Higman, D.G.
Math. Zeitschr. 86, 145—156 (1964)

Finite permutation groups of rank 3*

By
Donald G. Higman

By the rank of a transitive permutation group we mean the number of orbits of the stabilizer of a point — thus rank 2 means multiple transitivity. Interest is drawn to the simply transitive groups of "small" rank >2 by the fact that every known finite simple group admits a representation as a primitive group of rank at most 5 while not all of these groups have doubly transitive representations. In this paper we consider finite transitive groups of rank 3, a class of groups which seems to have received little direct attention.

Wielandt [*6*, *7*] proved that a primitive group of degree $2p$, p a prime, has rank at most 3. Actually $p=5$ is the only prime for which a non-doubly transitive group of degree $2p$ is known to exist. Any 4-fold transitive group has rank 3 when considered as a group of permutations of the unordered pairs of distinct letters. Thus, in addition to the symmetric and alternating groups, the four 4-fold transitive Mathieu groups are included amongst the rank 3 groups. The (projective) classical groups of linear type are doubly transitive on the points of projective space, but are primitive of rank 3 on the lines when the degree is at least 4. Those of symplectic and unitary types of degree at least 4 are primitive of rank 3 when considered as groups of permutations of the absolute points. The groups of orthogonal type of degree at least 5 are primitive of rank 3 on the singular points, the groups of characteristic 2 being excluded for odd degrees. The representations mentioned here for the classical groups are closely related to their structures as groups of Lie type in that the stabilizer of a point contains a Borel subgroup. The exceptional groups of type E_6 discovered by Dickson[1]) also have primitive rank 3 representations of this kind, while the remaining groups of Lie type have such representations of ranks 2, 4 or 5.

The examples of classical type suggest associating with each rank 3 group a certain block design having the given group as a collineation group. From this point of view, the problem is to determine the designs which admit rank 3 collineation groups. We use the method developed by Wielandt [*6*, *7*] to obtain certain necessary conditions. As a simple application it is shown that a rank 3 group of degree k^2+1, where k is an orbit length for the stabilizer of a point, must have degree 5, 10, 50 or 3250. Such groups of degrees 5, 10 and 50 exists. Degree 3250 remains undecided.

* Research supported in part by the National Science Foundation.

[1]) The fact that the finite groups of type E_6 were already known to Dickson was pointed out to the author by J.E. McLaughlin.

Further consideration of the block designs yields a characterization of the symplectic group $S_4(q)$ from which the known isomorphisms $S_4(q) \approx O_5(q)$, q odd, $S_4(2) \approx S_6$ and $S_4(3) \approx U_4(2)$ are very easily derived. (In this paper we use the notation of ARTIN [*1*] for the classical simple groups.)

Fortunately the book of WIELANDT [7] is now available to be used as a general reference for the theory of permutation groups. For the convenience of the reader, and because of the difference of point of view, we have made §§ 2–5 of our paper more complete than is strictly necessary in view of the availability of [*6*] and [7].

The author is indebted to Professors WIELANDT and J. E. MCLAUGHLIN for valuable remarks and suggestions.

Remarks on Notation. For the most part, our notation is consistent with that of [7]. Given a group G of permutations of a set Ω, we denote by a^g the image of $a \in \Omega$ under $g \in G$, and for a subset X of Ω we let $X^g = \{a^g \mid a \in X\}$. G_a denotes the stabilizer of a, $G_a = \{g \in G \mid a^g = a\}$, and G_X denotes the stabilizer of X, $G_X = \{g \in G \mid X^g = X\}$. (The notation G_X differs from that of [7], but is usual in geometric situations, where X might be, say, a line, and is most convenient here.) If X is an orbit for a subgroup S of G (briefly, an S-orbit), then S^X denotes the corresponding transitive constituent of X, i.e., the group of permutations of X induced by S. $|A|$ denotes the cardinality of the set A.

1. Paired orbits

Let G be a transitive group of permutations of a set Ω. A *pairing* of the G_a-orbits, $a \in \Omega$, is obtained by associating with each such orbit $\Delta(a)$ the orbit

$$\Delta'(a) = \{a^g \mid g \in G,\ a^{g^{-1}} \in \Delta(a)\}.$$

Lemma 1. (cf. WIELANDT [7], 16.6). *G_a has a self-paired orbit $\neq \{a\}$ if and only if $|G|$ is even.*

2. Rank 3 groups

Given a transitive group G of permutations of Ω, the number of G_a-orbits is independent of the particular $a \in \Omega$; we shall call this number the *rank* of G. The trivial orbit $\{a\}$ is to be counted, so that the rank is always at least 2 unless $|\Omega| = 1$, and rank 2 means multiple transitivity.

From now on in this paper we are going to assume that the rank of G is 3, *and that the degree $n = |\Omega|$ of G is finite.* Thus G is a transitive group of permutations of Ω such that for $a \in \Omega$, G_a has exactly 3 orbits

$$\{a\}, \quad \Delta(a), \quad \Gamma(a).$$

We choose the notation in such a way that $\Delta(a)^g = \Delta(a^g)$ and $\Gamma(a)^g = \Gamma(a^g)$ for all $a \in \Omega$ and all $g \in G$, and set $k = |\Delta(a)|$ and $l = |\Gamma(a)|$ so that $n = 1 + k + l$.

Concerning the intersections of orbits we easily obtain

Lemma 2.

$$|\Delta(a) \cap \Delta(b)| = \begin{cases} \lambda \textit{ for } b \in \Delta(a) \\ \mu \textit{ for } b \in \Gamma(a) \end{cases}$$

with λ and μ independent of the particular a and $b \in \Omega$. Moreover,

$$|\Gamma(a) \cap \Gamma(b)| = \begin{cases} \lambda_1 \text{ for } b \in \Gamma(a) \\ \mu_1 \text{ for } b \in \Delta(a) \end{cases}$$

where $\lambda_1 = l - k + \mu - 1$ and $\mu_1 = l - k + \lambda + 1$.

Lemmas 1 and 2 imply at once

Lemma 3. *If $|G|$ is even, then $\Delta(a)$ and $\Gamma(a)$ are both self-paired. If $|G|$ is odd, then $\Delta'(a) = \Gamma(a)$, and hence $k = l$, $n = 2k + 1$ and $\lambda = \mu$.*

If now $a \in \Delta(b)$, $b = a^g$, then $a^{g^{-1}} \in \Delta(b)^{g^{-1}} = \Delta(a)$ and hence $b = a^g \in \Delta'(a)$, i.e., $a \in \Delta(b)$ implies $b \in \Delta'(a)$. Hence by Lemma 3 we have

Corollary. *If $|G|$ is even, then $a \in \Delta(b)$ implies $b \in \Delta(a)$. If $|G|$ is odd, then $a \in \Delta(b)$ implies $b \in \Gamma(a)$.*

The possible systems of imprimitivity for G are easily determined. Namely

Lemma 4. *The following conditions are equivalent:*

(i) *G is imprimitive and $k \leqq l$.*

(ii) *$G_a \neq G_{\Gamma(a)}$.*

(iii) *$\Gamma(a) = \Gamma(b)$ for some $a \neq b$.*

These conditions imply that the systems of imprimitivity for G are the sets $\{a\} \cup \Delta(a)$, and hence that $k + 1 \mid n$ and $k < l$.

Proof. (i) *implies* (ii). If Φ is a system of imprimitivity containing a, then either $\Phi = \{a\} \cup \Delta(a)$ or $\Phi = \{a\} \cup \Gamma(a)$. In the latter case $l + 1 \mid n$, which is impossible since $n = 1 + k + l$ and $k \leqq l$. Hence $\Phi = \{a\} \cup \Delta(a)$ and therefore $G_a \neq G_{\Gamma(a)}$ since $G_a \leqq G_{\Gamma(a)} = G_{\{a\} \cup \Delta(a)}$.

(ii) *implies* (i) *and* (iii). $G_a \neq G_{\Gamma(a)}$ implies that $G_{\Gamma(a)}$ is transitive on $\{a\} \cup \Delta(a)$, and hence the set is a system of imprimitivity since $G_a \leqq G_{\Gamma(a)} = G_{\{a\} \cup \Delta(a)}$. Hence $k + 1 \mid n$ and $k \leqq l$. Moreover, if $a^g \in \Delta(a)$, then

$$(\{a\} \cup \Delta(a))^g = \{a^g\} \cup \Delta(a^g) = \{a\} \cup \Delta(a) \quad \text{whence} \quad \Gamma(a^g) = \Gamma(a).$$

(iii) *implies* (ii). Suppose $\Gamma(a) = \Gamma(b)$, $a \neq b$, and assume that $G_a = G_{\Gamma(a)}$. Then $G_a = G_{\Gamma(a)} = G_{\Gamma(b)} = G_b$. If $\Delta(a) = \{b\}$, then $G_{\Gamma(a)} = G_{\{a\} \cup \Delta(a)} = G_{\{a,b\}} \neq G_a$. Hence $\Gamma(a) = \{b\} = \Gamma(b)$, which is impossible. This completes the proof of the equivalence of (i) through (iii).

In the proof that (i) implies (ii) it was shown that every system of imprimitivity has the form $\{a\} \cup \Delta(a)$. Since G is transitive on the sets of this form, they are all systems of imprimitivity.

Of course there is the analogous result to Lemma 4 with Δ and Γ interchanged.

Corollaries. 1. *If $k \leqq l$, then* (a) *$G_a = G_{\Delta(a)}$ and* (b) *$\Delta(a) = \Delta(b)$ implies $a = b$.*

2. *if G is imprimitive, there is precisely one decomposition of Ω into systems of imprimitivity, and G is doubly transitive on the systems of imprimitivity.*

3. *A rank 3 group of odd order is primitive.*

We conclude this section with the following question about rank 3 groups. That G is a transitive group of rank 3 means that G has three double cosets modulo G_a. Do primitive rank 3 groups of even order exists in which one of these double cosets contains no involutions? (Imprimitive ones are easily constructed.)

3. The block designs

With the transitive rank 3 group G we associate a block design $\boldsymbol{A}$ whose points are the elements of Ω and whose blocks are the symbols $\Delta^*(b)$, one for each $b \in \Omega$. A point a and a block $\Delta^*(b)$ are defined to be incident if $a \in \Delta(b)$. There is a second design $\boldsymbol{B}$ defined in the same way as $\boldsymbol{A}$, but with Γ in place of Δ.

We can represent G as a group of collineation of $\boldsymbol{A}$ by letting each $g \in G$ act on the points and blocks according to

$$g: \begin{cases} a \to a^g \\ \Delta^*(b) \to \Delta^*(b^g). \end{cases}$$

In the same way, G may be regarded as a collineation group of $\boldsymbol{B}$. If $|G|$ is even, a polarity of $\boldsymbol{A}$ is defined by the correspondence $a \leftrightarrow \Delta^*(a)$, and the collineations induced by elements of G commute with this polarity. If $|G|$ is odd, the mappings $a \to \Gamma^*(a)$ and $\Delta^*(a) \to a$ define a correlation of $\boldsymbol{A}$ onto $\boldsymbol{B}$, and the collineations induced by G commute with this correlation.

Both $\boldsymbol{A}$ and $\boldsymbol{B}$ have n points and n blocks. In $\boldsymbol{A}$, the number of points incident with each block is equal to the number of blocks incident with each point, and this number is k. In $\boldsymbol{B}$, the corresponding number is l. It can happen that two distinct blocks are incident with precisely the same points; this happens in $\boldsymbol{A}$ precisely if G is imprimitive and $k > l$ (Lemma 4). In $\boldsymbol{A}$, the number of points common to two blocks $\Delta^*(a)$ und $\Delta^*(b)$ is λ is $a \in \Delta(b)$ and μ if $a \in \Gamma(b)$ (this statement is true even if G is imprimitive and $k > l$ because in that case $\mu = k$). The corresponding intersection numbers for $\boldsymbol{B}$ are $\lambda_1 = l - k + \mu - 1$ and $\mu_1 = l - k + \lambda + 1$.

Lemma 5. $\mu\, l = k(k - \lambda - 1)$.

Proof. Choose a block B in $\boldsymbol{A}$ and count the pairs (A, a) with A a block $\neq B$ and a a point on A and B. $B = \Delta^*(b)$ for some b, and each of the k blocks through b is $\neq B$ and meets B in λ points. Furthermore, each of the l blocks $\neq B$ not through b meets B in μ points. On the other hand, each of the k points on B lies on $k-1$ blocks $\neq B$. Hence $\lambda k + \mu l = k(k-1)$, or $\mu l = k(k - \lambda - 1)$.

Corollary 1. *If* $|G|$ *is odd, then* $\lambda = \mu = \dfrac{k-1}{2}$.

Corollary 2. *The conditions*

(a) *G is primitive and* $k \leqq l$,

(b) $\mu = 0$,

(c) $\lambda = k - 1$,

are equivalent.

Proof. (a) *implies* (b): If G is imprimitive and $k \leqq l$, then by Lemma 4, the set $a^{\perp}=\{a\} \cup \Delta(a)$ is a system of imprimitivity for each a. Hence, for $b \in \Gamma(a)$, $a^{\perp} \cap b^{\perp}=\emptyset$ and therefore $\mu=0$.

(b) *implies* (c) by Lemma 5.

(c) *implies* (d): $\lambda=k-1$ implies $|G|$ even by Corollary 1, and hence $a^{\perp}=b^{\perp}$ for $b \in \Delta(a)$ by the Corollary to Lemma 3. Hence $\Gamma(a)=\Gamma(b)$ and therefore G is imprimitive and $k \leqq l$ by Lemma 4.

Applying this to $\boldsymbol{B}$ instead of $\boldsymbol{A}$ we see that the conditions (a′) G is imprimitive and $l \leqq k$, (b′) $\lambda=k-l-1$ and (c′) $\mu=k$ are equivalent. In particular

Corollary 3. *G is primitive if and only if $\mu \neq 0, k$.*

4. The incidence matrices

Let A be the incidence matrix for $\boldsymbol{A}$ with rows enumerated by the points in some fixed order $a, b, c, \ldots$ and columns by the blocks in the corresponding order $\Delta^*(a), \Delta^*(b), \Delta^*(c), \ldots$. Let B be the corresponding incidence matrix for $\boldsymbol{B}$. Thus A and B are $n \times n$-matrices of 0's and 1's, and from the properties of $\boldsymbol{A}$ and $\boldsymbol{B}$ given in §3 we have

(i) *A has k 1's in each row and column and B has l 1's in each row and each column.*

(ii) *$I+A+B=F$, the $n \times n$-matrix with 1's in every entry.*

(iii) $AA^t=kI+\lambda A+\mu B$.

(iv) *If $|G|$ is even, then A and B are symmetric. If $|G|$ is odd, then $A^t=B$.*

(v) *A and B have trace* 0.

Now (i) through (iv) give

$$(A-kI)\left(A^2-(\lambda-\mu)A-(k-\mu)I\right)=0 \qquad \text{if } |G| \text{ is even}$$

and

$$(A-kI)\left(A^2+A+\frac{k+1}{2}I\right)=0 \qquad \text{if } |G| \text{ is odd}.$$

Hence

Lemma 6. *In addition to the eigenvalue k (of multiplicity 1) the matrix A has exactly the two distinct eigenvalues s and t, where*

$$\left\{\begin{matrix} s \\ t \end{matrix}\right\}=\frac{(\lambda-\mu)\pm\sqrt{d}}{2}, \quad d=(\lambda-\mu)^2+4(k-\mu) \qquad \textit{if } |G| \textit{ is even},$$

and

$$\left\{\begin{matrix} s \\ t \end{matrix}\right\}=\frac{-1+\sqrt{-\mu}}{2} \qquad \textit{if } |G| \textit{ is odd}.$$

5. The permutation representation

Let $D: G \rightarrow GL_n(C)$, C the complex number field, be the matrix representation of G obtained by associating with each $g \in G$ the corresponding permutation matrix $D(g)$ relative to the same ordering of Ω used in constructing the incidence matrices A and B in §4. The fact that $g \in G$ induces a collineation of A such that $\Delta^*(a)^g = \Delta^*(a^g)$ means precisely that $D(g)$ commutes with the incidence matrix A. (In fact, one sees easily that $\{I, A, B\}$ is the basis of the commuting algebra of D described in [7], 28.4, with $A = V(\Delta)$ and $B = V(\Gamma)$.) Because G has rank 3, D has exactly 3 inequivalent irreducible constituents $D_1 = 1$, D_2 and D_3, each with multiplicity 1 (see [7], §29). It follows that one of the eigenvalues s, t of A, say s, has multiplicity equal to the degree f_2 of D_2, while the other, t, has multiplicity equal to the degree f_3 of D_3. Since A has trace 0, we have

$$0 = k + s f_2 = t f_3 .$$

But D has degree $n = 1 + f_2 + f_3$, hence $f_2 + f_3 = k + l$, and therefore

$$f_2 = \frac{k + t(k+l)}{t - s} \quad \text{and} \quad f_3 = \frac{k + s(k+l)}{s - t}.$$

Hence, by Lemma 6

$$\begin{Bmatrix} f_2 \\ f_3 \end{Bmatrix} = \frac{2k + (\lambda - \mu)(k+l) \mp \sqrt{d}\,(k+l)}{\mp 2\sqrt{d}} \qquad \textit{if } |G| \textit{ is even}$$

while

$$f_2 = f_3 = k \qquad \text{if } |G| \textit{ is odd.}$$

Now we have at once

Lemma 7. *If* $|G|$ *is even, then either*

I. $k = l$, $\mu = \lambda + 1 = k/2$ *and* $f_2 = f_3 = k$, *or*

II. $d = (\lambda - \mu)^2 + 4(k - \mu)$ *is a square, and*

(i) *if* n *is even,* $\sqrt{d}$ *divides* $2k + (\lambda - \mu)(k + l)$ *and* $2\sqrt{d}$ *does not, while*

(ii) *if* n *is odd,* $2\sqrt{d}$ *divides* $2k + (\lambda - \mu)(k + l)$.

In case (ii) $f_2 \neq f_3$ *and the eigenvalues of* A *are integers.*

6. Rank 3 groups of degree $k^2 + 1$

If G is a primitive rank 3 group, then $\mu \neq 0$ by Corollary 2 to Lemma 5. Hence, by Lemma 5, the maximum possible l for given k is $l = k(k-1)$ given by $\lambda = 0$ and $\mu = 1$. Thus the degree n of G is at most $k^2 + 1$. On the other hand, if G is a transitive rank 3 group of degree $k^2 + 1$, then G is primitive by Lemma 4 and $\lambda = 0$, $\mu = 1$.

Theorem 1. *If* G *is a transitive group of rank* 3 *and degree* $n = k^2 + 1$, *where* k *is the length of a* G_a*-orbit, then* $n = 5$, 10, 50 *or* 3250.

Proof. $|G|$ is even since one of k, $k^2 + 1$ is even. By Lemma 7 there are two cases:

Case I. $k = l = 2$. In this case $n = 5$.

Case II. $d = 1 + 4(k-1) = 4k - 3$ is a square and $\sqrt{4k-3}$ divides $2k + (-1)(k + k(k-1)) = -k(k-2)$. Since $(4k-3, k)$ divides 3 and

$(4k-3,\ k-2)$ divides 5, it follows that in this case $4k-3 \mid 15^2$. Hence $k=3$, 7, or 57, giving $n=10$, 50 or 3250.

Such groups of degrees 5, 10 and 50 exist, namely

(1) The dihedral group of order 10 has such a representation of degree 5,

(2) the alternating and symmetric groups on 5 letters acting on the unordered pairs of distinct letters provide examples of degree 10, and

(3) $U_3(5)$ has a rank 3 representation of degree 50 of this kind, as does the group obtained from it by adjoining the field automorphism (cf. [*4b*]).

This list is actually complete for these degrees as will be shown in a later paper. Degree 3250 remains undecided.

Theorem 1 has an application in the theory of Möbius planes. Namely, a Möbius plane of type (VI.1) in the classification given by HERING [*3*] has prime power order q and admits a rank 3 collineation group for which the orbit length are 1, q and $q(q+1)$. By Theorem 1, therefore, we must have $q=2$, 3 or 7. The Michaelian planes of order 2 and 3 do, in fact, admit such groups.

7. The block design A'

As suggested by the "natural" representation of the projective symplectic group, we modify the block design A by "adjoining" to each block $\Delta^*(b)$ its "pole" b. Precisely, we consider the block design A' whose points are the elements of Ω, and whose blocks are the symbols $b^\perp$, one for each $b\in\Omega$. A point a and a block $b^\perp$ are defined to be incident if $a\in\{b\}\cup\Delta(b)$. In A', two blocks $a^\perp$ and $b^\perp$ have $\lambda+2$ points in common if $b\in a^\perp$, $b\neq a$, and μ points in common if $b\notin a^\perp$. The group G is faithfully represented as a group of collineations of A' when the action of $g\in G$ on the points and blocks is defined by

$$g\colon \begin{cases} a\to a^g \\ a\to (a^g)^\perp. \end{cases}$$

If $|G|$ is even, the Corollary to Lemma 3 implies that the correspondence $a\leftrightarrow a^\perp$ defines a polarity δ of A'; the collineations induced by G commute with δ.

Now we look at the "lines" of A'. *Here we assume that G is primitive,* $|G|$ *is even and that* $\mu>\lambda+1$. We shall see in §8 that these assumptions hold if A' is a symmetric incomplete block design.

Given two distinct points a, b in A', we set

$$a+b=\bigcap_{a,\,b\,\in x^\perp} x^\perp,$$

and refer to this set $a+b$ as a *totally singular line* or a *hyperbolic line* according as $a\in b^\perp$ or $a\notin b^\perp$. We remark a number of facts concerning lines. First, it is clear from the definition of $a+b$ that

(i) $(a+b)^g=a^g+b^g$ *for all* $g\in G$. *Hence* G_a *is transitive on the totally singular (resp., hyperbolic) lines through a, and G is transitive on the totally singular (resp., hyperbolic) lines.*

Next we note that

(ii) *If* $x \in a+b$, $x \neq a$, *then* $a+x=a+b$.

We prove (ii) for a hyperbolic line $a+b$, the corresponding fact for totally singular lines being almost abvious. If $x \in a+b$, $x \neq a$, then $x \in z^\perp$ for all z such that $a, b \in z^\perp$. Hence $a+x \leqq a+b$ and $x^\perp \geqq a^\perp \cap b^\perp = \Delta(a) \cap \Delta(b)$ so that $x \notin a^\perp$ since $\mu > \lambda+1$. Therefore $a+x$ is a hyperbolic line, so that $a+x=a+b$ by (i).

(iii) G_{a+b} *is doubly transitive on the points of* $a+b$, *unless* $a+b=\{a, b\}$.

To prove this for a hyperbolic line $a+b$, consider $x, y \in a+b$, $x, y \neq a$. Then $x, y \notin a^\perp$ by (ii), i.e., $x, y \in \Gamma(a)$. Hence there exists $g \in G_a$ such that $x^g = y$. Then $(a+b)^g = (a+x)^g = a+y = a+b$, so $g \in G_{a+b} \cap G_a$. The result for totally singular lines is proved in the same way.

(iv) *If* $a+b$ *is a totally singular (resp., hyperbolic) line, then* $a+b-\{a\}$ *is a system of imprimitivity for* G_a^Δ *(resp.,* G_a^Γ*) unless it consists of the single point* b [2]).

Proof. We prove the result for hyperbolic lines. By (i) and (ii) it suffices to show that $a+b \not\geqq \Gamma(a)$. But $a+b \geqq \Gamma(a)$ implies that $\Gamma(a) \leqq \Delta(x)$ for all $x \in \Delta(a) \cap \Delta(b)$. This implies that $l=k-\lambda-1$, and hence that $\mu=k$ by Lemma 5. This contradicts the primitivity of G by Corollary 3 to Lemma 5.

The totality of elements of G fixing $a^\perp$ pointwise is precisely the kernel of the representation of G_a on $\Delta(a)$. We denote this normal subgroup of G_a by $T(a)$, and note that

(v) $T(a)$ *fixes all lines through* a.

Hence by (iv) and the normality of $T(a)$ in G_a we have

(vi) *If* $T(a) \neq 1$, *then the* $T(a)$*-orbits in* $\Gamma(a)$ *are systems of imprimitivity for* G_a^Γ, *and* $a+b-\{a\}$ *is a union of such orbits for every hyperbolic line* $a+b$ [2]).

(vii) $T(a)$ *is semiregular on* $\Gamma(a)$.

Proof. We use (ii). Let $\alpha \in T(a)_x$, $x \in \Gamma(a)$. If $z \in x^\perp$, $z \notin a^\perp$ then $a+z$ and $x^\perp$ are fixed by α and hence so is $z=(a+z) \cap x^\perp$. Hence $\alpha \in T(x)$. If now $y \in \Gamma(a) \cap \Gamma(x)$, $y \notin a+x$, then $a+y$ and $x+y$ are fixed by α and hence so is y. Thus α fixes every point not on $x+a$. If $u \in x+a$, then $u^\perp \cap (x+a) = \{u\}$ so $\alpha \in T(u)$. Hence α fixes u, and therefore $\alpha=1$.

By (vi) and (vii)

(viii) $|T(a)|$ *divides* $h-1$, *where* h *is the number of points on a hyperbolic line.*

(ix) *If* $b \in \Delta(a)$, *then* $\langle T(a), T(b) \rangle = T(a) \otimes T(b)$.

Proof. $T(a)$ and $T(b)$ are normal subgroups of $G_{a,b}$, and $T(a) \cap T(b) = 1$ by (vii) since $\Delta(b) \cap \Gamma(a) \neq \Phi$.

8. The symplectic group

In looking for a characterization of the symplectic groups amongst the rank 3 groups a basic question is: when is A' (or the similarly defined B')

[2]) We write G_a^Δ (resp. G_a^Γ) in place of $G_a^{\Delta(a)}$ (resp. $G_a^{\Gamma(a)}$).

a projective space? As a first step in this direction we remark that from the definitions follows

Lemma 8. *A' is a symmetric balanced incomplete block design if and only if $\mu=\lambda+2$ and $n\neq k+2$.*

When A' is a symmetric balanced incomplete block design (or briefly, when A' is symmetric; see, e.g., [*2*] for the definition) the parameters are $(n, k+1, \mu)$. That is, A' has n points and n blocks, $k+1$ points (blocks) are incident with each block (point), and any two distinct points (blocks) are incident with exactly μ blocks (points). The condition $n\neq k+2$ is equivalent to the requirement that $0<\mu<k+1<n-1$.

It would be interesting to determine rank 3 groups, in addition to the symplectic groups, whose associated designs A' are symmetric; at present we know only the orthogonal groups $0_{2m+1}(q), m\geqq 2$, q odd (see the remarks following the proof of Theorem 2). We mention the following facts.

Lemma 9. *If A' is symmetric, then G is primitive of even order, $k+1-\mu=e^2$, a square, and e but not $2e$ divides $n-(k+1)$ if n is even, while $2e$ divides $n-(k+1)$ if n is odd.*

Proof. If G is imprimitive, then $\mu=0$ or k by Corollary to Lemma 5. Hence, if A' is symmetric, then $\mu=k$ and $\lambda=k-2$, and therefore, by Lemma 5, we have $l=1$, giving $n=k+2$, which is not allowed. Hence G is primitive. $|G|$ is even by Corollary 1 to Lemma 5. The rest of the Lemma follows at once from Lemma 7.

If A' is a projective space $\boldsymbol{P}=\boldsymbol{P}_d(q)$ of dimension d over a Galois field $\boldsymbol{F}_q$, then δ is a null polarity of $\boldsymbol{P}$ and the collineations commuting with δ are the so-called symplectic collineations. Thus, in this case, G is a group of symplectic collineations, and the elements $\neq 1$ of $T(a)$ are symplectic elations. Here results of [*4*] can be applied. For instance, by Theorem 1 of [*4*], $T(a)\neq 1$ then implies that G contains the group $S_{d+1}(q)$, generated by all the symplectic elations, as a normal subgroup. We carry this through in this simplest case.

Lemma 10. *A' is a projective space of dimension 3 if and only if $\mu=\lambda+2$, $n\neq k+2$ and hyperbolic lines contain μ points. In this case, the coordinatizing field is $\boldsymbol{F}_q$, $q=\mu-1$.*

Proof. The necessity of the conditions is clear. To prove the sufficiency, assume that $|a+b|=\mu=\lambda+2$ for $b\notin a^{\perp}$, and that $n\neq k+2$. Then A' is a symmetric block design with parameters $(n, k+1, \mu)$ by Lemma 8. According to a result of Dembowski and Wagner [*2*] we have only to show that every line contains μ points, and we are assuming this for hyperboic lines. Consider a totally singular line $x+y$. We show that $x+y=x^{\perp}\cap y^{\perp}$, whence it follows that $|x+y|=\lambda+2=\mu$. If $x, y\in z^{\perp}$ then $z\in x^{\perp}\cap y^{\perp}$. Suppose there is a $u\in x^{\perp}\cap z^{\perp}$, $u\notin y^{\perp}$. Then the hyperbolic line $y+u$ is contained in $x^{\perp}\cap z^{\perp}$. Moreover, neither x nor z is on $y+u$ by (ii) of § 7. Hence $\lambda+2=|x^{\perp}\cap z^{\perp}|\geqq|y+u|+2=\mu+2$, or $\lambda\geqq\mu$, a contradiction. This proves that $x+y=x^{\perp}\cap y^{\perp}$.

We note that when A' is a projective space of dimension $d\leqq 7$, Theorem 4 of [*4*] implies that G contains the corresponding $S_{d+1}(q)$, with the single exception of $d=3$ and $G\approx A_6$. In the application below, however, our assumptions imply the existence of at least some elations in G, and we do not need to apply this result.

Theorem 2. *Let G be a transitive rank 3 permutation group such that the orbit lengths for the stabilizer G_a of a point a are 1, $q(q+1)$ and q^3, q an integer >2. Assume that G_a is not faithful on its orbit of length $q(q+1)$, and assume that one of the following conditions holds:*

(i) *There are at least q elements of G fixing a G_a-orbit of length $q(q+1)$ pointwise.*

(ii) *$q=p^r$ with p a prime and r a power of 2.*

Then G contains a normal subgroup isomorphic with $S_3(q)$. More precisely, G is isomorphic with a group of symplectic collineations of projective 3-space over $\boldsymbol{F}_q$ containing all the symplectic elations.

Proof. Take $k=q(q+1)$, $l=q^3$. From Lemma 5 it follows that $q+1$ divides μ, $\mu=\mu_1(q+1)$, and $\mu_1 q^2=q(q+1)-\lambda-1$. If μ_1 were $\geqq 2$ we would have $\lambda=q^2(1-\mu_1)+q-1\leqq -q^2+q-1<0$, which is impossible. Hence $\mu_1=1$, $\mu=q+1$ and $\lambda=q-1$. Hence, by Lemmas 8 and 9, A' is symmetric and G is primitive.

Now we want to apply Lemma 10. The condition (i) means that $|T(a)|\geqq q$, and hence by (viii) of § 7, each hyperbolic line, contains at least $q+1$ points. But the number of such points is $\leqq\mu=q+1$. Hence, in this case, each hyperbolic line contains exactly $\mu=q+1$ points. By Lemma 10, therefore, A' is a projective space of dimension 3 over $\boldsymbol{F}_q$. G is a group of symplectic collineations on A', and condition (i) means that G contains all the symplectic elations.

Now assume condition (ii). Since $T(a)\neq 1$, (vi) of § 7 implies that the number of points on a hyperbolic line is of the form p^t+1, $0<t\leqq r$, since in this case $|\Gamma(a)|=q^3$ is a power of p. Moreover, the number of hyperbolic lines through a point is $q^3/p^t=p^{3r-t}$. If x is the total number of hyperbolic lines, we have

$$n\,p^{3r-t}=(p^t+1)\,x$$

and, if y is the total number of hyperbolic lines in each block, then

$$ny=x(q+1).$$

Here we use the fact that in a symmetric design, the number of blocks through two points is equal to the number of points common to two blocks. It follows that p^t+1 divides $q+1$, and hence that $p^t+1=q+1$ since r is a power of 2. Hence A' is a projective space by Lemma 10, and the conclusion of the theorem follows at once by Theorem 1 of [4].

It is to be conjectured that the conditions (i) and (ii) can be dispensed with in Theorem 2, and that analogous characterizations of the higher dimensional symplectic groups can be obtained. The following examples show, however, that the assumption $T(a)\neq 1$ is needed for the conclusion that A' be a projective space.

The orthogonal group $0_{2m+1}(q)$, $m \geqq 2$, q odd, acting on the absolute points of the corresponding orthogonal projective space, has rank 3. The orbit lengths

$$k = q\frac{q^{2m-2}-1}{q-1}, \qquad l = q^{2m-1}$$

and intersection numbers

$$\mu = \frac{q^{2m-2}-1}{q-1}, \qquad \lambda = \mu - 2$$

are exactly the same as those for the symplectic group $S_{2m}(q)$ in its natural rank 3 representation. Hence the corresponding design A' is a symmetric balanced incomplete block design with the same parameters as the block design of points and hyperplanes of $(2m-1)$-dimensional projective space over F_q. But A' is not a projective space, since hyperbolic lines degenerate to pairs of points. This implies that $T(a)=1$, which is the well-known fact that the orthogonal group does not contain elations.

It is well known that $0_{2m+1}(q)$ an $S_{2m}(q)$, q odd, $m \geqq 2$, have the same order, but are isomorphic only for $m=2$. The isomorphism of $0_5(q)$ with $S_4(q)$, q odd, can easily be obtained from our theorem as follows. Let G be the group $0_5(q)$ regarded as a group of permutations of the totally singular lines of the corresponding projective 4-space. Then G has rank 3, with $k = q(q+1)$, $l = q^3$. Given a totally singular line m, the G_m-orbit of length $q(q+1)$ consists of all totally singular lines meeting m. The existence of a group of q orthogonal transformations fixing all of these lines is well known (cf. [5]). Hence, by Theorem 2, G contains a subgroup isomorphic with $S_4(q)$, and since $|0_5(q)| = |S_4(q)|$ we have the desired isomorphism.

We conclude with two further illustrations of Theorem 2. First, let G be the symmetric group on $m \geqq 4$ letters, considered as a group of permutations of the $n = m(m-1)/2$ unordered pairs of distinct letters. Then we see that G and H are transitive groups of rank 3 with $k = (m-2)(m-3)/2$, $l = 2(m-2)$, $\lambda = (m-4)(m-5)/2$ and $\mu = (m-3)(m-4)/2$. (The same thing works for any 4-fold transitive group.) G and H are imprimitive for $m=4$ and primitive for $m \geqq 5$. For $m=5$ we have groups of degree 10 as in Theorem 1. For $m=6$ we have $k = 6 = 2(2+1)$ and $l = 8 = 2^3$. Since there is an involution in G fixing an orbit of length 6 pointwise, it follows from Theorem 2 that A' is a projective 3-space over F_2 and that G contains $S_4(2)$. Comparing orders we obtain a proof of the well-known fact that $S_4(2)$ is isomorphic with the symmetric group of degree 6. We also see the alternating group of degree 6 acts as a rank 3 subgroup. Of course it is not difficult to prove directly that A' is a projective space in this case, and this gives a simple direct proof of these facts.

Finally, let G be the projective special unitary group $U_4(2)$ considered as a (transitive) group of permutations of the 40 ordinary (i.e., non-absolute) points of the unitary projective space $P_3(4)$. If Q is an ordinary point, then it is easy to see that G_Q is transitive on the 12 ordinary points on $Q^\perp$ and on the 27 ordinary points $\neq Q$ off $Q^\perp$. Thus G has rank 3 (in fact, $U_m(2)$, $m \geqq 4$, always has rank 3 on the ordinary points as well as on the absolute points) with the orbit lengths 1, $12=3(3+1)$ and $27=3$ for the stabilizer of a point. Moreover, for each ordinary point Q, G contains a $(Q, Q^{\perp})$-homology which is in particular an element $\neq 1$ fixing an orbit of length 12 pointwise. Hence by Theorem 2, G contains a subgroup isomorphic with $S_4(3)$. Comparing orders we obtain the well-known isomorphism $U_4(2)\approx S_4(3)$.

References

[*1*] ARTIN, E.: The orders of the classical simple groups. Comm. Pure and Appl. Math. **8**, 455–472 (1955).

[*2*] DEMBOWSKY, P., and A. WAGNER: Some characterizations of finite projective spaces. Archiv der Math. **11**, 465–469 (1960).

[*3*] HERING, CH.: Eine Klassifikation der Möbius-Ebenen. Math. Z. (In preparation).

[*4a*] HIGMAN, D. G., and J. E. MCLAUGHLIN: Rank 3 subgroups of finite classical groups. (To appear in J. reine u. angew. Math.)

[*4b*] —— Some properties of finite unitary groups. (In preparation.)

[*5*] TAMAGAWA, T.: On the structure of orthogonal groups. Amer. J. Math. **80**, 191–197 (1958).

[*6*] WIELANDT, H.: Primitive Permutationsgruppen vom Grad $2p$. Math. Z. **63**, 478–485 (1955).

[*7*] — Finite permutation groups. New York: Academic Press 1964.

Dept. of Math., University of Michigan, Ann Arbor, Mich., U.S.A.

(Received June 12, 1964)