CYCLIC AFFINE PLANES

A. J. HOFFMAN

1. Introduction. Let Π be an affine plane which admits a collineation τ such that the cyclic group generated by τ leaves one point (say X) fixed, and is transitive on the set of all other points of Π. Such "cyclic affine planes" have been previously studied, especially in India, and the principal result relevant to the present discussion is the following theorem of Bose [**2**]: every finite Desarguesian affine plane is cyclic. The converse seems quite likely true, but no proof exists. In what follows, we shall prove several properties of cyclic affine planes which will imply that for an infinite number of values of n there is no such plane with n points on a line. Our results are approximately parallel to those obtained by Hall [**6**] in his investigation of cyclic projective planes (projective planes admitting a collineation τ such that the group generated by τ is transitive on *all* the points), and our methods are derived from his stimulating and penetrating work. One contrast with the projective case, however, is that every cyclic plane is necessarily finite; for if P and Q are points collinear with X, and if $Q = \tau^d P$, then τ^d leaves the line $P\,Q\,X$ fixed, which implies that the orbit of P under τ belongs to a finite set of lines, and hence cannot contain all points of an infinite plane.

2. Affine difference sets. The integer n will always be the number of points on a line of the cyclic affine plane Π and $N = n^2 - 1$. We now show that the study of cyclic affine planes is equivalent to the study of "affine difference sets" of order n. (This was done by Bose [**2**] under the additional hypothesis that Π was Desarguesian.) The connection between cyclic projective planes and difference sets was first pointed out by Singer [**7**] in a paper which essentially inaugurated the subject.

The order of the cyclic collineation τ is N. Let P be any point of Π other than X. Then each point of Π other than X can be expressed uniquely as $\tau^r P$, where r runs over all residue classes mod N. If we write r in place of $\tau^r P$, the lines of the plane may be tabulated as follows:

(2.1) *The ith line containing X $(i = 0, \ldots, n)$ consists of X and all $r \equiv i$* (mod $n + 1$);

(2.2) *The ith line not containing X $(i = 0, \ldots, N - 1)$ consists of $d_1 + i, \ldots, d_n + i$* (mod N), *where the members of the "affine difference set" $\{d_\nu\}$ are residue classes* mod N *such that the $n^2 - n$ differences $d_\alpha - d_\beta$ $(\alpha \neq \beta)$ are precisely the $n^2 - n$ residues* mod N *which are not* 0 (mod $n + 1$). *Further, the $\{d_\nu\}$ are in "standard form":*

$$d_\nu \not\equiv 0 \pmod{n+1}, \qquad \nu = 1, \ldots, n.$$

Received January 29, 1951. This work was done under a grant from ONR.

https://doi.org/10.4153/CJM-1952-026-8 Published online by Cambridge University Press

Proof. Let m be the smallest positive power of τ leaving PX fixed. It is clear that τ^r leaves PX fixed if and only if r is a multiple of m. In particular, $m|N$. Since PX contains $n - 1$ points other than X, there are exactly $n - 1$ distinct residue classes mod N congruent to 0 (mod m). Hence $m = n + 1$, and PX contains X and all residues mod N congruent to 0 (mod $n + 1$); $\tau^i PX$ contains X and all residues mod N congruent to i (mod $n + 1$). This proves (2.1).

Let l be any line of Π parallel to PX, and let the points of l be $d_1, \ldots, d_n$. Let $d \not\equiv 0$ (mod $n + 1$). Then $\tau^d l \neq l$, nor is $\tau^d l$ parallel to l. For in either case we would have $\tau^d PX = PX$, contrary to 2.1. Hence $\tau^d l$ meets l in a single point $d_\alpha \equiv d_\beta + d$ (mod N); thus $d_\alpha - d_\beta \equiv d$ (mod N). It is also easy to see that $\tau^i l = l$ if and only if $i \equiv 0$ (mod N). This proves (2.2).

Conversely, if an affine difference set is given, it can be put in standard form [**2**], and (2.1) and (2.2) describe an affine plane with the cyclic collineation $X \rightarrow X$, $i \rightarrow i + 1$ (mod N). Some trivial remarks follow at once:

(2.3) *The projective extension of* Π *admits a polarity* ρ.

Proof. Define ρ to be the following correspondence: $X \leftrightarrow$ the line at infinity, the point $i \leftrightarrow$ the $(-\,i)$th line of (2.2), the intersection of the line at infinity with the ith line of (2.1) $\leftrightarrow$ the $(-\,i)$th line of (2.1).

(2.4) *A necessary and sufficient condition that* Π *be Desarguesian is that it admit a collineation that moves* X.

Proof. The necessity is clear. For the sufficiency, it is easy to verify that if the vertices of two triangles are perspective from X, and if two of the pairs of corresponding sides are parallel, then the third pair of corresponding sides is parallel. It is then obvious that the given condition is sufficient for the validity of the affine Desargues' theorem.

(2.5) *Let* s *be a number and* σ *the mapping* $\sigma : X \rightarrow X$, $i \rightarrow si$ (mod N). *Then a necessary and sufficient condition that* σ *be a collineation is that there exist a number* k *such that* $sd_1, \ldots, sd_n$ (mod N) *is a rearrangement of* $d_1 + k, \ldots, d_n + k$ (mod N).

Proof. The necessity is immediate. For the sufficiency, it is clear that all we need show is that $(s, N) = 1$. But the given condition implies that the set $\{sr\} = \{s(d_\alpha - d_\beta)\}$, where r runs over all residues mod N except multiples of $n + 1$, is again the set $\{r\} = \{d_\alpha - d_\beta\}$ (mod N). If $(s, N) = t > 1$, then $s1 \equiv s(1 + N/t)$ (mod N), violating the condition.

A number s with the property described in (2.5) is called a *multiplier* of the difference set (or a multiplier of the plane).

3. Multipliers.

We first prove a theorem conjectured by Chowla [**4**] in 1945. We wish to thank Dr. Gerald Estrin for a valuable suggestion contributed to the proof.

3.1. THEOREM. *$p|n$ implies p is a multiplier.*

https://doi.org/10.4153/CJM-1952-026-8 Published online by Cambridge University Press

Proof. For convenient reference, we list several ideas:

(3.1.1) If a and b are non-negative integers and m is a positive integer, then $a \equiv b \pmod{m}$ if and only if $x^a \equiv x^b \pmod{x^m - 1}$.

(3.1.2) If $f(x)$ is a polynomial all of whose coefficients are non-negative, and if $g(x)$ is a polynomial of degree less than m, then $f(x) \equiv g(x) \pmod{x^m - 1}$ implies that the coefficients of $g(x)$ are non-negative.

(3.1.3) $f(x) \equiv g(x) \pmod{x^m - 1}$ implies that the sum of the coefficients of $f(x)$ equals the sum of the coefficients of $g(x)$.

(3.1.4) If $d|m$, $f(x) = 1 + x^d + \ldots + x^{(m/d-1)d}$, and $g(x)$ is any polynomial, then there is a polynomial $g_1(x)$ of degree less than d such that $f(x)\,g(x) \equiv f(x)\,g_1(x) \pmod{x^m - 1}$.

(3.1.5) In the special case of (3.1.4) in which all the non-zero terms of $g(x)$ are of the form cx^{kd}, we have $g(x)\,f(x) \equiv gf(x) \pmod{x^m - 1}$, where g is the sum of the coefficients of $g(x)$.

Now for the proof proper. We may assume that $0 < d_i < N$ (recall that $\{d_\nu\}$ is a standard difference set), and that p is a prime. Let $\theta(x) = x^{d_1} + \ldots x^{d_n}$. Then

(3.1.6) $$\theta(x)\theta(x^{N-1}) \equiv n + P(x)(R(x) - 1) \qquad \bmod x^N - 1,$$

where $P(x) = 1 + x^{n+1} + \ldots + x^{(n-2)(n+1)}$, and

$$R(x) = 1 + x + \ldots + x^n.$$

Since p is prime to $n^2 - 1$, the numbers $pd_1, \ldots, pd_n$ form an affine difference set; hence by (3.1.1)

(3.1.7) $$\theta(x^p)\theta(x^{(N-1)p}) \equiv n + P(x)(R(x) - 1) \qquad \bmod x^N - 1.$$

$p|n$ and $P(x)|x^N - 1$, so we may change the modulus of (3.1.6) to the double modulus p, $P(x)$, obtaining

(3.1.8) $$\theta(x)\theta(x^{N-1}) \equiv 0 \qquad \operatorname{modd} p, P(x).$$

Hence, $\theta(x^p)\theta(x^{N-1}) \equiv \theta(x)^p\theta(x^{N-1}) \equiv \theta(x)^{p-1}\theta(x)\theta(x^{N-1}) \equiv 0$ (modd p, $P(x)$), which can be expressed as

(3.1.9) $$\theta(x^p)\theta(x^{N-1}) \equiv pf(x) + P(x)g(x) \qquad \bmod x^N - 1.$$

By (3.1.4), we may assume $g(x) = g_0 + g_1 x + \ldots + g_n x^n$, and because of the presence of the term $pf(x)$, we may take $0 \leqslant g_1 \leqslant p - 1$. Further, writing $f(x) = C_0 + C_1 x + \ldots + C_{N-1}x^{N-1}$, we have $C_i \geqslant 0$, by (3.1.2). Since $R(x)|x^{n+1} - 1$, and $P(x) \equiv n - 1 \pmod{x^{n+1} - 1}$, (3.1.9) yields

(3.1.10) $$\theta(x^p)\theta(x^{N-1}) \equiv -g(x) \qquad \operatorname{modd} p, R(x).$$

On the other hand, since $d_1, \ldots, d_n$ is a standard difference set,

$$\theta(x) \equiv R(x) - 1 \qquad \bmod x^{n+1} - 1;$$

a fortiori,

(3.1.11) $$\theta(x) \equiv -1 \qquad \operatorname{modd} p, R(x).$$

https://doi.org/10.4153/CJM-1952-026-8 Published online by Cambridge University Press

From (3.1.6), we obtain

$$\theta(x)\theta(x^{N-1}) \equiv 1 \qquad \text{modd } p,\ R(x),$$

which combines with (3.1.11) to give

$$\theta(x^p)\theta(x^{N-1}) \equiv (-1)^{p-1} \equiv 1 \qquad \text{modd } p,\ R(x). \tag{3.1.12}$$

Hence the right side of (3.1.10) is congruent to the right side of (3.1.12) (modd p, $R(x)$), so using (3.1.5) with $d = 1$, we have

$$g(x) + 1 \equiv ph(x) + kR(x) \qquad \text{mod } x^{n+1} - 1, \tag{3.1.13}$$

where k is an integer (which we may take $0 \leqslant k \leqslant p - 1$) and $h(x)$ is some polynomial. Hence, $g_1 = \ldots = g_n = k \equiv g_0 + 1 \pmod{p}$. We cannot have $g_0 + 1 = p$, for from (3.1.9) and (3.1.3), this would imply

$$n^2 = pf + (n-1)(p-1),$$

where f is the sum of the coefficients of $f(x)$; that is $p|(n-1)(p-1)$, which is impossible. Therefore, $g_0 + 1 = k$, and

$$n^2 = pf + (n-1)(nk + k - 1);$$

that is, $p|k - 1$, so $k = 1$, $f = n/p$, $g(x) = R(x) - 1$. Therefore (3.1.9) can be rewritten

$$\theta(x^p)\theta(x^{N-1}) \equiv pf(x) + P(x)(R(x) - 1) \qquad \text{mod } x^N - 1. \tag{3.1.14}$$

Replace x in (3.1.14) by x^{N-1}, and from (3.1.1) obtain

$$\theta(x)\theta(x^{(N-1)p}) = pf(x^{N-1}) + P(x)(R(x^{N-1}) - 1) \quad \text{mod } x^N - 1. \tag{3.1.15}$$

The product of the left-hand sides of (3.1.14) and (3.1.15) equals the product of the left-hand sides of (3.1.6) and (3.1.7). Hence, the respective right-hand products are congruent.

$$\begin{aligned} n^2 + 2nP(x)(R(x) - 1) + P^2(x)(R(x) - 1)^2 &\equiv p^2 f(x) f(x^{N-1}) \\ &+ pP(x)[f(x)(R(x^{N-1}) - 1) + f(x^{N-1})(R\ (x) - 1)] \\ &+ P^2(x)(R(x) - 1)(R(x^{N-1}) - 1) \qquad \text{mod } x^N - 1. \end{aligned} \tag{3.1.16}$$

But $P(x)R(x) \equiv P(x)R(x^{N-1}) \equiv 1 + x + \ldots + x^{N-1}$ (mod $x^N - 1$). Using this and (3.1.5), (3.1.16) becomes

$$n^2 - 2nP(x) \equiv p^2 f(x) f(x^{N-1}) - pP(x)[f(x) + f(x^{N-1})] \text{ mod } x^N - 1. \tag{3.1.17}$$

Change the modulus to $x^{n+1} - 1$, and (3.1.17) reads

$$n^2 - 2n(n-1) \equiv p^2 \bar{f}(x)\bar{f}(x^{N-1}) - p(n-1)[\bar{f}(x) + \bar{f}(x^{N-1})] \qquad \text{mod } x^{n+1} - 1, \tag{3.1.18}$$

where

$$\bar{f}(x) = \sum_{i=0}^{n} e_i x^i, \quad e_i = \sum_{j=0}^{n-2} C_{j(n+1)+i}.$$

The term on the left of (3.1.18) must be the same as the constant term on the right of (3.1.16) after reduction mod $x^{n+1} - 1$. Therefore,

$$n^2 - 2n(n-1) = p^2 \sum_{i=0}^{n} e_i^2 - 2p(n-1)e_0.$$

Add $(n-1)^2$ to both sides. Then

$$1 = p^2 \sum_{i=1}^{n} e_i^2 + [pe_0 - (n-1)]^2.$$

Hence $e_1 = \ldots = e_n = 0$. Therefore,

$$f(x) = C_0 + C_{n+1}x^{n+1} + \ldots + C_{(n-2)(n+1)}x^{(n-2)(n+1)}.$$

By (3.1.5), this implies

$$P(x)f(x) \equiv P(x)f(x^{N-1}) \equiv \frac{n}{p}P(x) \qquad \bmod x^N - 1.$$

Therefore, (3.1.17) becomes

$$n^2 \equiv p^2 f(x)f(x^{N-1}) \qquad \bmod x^N - 1,$$

and recalling that the coefficients of $f(x)$ are non-negative, this obviously implies that $f(x)$ consists of a single term, say

$$f(x) = \frac{n}{p}x^{t(n+1)}.$$

Substituting in (3.1.14),

$$(3.1.19) \qquad \theta(x^p)\theta(x^{N-1}) \equiv nx^{t(n+1)} + P(x)(R(x) - 1) \qquad \bmod x^N - 1.$$

But by (3.1.1), this means that n of the differences $pd_\alpha - d_\beta$ have the same value mod N, namely, $t(n+1)$. Further, if $pd_\alpha - d_\beta \equiv pd_\mu - d_\nu \pmod N$, then $\alpha = \mu$ if and only if $\beta = \nu$. Hence the set of numbers $pd_1, \ldots, pd_n$ is a rearrangement of $d_1 + t(n+1), \ldots, d_n + t(n+1) \pmod N$. By (2.5), p is a multiplier.

3.2. Theorem. *Let σ be the collineation of* Π *corresponding to the multiplier s. The fixed elements of σ form a sub-plane* Π_1 *if and only if* $(s-1, n+1) \geqslant 3$. *In this case,* $(s-1, N) = ((s-1, n+1) - 1)^2 - 1$.

Proof. Since σ leaves X fixed, the set of fixed elements forms a sub-plane Π_1, if and only if σ fixes at least three lines of (2.1), that is, if and only if $sx \equiv x \pmod{n+1}$ has at least three solutions, which is equivalent to $(s-1, n+1) \geqslant 3$. The second part of the theorem follows from a simple counting.

It is also possible to show that Π_1 is cyclic, and every multiplier of Π is also a multiplier of Π_1, but we omit the details.

3.3. Theorem. *There is always at least one line of* (2.2) *left fixed by all multipliers.*

Proof. Let n be even. Then 2 is a multiplier, and the corresponding collineation fixes X, 0, the intersection of $X0$ and the line at infinity, and no other points

https://doi.org/10.4153/CJM-1952-026-8 Published online by Cambridge University Press

of the projective extension of Π. It fixes the line $X0$ and the line at infinity, so by a theorem of Baer [**1**, p. 155] exactly one other line must be left fixed. This line must be parallel to $X0$ (and hence belong to (2.2)), or another point would be fixed. By the reasoning of Hall [**6**, p. 1089], this line is fixed by all multipliers.

Let n be odd. Then S is a multiplier only if S is odd, so the $\frac{1}{2}(n + 1)$th line of (2.1) is fixed by all multipliers. Therefore the line of (2.2) containing 0, parallel to this line, is fixed by all multipliers.

4. Non-existence theorems. It is known from the projective case that the preceding results imply that, for various values of n, there is no cyclic affine plane with n points on a line.

4.1. Corollary. *There is no cyclic affine plane with n points on a line if n is divisible by both of the primes in any one of the following pairs:*

(2,3), (2,5), (2,7), (2,11), (2,13), (2,17), (2,19), (2,23), (2,29), (2,31), (2,47), (2,61), (2,67), (2,71), (2,79), (3,5), (3,7), (3,11), (3,13), (3,17), (3,19), (3,29), (5,7), (5,11), (5,13), (5,29).

Proof as in [**6**, p. 1089].

4.2. Corollary. *There is no cyclic affine plane with n points on a line if there exist primes p and q such that* $n \equiv 1 \pmod{p}$, $p \equiv 3 \pmod 4$, *q divides the square-free part of n and* $(-p|q) = 1$.

4.3. Corollary. *There is no cyclic affine plane with n points on a line if n is not a square and there is an odd prime p such that* (i) $n \equiv 1 \pmod{p}$, *and* (ii) *some product of divisors of n is a primitive root of p.*

Proof. Let $\epsilon = e^{2\pi i/p}$. Substituting in (3.6), we have $\theta(\epsilon)\,\overline{\theta(\epsilon)} = \theta(\epsilon)\,\theta(\epsilon^{-1}) = n$; 4.2 then follows from the method of Chowla and Ryser [**4**, p. 95]; 4.3 follows from the method of Hall [**6**, p. 1089].

The theorems of this section, and the celebrated theorem of Bruck and Ryser [**3**], which established the non-existence of affine planes (whether cyclic or not) for various values of the number of points on a line, along with 3.2, are sufficient to decide the question of existence for all $n < 212$.

5. Remark. It is natural in the context of investigations on cyclic planes to inquire what can be said about an affine plane that admits a collineation cyclic on *all* its points. The answer is easily given: such a plane can only have two points on a line. We leave to the reader the proof that no infinite plane has this property. Here is a sketch of the proof for finite planes, with n points on a line:

Designating the points of the plane by residue classes mod n^2 in the familiar manner, it turns out, using the theorem of Baer quoted in 3.3 and the methods of §2, that the plane contains one pencil of n parallel lines such that the ith line consists of all residues congruent to $i \pmod{n}$. Further, if l is any other line, with points $d_0, \ldots, d_{n-1}$, then the differences $d_\alpha - d_\beta$ $(\alpha \neq \beta)$ yield all residues mod n^2 exactly once, except multiples of n. Accordingly, we choose our notation

https://doi.org/10.4153/CJM-1952-026-8 Published online by Cambridge University Press

so that $d_i \equiv i \pmod{n}$. Now precisely n of these differences will yield residues mod n^2 which are congruent to 1 (mod n), namely,

$$\begin{array}{lrcll} & d_1 - d_0 & \equiv & a_0 n + 1, & \\ (5.1) & d_2 - d_1 & \equiv & a_1 n + 1, & \\ & \ldots & & \ldots & \\ & d_0 - d_{n-1} & \equiv & a_{n-1} n + 1 & \qquad \bmod n^2. \end{array}$$

The a^{ν} form a complete system of residues mod n. Adding equations (5.1), we obtain

$$0 \equiv \tfrac{1}{2}n^2(n-1) + n \qquad \bmod n^2,$$

which is impossible if $n > 2$. For $n = 2$, such a collineation clearly exists.

References

1. R. Baer, *Projectivities of finite projective planes*, Amer. J. Math., vol. 69 (1947), 653-684.
2. R. C. Bose, *An affine analogue of Singer's Theorem*, J. Indian Math. Soc., vol. 6 (1942), 1-15.
3. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., vol. 1 (1949), 88-93.
4. S. Chowla, *On difference-sets*, J. Indian Math. Soc., vol. 9 (1945), 28-31.
5. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., vol. 2 (1950), 93-99.
6. M. Hall, *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), 1079-1090.
7. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., vol. 43 (1938), 377-385.

Institute for Advanced Study
Princeton, N.J.