S) \cong Z_2 \times Z_{p-1}$. By Corollary 2.5, $|M| \leq n + 1$. Now $|M| = |\mathrm{Aut}(S)|_{2'} = (p-1)_{2'}$. This implies that for any nontrivial element $m \in M$, $C_S(m)$ is the Sylow 3-subgroup of S as $v = 3p$. Lemma 2.3 yields that for any nontrivial element $m \in M$, $P(m)$ is a set of 3 noncollinear points, which is independent of m as M is cyclic. The action of M on the points of a line incident with two of the fixed points provides that $n - 1 \equiv 0 \pmod{|M|}$. Hence $n \equiv 1 \pmod 3$ as 3 divides $|M|$. From $3(p-1) = (n-1)(n+2)$,

we get $p-1=((n-1)/3)(n+2)$ is an integral factorization of $p-1$. If n is odd, then $n+2$ is odd and $n+1 \geq |M| = (p-1)_{2'} \geq n+2$. This contradiction proves that n is even. We may assume that $n \neq 2$. Hence $n \equiv 0 \pmod 4$. (See, for example, [JV].) Thus $(n+2)/2$, $(n-1)/3$ are both odd. So $(n-1)(n+2)/6 = |M|$. Since $|M| \leq n+1$, this implies that $n=4$. But for $n=4$, $|M|=6$, which is not odd. This contradiction establishes the lemma.

Lemma 3.2. *If* $v = 3^i \cdot p^k$, $i \in \{0, 1\}$, $k \geq 2$ *for some prime* p, *then* $|M| \neq |\mathrm{Aut}(S)|_{2'}$.

Proof. Since 9 never divides v, which is always odd, $p > 3$. Suppose $|M| = |\mathrm{Aut}(S)|_{2'}$. Since 3 divides $|M|$, $|M| \geq 3 \cdot p^{k-1}$. By Corollary 2.5, $|M| \leq n+1$. Thus $n+1 \geq 3 \cdot p^{k-1}$. So $3^i \cdot p^k = v \geq (3p^{k-1}-1)^2 + 3p^{k-1}$. This implies $3^i p > 9p^{k-1} - 6$, which is impossible as $i \in \{0, 1\}$ and $k \geq 2$. This contradiction proves the lemma.

We now turn to the final step of the proof of Theorem 1.1. Let $S = Z_3^i \times S_1 \times \cdots \times S_h$ be the factorization of S into its Sylow subgroups. Then $i \in \{0, 1\}$. By 3.1.(1) we may assume $|M| = |\mathrm{Aut}(S)|_{2'}$. By 3.1(2) and 3.2, we may assume in addition that $h \geq 2$. Suppose there is $j \in \{1, \ldots, h\}$ such that $|S_j| = p_j^b$ with $b > 1$. Then there is $\alpha \in \mathrm{Aut}(S_j)$ of odd order. Hence $\alpha \in M$ and $C_S(M)$ contains all the Sylow subgroups of S except S_j. By Lemma 2.3, $\mathrm{Fix}(\alpha) = \Gamma$ is a subplane, which is not a triangle as $h \geq 2$. This subplane, which can be identified as $C_S(\alpha)$, is M invariant, and M induces a subgroup of the multiplier group on it. Since $|M| = |\mathrm{Aut}(S)|_{2'}$, the order of the group induced by M on Γ equals the odd part of the order of the automorphism group of a Singer group of Γ. By induction Γ has order 2, 3, or 8. This means $|C_S(\alpha)| = 7$, 13, or 73. In other words, $i=0$ and $S = S_j \times T$, where $|T| = 7$, 13, or 73. Now $\mathrm{Aut}(T)$ has an element β of odd order. Hence $\beta \in M$. Applying the above argument for α to β, we get $|S_j| = 7$, 13, or 73. This contradiction proves that each S_j has prime order for $j \in \{1, \ldots, h\}$.

Since 3 divides $|M|$, 3 divides $|\mathrm{Aut}(S_t)|$ for some $t \in \{1, \ldots, h\}$. So $\mathrm{Aut}(S_t)$ has an element γ of order 3. Applying the above argument for α to γ, we get $i=0$ and $S = S_t \times T$, where $|T| = 7$, 13, or 73 by induction. Using the same argument for T in the last paragraph, we obtain $|S_t| \in \{7, 13, 73\}$. Thus $|S| = 7 \cdot 13$, $7 \cdot 73$, or $13 \cdot 73$. If $|S| = 7 \cdot 13$, then S is a Singer group of the Desarguesian plane of order 9, and $|M| = 6$. This contradicts $|M|$ being odd. If $|S| = 7 \cdot 73$ or $13 \cdot 73$, then $|S| \neq n^2 + n + 1$. This completes the proof of Theorem 1.1.

References

[B] L. D. Baumert, *Cyclic difference sets*, Springer Lecture Notes in Math., vol. 182, New York, 1971.

[F] W. Feit, *Finite projective planes and a question about primes*, preprint, 1988, pp. 1–3.

[G] D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.

[Ho] C. Y. Ho, *On multiplier groups of finite cyclic planes*, J. Algebra **122** (1989), 250–259.

[HP] D. R. Hughes and F. C. Piper, *Projective planes*, Graduate Text, Springer, New York, 1973.

[JV] D. Jungnickel and K. Vedder, *On the geometry of planar difference sets*, European J. Combin. **5** (1984), 143–148.

[K] W. Kantor, *Primitive permutation groups of odd order and an application to finite projective planes*, J. Algebra **106** (1987), 15–45.

[O] U. Ott, *Endliche zyklische Ebenen*, Math. Z. **144** (1975), 195–215.

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

Mathematisches Institut, Justus-Liebig Universität, Arndtstr. 2, D-6300, Giessen, West Germany