THE FLAG-TRANSITIVE COLLINEATION GROUPS OF THE FINITE DESARGUESIAN AFFINE PLANES

DAVID A. FOULSER

1. Introduction. Let π be the Desarguesian affine plane of order $n = p^r$, for p a prime and r a positive integer. A collineation group G of π is defined to be *flag-transitive* on π if G is transitive on the set of incident point-line pairs, or *flags*, of π. Further, G is *doubly transitive* on π if G is doubly transitive on the points of π. Clearly, G is flag transitive if G is doubly transitive on π.

The purpose of the following study is the explicit determination of the flag-transitive and the doubly transitive collineation groups of π (I am indebted to D. G. Higman for suggesting this problem). The results can be summarized in Theorems 1′ and 2′ below (a complete description of the results is contained in Sections 12–15).

Since π is a Desarguesian plane, π can be represented by the Galois field $\mathrm{GF}(n^2)$ as a two-dimensional vector space over $\mathrm{GF}(n)$. That is, the points of π are represented by the elements of $\mathrm{GF}(n^2)$, and the lines of π are represented by the cosets of the one-dimensional subspaces of $\mathrm{GF}(n^2)$. Let $\mathbf{G}$ be the full collineation group of π, let E be the subgroup of $\mathbf{G}$ generated by the elations of π, and let U be the group of those collineations which are induced by the non-singular mappings of $\mathrm{GF}(n^2)$ of the form:

$$x \to ax^{p^b} + c.$$

THEOREM 1′. *With a finite number of exceptions, a flag-transitive collineation group of π either contains E, or is conjugate in $\mathbf{G}$ to a subgroup of U.*

THEOREM 2′. *With one exception, two flag-transitive collineation groups of π are isomorphic only if they are conjugate in $\mathbf{G}$.*

The class of flag-transitive subgroups of U described in Theorem 1′ can be very large for a given plane π. This fact contrasts with the corresponding theorem for a finite Desarguesian projective plane $\tilde{\pi}$; namely, with two exceptions, a flag-transitive group of $\tilde{\pi}$ contains the little projective group of $\tilde{\pi}$ **(8)**. However, the corresponding results for affine and projective spaces of higher dimensions are similar (see Theorem 6, Section 18). The question of the existence of finite non-Desarguesian flag-transitive affine planes is largely unanswered (the near-field plane of order 9 is one example of such a plane, see Section 16; recently, the author has found two such planes of order 25). However, A. Wagner **(15a)** has recently shown that such a plane is a translation

Received April 10, 1963. This research was supported by U.S. Air Force Contract AF-49-638-774.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

plane. One additional piece of information concerning doubly transitive planes is derived in Section 16 from **(8, 11)** and Theorem 1.

THEOREM 5. *An arbitrary finite affine plane which has a solvable doubly transitive collineation group is either a Desarguesian plane or the near-field plane of order* 9.

The proofs of the preceding theorems use elementary number theory, finite field theory, and the structures of π and $\mathbf{G}$. Of particular importance is the determination of all transitive collineation groups of L_∞, the Desarguesian projective line of order n, and this determination depends on the structure of $PGL_2(n)$, the group of linear collineations of L_∞.

The preceding results are contained in the author's doctoral dissertation at the University of Michigan. The author would like to express his appreciation to Professor D. G. Higman for his encouragement and supervision of the research which is discussed in this article.

2. Notation and definitions.

Let G be a permutation group acting on a set S. G is defined to be a *sharply k-fold transitive* permutation group if G is k-fold transitive on S, and if no non-identity element of G fixes k distinct elements of S. If $a, b, \ldots, c$ are elements of S, then $G_{(a,b,\ldots,c)}$ denotes the subgroup of G which fixes each element $a, b, \ldots, c$. G is a *Frobenius* group if G is transitive on S, $G_{(a)} \neq 1$, and $G_{(a,b)} = 1$, for any distinct elements a and b of S.

If H and K are subgroups of a group G, let $(G{:}H)$ denote the index of H in G, let $\mathbf{N}_K(H)$ and $\mathbf{C}_K(H)$ denote the normalizer and the centralizer of H in K, respectively, and let $\mathbf{A}(G)$ denote the group of automorphisms of G. Further, let $H \simeq K$ denote that H is isomorphic to K.

The symbol $\{\nu, \sigma, \ldots, \tau\}$ denotes the set of elements $\nu, \sigma, \ldots, \tau$. If $\nu, \sigma, \ldots, \tau$ are elements of a group G, then $\langle \nu, \sigma, \ldots, \tau\rangle$ denotes the subgroup of G generated by $\nu, \sigma, \ldots, \tau$. The order of G is denoted by $|G|$, and $|\eta| = |\langle\eta\rangle|$, for $\eta \in G$.

Let a, b, and c be integers. The greatest common divisor and the least common multiple of a and b are denoted by (a, b) and $\mathrm{LCM}(a, b)$, respectively. If $(a, c) = 1$, then $t = \mathrm{ord}_c\, a$ denotes the order of a (mod c), i.e., the least positive integer t such that $a^t \equiv 1 \pmod{c}$. If p is a prime, then $p^c \| a$ is defined by $a \equiv 0 \pmod{p^c}$ and $a \not\equiv 0 \pmod{p^{c+1}}$. The symbol $(2; 1)$ is defined by $(2; 1) = (p + 1, p - 1) = 1$ or 2 according as $p = 2$ or $p \neq 2$, respectively. Lastly, the symbol φ denotes Euler's function.

In addition to the preceding notation, the following number-theoretic lemmas will be required. Let p and q be primes, and let d, s, k, and t be positive integers.

2.1. LEMMA. *The set* $\{(p^{si} - 1)/(p^s - 1)\}$ *for* $1 \leqslant i \leqslant d$ *is a complete residue system* (mod d) *if and only if the primes of d divide* $p^s - 1$, *and either* $p^s \not\equiv 3$ (mod 4) *or* $d \not\equiv 0$ (mod 4).

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

Proof. The proof follows directly from Lemma (2.2).

2.2. Lemma. *Let* $p^s \equiv 1 \pmod q$. *If* $q^a \| t$, *then* $q^a \| (p^{st} - 1)/(p^s - 1)$ *except if* $p^s \equiv 3 \pmod 4$, $q = 2$, *and t is even. In this case,* $2^{a+b-1} \| (p^{st} - 1)/(p^s - 1)$, *where* $2^b \| p^s + 1$ and $b \geqslant 2$.

Proof. The proof follows from **(12**, Theorem 4–5, p. 50**)**, with modifications if $q = 2$.

2.3. Lemma. *The relation* $(p^d + 1, p^s - 1) = p^{(d,s)} + 1$ *holds if* $d/(d, s)$ *is odd and* $s/(d, s)$ *is even. Otherwise,* $(p^d + 1, p^s - 1) = (p + 1, p - 1)$.

Proof. Note that $(p^d + 1, p^s - 1)$ divides

$$(p - 1, p + 1)\{(p^{(2d,s)} - 1)/(p^{(d,s)} - 1)\}.$$

2.4. Lemma. *There exists a prime q such that* $p^t - 1 \equiv 0 \pmod q$, *but* $t \not\equiv 0 \pmod q$ *and* $p^k - 1 \not\equiv 0 \pmod q$ *for* $k < t$, *except in the following cases:* (i) $t = 2$ *and* $p + 1 = 2^x$, *for some positive integer x;* (ii) $p^t = 64$.

Proof. See **(3**, Theorem V, p. 177**)**.

3. Outline of the proof. Let π be the Desarguesian affine plane of order $n = p^r$ represented as in Section 1 by $GF(n^2)$. Let ω be a primitive root of $GF(n^2)$, and let α be the automorphism of $GF(n^2)$ of order $2r$ defined by $\alpha(x) = x^p$. The mappings $x \rightarrow \omega x$, $x \rightarrow \alpha(x)$, and $x \rightarrow x + a$ (for $a \in GF(n^2)$) induce collineations of π, which will be denoted by ω, α, and τ_a, respectively. Let $V = \langle \omega, \alpha \rangle$, $T = \langle \tau_a : a \in GF(n^2) \rangle$, and $U = \langle T, V \rangle$. Let $\Gamma L = \Gamma L_2(n)$ be the group of all non-singular semilinear transformations of π as a two-dimensional vector space over $GF(n)$. Then $\mathbf{G}$, the collineation group of π, is the split extension of T by ΓL; and $\Gamma L = \mathbf{G}_{(0)}$ is the subgroup of $\mathbf{G}$ fixing the point 0 of π. Similarly, $U = T \cdot V$ is the split extension of T by V, and $V = U_{(0)}$. Note that $|T| = n^2$, $|\Gamma L| = rn(n - 1)^2(n + 1)$, and $|V| = 2r(n^2 - 1)$.

Let L_∞ be the Desarguesian projective line of order n. The line L_∞ can also be represented by $GF(n^2)$ by regarding the one-dimensional subspaces of $GF(n^2)$ over $GF(n)$ as the points of L_∞. Moreover, L_∞ can be regarded as the line at infinity of π. Let $P\Gamma L = P\Gamma L_2(n)$ be the collineation group of L_∞ and note that $|P\Gamma L| = rn(n^2 - 1)$. Let ρ be the natural homomorphism mapping $\mathbf{G}$ onto $P\Gamma L$. The kernel of ρ is $T \cdot \langle \omega^{n+1} \rangle$, of order $n^2(n - 1)$.

3.1. Lemma. *Let* $\mathbf{G}$ *be a collineation group of* π. *Then G is flag-transitive on* π *if and only if the following conditions are satisfied:*

(1) $T \subset G$,

(2) $\rho(G)$ *is transitive on* L_∞.

Proof. If G is flag-transitive on π, then clearly $\rho(G)$ is transitive on L_∞. Moreover, $n^2(n + 1)$ divides $|G|$ and $|\rho(G)|$ divides $rn(n^2 - 1)$. Since $r \not\equiv 0 \pmod{p^r}$, it follows that $T \cap G \neq 1$. Hence $T \subset G$ since $T \cap G \lhd G$ and since G is a primitive permutation group on the points of π **(8**, Proposition 3**)**.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

Conversely, if $T \subset G$, then $G = TG_{(0)}$ is the split extension of T by the subgroup of G fixing the point 0, and $\rho(G) = \rho(G_{(0)})$. So G is transitive on the points of π, and Condition (2) implies that $G_{(0)}$ is transitive on the lines of π which contain 0. Therefore, G is flag-transitive on π.

3.2. *Definition.* If X is a class of collineation groups of L_∞, define $\rho^{-1}(X)$ to be the class consisting of those subgroups G of $\mathbf{G}$ such that $T \subset G$ and $\rho(G) \in X$. If J is a collineation group of L_∞, define $\rho^{-1}(J)$ to be the largest subgroup G of $\mathbf{G}$ such that $\rho(G) = J$.

3.3. Corollary. *If $\mathfrak{F}$ and $\mathfrak{T}$ are the class of flag-transitive collineation groups of π and the class of transitive collineation groups of L_∞, respectively, then $\mathfrak{F} = \rho^{-1}(\mathfrak{T})$.*

It is now possible to outline the proof of Theorem 1′. Sections 4–11 describe three classes of flag-transitive groups of π: $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$, and the corresponding classes of transitive groups of L_∞: $\mathfrak{A}_\rho$, $\mathfrak{B}_\rho$, and $\mathfrak{C}_\rho$. The class $\mathfrak{A}$ consists of the flag-transitive subgroups of U, $\mathfrak{B}$ consists of the subgroups of $\mathbf{G}$ which contain E, and $\mathfrak{C}$ consists of a finite number of additional flag-transitive groups. Moreover, these classes satisfy the relations: $\rho^{-1}(\mathfrak{A}_\rho) = \mathfrak{A}$, $\rho^{-1}(\mathfrak{B}_\rho) = \mathfrak{B}$, and $\rho^{-1}(\mathfrak{C}_\rho) = \mathfrak{C}$. In Section 12 it is shown that every transitive collineation group of L_∞ is conjugate to an element of $\mathfrak{A}_\rho$ or is contained in $\mathfrak{B}_\rho \cup \mathfrak{C}_\rho$. Theorem 1′ follows from this fact and Corollary (3.3). The isomorphisms between the elements of $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$ are determined in Sections 13 and 14, and the doubly transitive collineation groups of π are described in Section 15.

Before describing the classes $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$, it is necessary to examine the relation between the elements of $\mathfrak{F}$ and the elements of $\mathfrak{T}$.

3.4. *Definitions.* Let J be a collineation group of L_∞. A subgroup H of ΓL is defined to be a *pre-image* of J with respect to ρ if $\rho(H) = J$. The pre-image H is said to be *minimal* if no proper subgroup of H is a pre-image of J. The pre-image H in ΓL is defined to be the *unique minimal pre-image* of J if H is contained in every pre-image of J.

3.5. Lemma. *Let H be the unique minimal pre-image in ΓL of J, and let K be the kernel of ρ in H. Then every other pre-image H' of J in ΓL has the form $H' = K' \cdot H$, where $K' = H' \cap \langle \omega^{n+1} \rangle$ is a subgroup of $\langle \omega^{n+1} \rangle$ which contains K.*

3.6. Lemma. *Let G be a flag-transitive collineation group of π, let $H = G_{(0)}$, and let $\rho(H) = J$. Then G is a minimal flag-transitive group of π if and only if J is a minimal transitive collineation group of L_∞ and H is a minimal pre-image in ΓL of J.*

3.7. Lemma. *Let J_1 and J_2 be conjugate subgroups in $P\Gamma L$. Then each pre-image of J_1 in ΓL is conjugate in $\mathbf{G}$ to a pre-image of J_2 in ΓL. Conversely, if H_1 and H_2 are conjugate subgroups of ΓL, then $\rho(H_1)$ and $\rho(H_2)$ are conjugates in $P\Gamma L$.*

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

4. The class $\mathfrak{A}$. Let $\mathfrak{A}$ denote the class of subgroups of U which are flag-transitive on π. If $G \in \mathfrak{A}$, then $G = TH$, where $H = G_{(0)}$, and $H = \langle \omega^d, \omega^e\alpha^s\rangle$, for some integers d, e, and s. These integers can be chosen in a unique manner, as explained in the following lemma.

4.1. Lemma. *A subgroup H of V has a unique expression of the form $H = \langle \omega^d, \omega^e\alpha^s\rangle$, with integers d, e, and s which satisfy the following conditions:*

(i) $d > 0$ *and* $n^2 \equiv 1 \pmod{d}$;

(ii) $s > 0$ *and* $2r \equiv 0 \pmod{s}$;

(iii) $0 \leqslant e < d$ *and* $e\{(p^{2r} - 1)/(p^s - 1)\} \equiv 0 \pmod{d}$.

Proof. Let θ: $(d, e, s) \rightarrow \langle \omega^d, \omega^e\alpha^s\rangle$ be a mapping from the triples of integers which satisfy Conditions (i)–(iii) into the subgroups of V. If $H \in V$, then H is in the range of θ, as follows. Let $H \cap \langle\omega\rangle = \langle\omega^d\rangle$, where d satisfies (i). Let $\omega^e\alpha^s$ be a representative of a generator of $H/\langle\omega^d\rangle$, where s satisfies (ii) and $0 \leqslant e < d$. Last, $(\omega^e\alpha^s)^t \in \langle\omega^d\rangle$, for $t = 2r/s$, and hence $e\{(p^{2r} - 1)/(p^s - 1)\} \equiv 0 \pmod{d}$. Thus, $\theta(d, e, s) = H$. Similarly θ is a one-to-one mapping.

4.2. *Definition.* If $G = T\cdot\langle\omega^d, \omega^e\alpha^s\rangle$ and if d, e and s satisfy (i)–(iii) of Lemma (4.1), then G is said to be represented in *standard form*, and G is denoted by $\langle d, e. s\rangle$.

If $G = \langle d, e, s\rangle$, then $|G| = \{2r(n^2 - 1)n^2\}/sd$ and the kernel of ρ in G is the subgroup $\langle d(n + 1)/g, 0, 2r\rangle$ of order $g(n - 1)n^2/d$, where $g = (d, n + 1)$. The following proposition describes the elements of $\mathfrak{A}$ in terms of the parameters d, e, and s.

4.3. Proposition. *Let $G = \langle d, e, s\rangle$. Then $G \in \mathfrak{A}$ if and only if the following conditions are satisfied:*

(i) *The primes of* $g = (d, n + 1)$ *divide* $p^s - 1$;

(ii) $2r \equiv 0 \pmod{gs}$;

(iii) $(g, e) = 1$.

Proof. Let $H = G_{(0)}$, and let l be the line of π which contains the points 0 and 1. Then $G \in \mathfrak{A}$ if and only if

$$|H_{(l)}| = \frac{|H|}{n + 1} = \frac{2r(n - 1)}{sd}.$$

Since l consists of the elements of GF(n), an arbitrary element $\eta = \omega^{id}(\omega^e\alpha^s)^m$ of H is in $H_{(l)}$ if and only if

$$id + e\left(\frac{p^{sm} - 1}{p^s - 1}\right) \equiv 0 \pmod{n + 1}. \tag{4.4}$$

Hence $|H_{(l)}|$ equals the number of solution pairs (i, m) for (4.4) with $1 \leqslant i \leqslant (n^2 - 1)/d$ and $1 \leqslant m \leqslant 2r/s$. Let $g = (d, n + 1)$, and let k be the number of solutions for m in (4.5) with $1 \leqslant m \leqslant 2r/s$:

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

$$(4.5) \qquad e\left(\frac{p^{sm}-1}{p^s-1}\right) \equiv 0 \pmod{g}.$$

Then $|H_{(l)}| = gk(n-1)/d$, and hence $G \in \mathfrak{A}$ if and only if $k = 2r/sg$.

Now suppose $G \in \mathfrak{A}$. Then $k = 2r/sg$ is an integer, so $2r \equiv 0 \pmod{sg}$. Further, $m = 2r/s$ is a solution of (4.5) by Lemma (4.1), and it follows that

$$m = \frac{2r}{s}\bigg/\frac{2r}{sg} = g$$

must be the minimal solution of (4.5). Therefore, the set of integers

$$S = \{e(p^{ms}-1)/(p^s-1)\} \quad \text{for } 1 \leqslant m \leqslant g$$

is a complete residue system $\pmod g$, and hence Lemma (2.1) implies (i) and (iii).

Conversely, suppose (i)–(iii) are satisfied by d, e, and s. Since $(2r/s, n+1) \equiv 0 \pmod g$, clearly $g \not\equiv 0 \pmod 4$, and thus by Lemma (2.1) the set S is a complete residue system $\pmod g$. Hence (4.5) has $k = 2r/sg$ solutions for m $\pmod{2r/s}$, and so $G \in \mathfrak{A}$.

4.6. Corollary. *Let $G = \langle d, e, s\rangle \in \mathfrak{A}$. Then $g \not\equiv 0 \pmod 4$; and if $2r/s$ is even, then $g = 1$ or 2. In particular, if d is even, then $g = 2$.*

Proof. Condition (ii) implies $g \not\equiv 0 \pmod 4$. Since the primes of g divide (p^r+1, p^s-1), g divides 2 if $2r/s$ is even, by Lemma (2.3).

4.7. Corollary. *Let $G = \langle d, e, s\rangle \in \mathfrak{A}$ with $H = G_{(0)}$, and let l be the line of π which contains 0 and 1. Then $H_{(l)} = \langle \omega^{d(n+1)}/g, \omega^{e'}\alpha^{sg}\rangle$, for some e' such that $e' \equiv 0 \pmod{n+1}$.*

Proof. The proof follows from the determination of the minimal solution for m in (4.4) and from the order of $H_{(l)}$.

It is useful to combine the conditions of Lemma (4.1) and Proposition (4.3) in such a manner that the conditions for d and s do not depend on e.

4.8. Lemma. *Let d and s be positive integers and let $g = (d, n+1)$. Then:*

(1) *There exist groups $\langle d, e, s\rangle \in \mathfrak{A}$, for some integers e, if and only if the following conditions are satisfied:*

(i) $p^{2r} - 1 \equiv 0 \pmod d$;

(ii) *the primes of g divide $p^s - 1$;*

(iii) $2r \equiv 0 \pmod{gs}$;

(iv) $(p^{2r}-1)/(p^s-1) \equiv 0 \pmod{2^c}$, where $2^c \| d$.

(2) *If d, g, and s satisfy Conditions* (i)–(iv) *of part* (1), *then there exist exactly $\varphi(g)d/gd^*$ groups $G = \langle d, e, s\rangle \in \mathfrak{A}$, where $d^* = d/t$* and

$$t = (d, (p^{2r}-1)/(p^s-1)),$$

one for each integer e which satisfies the following conditions:

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

(v) $0 \leqslant e < d$;
(vi) $e \equiv 0 \pmod{d^*}$;
(vii) $(e/d^*, g) = 1$.

Proof. The conditions (i)–(iv) are necessary for $\langle d, e, s\rangle$ to be in $\mathfrak{A}$, by Proposition (4.3) and Lemma (4.1). Conversely, if these conditions are satisfied, there exist $\varphi(g)d/gd^*$ integers e such that $\langle d, e, s\rangle \in \mathfrak{A}$, as follows. Integers d, e, and s satisfy Condition (iii) of Lemma (4.1) if and only if $0 \leqslant e < d$ and $e \equiv 0 \pmod{d^*}$. Next, the Conditions (i)–(iv) imply that $(d^*, g) = 1$, so if $e = kd^*$, then $(e, g) = 1$ if and only if $(k, g) = 1$. Since $d = 0 \pmod{gd^*}$, there exist exactly $\varphi(g)d/gd^*$ values of $e = kd^*$ such that $0 \leqslant e < d$, and $(e, g) = 1$. For these values of e, $\langle d, e, s\rangle \in \mathfrak{A}$.

5. The minimal elements of $\mathfrak{A}$.

5.1. Lemma. *Let $G_1 = \langle d_1, e_1, s_1\rangle \in \mathfrak{A}$, and let d_2 and s_2 be positive integers such that $\langle d_2, e_2, s_2\rangle \in \mathfrak{A}$ for some integer e_2. Let $g_i = (d_i, n+1)$ for $i = 1$ and 2, and let $u = (d_2, d_1(p^{2r}-1)/(p^{s_2}-1))$. Then G_1 contains*

$$\{\varphi(g_2)g_1u\}/\{\varphi(g_1)g_2d_1\},$$

or 0, *subgroups $G_2 = \langle d_2, e_2, s_2\rangle \in \mathfrak{A}$, as d_1, e_1, s_1, d_2, and s_2 do, or do not, satisfy the following conditions:*
(i) $d_2 \equiv 0 \pmod{d_1}$;
(ii) $s_2 \equiv 0 \pmod{s_1}$;
(iii) $(s_2/s_1, g_1) = 1$;
(iv) $e_1(p^{2r}-1)/(p^{s_1}-1) \equiv 0 \pmod{u}$.

Proof. Let $\langle d_2, e_2, s_2\rangle \in \mathfrak{A}$ be a subgroup of $\langle d_1, e_1, s_1\rangle$. Then $d_2 \equiv 0 \pmod{d_1}$, $s_2 \equiv 0 \pmod{s_1}$, and there exists an integer i such that:

$$e_1\left(\frac{p^{s_2}-1}{p^{s_1}-1}\right) + id_1 = e_2 \pmod{p^{2r}-1}. \tag{5.2}$$

Since $(e_2, g_2) = 1$ and $g_2 \equiv 0 \pmod{g_1}$, then $(s_2/s_1, g_1) = 1$. Condition (iii) of Lemma (4.1) states:

$$e_2\left(\frac{p^{2r}-1}{p^{s_2}-1}\right) = 0 \pmod{d_2}. \tag{5.3}$$

Substituting (5.2) in (5.3) one obtains:

$$id_1\left(\frac{p^{2r}-1}{p^{s_2}-1}\right) + e_1\left(\frac{p^{2r}-1}{p^{s_1}-1}\right) = 0 \pmod{d_2}. \tag{5.4}$$

The congruence (5.4) implies Condition (iv) of the lemma.

Conversely, suppose Conditions (i)–(iv) are satisfied by the integers d_1, e_1, s_1, d_2, and s_2. From Conditions (i) and (ii), it is sufficient to determine the number of integers e_2 such that e_2 is a solution of (5.2) and (5.3) for some i, $(e_2, g_2) = 1$, and $0 \leqslant e_2 < d_2$.

Consider the integers e_2 defined by (5.2) for $1 \leqslant i \leqslant d_2/d_1$. Such an e_2 satisfies (5.3) if and only if the corresponding i satisfies (5.4). There exist solutions for i in (5.4) by Condition (iv), and these solutions are unique (mod d_2/u). (Note that $u = 0$ (mod d_1) and $d_2 = 0$ (mod u).) Let $i = i_0 + j(d_2/u)$, for $1 \leqslant j \leqslant u/d_1$ be the solutions for i (mod d_2/d_1) for (5.4). It is sufficient to determine the integers j in this range for which $(e_2, g_2) = 1$. Substituting for i in (5.2), one obtains:

$$e_2 \equiv \left\{ e_1\left(\frac{p^{s_2}-1}{p^{s_1}-1}\right) + i_0 d_1 \right\} + j\left(\frac{d_1 d_2}{u}\right) \equiv a + j\left(\frac{d_1 d_2}{u}\right) \quad (\text{mod } p^{2r}-1),$$

where a is the quantity in brackets, and $1 \leqslant j \leqslant u/d_1$. Let t be the largest factor of g_2 prime to g_1. Since $d_1 d_2/u \equiv 0$ (mod g_1) and $(s_2/s_1, g_1) = 1$, it follows that $(g_2, e_2) = 1$ if and only if $(t, e_2) = 1$. Let $d_2{}^* = d_2/t_2$, where

$$t_2 = (d_2, (p^{2r}-1)/(p^{s_2}-1))$$

and note that $d_1 d_2/u = d_2/k$ where $k = (d_2/d_1, (p^{2r}-1)/(p^{s_2}-1))$. It is now clear that $(d_1 d_2/u, t) = 1$, since $(d_2{}^*, g_2) = 1$. Hence the set $\{a + j(d_1 d_2)/u\}$, for $1 \leqslant j \leqslant t$, is a complete residue system (mod t). Since $u/d_1 \equiv 0$ (mod t), there exist $\varphi(t)u/td_1$ integers j (mod u/d_1) for which $(e_2, g_2) = 1$. By writing $g_2 = g_1\hat{g}t$, it follows that there exist $\{\varphi(g_2)g_1 u\}/\{\varphi(g_1)g_2 d_1\}$ subgroups $\langle d_2, e_2, s_2\rangle$ of $\langle d_1, e_1, s_1\rangle$ which are in $\mathfrak{A}$.

The following proposition describes the minimal elements of $\mathfrak{A}$. It is clear that the minimal elements of $\mathfrak{A}$ are also minimal flag-transitive collineation groups of π.

5.5. Proposition. *The class of minimal elements of* $\mathfrak{A}$ *is the disjoint union of the following two subclasses:*

$\mathfrak{M}_1 = \{\langle d, e, s\rangle \in \mathfrak{A}\}$ *such that*

(i) $2r/sg = 1$ *for* $g = (d, n+1)$;

(ii) $d/g = (n-1)/2^b$, *where* $2^b \| n-1$;

$\mathfrak{M}_2 = \{\langle d, e, s\rangle \in \mathfrak{A}\}$ *such that*

(i) $2r/sg = 2^x$ *for some* $x \geqslant 1$, *where* $g = (d, n+1)$;

(ii) $g = 2$ *and* $d/2 = (n-1)/2^a$, *where* $2^a \| p^s - 1$.

Proof. Let $G = \langle d, e, s\rangle$ be a minimal element of $\mathfrak{A}$. Let m be the largest factor of $2r/sg$ which is prime to g. Let $k = 2r/smg$ unless $g = 2$, in which case let $k = 1$. Let t be the largest odd factor of $g(n-1)/d$. The integers ktd and sm satisfy Conditions (i)–(iv) of Lemma (4.8). Therefore, Lemma (5.1) can be applied to demonstrate that G contains a subgroup $G' = \langle ktd, e', sm\rangle \in \mathfrak{A}$, for some e'. The application of Lemma (5.1) is possible because $(t, 2r/sm) = 1$ and hence:

$$e\left(\frac{p^{2r}-1}{p^s-1}\right) \equiv 0 \quad (\text{mod } u),$$

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

where $u = (ktd, d(p^{2r} - 1)/(p^{sm} - 1))$, by the definitions of m, k, and t. Since G is a minimal element of $\mathfrak{A}$, $k = m = t = 1$, so $g(n - 1)/d$ is a power of 2, and either $2r/sg = 1$, or $g = 2$ and $2r/sg = 2^x$ for some $x \geqslant 1$.

Suppose $2r/sg = 1$ and $g(n - 1)/d$ is a power of 2. If $2^b \| n - 1$, then $d/g = (n - 1)/2^b$, except if $d \equiv 0 \pmod 4$. In this case, from Corollary (4.6), $g = 2$, $r = s$, e is odd, and $e\{(p^{2r} - 1)/(p^s - 1)\} = e(p^r + 1) \equiv 0 \pmod d$. This implies $g = 0 \pmod 4$, and therefore $d/g = (n - 1)/2^b$.

Suppose $g = 2$, $2r/sg = 2^x > 1$, and $g(n - 1)/d$ is a power of 2. Since $p^r \equiv 1 \pmod 4$ and $\langle d, e, s\rangle$ is a minimal element of $\mathfrak{A}$, it follows from Lemmas (4.8) and (5.1) that d contains the highest power of 2 consistent with the condition: $e\{(p^{2r} - 1)/(p^s - 1)\} = 0 \pmod d$. Since e is odd, $2(n - 1)/d = 2^a$, where $2^a \| p^s - 1$.

Conversely, similar remarks imply that the elements of $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are minimal elements of $\mathfrak{A}$.

5.6. Corollary. *Let* $G = \langle d, e, s\rangle \in \mathfrak{M}_1 \cup \mathfrak{M}_2$. *Then:*

(1) *G is a Frobenius group on the points of π;*

(2) *G contains no affine perspectivities* (i.e., perspectivities with an affine line of π as axis.)

Proof. (1). Apply Proposition (17.5).

(2) $G = \langle d, e, s\rangle$ contains affine perspectivities if and only if $r \equiv 0 \pmod s$ and $e\{(p^r - 1)/(p^s - 1)\} \equiv 0 \pmod{(d, n - 1)}$.

Let l be the line of π which contains 0 and 1, and let F be the flag $(0, l)$ of π. Note that if $G \in \mathfrak{M}_1$, then $G_{(F)}$ is the Sylow 2-subgroup of the $(0, L_\infty)$-homologies of π. If $G \in \mathfrak{M}_2$, then $G_{(F)}$ is a 2-subgroup which fixes two lines through 0, and the $(0, L_\infty)$-homologies of $G_{(F)}$ are exactly those elements which fix a third line through 0(cf. Corollary (6.8)).

6. The Class $\mathfrak{A}_\rho$. Since L_∞ is represented by $GF(n^2)$ as in Section 3, the points of L_∞ can be denoted by W^i, $0 \leqslant i < n + 1$, where W^i denotes the subspace of $GF(n^2)$ which contains the element ω^i. In addition, let W^i denote the collineation $\rho(\omega^i)$ of L_∞, and let A denote the collineation $\rho(\alpha)$. Let $Y = \rho(U) = \langle W, A\rangle$, and let $\mathfrak{A}_\rho$ consist of the subgroups of Y which are transitive on L_∞. Clearly $\rho^{-1}(\mathfrak{A}_\rho) = \mathfrak{A}$, since the kernel of ρ is contained in U.

If J is a subgroup of Y, then $J = \langle W^g, W^eA^s\rangle$ for some integers g, e, and s. These integers can be chosen in a unique manner, as explained in the following lemma.

6.1. Lemma. *A subgroup J of Y has a unique expression of the form $\langle W^g, W^eA^s\rangle$, with integers g, e, and s which satisfy the following conditions:*

(i) $g > 0$ *and* $n + 1 \equiv 0 \pmod g$;

(ii) $s > 0$ *and* $2r \equiv 0 \pmod s$;

(iii) $0 \leqslant e < g$ *and* $e\{(p^{2r} - 1)/(p^s - 1)\} \equiv 0 \pmod g$.

Proof. See the proof of Lemma (4.1).

6.2. *Definition.* If $J = \langle W^g, W^e A^s \rangle$ and if g, e, and s satisfy (i)–(iii) of Lemma (6.1), then J is said to be represented in *standard form*, and J is denoted by $[g, e, s]$. Note that $|[g, e, s]| = 2r(n + 1)/sg$.

6.3. Corollary. *Let $G = \langle d, e, s \rangle$. Then $\rho(G) = [g, e', s]$, where $g = (d, n + 1)$ and e' satisfies $0 \leqslant e' < g$ and $e' \equiv e (\text{mod } g)$. Conversely, let $J = [g, e', s]$. Then $G = T \cdot \langle \omega^g, \omega^{e'} \alpha^s \rangle$ is represented in standard form, and $\rho(G) = J$.*

6.4. Lemma. *$J = [g, 0, 2r]$ has a unique minimal pre-image J^* in ΓL.*

Proof. $J^* = \langle \omega^t \rangle$, where $t = \text{LCM}(u)$ for all u such that $n^2 \equiv 1 \pmod u$ and $(u, n + 1) = g$.

The following proposition describes the elements of $\mathfrak{A}_p$ in terms of the parameters g, e, and s.

6.5. Proposition. *Let $J = [g, e, s]$. Then $J \in \mathfrak{A}_p$ if and only if the following conditions are satisfied:*

(i) *The primes of g divide $p - 1$;*

(ii) $2r \equiv 0 \pmod{gs}$;

(iii) $(e, g) = 1$.

Proof. $J \in \mathfrak{A}_p$ if and only if $G = \langle g, e, s \rangle \in \mathfrak{A}$, by Corollary (6.3). Now apply Proposition (4.3).

6.6. Corollary. *Let $J = [g, e, s] \in \mathfrak{A}_p$. Then $J_{(1)} = \langle A^{sg} \rangle$, where $J_{(1)}$ is the subgroup of J fixing the point $1 = W^0$ of L_∞.*

Proof. Apply Corollary (4.7).

The following proposition describes the minimal elements of $\mathfrak{A}_p$. Clearly, the minimal elements of $\mathfrak{A}_p$ are minimal transitive collineation groups of L_∞.

6.7. Proposition. *The class of minimal elements of $\mathfrak{A}_p$ is the disjoint union of the following two subclasses:*

(1) *the sharply transitive subgroups of Y;*

(2) *the groups $J = [2, 1, s] \in \mathfrak{A}_p$ such that $r/s = 2^x$ for some $x \geqslant 1$.*

Proof. From Lemma (3.6) and Proposition (5.5) the class of minimal elements of $\mathfrak{A}_p$ is $\rho(\mathfrak{M}_1) \cup \rho(\mathfrak{M}_2)$.

6.8. Corollary. *Let $J = [2, 1, s]$ be a minimal element of $\mathfrak{A}_p$ such that J is not a sharply transitive group. Then $J_{(1)} = \langle A^{2s} \rangle$ fixes the two points 1 and W^t, for $t = (n + 1)/2$, and no non-identity element of $J_{(1)}$ fixes any other point of L_∞.*

Proof. Since $r/s = 2^x$, Lemma (2.3) implies the collineation $A^{2ks} \neq 1$ fixes exactly $(p^r + 1, p^{2ks} - 1) = 2$ points of L_∞, namely 1 and W^t.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

7. The structure of $\mathrm{PG}L_2(n)$.

Before describing the classes $\mathfrak{B}$ and $\mathfrak{C}$, it is convenient to review some well-known facts about certain collineation groups of L_∞.

Let $GL_2(n)$, or more simply GL, denote the group of non-singular linear transformations of π over $\mathrm{GF}(n)$, and let $SL_2(n)$, abbreviated by SL, denote the subgroup of GL whose elements have determinant $+1$. The kernel of ρ in SL is $\{\pm 1\}$. Moreover, if $p \neq 2$, then -1 is the only element of SL of order 2. Let $PGL_2(n)$ and $PSL_2(n)$, abbreviated by PGL and PSL, denote $\rho(GL)$ and $\rho(SL)$, respectively, and note that $(PGL\colon PSL) = (2;\ 1)$, and $|PSL| = n(n^2 - 1)/(2; 1)$. The group PSL also can be described as the subgroup of PGL whose elements are even permutations of the points of L_∞. It is well known that $PSL_2(n)$ is a simple group except when $n = 2$ or 3 (**6**, p. 87 or p. 286, or **2**, Theorem 4.10). In all cases, PSL is a characteristic subgroup of $P\Gamma L$.

The following proposition concerning the structure of PGL is extremely useful (**6**, Chapter XII).

7.1. Proposition. *Every non-identity element of $PGL_2(n)$ belongs to exactly one of the following subgroups:*

(1) *$n(n - 1)/2$ conjugate cyclic subgroups of order $n + 1$, each of which is sharply transitive on L_∞;*

(2) *$n + 1$ conjugate elementary abelian subgroups of order n, each of which fixes one point of L_∞ and is sharply transitive on the remaining points;*

(3) *$n(n + 1)/2$ conjugate cyclic subgroups of order $n - 1$, each of which fixes two points of L_∞ and is sharply transitive on the remaining points.*

Proof. Let P and Q be distinct points of L_∞. The proposition is a consequence of the following facts: (1) $PGL_{(P)}$ is a doubly transitive Frobenius group; (2) $PGL_{(P,Q)}$ is a cyclic group; (3) $\langle W\rangle$ is a sharply transitive subgroup of PGL which has $n(n - 1)/2$ pairwise disjoint conjugates, from Corollary (13.6).

7.2. Lemma. *Let J be a transitive subgroup of PGL which is generated by its elements which fix no point of L_∞. Then:*

(1) *there exists a unique minimal pre-image J^* of J in ΓL;*

(2) *if $J \subset PSL$, then $J^* = \rho^{-1}(J) \cap SL$, $-1 \in J^*$, and $|J^*| = (2; 1)|J|$.*

Proof. The cyclic subgroups of J which fix no point of L_∞ have unique minimal pre-images in ΓL, by Lemma (6.4) and Proposition (7.1), and these pre-images generate J^*. If $J \subset PSL$, then $J^* \subset SL$, and $-1 \in J^*$ from a previous remark. Therefore $J^* = \rho^{-1}(J) \cap SL$ and $|J^*| = (2; 1)|J|$.

8. The class $\mathfrak{B}$.

Let $\mathfrak{B}$ consist of the collineation groups of π which contain E, the group generated by all the elations of π. The group E has the form $E = T\cdot SL$, since SL is generated by all the elations of π which have as axis a line of π containing the point 0 (**2**, Theorem 4.6). The elements of $\mathfrak{B}$ are described in the following lemma.

8.1. Lemma. *Let $G \in \mathfrak{B}$. Then G has a unique representation in the form $G = T\cdot\langle SL, \omega^d, \omega^e\alpha^s\rangle$, with integers d, e, and s which satisfy the following conditions:*

(i) $d > 0$ *and* $n - 1 \equiv 0 \pmod{d}$;

(ii) $s > 0$ *and* $r \equiv 0 \pmod{s}$;

(iii) $0 \leqslant e < d$ *and* $e(n-1)/(p^s - 1) \equiv (n-1)/(2;1) \pmod{d}$.

Proof. From the properties of SL, $SL \cap \langle\omega\rangle = \langle\omega^{n-1}\rangle$. Moreover, $\omega^t\alpha^r \in SL$, for $t = (n-1)/(2;1)$, as follows. Clearly $A^r \in PGL$; moreover, A^r and W^t are both odd, or both even permutations of L_∞, so that $W^tA^r \in PSL$ and $(W^tA^r)^2 = 1$. Therefore, there exists an integer k such that $\nu = \omega^{t+k(n+1)}\alpha^r \in SL$, and $\nu^2 = -1$. This implies that $k(n+1) = 0 \pmod{(n-1)}$, and hence $\omega^t\alpha^r \in SL$. Now proceed as in the proof of Lemma (4.1).

8.2. *Definition.* An element $G = T\cdot\langle SL, \omega^d, \omega^e\alpha^s\rangle$ of $\mathfrak{B}$ is said to be represented in *standard form* if d, e, and s satisfy Conditions (i)–(iii) of Lemma (8.1).

8.3. Lemma. *The elements of $\mathfrak{B}$ are doubly transitive collineation groups of π.*

9. The class $\mathfrak{B}_\rho$.

Let $\mathfrak{B}_\rho$ be the class of collineation groups of L_∞ which contain $\rho(E) = PSL$. These groups can be described as follows.

9.1. Lemma. *Let $J \in \mathfrak{B}_\rho$. Then J has a unique expression of the form $J = \langle PSL, W^g, W^eA^s\rangle$, with integers g, e, and s which satisfy the following conditions:*

(i) $g > 0$ *and* $(n+1, n-1) \equiv 0 \pmod{g}$;

(ii) $s > 0$ *and* $r \equiv 0 \pmod{s}$;

(iii) $0 \leqslant e < g$ *and* $e(p^r - 1)/(p^s - 1) \equiv (p^r - 1)/(2;1) \pmod{g}$.

Proof. See Lemma (8.1).

9.2. Corollary. *If $J \in \mathfrak{B}_\rho$, then $J \lhd P\Gamma L$.*

Proof. $J \lhd P\Gamma L$ since both PSL and PGL are normal in $P\Gamma L$ and W^eA^s is normal in $P\Gamma L$ mod$\langle PSL, W^g\rangle$.

It is important in the proof of Theorem 1 to know that $\rho^{-1}(\mathfrak{B}_\rho) = \mathfrak{B}$. This fact is a consequence of the following lemma.

9.3. Lemma. *SL is the unique minimal pre-image in ΓL of PSL.*

Proof. The proof follows from Lemma (7.2) if PSL is simple. If PSL is not simple, then $n = 2$ or 3, and SL is the only pre-image of PSL in ΓL.

9.4. Corollary. $\rho^{-1}(\mathfrak{B}_\rho) = \mathfrak{B}$.

10. The class $\mathfrak{C}_\rho$.

For many values of n, the group $\mathrm{PG}L_2(n)$ contains subgroups of order 12, 24, and 60 which are isomorphic (as abstract groups) to A_4, S_4, and A_5, the alternating group of degree 4, the symmetric group of degree 4, and the alternating group of degree 5, respectively. For example

$PSL_2(3)$, $PGL_2(3)$, and $PSL_2(4)$ are isomorphic to A_4, S_4, and A_5 respectively, and in these cases the groups are isomorphic as permutation groups. In addition, there exist cases, for example when $n = 4$ and $n = 9$, for which $P\Gamma L_2(n)$ contains subgroups of order 120 which are isomorphic to S_5, the symmetric group of degree 5. The notation G_{12}, G_{24}, G_{60}, and G_{120} will denote subgroups of $P\Gamma L$ isomorphic to A_4, S_4, A_5, and S_5, respectively. The following proposition is a complete summary of the occurrence of the groups G_{12}, G_{24}, and G_{60}, in PGL (**6**, Sections 257–260).

10.1. Proposition. (1) *Let $p \neq 2$. Then:*

(*a*) *$PGL_2(n)$ contains exactly $n(n^2 - 1)/24$ subgroups isomorphic to A_4, forming one conjugacy class.*

(*b*) *$PGL_2(n)$ contains exactly $n(n^2 - 1)/24$ subgroups isomorphic to S_4, forming one conjugacy class.*

(2) *Let $n \equiv \pm 1 \pmod{10}$. Then $PGL_2(n)$ contains exactly $n(n^2 - 1)/60$ subgroups isomorphic to A_5, forming one conjugacy class.*

(3) *The groups in* (1) *and* (2) *are contained in $PSL_2(n)$, with the exception of the groups isomorphic to S_4, which are contained in $PSL_2(n)$ if and only if $n \equiv \pm 1$* (mod 8).

(4) *If $n = 2^r$ and r is even, then PGL contains subgroups isomorphic to A_4 and A_5. If $p = 5$, then PGL contains subgroups isomorphic to A_5.*

Let the class $\mathfrak{C}_p$ consist of the subgroups of $P\Gamma L$ which are isomorphic to A_4, S_4, A_5, or S_5, for the cases listed in Table I. (When $n = 9$, $G_{120} = \mathbf{N}_{P\Gamma L}(G_{60})$ is isomorphic to S_5, from Lemma (11.2).) "(m)" indicates the minimal transitive groups of Table I (see Proposition (10.2)).

TABLE I

The Class $\mathfrak{C}_p$

n	Subgroups	n	Subgroups
5	$G_{12}(m)$; G_{24}	19	$G_{60}(m)$
7	G_{24}	23	$G_{24}(m)$
9	$G_{60}(m)$; G_{120}	29	$G_{60}(m)$
11	$G_{12}(m)$; G_{24}; G_{60}	59	$G_{60}(m)$

10.2. Proposition. 1. *The elements of the class $\mathfrak{C}_p$ are transitive collineation groups of L_∞.*

2. *The elements of $\mathfrak{C}_p$ which are minimal transitive groups of L_∞ are indicated by "(m)" in Table I.*

Proof. The proof follows from Propositions (7.1) and (10.1). For example, let $n = 7$, let $J = G_{24}$, and let S be a subgroup of J of order 8. The non-identity elements of S have orders 2 and 4, and hence fix no point of L_∞. Therefore, S is transitive on L_∞, and J is transitive, but not minimally transitive, on L_∞. Note that S is conjugate to $\langle W^2, WA \rangle \in \mathfrak{A}_p$.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

11. The class $\mathfrak{C}$.

Define the class $\mathfrak{C}$ by the relation $\mathfrak{C} = \rho^{-1}(\mathfrak{C}_\rho)$. The elements of $\mathfrak{C}$ are flag-transitive collineation groups by Lemma (3.1) and Proposition (10.2). The class $\mathfrak{C}$ is described in Proposition (11.3) below.

11.1. LEMMA. *Let $J = G_{12}$, G_{24}, or G_{60} in $\mathfrak{C}_\rho$. Then J has a unique minimal pre-image in ΓL, denoted by $J^* = G_{12}^*$, G_{24}^*, or G_{60}^*, respectively. The kernel of ρ in J^* has order* 2, *except that if $n = 5$, then* $|G_{24}^*| = 96$.

Proof. The proof follows from Lemma (7.2), except for the cases $n = 5$ or 11 and $J = G_{24}$, which must be treated separately.

11.2. LEMMA. *Let $n = 9$, let G_{60} be a subgroup of PGL isomorphic to A_5, and let $J = \mathbf{N}_{P\Gamma L}(G_{60})$. Then:*

(1) $J \simeq S_5$ (J is denoted by G_{120} in Table I).

(2) J has 4, 2, *and* 1 *pre-images in ΓL having kernels of order* 2, 4, *and* 8 *respectively, as illustrated in Figure* 1 *below.*

(3) *The groups $G_6 = T \cdot H_6$ and $G_7 = T \cdot H_7$ are the minimal doubly transitive groups of π in Figure* 1.

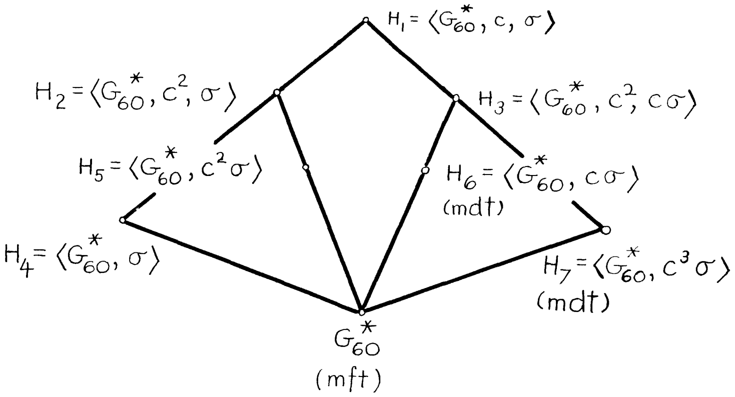
$H_1 = \langle G_{60}^*, c, \sigma\rangle$
$H_2 = \langle G_{60}^*, c^2, \sigma\rangle$
$H_3 = \langle G_{60}^*, c^2, c\sigma\rangle$
$H_5 = \langle G_{60}^*, c^2\sigma\rangle$
$H_6 = \langle G_{60}^*, c\sigma\rangle$
(mdt)
$H_4 = \langle G_{60}^*, \sigma\rangle$
$H_7 = \langle G_{60}^*, c^3\sigma\rangle$
(mdt)
G_{60}^*
(mft)

FIGURE 1. The pre-images in ΓL of G_{120}, for $n = 9$.

Proof. Let $c = \omega^{10}$, and let

$$\delta = \begin{pmatrix} c^5 & c^2 \\ c^4 & c^4 \end{pmatrix}, \qquad \chi = \begin{pmatrix} c^2 & 0 \\ 0 & c^6 \end{pmatrix}, \qquad \beta = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix},$$

and σ: $(a, b) \longrightarrow (a^3, b^3)$ be elements of ΓL (operating on the left), with respect to the basis $(\omega^5, 1)$ of π. From Bussey's Tables for GF(81) **(4)**, with $i = \omega$, it follows that

$$D = \rho(\delta) = (01856)(27394), \qquad X = \rho(\chi) = (19)(28)(37)(46),$$
$$B = \rho(\beta) = (17269384), \qquad S = \rho(\sigma) = (19)(36)(47),$$

where j denotes the point W^j of L_∞, for $0 \leqslant j \leqslant 9$.

(1) The group $G_{60} = \langle D, X\rangle$ is isomorphic to A_5 since $(XD)^3 = 1$ (**6**, Section 267). (Note that the mapping $D \rightarrow (01856)(27394)$ is an anti-isomorphism.) Then $G_{120} = \mathbf{N}_{P\Gamma L}(G_{60}) = \langle G_{60}, S\rangle$, since $SXS^{-1} = X$ and $SDS^{-1} = (XD^3)^2 \in G_{60}$. Moreover, G_{120} is isomorphic to S_5 by its action on the five conjugate subgroups of G_{60} of order 12, one of which is $G_{12} = \langle X, U\rangle$, where $U = D^2(XD)D^{-2}$.

(2) The group $G_{60}^* = \langle \delta, \chi\rangle$ is the unique minimal pre-image in ΓL of G_{60}. Note that σ normalizes G_{60}^* and that $(a\sigma)^2 = \pm 1$, for $a \neq 0$ in GF(9). Therefore, the pre-images of G_{120} in ΓL are H_i $(1 \leqslant i \leqslant 7)$, as illustrated in Figure 1.

(3) Let $G_i = T\cdot H_i$ $(1 \leqslant i \leqslant 7)$. Then G_4 is conjugate to G_5 and G_6 is conjugate to G_7 under c, and G_2 and G_3 are normal in G_1. Since $a\sigma$ maps the point $(1, 0)$ onto $(a, 0)$, for $a \neq 0$ in GF(9), and since $\chi \in G_{60}^*$, it follows that G_1 and G_3 are doubly transitive groups, G_6 and G_7 are minimal doubly transitive groups, and G_2, G_4, and G_5 are not doubly transitive groups of π.

11.3. Proposition. *The elements of* $\mathfrak{C}$ *and their properties are described in Table* II.

TABLE II

The Class $\mathfrak{C}$

n	J	$\lvert K\rvert$	Properties	n	J	$\lvert K\rvert$	Properties
5	G_{12}	2	mft, mdt, F	11	G_{60}	2	mdt, F
		4	dt			10	dt
	G_{24}	4	dt	19	G_{60}	2	mft, F
7	G_{24}	2	mdt, F			6	—
		6	dt			18	mdt
9	G_{60}	2	mft	23	G_{24}	2	mft, F
		4	—			22	mdt, F
		8	mdt	29	G_{60}	2	mft, F
	G_{120}	(see Lemma 11.2))				4	—
11	G_{12}	2	mft, F			14	mdt, F
		10	mdt, F			28	dt
	G_{24}	2	—	59	G_{60}	2	mft, F
		10	dt			58	mdt, F

(*Let* $G \in \mathfrak{C}$, *let* $\rho(G) = J$, *and let* K *be the kernel of* $G_{(0)}$. *Then* G *can be identified by* J *and* $\lvert K\rvert$, *except in the case* $n = 9$ *and* $J = G_{120}$ (in which case, see Lemma (11.2)). *The notation* mft, dt, mdt, *and* F *denote the minimal flag transitive, the double transitive, the minimal doubly transitive, and the Frobenius groups of* $\mathfrak{C}$, *respectively.*)

Proof. The existence of the elements of $\mathfrak{C}$ follows from Lemmas (3.5), (11.1), (11.2), and the definition of $\mathfrak{C}_\rho$. The minimal flag-transitive groups of $\mathfrak{C}$ are determined by Lemma (3.6) and Proposition (10.2). The doubly transitive groups and the Frobenius groups of $\mathfrak{C}$ are determined by Lemmas (11.2) and (11.4), except in the cases $n = 5$ or 11 and $J = G_{24}$, and in these cases the

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

results are obvious. The minimal doubly transitive groups of $\mathfrak{C}$ can be determined from the preceding information and Lemma (11.2).

Part of the proof of Proposition (11.3) depends on the following lemma.

11.4 Lemma. *Let J be a transitive subgroup of PSL which has a unique minimal pre-image J^* in ΓL. Let H be an arbitrary pre-image of J in ΓL, with kernel K of order k, and let $G = T\cdot H$. Let $m = (n, |J|)$, let $t = |J|/\{(n+1)m\}$, and let $u = (2;1)t$. Then:*

(1) *G is doubly transitive on π if and only if* $\mathrm{LCM}(u, k) = n - 1$;

(2) *G is a Frobenius group of π if and only if $m = 1$ and $(u, k) \leqslant 2$.*

Proof. By Lemma (3.5), $H = K\cdot J^*$; and from the proof of Lemma (7.2), $J^* = \rho^{-1}(J) \cap SL$. Let Q be a point of L_∞, and for η in $H_{(Q)}$ let

$$\eta = \begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}.$$

Define a homomorphism θ from $H_{(Q)}$ to $\mathrm{GF}(n)$ by $\theta(\eta) = a$, and let L be the kernel of θ.

(1) Then $|\theta(H_{(Q)})| = |\langle\theta(J_{(Q)}{}^*), \theta(K)\rangle| = \mathrm{LCM}(u, k)$, since the elements of $J_{(Q)}{}^*$ of order p are in L. Therefore, G is doubly transitive on π if and only if $|\theta(H_{(Q)})| = \mathrm{LCM}(u, k) = n - 1$, as required.

(2) Further,

$$|L| = \frac{|H_{(Q)}|}{|\theta(H_{(Q)})|} = \frac{tmk}{\mathrm{LCM}(u, k)} = \frac{m(u, k)}{(2;1)}.$$

Therefore, G is a Frobenius group if and only if $|L| = 1$, i.e., if and only if $m = 1$ and $(u, k) = (2; 1)$.

12. The flag-transitive collineation groups of π.

In the following section, it is proved that every flag-transitive group of π is conjugate to an element of $\mathfrak{A}$ or is contained in $\mathfrak{B} \cup \mathfrak{C}$, by showing that every transitive group J of L_∞ is conjugate to an element of $\mathfrak{A}_\rho$, or is contained in $\mathfrak{B}_\rho \cup \mathfrak{C}_\rho$. This last fact depends on the following lemma.

12.1. Lemma. *Let J be a transitive subgroup of $P\Gamma L$ and let $M = J \cap PSL$. Then one of the following conditions is satisfied:*

(1) J is contained in a conjugate of $\langle W, A\rangle$;

(2) $M = PSL$;

(3) $M \simeq A_4, S_4$, *or* A_5, *and* $n = 5, 7, 9, 11, 19, 23, 29$, *or* 59.

Proof. The subgroups of PSL are summarized in (**6**, p. 285). From this summary or from (**6**, Theorem, Section 262), it follows that M satisfies at least one of the following conditions:

(a) $M \subseteq PSL_{(Q)}$, for some point Q of L_∞;

(b) $M \subseteq \mathrm{N}(PSL_{(Q,R)})$, for two distinct points Q and R of L_∞;

(c) M is conjugate to a subgroup N of $PSL \cap \langle W, A\rangle$;

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

(d) M is isomorphic to $PSL_2(p^k)$ or to $PGL_2(p^k)$, for $k \leqslant r$;

(e) $M \simeq A_4, S_4$, or A_5.

The proof is immediate in case $p^r = 3$, so suppose $p^r \neq 3$. Since J is a transitive collineation group of L_∞, it follows that

$$(2;1)\cdot r \cdot |M| \equiv 0 \pmod{n+1}.$$

This congruence and Lemma (2.4) imply that M does not satisfy Condition (a) or (b) above. Moreover, if M satisfies Condition (c), then N is a cyclic or dihedral group, and hence $N \cap \langle W\rangle$ is a characteristic subgroup of N since $n \neq 3$. Therefore, J is contained in a conjugate of $\langle W, A\rangle$ by Corollary (13.6). If M satisfies Condition (d), then either $M = PSL$ or Lemma (2.4) implies that $n = 8$, $M \simeq PSL_2(2)$, and $|M| = 6$. However, in this case M also satisfies Condition (c). Last, suppose M satisfies Condition (e). If $r = 1$, then clearly $n = 3, 4, 5, 7, 11, 19, 23, 29$, or 59. But if $n = 3$ or 4, then M also satisfies Condition (d). If $r > 1$, then it can be verified directly that $n = 9$, since no groups G_{12}, G_{24}, or G_{60} occur for $n = 8$.

12.2. Proposition. *A transitive collineation group of L_∞ is either conjugate in $P\Gamma L_2(n)$ to an element of $\mathfrak{A}_\rho$, or is contained in $\mathfrak{B}_\rho \cup \mathfrak{C}_\rho$.*

Proof. The proof follows from Lemma (12.1) and the definitions of $\mathfrak{A}_\rho$, $\mathfrak{B}_\rho$, and $\mathfrak{C}_\rho$. Note that $\mathfrak{A}_\rho$, $\mathfrak{B}_\rho$, and $\mathfrak{C}_\rho$ are pairwise disjoint except if $n = 2$, in which case $\langle W, A\rangle = P\Gamma L \in \mathfrak{A}_\rho \cap \mathfrak{B}_\rho$.

12.3. Proposition. *The class of minimal transitive collineation groups of L_∞ consists of the following groups:*

(1) *the conjugates of the minimal elements of* $\mathfrak{A}_\rho$;

(2) $PSL_2(n)$, *for* $n \equiv 1 \pmod 4$ *and* $n \neq 5, 9$, or 29;

(3) G_{12} *for* $n = 5$ *and* 11; G_{24} *for* $n = 23$; *and* G_{60} *for* $n = 9, 19, 29$, *and* 59.

Proof. Parts 1 and 3 follow from the definition of $\mathfrak{A}_\rho$ and from Table I, respectively. As for part 2, if $p = 2$, then $\langle W\rangle \subset PSL$, and if $n \equiv 3 \pmod 4$, then $\langle W^2, WA\rangle \subset PSL$. If $n \equiv 1 \pmod 4$, then PSL contains no elements of $\mathfrak{A}_\rho$, and PSL contains elements of $\mathfrak{C}_\rho$ only if $n = 5, 9$, or 29, from Table I.

Theorem 1. *Every flag-transitive group of π is conjugate to an element of $\mathfrak{A}$, or is contained in $\mathfrak{B} \cup \mathfrak{C}$.*

Proof. The proof follows from Proposition (12.2), Corollary (3.3), Lemma (3.7), and the fact that $\rho^{-1}(\mathfrak{A}_\rho) = \mathfrak{A}$, $\rho^{-1}(\mathfrak{B}_\rho) = \mathfrak{B}$ (Corollary (9.4)), and $\rho^{-1}(\mathfrak{C}_\rho) = \mathfrak{C}$.

12.4. Proposition. *The class of minimal flag-transitive groups of π consists of the following groups:*

(1) *The conjugates of the minimal elements of* $\mathfrak{A}$;

(2) $G = T\cdot H$ *with* $H = SL_2(n)$, *for* $n = 1 \pmod 4$ *and* $n \neq 5, 9$, *or* 29;

(3) $G = T\cdot H$ *with* $H = G_{12}{}^*$ *for* $n = 5$ *and* 11, $H = G_{24}{}^*$ *for* $n = 23$, *and* $H = G_{60}{}^*$ *for* $n = 9, 19, 29$, *and* 59.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

Proof. The proof follows from Proposition (12.3), and Lemmas (3.6), (9.3), and (11.1).

12.5. COROLLARY. *Let G be a minimal flag-transitive group of π. Then:*

(1) *G contains $(0, L_\infty)$-homologies if and only if $p \neq 2$;*

(2) *G contains affine perspectivities* (i.e., perspectivities with an affine axis) *if and only if either $G \in \mathfrak{B}$, or $n = 9$ and $\rho(G) = G_{60}$.*

Proof. (1) See Proposition (5.5), Corollary (4.7), and Lemma (7.2).

(2) If $G \in \mathfrak{A}$, see Corollary (5.6). If G contains affine elations, then $|G| = 0$, (mod p). Moreover, every element of order p in SL, and in $G_{60}{}^*$ for $n = 9$, is an affine elation. Last, SL contains no affine homologies.

12.6. COROLLARY. *A minimal flag-transitive group of π is sharply flag-transitive if and only if $p = 2$.*

13. Isomorphisms.

13.1. LEMMA. *Let G be a flag-transitive collineation group of π. Then T is the unique minimal normal subgroup of G.*

Proof. From Lemma (3.1) and (**8**, Proposition 3), T is a minimal normal subgroup of G. If T' is some other minimal normal subgroup, then $T \cap T' = 1$ and hence $T' \subset \mathbf{C}_G(T)$. Since T is an abelian transitive permutation group of the points of π, (**18**, Theorem 5, p. 55) implies $\mathbf{C}_G(T) = T$, contrary to the assumption about T'.

As a result of Lemma (13.1), isomorphisms cannot occur between flag-transitive groups acting on planes of different orders. Let G_i be a flag-transitive group of π with H_i the subgroup fixing 0, for $i = 1$ and 2; let P be the group of all permutations of the points of π; and let $GL_{2r}(p)$ be the group of additive automorphisms of the points of π.

13.2. LEMMA. *$G_1 \simeq G_2$ only if G_1 is conjugate to G_2 in P.*

Proof. If σ is an isomorphism from G_1 onto G_2, then $\sigma(T) = T$, and $K = \sigma(H_1)$ is a complement of T in G_2. Since T is abelian, there exists an isomorphism θ of G_1 onto G_2 which maps the conjugates of H_1 onto the conjugates of H_2 (**13**, p. 243); cf. the proof of Lemma (14.2). It follows that θ is induced by conjugation by an element of P (**18**, Theorem 4, p. 54).

13.3. LEMMA. *Let $\psi \in P$ such that ψ fixes 0 and $\psi T \psi^{-1} = T$. Then $\psi \in GL_{2r}(p)$.*

Proof. For $\tau_a \in T$, $\psi \tau_a \psi^{-1} = \tau_{\psi(a)}$. So $\tau_{\psi(a+b)} = \tau_{\psi(a)+\psi(b)}$, and hence $\psi \in GL_{2r}(p)$, as required.

13.4. COROLLARY. *$G_1 \simeq G_2$ only if G_1 is conjugate to G_2 in $GL_{2r}(p)$.*

13.5. LEMMA. *Let $\langle \omega^d \rangle$ be a multiplicative subgroup of $GF(n^2)$ which is contained in no proper subfield of $GF(n^2)$. Let $\langle \omega^d \rangle$ also denote the corresponding collineation group of π. Then the normalizer of $\langle \omega^d \rangle$ in $GL_{2r}(p)$ is $V = \langle \omega, \alpha \rangle$.*

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

Proof. Let $\psi \in GL_{2r}(p)$ normalize $\langle\omega^d\rangle$. Define $\sigma(x) = \psi(1)^{-1}\cdot\psi(x)$, for $x \in \pi$, so that $\sigma \in GL_{2r}(p)$. By applying the map $\psi\nu\psi^{-1}$ to the element $\psi(1)$ of π, for $\nu \in \langle\omega^d\rangle$, it is clear that σ is an automorphism of the subgroup $\langle\omega^d\rangle$ of GF(p^{2r}), and hence σ is a field automorphism of GF(p^{2r}). Therefore $\psi \in V = \langle\omega, \alpha\rangle$.

13.6. Corollary. *Let* $J = \langle W^g\rangle \neq 1$ *for* $n + 1 \equiv 0$ (mod g.) *Then* $\mathbf{N}_{P\Gamma L}(J) = \langle W, A\rangle$.

Proof. Let C normalize J, and let $\nu \in \Gamma L$ such that $\rho(\nu) = C$. Then ν normalizes $\langle\omega^g\rangle$, and hence $\nu \in \langle\omega, \alpha\rangle$ by Lemma (13.5). Therefore, $C \in \langle W, A\rangle$.

If $G_1, G_2 \in \mathfrak{A} \cup \mathfrak{B} \cup \mathfrak{C}$ and $G_1 \simeq G_2$, then it is clear that G_1 and G_2 belong to the same class $\mathfrak{A}$, $\mathfrak{B}$, or $\mathfrak{C}$. Hence, it is sufficient to describe the isomorphisms between the elements of each of these three classes.

Let $G \in \mathfrak{A}$ and $H = G_{(0)}$. The following two lemmas are concerned with the structure of H.

13.7. Lemma. *Let* $G = \langle d, e, s\rangle \in \mathfrak{A}$ *and* $H = G_{(0)}$. *Let* η *be an arbitrary element of* H *whose order* (mod $\langle\omega^d\rangle$) *is* $2r/sm > 1$, *for some* m. *Then*:

(1) $(2r/sm)\ (p^{sm} - 1) \equiv 0$ (mod $|\eta|$);

(2) *there exists a prime* q *such that* $p^{2r} - 1 \equiv 0$ (mod q), *but* $z \not\equiv 0$ (mod q) *for* $z = 2r$, d, $|\eta|$, *or* $(p^t - 1)$, *with* $t < 2r$, *except in the following cases:*

(i) $r = 1$ *and* $p + 1 = 2^x$ *for some* x;

(ii) $p^{2r} = 64$.

Proof. (1) Let $\eta = \omega^{id}(\omega^e\alpha^s)^m = \omega^k\alpha^{sm}$, for some integer i and for $k = id + e(p^{sm} - 1)/(p^s - 1)$. The proof follows from the computation of $|\eta|$.

(2) The proof follows from Lemma (2.4) and Part (1) above.

13.8. Lemma. *Let* $G = \langle d, e, s\rangle \in \mathfrak{A}$ *and* $H = G_{(0)}$. *Then*:

(1) *The subgroup* $\langle\omega^d\rangle$ *is the unique characteristic cyclic subgroup of* H *of order* $(p^{2r} - 1)/d$, *with the following exceptions:*

(i) *If* $p^{2r} = 9$, *then* $H = \langle\omega^2, \omega\alpha\rangle$ *is isomorphic to the quaternion group, and so contains three normal, cyclic, non-characteristic subgroups of order* 4, *namely* $\langle\omega^2\rangle$, $\langle\omega\alpha\rangle$, *and* $\langle\omega^3\alpha\rangle$.

(ii) *If* $p^{2r} = 64$, *and* $G = \langle 7, e, 2\rangle \in \mathfrak{A}$, *then* H *is isomorphic to the group of order* 27 *which is generated by two elements* a *and* b, *subject to the following relations:* $a^9 = b^3 = 1$ *and* $b^{-1}ab = a^4$ (cf. **18**, p. 150). *Therefore,* H *contains three normal, cyclic, non-characteristic subgroups of order* 9, *namely* $\langle\omega^7\rangle$ *and* $\langle\omega^{21}, \omega^{e_i}\alpha^2\rangle$ *for* $i = 1$ *and* 2, *where* $0 \leqslant e_1, e_2 < 21$, $e_1 \equiv e_2 \equiv e$ (mod 7), *and* $e_i \not\equiv 0$ (mod 3).

(2) *If* d_1 *divides* $(n - 1)(n + 1, 2r)$, *and* $0 < d_1 < d$, *then* H *contains no cyclic subgroup of order* $(p^{2r} - 1)/d_1$, *with the following exception. If* $p^{2r} = 64$ *and* $G = \langle 21, e, 2\rangle \in \mathfrak{A}$, *then* H *is cyclic of order* $9 = 63/d_1$, *for* $d_1 = 7$.

(3) *The multiplicative subgroup* $\langle\omega^d\rangle$ *of* GF(p^{2r}) *is contained in no proper subfield of* GF(p^{2r}), *except that if* $p^{2r} = 64$, *then* $\langle\omega^{21}\rangle \subseteq$ GF(4).

Proof. Suppose there exists an element η of $H - \langle\omega^d\rangle$ such that $|\eta| = (n^2 - 1)/d_1$, where d_1 divides $(n-1)(n+1, 2r)$ and $0 < d_1 \leqslant d$. Then from Lemma (13.7),

$$\frac{d_1 2r}{sm}(p^{sm} - 1) \equiv 0 \pmod{p^{2r} - 1}$$

and hence either (i) $r = 1$ and $p + 1 = 2^x$, or (ii) $p^{2r} = 64$. In Case (i), $2d_1 \equiv 0 \pmod{2^x}$, so $d_1 = d = 2$ and $p = 3$. This case is an exception to (1), as described above. In Case (ii),

$$\frac{6d_1}{sm}(2^{sm} - 1) \equiv 0 \pmod{63}$$

and d_1 divides 21. The following subcases can occur: $sm = 2$ and $d_1 = 7$ or 21. Note that $sm = 1$ and $d_1 = 21$ is impossible, for then $d = 21$, $g = (n + 1, d) = 3$, and hence $s = 2$ by Proposition (4.3). Similarly, if $d_1 < d$, then $d = 21$, $d_1 = 7$, $s = 2$, and $m = 1$. Therefore, $G = \langle 21, e, 2\rangle$ with $(3, e) = 1$ and $0 \leqslant e < 21$ are the only exceptions to (2).

To complete the proof of (1), let $p^{2r} = 64$ and $d = d_1$, and consider the following cases:

(a) Let $d = 7$, $s = 1$, and $m = 2$. Then H contains exactly three cyclic subgroups of order 9, two of which are conjugate in H. Therefore, this case is not an exception to (1).

(b) *Let* $d = 7$, $s = 2$, and $m = 1$. Then H has two generators, $a = \omega^7$ and $b = (\omega^{e'}\alpha^2)^{-1}$, for some e', as described in (ii).

(c) Let $d = 21$, $s = 2$, and $m = 1$. Then H is cyclic of order 9, and hence this case is not an exception to (1).

To prove Part (3), note that if $\langle\omega^d\rangle \subseteq \mathrm{GF}(p^t)$ for $t < 2r$, then $d(p^t - 1) \equiv 0 \pmod{p^{2r} - 1}$. As above, it follows that $p^{2r} = 64$ and $d = 21$; in this case, $G = \langle 21, e, 2\rangle$ for $(3, e) = 1$, and $\langle\omega^{21}\rangle \subseteq \mathrm{GF}(4)$.

13.9. LEMMA. *Two elements of $\mathfrak{A}$ are isomorphic only if they are conjugate under an element of $\langle\omega, \alpha\rangle$, with the following exception. If $n = 8$, then the groups $G_1 = \langle 7, 0, 6\rangle$ and $G_2 = \langle 21, e, 2\rangle \in \mathfrak{A}$ are isomorphic, but are not conjugate in* $\mathbf{G}$.

Proof. Let $G_i = \langle d_i, e_i, s_i\rangle = T\cdot H_i \in \mathfrak{A}$, where $H_i = (G_i)_{(0)}$, for $i = 1$ and 2. If $G_1 \simeq G_2$, then by Corollary (13.4) there exists $\psi \in GL_{2r}(p)$ such that $\psi H_1 \psi^{-1} = H_2$. From (1) and (2) of Lemma (13.8), it follows that $d_1 = d_2 = d$, $s_1 = s_2 = s$, and $\psi\langle\omega^d\rangle\psi^{-1} = \langle\omega^d\rangle$, with the possible exceptions of the cases $n = 3$ and $n = 8$. From Lemma (13.5) and Part (3) of Lemma (13.8), it follows that $\psi \in \langle\omega, \alpha\rangle$, except possibly if $n = 8$.

From the exceptions of Lemma (13.8), it is clear that the only possible exception to Proposition (13.9) is the case $n = 8$, $G_1 = \langle 7, 0, 6\rangle$ and

$$G_2 = \langle 21, e, 2\rangle \in \mathfrak{A}.$$

This case is an exception, as follows.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

With respect to the basis $\{\omega^i\}$, $0 \leqslant i \leqslant 5$, for π over GF(2), let

$$\eta = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Using Bussey's tables **(4)** for GF(2^6) with $\omega = i$, it follows that $\eta\omega^7\eta^{-1} = \omega^{22}\alpha^2$, $\eta^2\omega^7\eta^{-2} = \omega^{40}\alpha^4 = (\omega^8\alpha^2)^2$, and $\eta^3 = 1$. Hence η normalizes $G = \langle 7, 1, 2\rangle$. Moreover, $G_1 = \langle 7, 0, 6\rangle$ and $G_2' = \langle 21, 1, 2\rangle$ are conjugate under η, $G_2 \simeq G_2'$, and hence $G_1 \simeq G_2$. However, $\eta \notin \mathbf{G}$, since η does not preserve the lines of π. Moreover, there exists no collineation $\nu \in \mathbf{G}$ such that $\nu G_1 \nu^{-1} = G_2'$. For if so, then $\eta^{-1}\nu$ normalizes $\langle\omega^7\rangle$, $\eta^{-1}\nu \in V$ by Lemma (13.5) and $\eta \in \mathbf{G}$. Therefore, G_1 is not conjugate to G_2 in $\mathbf{G}$.

13.10. Corollary. *Let $G_i = \langle d, e_i, s\rangle \in \mathfrak{A}$, for $i = 1$ and 2. Then $G_1 \simeq G_2$, if and only if $e_2 \equiv e_1 p^k \pmod h$ for some k, where $h = (d, p^s - 1)$.*

13.11. Lemma. *Two elements G_1 and G_2 of $\mathfrak{B}$ are isomorphic only if they are conjugate under $\langle\omega, \alpha\rangle$.*

Proof. If $G_1 \simeq G_2$, then from Corollary (13.4) there exists $\psi \in GL_{2r}(p)$ such that $\psi G_1 \psi^{-1} = G_2$, $\psi(SL)\psi^{-1} = SL$, and $\psi\langle\omega^{n-1}\rangle\psi^{-1} = \langle\omega^{n-1}\rangle$. Then Lemma (13.5) implies $\psi \in \langle\omega, \alpha\rangle$, as required.

13.12. Lemma. *Two elements of $\mathfrak{C}$ are isomorphic only if they are conjugate in* $\mathbf{G}$.

Proof. If $n \neq 9$, apply Corollary (13.4). If $n = 9$, use the proof of Lemma (13.11), with G_{60}^* playing the role of SL.

Theorem 2. *Two flag-transitive collineation groups of π are isomorphic only if they are conjugate in $\mathbf{G}$, with the following exception. If G_1 and G_2 are conjugate in $\mathbf{G}$ to the elements $\langle 7, 0, 6\rangle$ and $\langle 21, e, 2\rangle$ of $\mathfrak{A}$, respectively, then $G_1 \simeq G_2$ but G_1 is not conjugate to G_2 in $\mathbf{G}$.*

14. Automorphisms. Let $G = T\cdot H$ be a flag-transitive collineation group of π, with $H = G_{(0)}$. Let $\mathbf{A}(G)$ and $\mathbf{O}(G)$ be the automorphism group and the outer automorphism group of G, respectively, and let K be the normalizer of H in $GL_{2r}(p)$. Finally, let $B^1(H, T)$, $Z^1(H, T)$, and $H^1(H, T)$ be the 1-coboundary, 1-cocycle, and 1-cohomology groups of H with coefficients in T, respectively.

14.1. Lemma. *$\mathbf{N}_P(G)$ is isomorphic to a subgroup of $\mathbf{A}(G)$; and $\mathbf{N}_P(G) = T\cdot K$.*

Proof. From (**18**, Theorem 5, p. 55), $\mathbf{C}_P(G) = 1$, since H is a maximal subgroup (**8**, Proposition 3) which is not normal in G. Therefore, the natural mapping from $\mathbf{N}_P(G)$ into $\mathbf{A}(G)$ is a monomorphism. From Lemma (13.3), $\mathbf{N}_P(G) \subset \langle T, GL_{2r}(p)\rangle$, so $\mathbf{N}_P(G) = T \cdot K$.

14.2. Lemma. $\mathbf{A}(G) = \mathbf{D} \cdot \mathbf{J}$ *is the split extension of* $\mathbf{D}$ *by* $\mathbf{J}$, *where* $\mathbf{D} \simeq Z^1(H, T)$, *and* $\mathbf{J} \simeq K$.

Proof. Let $\mathbf{D}$ be the group of automorphisms of G which induce the identity mappings in T and G/T, and let $\mathbf{J}$ be the group of automorphisms of G which fix H. Then $\mathbf{D} = Z^1(H, T)$ (**13**, Theorem 13, p. 244), and the elements $\theta \in \mathbf{D}$ are in one-to-one correspondence with the complements of T under the mapping $\theta \rightarrow \theta(H)$. It follows that $\mathbf{A}(G)$ is the split extension of $\mathbf{D}$ by $\mathbf{J}$. In addition, $\mathbf{J} \simeq K$ from (**18**, Theorem 4, p. 54) and Lemma (14.1). Moreover, $\mathbf{D}$ contains a subgroup $\mathbf{T}$ of automorphisms induced by conjugation in G by elements of T, and $\mathbf{T} \simeq B^1(H, T)$.

14.3. Corollary. $\mathbf{A}(G) \simeq \mathbf{N}_P(G)$ *if* $H^1(H, T) = 0$.

Proof. $H^1(H, T) = 0$ implies $\mathbf{T} = \mathbf{D}$ and $\mathbf{A}(G) = \mathbf{T} \cdot \mathbf{J} \simeq T \cdot K = \mathbf{N}_P(G)$.

14.4. Lemma. *Let H be a group of non-singular linear transformations of a finite vector space T. Let $\langle \eta \rangle$ be a cyclic normal subgroup of H such that η fixes no non-zero element of T. Then $H^1(H, T) = 0$.*

Proof. Let f be a 1-cocycle of H in T. Since η fixes no element $\neq 0$ of T, f is a 1-coboundary on $\langle \eta \rangle$ with respect to a unique element τ of T. By solving the equation $f(\nu \cdot \eta) = f((\nu\eta\nu^{-1}) \cdot \nu)$ for $f(\nu)$, with $\nu \in H$, it follows that f is a 1-coboundary on $\langle \nu, \eta \rangle$ with respect to τ. Therefore, f is a 1-coboundary on H.

14.5. Corollary. *Let* $G = T \cdot H \in \mathfrak{A} \cup \mathfrak{B} \cup \mathfrak{C}$, *with* $H = G_{(0)}$. *Then* $H^1(H, T) = 0$, *except for the case* $p = 2$, $r > 1$, *and* $H = \langle SL, \omega^{n-1}, \omega^e \alpha^s \rangle$.

Proof. Apply Lemma (14.4) with $\eta = \omega^d$ if $G \in \mathfrak{A}$, and $\langle \eta \rangle = K$, the kernel of H, if $G \in \mathfrak{B} \cup \mathfrak{C}$. $K = 1$ only if $H = \langle SL, \omega^{n-1}, \omega^e \alpha^s \rangle$, $p = 2$ and $r > 1$, and then $H^1(H, T) \neq 0$ (see Lemma (14.7)).

14.6. Lemma. *Let* $G = \langle d, e, s \rangle \in \mathfrak{A}$. *Then:*

(1) $\mathbf{A}(G) \simeq \mathbf{N}_{\mathbf{G}}(G)$ *with the following exceptions*:

(i) *If* $n = 8$ *and* $G = \langle 21, e, 2 \rangle \in \mathfrak{A}$, *then* $\mathbf{A}(G) \simeq U$.

(ii) *If* $n = 8$ *and* $G = \langle 7, e, 2 \rangle \in \mathfrak{A}$, *then* $\mathbf{O}(G) \simeq S_3$, *the symmetric group of degree* 3.

In each case, $\mathbf{A}(G)$ *is not isomorphic to* $\mathbf{N}_{\mathbf{G}}(G)$.

(2) $\mathbf{N}_{\mathbf{G}}(G) = \langle d/h, e', \mathrm{ord}_v p \rangle$ *for some* e', *where* $h = (d, p^s - 1)$, *and* $v = h/(h, e)$, *with the following exception:*

(iii) *If* $n = 3$ *and* $G = \langle 2, 1, 1 \rangle$, *then* $\mathbf{N}_{\mathbf{G}}(G) = \mathbf{G}$. *In this case,* $\mathbf{A}(G) \simeq \mathbf{G}$, *and* $\mathbf{O}(G) \simeq S_3$.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

Proof. $\mathbf{A}(G) \simeq \mathbf{N}_P(G)$ from Corollaries (14.3) and (14.5). From Lemmas (13.5), (13.8), and (14.1) $\mathbf{N}_P(G) = \mathbf{N}_{\mathbf{G}}(G) = T\cdot\mathbf{N}_V(H)$, except possibly when $n = 3$ or 8.

If $n = 3$, then $G = \langle 2, 1, 1\rangle$ is an exception, as follows. If $J = \rho(G)$, then $\mathbf{N}_{\mathbf{G}}(G) = \rho^{-1}(\mathbf{N}_{PGL}(J)) = \mathbf{G}$, and $\mathbf{G}/G \simeq PGL/J \simeq S_3$.

If $n = 8$, it is clear from Lemma (13.8) that the possible exceptions are $G_1 = \langle 21, e, 2\rangle$ and $G_2 = \langle 7, e, 2\rangle$ of $\mathfrak{A}$. From Lemma (13.9), $\mathbf{A}(G_1) \simeq U$ since $G_1 \simeq \langle 7, 0, 6\rangle$, and $\mathbf{A}(G_1)$ is not isomorphic to $\mathbf{N}_{\mathbf{G}}(G_1)$.

Let $n = 8$, $G = \langle 7, 1, 2\rangle$, and $H = G_{(0)}$. If $\nu \in GL_{2r}(p)$ normalizes H and fixes each of the three normal cyclic subgroups $\langle\omega^7\rangle$, $\langle\omega\alpha^2\rangle$, $\langle\omega^8\alpha^2\rangle$ of H, then $\nu \in H$. Hence $\mathbf{O}(G) \subseteq S_3$ as a permutation group of these three subgroups. Moreover, $\omega^5\alpha$ and η normalize G, and induce elements of $\mathbf{O}(G)$ of orders 2 and 3, respectively (cf. the proof of Lemma (13.9)). Therefore,

$$\mathbf{A}(G) \simeq T\cdot\langle\omega^7, \omega^5\alpha, \eta\rangle,$$

and $\mathbf{O}(G) \simeq S_3$. Clearly $\mathbf{A}(G)$ is not isomorphic to $\mathbf{N}_{\mathbf{G}}(G)$.

14.7. Lemma. *Let $p = 2$ and $r > 1$. Let $G = T\cdot H \in \mathfrak{B}$, with*

$$H = \langle SL, \omega^{n-1}, \omega^e\alpha^s\rangle$$

represented in standard form. Then $|H^1(H, T)| = 2^s$.

Proof. Replace H by its conjugate $K = \langle SL, \omega^{n-1}, \sigma^s\rangle$, where $\sigma\colon (a, b) \to (a^2, b^2)$. The group $H^1(K, T)$ can be computed using elementary techniques. However, J. E. McLaughlin has constructed a much shorter proof, as follows. Let

$$M = \left\{\begin{pmatrix} 1 & 0 \\ x & 1\end{pmatrix} : x \in \mathrm{GF}(n)\right\}$$

be a Sylow 2-subgroup of SL. By (**5**, Theorem 10.1, p. 259), $H^1(SL, T)$ is isomorphic to the subgroup of $H^1(M, T)$ induced by the 1-cocycles f satisfying $f(\lambda\chi\lambda^{-1}) \sim \lambda f(\chi)$, for $\chi \in M$ and

$$\lambda \in \mathbf{N}_{SL}(M) = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix} : a \neq 0 \quad \text{in } \mathrm{GF}(n)\right\}.$$

A direct computation shows that if $r > 1$, then the representative stable 1-cocycles of M have the form

$$f_c\begin{pmatrix} 1 & 0 \\ x & 1\end{pmatrix} = (0, c\sqrt{x}),$$

for $c \in \mathrm{GF}(n)$. Moreover, by (**5**, (4), p. 350) or (**10**, Theorem 2, p. 129),

$$O \to H^1(H/SL, T^{SL}) \to H^1(H, T) \to (H^1(SL, T))^H \to H^2(H/SL, T^{SL})$$

is an exact sequence. Since $T^{SL} = 0$, it follows that $H^1(H, T) \simeq (H^1(SL, T))^H$. The representative 1-cocycle f_c of SL is invariant under σ^s if and only if $c^{2^s} = c$. Therefore, $|H^1(H, T)| = 2^s$, as required.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

14.8. Lemma. *Let $G = T \cdot H \in \mathfrak{B}$, with $H = \langle SL, \omega^d, \omega^e\alpha^s\rangle$ represented in standard form. Then $\mathbf{A}(G) \simeq \mathbf{N_G}(G)$, except if $p = 2$, $r > 1$, and $d = n - 1$. In this case, $\mathbf{A}(G) = \mathbf{D}\cdot\mathbf{J}$ is the split extension of $\mathbf{D}$ by $\mathbf{J}$, where $\mathbf{D}$ is an elementary abelian group of order 2^{2^r+s}, and $\mathbf{J} \simeq \mathbf{N_G}(H)$.*

Proof. Apply Lemma (14.2), Corollaries (14.3) and (14.5), and Lemma (14.7); cf. proof of Lemma (13.11).

14.9. Lemma. *$G \in \mathfrak{C}$ implies $\mathbf{A}(G) \simeq \mathbf{N_G}(G)$.*

Theorem 3. *If G is a flag-transitive collineation group of π, then $\mathbf{A}(G) \simeq \mathbf{N_G}(G)$, with the following exceptional cases:*

(1) $n = 8$ and G conjugate to $\langle 7, 1, 2\rangle$ or to $\langle 21, 1, 2\rangle \in \mathfrak{A}$;

(2) $p = 2$, $r > 1$, and $G = T\cdot\langle SL, \omega^{n-1}, \omega^e\alpha^s\rangle \in \mathfrak{B}$.

15. The doubly transitive collineation groups of π. From Theorem 1, every doubly transitive collineation group G of π is conjugate to an element of $\mathfrak{A} \cup \mathfrak{B} \cup \mathfrak{C}$. Every element of $\mathfrak{B}$ is doubly transitive, and the doubly transitive elements of $\mathfrak{C}$ are determined in Proposition (11.3) (see Table II). Therefore, in order to describe the doubly transitive groups of π, it is sufficient to determine the doubly transitive elements of $\mathfrak{A}$. However, it is no more difficult to determine the class $\mathfrak{D}$ of doubly transitive collineation groups of the finite Desarguesian affine lines. Then $\mathfrak{A} \cap \mathfrak{D}$ is the subclass of doubly transitive elements of $\mathfrak{A}$.

Let L be the Desarguesian affine line of order $n = p^t$ represented by $\mathrm{GF}(p^t)$; that is, the points of L are represented by the elements of $\mathrm{GF}(p^t)$. Let ω be a primitive root of $\mathrm{GF}(p^t)$, and let α be the automorphism of $\mathrm{GF}(p^t)$ defined by $\alpha(x) = x^p$. As before, let ω, α, and τ_a denote the following maps of L: $x \to \omega x$, $x \to \alpha(x)$, and $x \to x + a$ (for $a \in \mathrm{GF}(p^t)$). Let $T = \langle \tau_a : a \in \mathrm{GF}(p^t)\rangle$, $V = \langle \omega, \alpha\rangle$, and $U = \langle T, V\rangle$. Then U is the full collineation group of L, U is the split extension of T by V, and $V = U_{(0)}$. If $t = 2r$, then T, V, and U are the groups previously defined in Section 3.

15.1. Definition. *Let $\mathfrak{D}$ be the class of doubly transitive collineation groups of L.*

15.2. Lemma. *Let $G \in \mathfrak{D}$. Then $T \subset G$, and $G = T\cdot H$ is the split extension of T by $H = G_{(0)}$.*

Proof. See the proof of Lemma (3.1).

If $G \in \mathfrak{D}$, then $H = G_{(0)}$ has the form $H = \langle \omega^d, \omega^e\alpha^s\rangle$, for integers d, e, and s. As in Lemma (4.1), d, e, and s can be chosen uniquely, subject to the conditions: (i) $d > 0$ and $n \equiv 1 \pmod{d}$; (ii) $s > 0$ and $t \equiv 0 \pmod{s}$; (iii) $0 \leqslant e < d$, and $e\{(n-1)/(p^s-1)\} \equiv 0 \pmod{d}$. As before, if d, e, and s satisfy the conditions (i)–(iii), then G is said to be in *standard form* and G is denoted by $\langle d, e, s\rangle$.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

The elements of $\mathfrak{D}$ are described in the following propositions in terms of the parameters d, e, and s. The proofs are very similar to the proofs in Sections 4 and 5, and hence are omitted.

15.3. Proposition. *Let* $G = \langle d, e. s\rangle$. *Then* $G \in \mathfrak{D}$ *if and only if the following conditions are satisfied:*

(i) *the primes of* d *divide* $p^s - 1$;
(ii) *if* $p^s \equiv 3 \pmod 4$, *then* $d \not\equiv 0 \pmod 4$;
(iii) $t \equiv 0 \pmod{sd}$;
(iv) $(e, d) = 1$.

15.4. Corollary. *If* $G = \langle d, e, s\rangle \in \mathfrak{D}$, *then* $H_{(1)} = \langle \alpha^{sd}\rangle$.

15.5. Proposition. *The class of minimal elements of* $\mathfrak{D}$ *is the disjoint union of the following two classes:*

(1) *the sharply* 2-*fold transitive collineation groups of L;*
(2) *the groups* $\langle d, e, s\rangle \in \mathfrak{D}$ *which satisfy the following conditions:*
  (i) d *is even,*
  (ii) $p^s \equiv 3 \pmod 4$,
  (iii) $t/sd = 2^x$ *for some* $x \geqslant 1$.

Theorem 4. *The class of doubly transitive collineation groups of* π *consists of the following groups:*

(1) *the conjugates of the elements of* $\mathfrak{A} \cap \mathfrak{D}$;
(2) *the elements of* $\mathfrak{B}$;
(3) *certain elements of* $\mathfrak{C}$ *as summarized in Table* II.

15.6. Proposition. *The class of minimal doubly transitive groups of* π *consists of the following groups:*

(1) *the conjugates of the minimal elements of* $\mathfrak{A} \cap \mathfrak{D}$;
(2) $G = T\cdot SL$ *with* $n \neq 2, 3, 5, 7,$ *or* 11;
(3) *certain elements of* $\mathfrak{C}$ *as summarized in Table II.*

Theorem 2″. *Two doubly transitive collineation groups of* π *are isomorphic only if they are conjugate in* $\mathbf{G}$.

16. Solvable doubly transitive planes. If G is a doubly transitive collineation group of the Desarguesian affine plane π of order n, then with one exception, G uniquely determines π. To be more precise, let G' be a doubly transitive group of an arbitrary affine plane π'.

16.1. Proposition. *With one exception, if* $G \simeq G'$, *then* $\pi \simeq \pi'$.

Proof. If $G \simeq G'$, then G acts faithfully as a doubly transitive group of π'. Let M and K be the subgroups of G fixing an incident point and line, respectively, of π'. From (**8**, Proposition 1), G acts naturally on the incidence system $\pi(G, M, K)$ whose points and lines are the left cosets of M and K, respectively, and $\pi' \simeq \pi(G, M, K)$. It is sufficient to show that M and K are the subgroups

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

of G fixing a point and line, respectively, of π, for then $\pi \simeq \pi(G, M, K) \simeq \pi'$.

From **(8**, Proposition 3**)** M is a complement of T, and thus it can be assumed that $M = G_{(0)}$, for $0 \in \pi$; see the proof of Lemma (13.2). Hence, the points of π and π' can be identified. Let $R = K \cap T$, let $J = K \cap M$, and let l' be the line of π' fixed by K. Then $|J| = |M|/(n+1) = |K|/n$ from **(8**, Proposition 1**)**. Since π' is a translation plane from **(14**, Theorem 1**)**, it follows that $|R| = n$ and $K = R \cdot J$.

(1) Let $G \in \mathfrak{A} \cap \mathfrak{D}$ and assume that $1 \in l'$. Lemma (2.4) and the order of J imply that $J \cap \langle \omega \rangle$ transforms 1 into points of π which generate the additive subgroup GF(n) of π, except in a few cases which must be treated separately. In every case, l' is a line of π, as required.

(2) Let $G \in \mathfrak{B}$. Then $T \cdot SL$ acts as a doubly transitive group on π', so it is sufficient to assume that $G = T \cdot SL$ and $M = SL$. From **(6**, Theorem, Section 262**)**, the subgroups of index $n + 1$ in SL form one conjugacy class in SL. Moreover, the only subset of order n of π which is fixed by such a subgroup of SL is a line of π. Therefore, $\pi = \pi'$.

(3) If $G \in \mathfrak{C}$ and $n \neq 9$, then $\pi \simeq \pi'$ since there exists only one translation plane of order $n = p$. If $n = 9$ and $G = T \cdot \langle G_{60}^*, c \rangle$ of Table II or $G = G_1$ of Figure 1, then $\pi = \pi'$ since $J \cap \langle c \rangle$ generates GF(9). However, G_6 of Figure 1 occurs as a doubly transitive group on the plane π' whose lines are the images under G_6 of the additive subgroup $V = \{(1, c^6), (c^6, 1)\}$ of π. Moreover, the subgroup J_1 of H_6 fixing V and a subgroup J_2 of H_6 fixing a line of π are not isomorphic. For $J_1 = \langle \chi, \psi \rangle$, where $\psi = -\delta^2\chi\delta^{-1}$, and $\rho(J_1) \simeq A_4$ in S_5, while $\rho(J_2)$ is isomorphic to the normalizer in S_5 of an element of order 3. Therefore, it follows from Theorem 2 that π is not isomorphic to π'. In fact, it can be shown that π' is the near-field plane of order 9. Finally, it can be shown directly that G_3 of Figure 1 uniquely determines π.

Theorem 5. *A finite affine plane π' which has a solvable doubly transitive collineation group G is either a Desarguesian plane or the near-field plane of order* 9.

Proof. Let m be the order of π'. From **(11)** and Proposition (16.1), either π' is a Desarguesian plane or G is one of a finite number of exceptional groups described by Huppert. The exceptional groups of Huppert which occur for $m = 3, 5, 7, 11$, and 23 can easily be identified with the corresponding solvable double transitive groups of $\mathfrak{B} \cup \mathfrak{C}$ (see Table II), and hence in these cases π' is Desarguesian.

For $n = 9$, the three exceptional groups of Huppert occur as collineation groups of the near-field plane of order 9, as follows. Let ω be a primitive root of GF(9), and define $\omega^i \circ \omega^j = \omega^{i+ej}$ by $e = 1$ if i is even and $e = 3$ if i is odd. Let $K = \{\text{GF}(9), +, \circ\}$ be the (left) near-field of order 9, and let π' be the corresponding affine plane. Define σ, an automorphism of K, by $\sigma(\omega^2) = \omega^3$, $\sigma(\omega) = \omega^5$, and $\sigma^2 = 1$. Define the following collineations A, B, C, D, F, and G of π', using the notation of **(1**, Sections 2 and 4–6**)**:

$$A = \epsilon(\underline{-1}),\ B = (\overline{-1}),\ C = \underline{\omega^7}\overline{\omega^7},\ D = \underline{\omega^5}\overline{\omega^5},\ F = (\overline{-1})(\underline{\omega^2}\eta)^2\underline{\omega^7}(\overline{-1}),$$
$$\text{and } G = \underline{\omega^2}\overline{\omega^5}\sigma.$$

By regarding π' as a two-dimensional vector space over K, and K as a two-dimensional space over GF(3) with basis $(\omega, 1)$, the collineations $A, \ldots, G$, can be represented as 4×4 matrices, using Bussey's tables **(4)** for GF(9). These matrices can also be derived from the generators $A, \ldots, G$ of Huppert's groups **(11**, p. 127**)** by interchanging the second and third rows and columns of each matrix. Therefore, Huppert's groups occur as doubly transitive collineation groups of π'. Using the technique of Proposition (16.1) and the structure of π'**(1)**, it is possible to show that each of these three groups uniquely determines π'. The details of this final step in the proof of Theorem 5 are straightforward but lengthy, and hence are omitted.

In addition to the three exceptional groups of Huppert, it can be shown that there exist exactly four other flag-transitive collineation groups of the near-field plane π' of order 9 (up to conjugacy in the full collineation group of π'). These groups are $G_i = T \cdot H_i$ $(1 \leqslant i \leqslant 4)$, where $H_1 = \langle A, B, C, D, F, G, S\rangle$, $H_2 = \langle A, B, C, D, F, G^2, S\rangle$, $H_3 = \langle F, BAG, S\rangle$, $H_4 = \langle F, BAG\rangle$, and S is the collineation of π' induced by the automorphism λ of the near field K defined by $\lambda\colon \omega \to \omega^2 \to \omega^7$, and $\lambda^3 = 1$. The groups G_1, G_2, and G_3 are non-solvable, doubly transitive groups of π', while G_4 is a solvable group which is not doubly transitive on π'. Moreover, G_3 is isomorphic to the doubly transitive group $G_6 = T \cdot \langle G_{60}{}^*, c\sigma\rangle$ of the Desarguesian plane π of order 9 (see Figure 1 and Proposition (16.1)), and G_4 is isomorphic to the flag-transitive group $\langle 8, 1, 1\rangle$ of π; see Proposition (4.3). Finally, it can be shown directly that π and π' are the only translation planes of order 9.

17. Near-fields. Let G_i be a finite doubly transitive Frobenius group acting on a set $Q = \{0, 1, \ldots\}$ with sharply transitive subgroup T_i and with $H_i = (G_i)_{(0)}$, for $i = 1$ and 2. Let $Q_1 = \{Q, +, \circ\}$ and $Q_2 = \{Q_2, +, *\}$ be the associated complete (left) near fields. The notation and definitions of **(16)** will be assumed. From **(17)** it is clear that $G_i \in \mathfrak{D} \cup \mathfrak{C}$, for $i = 1$ and 2.

17.1. Proposition. *$G_1 \simeq G_2$ if and only if $Q_1 \simeq Q_2$.*

Proof. If $G_1 \simeq G_2$, then, as in Lemmas (13.2) and (13.3), it follows that there exists an additive automorphism ψ of Q such that ψ fixes 1 and $\psi G_1 \psi^{-1} = G_2$. Moreover, $\psi(a \circ b) = \psi(a) * \psi(b)$, for a and b in Q. For $\psi H_1 \psi^{-1} = H_2$ and $\psi(1) = 1$ imply that $\psi M_a \psi^{-1} = M_{\psi(a)}$, for $a \neq 0$ in Q. Hence, $M_{\psi(a \circ b)} = M_{\psi(a) * \psi(b)}$, as required. Therefore, ψ is a near-field isomorphism from Q_1 onto Q_2. Conversely, if ψ is a near-field isomorphism from Q_1 onto Q_2, then ψ is an additive isomorphism of Q which fixes 1, and $\psi G_1 \psi^{-1} = G_2$. For if $A_a M_b \in G_1$, then $\psi A_a M_b \psi^{-1} = A_{\psi(a)} M_{\psi(b)} \in G_2$. Therefore, $G_1 \simeq G_2$.

Now let $G = G_1$, $H = H_1$, $Q = Q_1$, and $|Q| = n = p^t$; let $\mathbf{A}(Q)$ be the group of near-field automorphisms of Q.

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

17.2. Corollary. *$\mathbf{A}(G)$ is isomorphic to $G \cdot \mathbf{A}(Q)$, the split extension of G by $\mathbf{A}(Q)$.*

Proof. From Lemma (14.1) and Corollary (14.3), $\mathbf{A}(G) \simeq T \cdot K$, where K is the normalizer of H in the group of additive automorphisms of Q. From the proof above, $\mathbf{A}(Q) \subseteq K$, and $\mathbf{A}(G)$ is the split extension of G by $\mathbf{A}(Q)$.

17.3. Corollary. *Let $G = \langle d, e. s\rangle \in \mathfrak{D}$, for $|Q| = p^t$. Then $\mathbf{A}(Q) = \langle \alpha^{\mathrm{ord}_d p}\rangle$ is a cyclic group of order $t/(\mathrm{ord}_d\, p)$, with the following exception. If $p^t = 9$ and $G = \langle 2, 1, 1\rangle$, then $\mathbf{A}(Q) \simeq S_3$, the symmetric group of degree 3.*

Proof. As in the proof of Lemma (14.6), $\mathbf{A}(Q) \subseteq \langle\alpha\rangle$ except when $p^t = 9$.

17.4. Corollary. *Let $G \in \mathfrak{C}$. Then $\mathbf{A}(Q)$ is a cyclic group of the order given in Table III.*

TABLE III

n	$\rho(H)$	$\lvert\mathbf{A}(Q)\rvert$	n	$\rho(H)$	$\lvert\mathbf{A}(Q)\rvert$
5	G_{12}	4	23	G_{24}	1
7	G_{24}	3	29	G_{60}	2
11	G_{12}	2	59	G_{60}	1
11	G_{60}	5			

Proof. The proof follows from Table II by noting that $\mathbf{A}(Q) \simeq \rho(\mathbf{A}(Q)) = (\mathbf{N}_{P\Gamma L}(\rho(H)))_{(R)}$, where R is the intersection of L_∞ and l, the line of π containing 0 and 1.

Let L be the Desarguesian affine line of order $n = p^t$, as in Section 15. It is possible using the techniques of Theorems 1 and 4 to determine all Frobenius subgroups of U which contain T. Let $G = \langle d, e, s\rangle \subseteq U$ such that $G \neq T$ and let g be the largest factor of d whose primes divide $p^s - 1$. If q is a prime divisor of g, define a, b, and f as follows: $q^a \| p^s - 1$, $q^b \| g$, and $q^f \| e$. If $p^s \equiv 3 \pmod 4$ and $q = 2$, define c by $2^c \| p^s + 1$.

17.5. Proposition. *$G = \langle d, e, s\rangle$ is a Frobenius permutation group of L if and only if the following conditions are satisfied:*

(a) if $g \equiv 0 \pmod q$ for q a prime, and if $b > a$, then $a > f$;

(b) $t/s = g/(g, c)$, except if $p^s \equiv 3 \pmod 4$, $d \equiv 0 \pmod 2$, and $e \equiv 1 \pmod 2$, in which case:

$$(b') \qquad \frac{t}{s} = \frac{2g}{(g, 2^c e)}.$$

Proof. No non-identity element of G fixes two points of L if and only if t/s is the minimal solution for m in the following congruence:

$$e\left(\frac{p^{ms} - 1}{p^s - 1}\right) \equiv 0 \quad (\mathrm{mod}(d, p^{ms} - 1)).$$

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

By repeated use of Lemma (2.2), it is possible to show that this statement is equivalent to Conditions (a), (b), and (b').

18. Flag-transitive affine spaces. Let $A = A_t(n)$ be an affine space of order $n = p^r$ and of dimension $t \geqslant 3$. A *flag* of A is a sequence

$$S_0 \subset S_1 \subset \ldots \subset S_{t-1}$$

of linear subvarieties of A such that S_i has dimension i $(0 \leqslant i \leqslant t-1)$. A collineation group G of A is *flag-transitive* on A if G is transitive on the flags of A; cf. **(9)**. The flag-transitive groups of A are described in the following theorem (cf. Theorem 1′).

THEOREM 6. *A flag-transitive collineation group of $A_t(n)$ contains E, the subgroup generated by the elations of $A_t(n)$, except possibly if $A_t(n) = A_3(2)$, $A_3(8)$, or $A_4(2)$.*

Proof. As in Section 3, let $\mathbf{G}$, T, $\Gamma L = \Gamma L_t(n)$, and $SL = SL_t(n)$ be the groups of collineations, translations, non-singular semilinear transformations, and unimodular linear transformations of A, respectively. As before, $\mathbf{G} = T\cdot\Gamma L$, $T \cap \Gamma L = 0$, and $\Gamma L = \mathbf{G}_{(0)}$. Let $P = P_{t-1}(n)$ be the Desarguesian projective space of order n and dimension $t-1$, regarded as the hyperplane at infinity of A. Let ρ be the natural homomorphism from $\mathbf{G}$ onto $P\Gamma L = P\Gamma L_t(n)$, the collineation group of P, and let $PSL = PSL_t(n)$ denote $\rho(SL)$, the little projective group of P. Finally, note that A contains n^t points,

$$|\Gamma L| = rn^{\frac{1}{2}t(t-1)} \prod_{i=1}^{t} (n^i - 1), \quad \text{and} \quad |PSL| = \frac{1}{d} n^{\frac{1}{2}t(t-1)} \prod_{i=2}^{t} (n^i - 1),$$

where $d = (n-1, t)$ **(2**, Theorem 4.11**)**.

18.1. LEMMA. *If G is a flag-transitive group of A, then $T \subset G$, except possibly if $A = A_3(2)$, $A_3(8)$, or $A_4(2)$.*

Proof. Clearly $\rho(G)$ and $\rho(G_{(0)})$ are flag-transitive on P, so excluding the exceptional cases, $\rho(G) \supseteq \rho(G_{(0)}) \supseteq PSL$ **(9**, Theorem**)**. Let K be the kernel of ρ in G. If $K = 1$, then $(G\colon G_{(0)}) = n^t$ implies that $n^t\cdot|PSL|$ divides $|\Gamma L|$, which is impossible. Therefore, $K \neq 1$, and it follows from **(9**, Proposition 1 and Lemma 1**)** or from **(15**, VI and VII, p. 414**)** that $T \subseteq K$.

18.2. LEMMA. *The group SL is the unique minimal pre-image of PSL in ΓL.*

Proof. As in Lemma (9.3), SL has a unique minimal pre-image in ΓL, say PSL^*. By **(2**, Theorem 4.6**)** the transvections of A generate SL. Let $\lambda\gamma \in PSL^*$ for γ a transvection and $\lambda \in \mathbf{C}(SL)$ **(2**, Theorem 4.8**)**. If u is the order of λ, then $(p, u) = 1$ and hence $\gamma \in PSL^*$. Therefore, $SL = PSL^*$ as required.

The proof of Theorem 6 follows at once. For if the exceptional cases are excluded, then a flag-transitive group G has the form $G = T\cdot G_{(0)}$, $\rho(G_{(0)}) \supset$

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press

PSL by **(9)**, so $G_{(0)} \supset SL$ and $G \supset T \cdot SL = E$. Conversely, it is clear from **(9)** that E is flag-transitive on A.

Another generalization of Theorem 1′ to higher dimensions is suggested by the following lemma.

18.3. Lemma. *Let π' be an arbitrary finite affine plane and let G be a collineation group of π'. Then G is flag-transitive on π' if and only if G is transitive on the set of affine lines of π'.*

Proof. Apply **(15**, IV and I, Section 3**)**.

Let X be the class of subgroups of $\mathbf{G}$ which are transitive on the affine hyperplanes of A. Then as in Lemma (18.3), $G \in X$ if and only if G is transitive on the points of A and $\rho(G_0)$ is transitive on the points of P. The description of X is very difficult for dimensions $t > 2$. First, if $G \in X$, it is not clear that $T \subset G$. And second, the transitive groups of P, even the doubly transitive groups of P, are difficult to determine; see **(15)** for example. However, it is clear that X contains a subclass analogous to $\mathfrak{A}$. Therefore, the large numbers of affine flag-transitive groups for dimension $t = 2$ is not surprising in the light of this second generalization of "flag transitivity" to higher dimensions.

References

1. Johannes André, *Projektive Ebenen über Fastkörpern*, Math. Z., *62* (1955), 137–160.

2. E. Artin, *Geometric algebra* (New York, 1957).

3. Geo. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. Math., Ser. 2, *5* (1904), 173–180.

4. W. H. Bussey, *Galois field tables for $p^n < 169$*, Bull. Am. Math. Soc., *12* (1905), 22–38.

5. Henri Cartan and Samuel Eilenberg, *Homological algebra* (Princeton, 1956).

6. L. E. Dickson, *Linear groups* (New York, 1958).

7. Marshall Hall, Jr., *The theory of groups* (New York, 1959).

8. D. G. Higman and J. E. McLaughlin, *Geometric ABA-groups*, Ill. J. Math., *5* (1961), 382–397.

9. D. H. Higman, *Flag-transitive collineation groups of finite projective spaces*, Ill. J. Math., *6* (1962), 434–446.

10. G. Hochschild and J-P. Serre, *Cohomology of group extensions*, Trans. Am. Math. Soc., *74* (1953), 110–134.

11. Bertram Huppert, *Zweifach transitive, auflösbare Permutationsgruppen*, Math. Z., *68* (1957), 126–150.

12. William J. LeVeque, *Topics in number theory*, vol. I (Reading, Mass., 1956).

13. D. G. Northcott, *An introduction to homological algebra* (Cambridge, 1960).

14. T. G. Ostrom and A. Wagner, *On projective and affine planes with transitive collineation groups*, Math. Z., *71* (1959), 186–199.

15. A. Wagner, *On collineation groups of projective spaces*, I, Math. Z., *76* (1961), 411–426.

15a. ——— *On finite affine line transitive planes*, to appear in Math. Z.

16. Hans Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Seminar Univ. Hamburg, *11* (1935), 17–40.

17. ——— *Über endliche Fastkörper*, Abh. Math. Seminar Univ. Hamburg, *11* (1935), 187–220.

18. ——— *The theory of groups*, 2nd ed. (New York, 1958).

Oxford University

https://doi.org/10.4153/CJM-1964-047-3 Published online by Cambridge University Press