HIGMAN, D. G.
Math. Zeitschr. 91, 70–86 (1966)

Primitive rank 3 groups with a prime subdegree

By
DONALD G. HIGMAN*

As a continuation of the study of rank 3 permutation groups G begun in [4] we consider in this paper primitive rank 3 groups of even order in which the stabilizer G_a of a point a has an orbit of prime length. We show in particular that if G has no regular normal subgroup then the minimal normal subgroup M of G is a simple group of rank 3 and the constituent of M_a on the orbit of prime length is nonsolvable and hence doubly transitive.

In the first section we present a theorem of WIELANDT on primitive permutation groups (hitherto unpublished) which is important for our discussion and certainly of independent interest. After listing some preliminary facts about rank 3 groups in § 2, we summarize our main results in § 3. The remaining sections contain the proofs of these results, essential use being made in § 4 of a theorem of BRAUER and REYNOLDS [2].

The author is indebted to Professor WIELANDT for communicating the theorem of § 1 and its proof, and for much other valuable help. In particular, the short proof of (3.3) and the method of § 6 are due to Professor WIELANDT. The author is also indebted to Professor J. E. MCLAUGHLIN for many valuable discussions.

We take this opportunity to list some corrections to [4]:

p. 147 omit the second sentence of Lemma 2. Add to the Cor. to Lemma 3: *Hence*

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

where $\lambda_1=l-k+\mu-1$ *and* $\mu_1=l-k+\lambda+1$ *if* $|G|$ *is even and* $\lambda_1=\mu_1=\lambda=\mu$ *if* $|G|$ *is odd.*

p. 148 Cor. 2, read "*imprimitive*" for "*primitive*".

p. 149 line 5, read "(a)" for "(d)".

Lemma 6, $\begin{Bmatrix}s\\t\end{Bmatrix}=(-1+\sqrt{-n})/2$ *if* $|G|$ *is odd.*

p. 150 line 9, $0=k+sf_2+tf_3$.

Lemma 7, replace the last sentence by: "*If* $f_2=f_3$ *then case* I. *holds. In case* II. *the eigenvalues of* A *are integers.*"

lines 4 and 5 of § 6, read "... *then* G *is primitive and* $\lambda=0$, $\mu=1$ *by Lemma 5 and Corollary 3.*"

* Research supported in part by the National Science Foundation.

p. 153 line 15, Miquelian.
line 10 of § 7, $a^{\perp} \to (a^g)^{\perp}$.
p. 154 Theorem 2, first sentence, read "... *q an integer* $\geqq 2$." and in the next to last sentence, read "... *with* $S_4(q)$."

1. A theorem of Wielandt

If X is a subset of a set Ω and H is a group of permutations of Ω stabilizing X, we write H^X for the restriction of H to X.

(1.1) **Theorem.** *Given a nonregular primitive permutation group G on a set Ω, let $\Delta(a)$ be a G_a-orbit $\neq \{a\}$, let $b \in \Delta(a)$ and let $b' \in \Delta'(a)$, where $\Delta'(a)$ is the G_a-orbit paired with $\Delta(a)$ (for the definition of paired orbits see* [7], § 16). *Then every composition factor of the pointwise stabilizer $T(a)$ of $\{a\} + \Delta(a)$ is a composition factor of $G_{a,b}^{\Delta(a)}$ or of $G_{a,b'}^{\Delta'(a)}$.*

Proof. For a subgroup H of G, denote by H^* the smallest subnormal subgroup of H such that every composition factor between H and H^* is a composition factor of $G_{a,b}^{\Delta(a)}$ or of $G_{a,b'}^{\Delta'(a)}$; H^* is a characteristic subgroup of H (WIELANDT [6], Th. 13, p. 220). Now $G_{a,b}^{\Delta(a)} \approx G_{a,b}/T(a)$ and therefore $G_{a,b}^* = T(a)^*$. Similarly $G_{a,b'}^* = U(a)^*$, where $U(a)$ denotes the pointwise stabilizer of $\{a\} + \Delta'(a)$. We can choose the notation so that $\Delta(a)^g = \Delta(a^g)$ for all $a \in \Omega$, $g \in G$. Then $\Delta'(a)^g = \Delta'(a^g)$ and $b \in \Delta(a)$ implies $a \in \Delta'(b)$ so $G_{a,b}^* = U(b)^*$. Hence $T(a)^* = U(b)^* \lhd \langle G_a, G_b \rangle = G$ so that $T(a)^* = 1$ and the theorem is proved.

2. Notations and preliminary results

If G is a transitive permutation group on a finite set Ω, we call the number of orbits of the stabilizer G_a of a point a the *rank* of G, and, following a suggestion of WIELANDT, we call the lengths of these orbits the *subdegrees* of G. Of course, the rank and the subdegrees do not depend on the particular point chosen. From now on in this paper we are interested in rank 3 groups of even order.

The following notations will be fixed throughout: G is a transitive rank 3 permutation group of even order on a finite set Ω. For $a \in \Omega$, the G_a-orbits are $\{a\}$, $\Delta(a)$ and $\Gamma(a)$, with $\Delta(a)^g = \Delta(a^g)$ and $\Gamma(a)^g = \Gamma(a^g)$ for all $a \in \Omega$, $g \in G$. The subdegrees are 1, $k = |\Delta(a)|$ and $l = |\Gamma(a)|$, so that the degree $n = |\Omega|$ of G is given by

$$n = 1 + k + l. \tag{2.1}$$

The intersection numbers λ, μ for G are defined by

$$|\Delta(a) \cap \Delta(b)| = \begin{cases} \lambda & \text{if} \quad b \in \Delta(a) \\ \mu & \text{if} \quad b \in \Gamma(a). \end{cases}$$

According to Lemma 5 of [4], the set (k, l, λ, μ) of parameters for G satisfies

$$\mu l = k(k - \lambda - 1). \tag{2.2}$$

The degrees of the irreducible constituents of the permutation representation of G can be computed from (k, l, λ, μ), giving further restrictions on the possible sets of parameters (cf. [4], Lemma 7).

As in § 1 we write H^X for the restriction of H to X where H is a group of permutations of Ω stabilizing a subset X of Ω. We write G_a^Δ for the transitive constituent $G_a^{\Delta(a)}$.

We now list some general facts about rank 3 groups to be used in the later sections. Since we are assuming that $|G|$ is even,

(2.3) *$a\in\Delta(b)$ implies $b\in\Delta(a)$* (cf. [4], Cor. to Lemma 3).

A useful criterion for primitivity is

(2.4) *G is primitive if and only if $\mu\neq 0, k$* (cf. [4], Cor. 3 to Lemma 5).

As in § 1 we denote by $T(a)$ the pointwise stabilizer of $a^\perp=\{a\}+\Delta(a)$. An immediate consequence of ([4], (vii), (viii)) is

(2.5) *If G is primitive and $\mu>\lambda+1$ then $T(a)$ is semiregular on $\Gamma(a)$ and $|T(a)|<k$.*

It will be seen that the discussion in § 4 could be very much shortened if the assumption $\mu>\lambda+1$ could be dispensed with in (2.5).

(2.6) *If G is primitive and G_a^Δ is doubly transitive then $\lambda=0$.*

Proof. If G_a^Δ is doubly transitive and $b\in\Delta(a)$, then $G_{a,b}$ is transitive on $\Delta(a)-\{b\}$. Hence $\Delta(a)-\{b\}\subseteq\Delta(b)$ or $\Gamma(b)$. But $\Delta(a)-\{b\}\subseteq\Delta(b)$ implies $\lambda=k-1$, and hence that G is imprimitive by (2.2) and (2.4). Hence $\Delta(a)-\{b\}\subseteq\Gamma(b)$ and $\lambda=0$.

(2.7) *If G is primitive and G_a^Δ is doubly primitive then either $T(a)=1$ or $\mu=1$.*

Proof. By (2.6), $\lambda=0$. Assume that $\mu>1$. The assumption that G_a^Δ be doubly primitive means that $G_{a,b}$ is primitive on $\Delta(a)-\{b\}$, $b\in\Delta(a)$. Hence, since $T(b)$ is a normal subgroup of $G_{a,b}$, either $T(b)^{\Delta(a)}=1$ or $T(b)$ is transitive on $\Delta(a)-\{b\}$. In the latter case, choose $c\in\Delta(a)-\{b\}$. Then $|\Delta(b)\cap\Delta(c)|=\mu>1$, and therefore $(\Delta(b)-\{a\})\cap\Delta(c)\neq\emptyset$. Hence $\Delta(b)-\{a\}\subseteq\Delta(c)$ since $T(a)\leqq G_c$, and it follows that $\mu=k$ since $a\in\Delta(c)$, contradicting the primitivity of G by (2.4). Hence $T(b)^{\Delta(a)}=1$, so that $T(a)=T(b)$, and therefore $T(a)\lhd\langle G_a, G_b\rangle=G$ so that $T(a)=1$.

(2.8) *If G is primitive then $\sum_{x\in a^\perp}\Delta(x)=\Omega$ and $\bigcap_{x\in\Delta(a)}T(x)=1$.*

Proof. Let
$$\Lambda=\sum_{x\in a^\perp}\Delta(x),$$
then $\Lambda\supseteq x^\perp$ for all $x\in a^\perp$ and $G_a\subseteq G_\Lambda$. Assuming that $\Lambda\neq\Omega$ we have $G_a=G_\Lambda$ since G is primitive, and $\Lambda=a^\perp$ since G has rank 3. Hence $\Lambda=x^\perp$ and therefore $G_a=G_{x^\perp}=G_x$ for all $x\in a^\perp$, contrary to the primitivity of G. Therefore $\Lambda=\Omega$ and this implies that
$$\bigcap_{x\in\Delta(a)}T(x)=1.$$

(2.9) *A primitive rank* 3 *group G has a unique minimal normal subgroup M. If M is regular it is elementary abelian, and if M is primitive it is simple.*

Proof. If M and N are minimal normal subgroups of G, $M \neq N$, then M and N are transitive and $\langle M, N\rangle = M \times N$. It follows that M is regular and a direct product of nonabelian simple groups ([3], Ch. X, Th. XII, p. 200). Hence G belongs to the holomorph of M, and since this holomorph has rank >3 so does G, a contradiction. This proves the first statement. The rest is proved in a similar way. (The holomorph of A_5 has rank 4 so (2.9) is false for rank 4 groups. Of course the argument shows that a primitive group with a nonregular minimal normal subgroup has a unique minimal normal subgroup.)

3. Primitive rank 3 groups with a prime subdegree

The main results of the present paper can be summarized as follows:

Theorem. *Let G be a primitive group of rank* 3 *and degree n, with $|G|$ even. If the subdegree k of G is a prime p, then either*

(i) *G has an (elementary abelian) regular normal subgroup,*

(ii) $\mu=1$, $\lambda=0$ *and* (a) $p=3$ *and G is isomorphic with A_5 or S_5, or* (b) $p=7$ *and G is isomorphic with $U_3(5)$ or an extension of $U_3(5)$ by a cyclic group of order* 2, *or*

(iii) $\mu>1$, $\lambda=0$ *and the minimal normal subgroup M of G is a simple rank* 3 *group such that the constituent of M_a of degree p is doubly transitive and non-solvable.*

In case (iii), $p=\alpha y-\mu+3$ *with α and y positive integers such that*

(1) *μ divides $\alpha y+2$ and α is even or odd according as $(\alpha y+2)/\mu$ is even or odd, and*

(2) $y^2-4\alpha y-(\mu-2)(\mu-6)=0$.

At present we do not have any example of case (iii).

The discussion for the cases $\mu>1$ (§§ 4, 5) and $\mu=1$ (§ 6) are quite different. Before turning to the case $\mu>1$ let us note the following facts.

Assume that G is primitive of even order and that the subdegree k of G is a prime p, $k=p$. Since $\mu<p$ by (2.3) we have by (2.2) that

(3.1) $\mu l=p(p-\lambda-1)$, *μ divides $p-\lambda-1$ and $n=1+sp$ with $s=1+(p-\lambda-1)/\mu$.*

(3.2) *G_a^Γ is faithful.*

Proof. Let $S(a)$ denote the kernel of G_a acting on $\Gamma(a)$. Then $S(a)\neq 1$ implies that $S(a)^{\Delta(a)}\neq 1$ and hence that $S(a)$ is transitive on $\Delta(a)$ since $S(a) \lhd G_a$. Since $p \leqq n/2$ by (3.1), this implies by ([7], 13.4) that G is triply transitive, a contradiction.

The case $\mu>1$ depends on an application of a theorem of Brauer and Reynolds [2], made possible in the first instance by

(3.3) $p \parallel |G|$.

Proof. Since G_a^Δ is a transitive group of degree p, $p \| |G_a|$ and therefore $p \nmid |G_{a,b}^{\Delta(a)}|$ for $b \in \Delta(a)$. Hence $p \nmid |T(a)|$ by (1.1), and, since $G:G_a = n \equiv 1 \pmod p$ by (3.1), $p \| |G|$.

For a subgroup H of G we write $N(H)$ for the normalizer of H in G.

(3.4) *If P is a subgroup of G_a of order p, then $N(P) \leqq G_a$ and $N(PT) = N(P)T$, $T = T(a)$.*

Proof. P fixes exactly a, for suppose that $P \leqq G_{a,b}$, $b \neq a$. Then $b \in \Gamma(a)$ by (3.3) so that $\mu = |\Delta(a) \cap \Delta(b)|$, and hence $\mu = 0$ or p, contrary to (2.4). Hence $N(P) \leqq G_a$. The rest follows by SYLOW's Theorem.

4. The case $\mu > 1$

Throughout this section we assume that G is a primitive rank 3 permutation group of even order, with $k = p$ and $\mu > 1$. The end result of the section is

(4.1) **Theorem.** *If G has no regular normal subgroup then the minimal normal subgroup M of G is a simple group. Moreover M is a rank 3 subgroup of G, and for each point a, M_a^Δ is doubly transitive and non-solvable.*

For H a subgroup of G, denote by $C(H)$ the centralizer of H in G. Choose a subgroup $P = \langle \pi \rangle$ of G_a of order p. The proof of our Theorem depends on

$$C(P) = P \times T(a). \qquad (4.2)$$

Proof. (a) If G_a^Δ is doubly transitive, then $\lambda = 0$ by (2.6), so $\lambda + 1 = 1 < \mu$ and hence $|T(a)| < p$ by (2.5). But $PT(a):N_{PT(a)}(P) \equiv 1 \bmod p$ and $PT(a):T(a) = p$. Hence $PT(a) = N_{PT(a)}(P)$, so $T(a) \leqq N(P)$ and hence $T(a) \leqq C(P)$. Since $PT(a)/T(a)$ is self centralizing in $G_a/T(a)$, we have $C(P) = P \times T(a)$.

(b) Now assume that G_a^Δ is not doubly transitive. Then by BURNSIDE's Theorem ([3]; Ch XVI, Th VII, p. 341) G_a^Δ is solvable. Unfortunately we do not known at this stage that $\mu > \lambda + 1$ so that (2.5) is not available and we have to make a rather long detour.

Since $G_a^\Delta \approx G_a/T(a)$ is a solvable group of prime degree we have that $G_a = N(P)\,T(a)$, and for $b \in \Delta(a)$, $G_{a,b}^{\Delta(a)} \approx G_{a,b}/T(a)$ is a cyclic group of order

$$q = \frac{p-1}{t}.$$

Now $T(a)$ and $T(b)$ are normal in $G_{a,b}$ and $T(a)/T(a) \cap T(b) \approx T(a)\,T(b)/T(a) \leqq G_{a,b}/T(a)$. Hence it follows by (2.8) that $T(a)$ is abelian and the order of every element of $T(a)$ divides q.

Put $W = C(P) \cap G_{a,b}$, then $W \leqq T(a)$. For, if $x \in W$ and $P = \langle \pi \rangle$, then π commutes with x and therefore permutes the fixed points of x. But x fixes $b \in \Delta(a)$ and $\langle \pi \rangle$ is transitive on $\Delta(a)$. Hence x fixes $\Delta(a)$ pointwise. Now we have $N(P) \cap T(a) = C(P) \cap T(a) = W$ since $N(P) \cap T(a) \leqq C(P)$. Therefore W is a normal subgroup of $N(P)$, and hence W is normal in G_a since $T(a)$ is abelian. It follows that W depends only on a, and not on $b \in \Delta(a)$ or $P \leqq G_a$.

We write $W=W(a)$. Furthermore, since $PT(a)/T(a)$ is self-centralizing in $G_a/T(a)$, $C(P)\leqq T(a)$ and therefore $C(P)=P\times W(a)$. We also note that for $b\in\Delta(a)$, $W(a)\cap T(b)=1$, and hence $W(a)$ and $T(b)$ commute elementwise. In fact, if $x\in W(a)\cap T(b)$, then x centralizes $P=\langle\pi\rangle$, so that $x=x^{\pi^i}\in T(b)^{\pi^i}=T(b^{\pi^i})$. Hence $x\in T(c)$ for all $c\in\Delta(a)$, and therefore $x=1$ by (2.8).

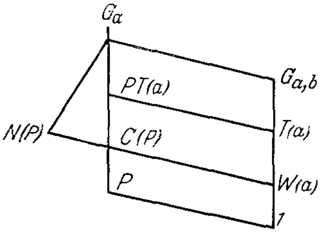

Fig. 1

We have $G_a=N(P)\,T(a)$ so $G_{a,b}=T(a)\,[N(P)\cap G_{a,b}]$. Using once more that $G_a/T(a)$ is isomorphic with the solvable transitive group G_a^Δ of degree p, we have $G_a=PT(a)\,G_{a,b}=PG_{a,b}$, and hence $N(P)=P[N(P)\cap G_{a,b}]$. Now

$$G_{a,b}/T(a)=T(a)\,[N(P)\cap G_{a,b}]/T(a)\approx[N(P)\cap G_{a,b}]/[N(P)\cap T(a)]$$
$$=[N(P)\cap G_{a,b}]/W.$$

If we take a generator $W\sigma$ of this cyclic group of order q then

$$N(P)\cap G_{a,b}=\langle W,\sigma\rangle,\qquad N(P)=\langle PW,\sigma\rangle\quad\text{and}\quad G_{a,b}=\langle T(a),\sigma\rangle.$$

Our aim is to show that $W(a)=T(a)$. This is accomplished in two further steps as follows:

(i) *If* $W(a)\neq T(a)$ *then* $W(a)=1$.

Assume that $W(a)\neq T(a)$ and use bars to denote residue classes modulo $W(a)$ in G_a. Then $\overline{N(P)}=N(\bar P)$, (normalizer in $\bar G_a$), and $\bar\sigma$ is an element of order q such that $N(\bar P)\cap\bar G_{a,b}=\langle\bar\sigma\rangle$, $N(\bar P)=\langle\bar P,\bar\sigma\rangle$ and $\bar G_{a,b}=\langle\overline{T(a)},\bar\sigma\rangle$. Moreover, $\bar P=\langle\bar\pi\rangle$ and $\bar\pi^{\bar\sigma}=\bar\pi^{\gamma^t}$ with γ a primitive root modulo p.

The element $\bar\pi$ induces a fixed point free automorphism of order p on $\overline{T(a)}\neq 1$. We have a homomorphism $\varphi\colon N(\bar P)\to\operatorname{Aut}(\overline{T(a)})$, the automorphism group of $\overline{T(a)}$, and

$$\varphi(\bar\pi)^{\varphi(\bar\sigma)}=\varphi(\bar\pi^{\bar\sigma})=\varphi(\bar\pi^{\gamma^t})=\varphi(\bar\pi)^{\gamma^t}.$$

Hence $\bar\sigma$ induces an automorphism of $\overline{T(a)}$ of order q, and φ is one-to-one.

Put $C=$ the centralizer in $\bar G_{a,b}$ of $\overline{T(a)}$. If $\bar z\in C$, then $\bar z=\bar t\,\bar\sigma^i$ with $\bar t\in\overline{T(a)}$, and $(\bar z,\overline{T(a)})=1$ implies $(\bar\sigma^i,\overline{T(a)})=1$ which in turn implies that $\bar\sigma^i=1$ and hence that $\bar z\in\overline{T(a)}$. This proves that $C=\overline{T(a)}$. But $\overline{W(b)}\leqq C$ and $W(b)\cap T(a)=1$ as we have seen above. Hence $\overline{W(b)}=1$. But $\overline{W(b)}\approx W(b)\,W(a)/W(a)\approx W(b)/W(a)\cap W(b)=W(b)$. Hence $W(b)=1$. This proves (i).

(ii) $W(a)=1$ *implies* $T(a)=1$.

Assume that $W(a)=1$ and let $b\in\Delta(a)$. In this case we have that σ is an element of order q such that $N(P)\cap G_{a,b}=\langle\sigma\rangle$, $N(P)=\langle P,\sigma\rangle$, $G_{a,b}=\langle T(a),\sigma\rangle$ and $\pi^\sigma=\pi^{\gamma^t}$. Moreover, π induces a fixed point free automorphism of order p on $T(a)$. Note that if U is any subgroup $\neq 1$ of $T(a)$ invariant under $N(P)$ then π induces a fixed point free automorphism of order p on U and σ induces an automorphism of order q on U.

If $T(a)\cap T(b)=1$ then $|T(a)|\mid q<p$, and the argument for case (a) shows that $T(a)$ centralizes P, whence $T(a)=1$. Assume that $T(a)\cap T(b)\neq 1$. If $T(a)=T(b)$ then $T(a)=1$ by (2.8). Assume $T(a)\neq T(b)$, and take an $x\in T(b)$, $x\notin T(a)$. Then $x\in G_{a,b}=\langle T(a),\sigma\rangle$ so that $x=t\,\tau$ with $t\in T(a)$, $\tau\in\langle\sigma\rangle$, $\tau\neq 1$. Since x centralizes $T(a)\cap T(b)$, so does τ.

Let r be a prime divisor of $|T(a)|$ such that τ centralizes elements of order r in $T(a)$. The totality V of elements of order r in $T(a)$ can be regarded as an $N(P)$-module over $\boldsymbol{F}_r$, the field of r elements. Let V_1 be an irreducible P-submodule of V containing fixed elements $\neq 0$ of τ. Then V_1 is invariant under τ since V_1^τ is again an irreducible P-module and $V_1\cap V_1^\tau$ contains the fixed elements of τ in V_1. If V_1 were fixed elementwise by τ then the same would be true of the $N(P)$-submodule W of V generated by V_1, contrary to the fact that $\sigma|W$ has order q. Hence the fixed point set U of V_1 is a proper subspace of V_1. Since $T(a)/T(a)\cap T(b)$ is cyclic, and since

$$T(a)\geqq V_1>U\geqq V_1\cap T(a)\cap T(b),$$

it follows that V_1/U has dimension 1.

Adjoin π to $F=\boldsymbol{F}_r$ in the ring of linear transformations of V_1 to obtain a commutative ring $A=F[\pi]$. Then V_1 is a faithful irreducible A-module, so A is a field and V_1 has dimension 1 over A. We may identify V_1 with A so that τ becomes a field automorphism with fixed field $U\supseteq F$. But then we have $1=\dim_F A/U=\dim_F A-\dim_F U=(o(\tau)-1)\dim_F U$, where $o(\tau)$ is the order of τ. Hence $\dim_F U=1$ so $U=F$, and $o(\tau)=2$ so $\dim_F A=2$. Therefore $|A|=r^2$ and, since π is fixed point free, $p\mid r^2-1$, and in particular $p\leqq r+1$. But $r\mid q$ and $q=(p-1)/t$, where $t>1$ since G_a^Δ is not doubly transitive. Hence $r<p-1$, so $p<r+1$, a contradiction. This proves (ii), completing the proof of (4.2).

(4.3) *If* $N\neq 1$ *is a normal subgroup of* G *such that* $p\nmid|N|$ *then* N *is regular.*

Proof. If $p\nmid|N|$ then $N_a^\Delta=1$, i.e., $N_a\leqq T(a)$ for all a. Hence

$$N_a\leqq T(a)\cap N\leqq N_b\leqq T(b)$$

for all $b\in\Delta(a)$, and therefore $N_a=1$ by (2.8).

From now on in this section we assume that G has no regular normal subgroup, and we let M be the minimal normal subgroup of G. Since M is a direct product of isomorphic simple groups, and since $p\,\|\,|M|$ by (3.3) and (4.3), it follows that M is simple.

Using (3.3) and (4.2) we have that the p-invariants of G (in the sense of BRAUER and REYNOLDS [2]) are (q, w, r) with

$$q=\frac{p-1}{t} \quad \text{and} \quad r=s+u+s\,u\,p,$$

s as in (3.1), i.e.,

$$s=1+\frac{p-\lambda-1}{\mu}, \quad \text{and} \quad 1+u\,p=G_a\colon N(P).$$

If we set $T_0=M\cap T(a)$ and $w_0=|T_0|$, then the p-invariants of M are

$$(q_0, w_0, r) \quad \text{with} \quad q_0=\frac{p-1}{t_0}, \quad t\,|\,t_0.$$

We want now to prove that M_a^{Δ} is non-solvable. Suppose that M_a^{Δ} is solvable. Then $u=0$, for $PT_0/T_0 \lhd M_a/T_0$ so that $PT_0 \lhd M_a$ and therefore $P\lhd M_a$. Hence $r=s$.

If G_a^{Δ} is solvable, then $G_{a,b,c}=T(a)$ for $b, c\in\Delta(a)$, $b\neq c$, and

$$G_{a,b}\colon T(a)=\frac{p-1}{t}.$$

Let $e\in\Gamma(a)\cap\Gamma(b)$, then

$$G_{a,b,e}=T(b), \quad G_{a,b}\colon G_{a,b,e}=\frac{p-1}{t} \quad \text{and} \quad G_a\colon G_{a,e}=p(s-1).$$

Hence

$$s-1\,\Big|\,\frac{p-1}{t}.$$

If G_a^{Δ} is doubly transitive, then

$$\lambda=0 \quad \text{and} \quad s=1+\frac{p-1}{\mu}.$$

In any case, r has the form

$$r=1+\frac{p-1}{x}.$$

By a theorem of BRAUER and REYNOLDS ([2], Theorem 2) applied to the simple group M, exactly one of the following cases holds:

(i) $r=1$,

(ii) $r=\frac{p-3}{2}$, p a Fermat prime,

(iii) r can be written in the form

$$r=\frac{h\,u\,p+u^2+u+h}{u+1}$$

with positive integers h, u.

Case (i). This is clearly impossible.

Case (ii). Here

$$1+\frac{p-1}{x}=\frac{p-3}{2},$$

giving $2(p-1+x)=x(p-3)$, i.e., $x(p-5)=2(p-1)$. Hence $p-5 \mid 8, p \leqq 13$ and therefore $p=5$ and $r=1$, a contradiction.

Case (iii). If

$$1+\frac{p-1}{x}=\frac{h u p+u^2+u+h}{u+1}, \quad \text{then} \quad h=\frac{(u+1)[p-1-x(u-1)]}{x(u p+1)}.$$

If $x \geqq 2$,

$$h \leqq \frac{(u+1)[p-2u+1]}{2(u p+1)} \leqq \frac{2u(p-1)}{2(u p+1)}<1,$$

hence $x=1$. But then $r=p$ and so

$$p=1+\frac{p-\lambda+1}{\mu}$$

giving $\lambda=0$, $\mu=1$, contrary to the assumption that $\mu>1$.

We have now proved that M_a^Δ is non-solvable, and hence it is doubly transitive by BURNSIDE's Theorem ([3], p. 341).

To complete the proof of Theorem (4.1) we must show that M has rank 3. But we know that M_a^Δ is doubly transitive. Therefore M_a permutes the sets $\Delta(x) \cap \Gamma(a)$, $x \in \Delta(a)$, transitively (even doubly transitively), and for $b \in \Delta(a)$, $M_{a,b}$ is transitive on the points of $\Delta(b)-\{a\}=\Delta(b) \cap \Gamma(a)$. Hence M_a^Γ is transitive by (2.8), which implies that M has rank 3.

5. Parameters of G in case $\mu>1$

Here we assume that G is a primitive rank 3 group with a prime subdegree $k=p$. We assume in addition that $\mu>1$ as in § 4, and that G contains no regular normal subgroup. By (4.1) we know that the minimal normal subgroup M of G is a simple group with the same properties. The following discussion applies equally well to M in place of G. By (4.1), G_a^Δ is doubly transitive and non-solvable, so $\lambda=0$. Hence, for $b \in \Delta(a)$ we have the following index diagram:

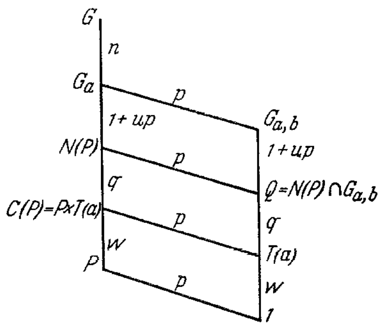

Fig. 2

where

(5.1) $$n=1+s p, \quad s=1+\frac{p-1}{\mu}, \qquad u \geqq 1 \quad \textit{and} \quad q=\frac{p-1}{t}.$$

Thus, in the notation of BRAUER and REYNOLDS [2],

(5.2) *The p-invariants of G are* (q, w, r), *with* $r=s+u+sup$. *The p-invariants for M are* (q_0, w_0, r_0) *with*

$$q_0=\frac{p-1}{t_0}, \quad t\,|\,t_0, \quad w_0=|M\cap T(a)|.$$

If $b, c\in\Delta(a)$, $b\neq c$, then

$$G_{a,b,c}: T(a)=\frac{G_{a,b}: T(a)}{G_{a,b}: G_{a,b,c}}=\frac{q(1+u\,p)}{p-1}=\frac{1+u\,p}{t},$$

hence

(5.3) $$t\,|\,1+u\,p.$$

By (2.5), $T(a)$ is semiregular on $\Gamma(a)$, and therefore $w\,|\,l$. But $p\nmid w$, so

$$w\,|\,l/p=\frac{p-1}{\mu}.$$

For $b, c\in\Delta(a)$, $b\neq c$, $T(a)$ fixes $\Delta(b)\cap\Delta(c)-\{a\}$, a subset of $\Gamma(a)$ of $\mu-1$ points. Hence $w\,|\,\mu-1$, and we have

(5.4) $$w\left|\left(\frac{p-1}{\mu}, \mu-1\right)\right..$$

By (1.1),

(5.5) *Any prime divisor of w divides* $q(1+u\,p)$.

The parameters associated with G (or M) in the sense of §2 are $(p, l, 0, \mu)$; we need only consider p and μ.

(5.6) **Theorem.** $p=\alpha\,y-\mu+3$, *where* α *and* y *are positive integers such that*

(i) $\mu\,|\,\alpha y+2$ *with* α *even or odd according as* $(\alpha y+2)/\mu$ *is even or odd, and*

(ii) $y^2-4\alpha y-(\mu-2)(\mu-6)=0$.

Proof. The case I of ([4], Lemma 7) is impossible since $\mu>1$ and $\lambda=0$. Hence case II applies, giving $\mu^2+4(p-\mu)=y^2$, a square, such that $y\,|\,p(p+\mu-3)$ and $2y\,|\,p(p+\mu-3)$ if and only if $(p-1)/\mu$ is odd. If $p\,|\,y$ then $p\,|\,\mu(\mu-4)$, which is impossible. Hence $p+\mu-3=\alpha y$. Then $y^2-4\alpha y=(\mu-2)(\mu-6)$, and

$$\frac{p-1}{\mu}=\frac{\alpha\,y+2}{\mu}-1$$

giving $p=\alpha y-\mu+3$, with α even or odd according as $(\alpha\,y+2)/\mu$ is even or odd. This proves (5.6).

It is easy to see that the conditions of (5.6) are equivalent to those of ([4]; Lemma 7) in our present case. We note that the incidence matrix $A=V(\Delta)$ of the block design $\boldsymbol{A}$ associated with G has the eigenvalues p with multiplicity 1 and

$$\begin{Bmatrix} s \\ t \end{Bmatrix}=\frac{-\mu+y}{2}$$

with multiplicities

$$\begin{Bmatrix} f_2 \\ f_3 \end{Bmatrix} = \pm \frac{p}{2} \left\{ \alpha \pm \frac{\alpha y + 2}{\mu} \right\}$$

respectively. $1, f_2, f_3$ are the degrees of the irreducible constituents of the permutation representation of G (cf. [*4*]; §§ 4, 5).

If $\mu = 2$, we have by (5.4) that $w = 1$, i.e., $T(a) = 1$ and G_a^{Δ} is faithful. The conditions of Theorem (5.6) are equivalent to: $p = 4\alpha^2 + 1$, α odd. The first three possibilities are as follows:

α	p	n
1	5	16
3	37	704
5	101	5152

For the first of these we must have $G_a = A_5$ or S_5, giving $|G| = 960$ or 1920. It is known (cf. [*1*], p. 403) that there is no simple group of either of these orders, hence this case is impossible.

If $\mu = 6$, (5.4) gives $w = 1$ or 5 and

$$w \,\Big|\, \frac{p-1}{6}.$$

The conditions of Theorem (5.6) become: $p = 4\alpha^2 - 3$, α odd, $3 \mid 2\alpha^2 + 1$. Here the first three possibilities are:

α	p	n	w
5	97	1,649	1
7	193	6,369	1
13	673	76,049	1

For each $\mu \neq 2, 6$ there are at most finitely many corresponding primes p, as follows at once from Theorem (5.6). Solutions of the conditions of Theorem (5.6) can be found, for example, by putting $\mu = 4\rho$ and assuming that $3 \mid \rho - 2$[1]. The smallest solution of this kind is $\mu = 116$, $p = 1{,}088{,}777$, $n = 10{,}222{,}340{,}312$. We do not know of any solution with μ odd and > 1.

6. The case $\mu = 1$

In this section we prove

(6.1) **Theorem.** *Let G be a primitive rank 3 permutation group of even order with $k = p$, a prime, and $\mu = 1$. Then either*

(i) *$p = 2$, $n = 5$ and G is a dihedral group of order* 10,

---

[1]) This possibility was pointed out by MARSHALL HESTENES jr.

(ii) $p=3$, $n=10$ *and* G *is isomorphic with one of* A_5 *or* S_5 *acting on the unordered pairs of distinct letters, or*

(iii) $p=7$, $n=50$ *and* G *is isomorphic with* $U_3(5)$ *or the group* $\hat{U}_3(5)$ *obtained by adjoining the field automorphism to* $U_3(5)$.

Proof. We first show that $\lambda=0$. Let a, b be points such that $b\in\Delta(a)$, then $|\Delta(a)\cap\Delta(b)|=\lambda$. If $\lambda=p-1$ then $\mu=0$, a contradiction. Hence $\lambda\leqq p-2$ and there is a $c\in\Delta(a)$, $c\neq b$, $c\notin\Delta(b)$. Then $|\Delta(c)\cap\Delta(a)|=\lambda$, $\Delta(c)\cap\Delta(b)=\{a\}$ and $b, c\notin\Delta(c)$. Hence $2\lambda\leqq p-2$. If $2\lambda=p-2$ then $p=2$ and $\lambda=0$. Otherwise $2\lambda<p-2$ and there is a point $d\in\Delta(a)$, $d\notin\Delta(c)$, $d\neq b, c$. Then $|\Delta(d)\cap\Delta(a)|=\lambda$, $\Delta(d)\cap\Delta(b)=\Delta(d)\cap\Delta(c)=\{a\}$ and $b, c, d\notin\Delta(d)$. Hence $3\lambda\leqq p-3$, and either $p=3$ and $\lambda<0$ or $3\lambda<p-3$. Continuing in this way we eventually get $p\lambda\leqq p-p=0$ and hence $\lambda=0$.

Now it follows at once from Theorem 1 of [4] that one of the following conditions holds:

(a) $p=2$, $n=5$.

(b) $p=3$, $n=10$.

(c) $p=7$, $n=50$.

We know that the groups listed in the theorem have representations of the stated type ([4], [5]). We must show that this list is exhaustive.

In case (a), G must be a Frobenius group ([7], § 18.7), and hence dihedral of order 10.

In case (b) let us arrange the points as follows: a, $\Delta(a)=\{b, c, d\}$, $\Delta(b)-\{a\}$, $\Delta(c)-\{a\}$, $\Delta(d)-\{a\}$. Then for suitable arrangement of the points in the sets $\Delta(x)-\{x\}$, $x\in\Delta(a)$, the incidence matrix of the block design A associated with G (cf. [4], §§ 3, 4; this is the matrix $V(\Delta)$ of [7], § 28) takes the form

$$\begin{array}{c|ccc|cc|cc|cc|}
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
1 & & & & 1 & 1 & & & & \\
1 & & 0 & & & & 1 & 1 & & \\
1 & & & & & & & & 1 & 1 \\ \hline
0 & 1 & & & \multicolumn{2}{c|}{0} & \multicolumn{2}{c|}{I} & \multicolumn{2}{c|}{X} \\
0 & 1 & & & & & & & & \\ \hline
0 & & 1 & & \multicolumn{2}{c|}{I} & \multicolumn{2}{c|}{0} & \multicolumn{2}{c|}{I} \\
0 & & 1 & & & & & & & \\ \hline
0 & & & 1 & \multicolumn{2}{c|}{X^t} & \multicolumn{2}{c|}{I} & \multicolumn{2}{c|}{0} \\
0 & & & 1 & & & & & & \\ \hline
\end{array}$$

Since the row sum is 3, X must be I or

$$J=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

and since $A^2+A=2I+F$ ([3], § 3), we must have $X=J$. Because S_5 has a representation of the given type, it follows that the full collineation group of A has a subgroup $S\approx S_5$. We easily see that S is the full collineation group and that any rank 3 subgroup contains the subgroup of S isomorphic with A_5.

To handle case (c) we apply a method due to WIELANDT (oral communication). Let G be a rank 3 group of degree 50 with $k=7$, $\lambda=0$ and $\mu=1$. Let A be the incidence matrix of the block design A associated with G. We know that

$$A^2+A=F+6I \tag{1}$$

where $F=F_{50}$ is the 50×50 matrix with all entries 1 and $I=I_{50}$ is the 50×50 identity matrix, and the eigenvalues of A are 7, -3 and 2 with multiplicities 1, 21 and 28 respectively (cf. [4], §§ 4, 5).

Choose a subgroup $H=\langle\pi\rangle$ of G of order 7. Then H fixes exactly one point a, has $\Delta(a)$ as an orbit and decomposes $\Gamma(a)$ into 6 orbits of length 7. We can arrange the points so that in the permutation representation D of G we have

$$D(\pi)=\operatorname{diag}\{1, C, \ldots, C\}$$

where $C=C_7$ is the 7×7 cyclic matrix

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ 1 & & \cdots & & 0 \end{pmatrix}$$

and at the same time A takes the form

$$\left(\begin{array}{c|c|ccc|c} 0 & 1\ldots 1 & 0 & \ldots & & 0 \\ \hline 1 & & & & & \\ \vdots & 0 & I_7 & \ldots & & I_7 \\ 1 & & & & & \\ \hline 0 & I_7 & B_{11} & \ldots & & B_{16} \\ & & \cdots & & & \\ \hline 0 & I_7 & B_{61} & \cdots & & B_{66} \end{array}\right)$$

where $B=(B_{ij})$ is a symmetric 42×42 matrix partitioned into 7×7 blocks B_{ij}. From the properties of A, in particular the relation (1), we have

$$\sum B_{ij}=F-I, \tag{2}$$

and

$$\sum B_{ij}B_{jk}+B_{ik}=\begin{cases} F+5I & \text{for } i=k \\ F-I & \text{for } i\neq k \end{cases} \tag{3}$$

(where, of course, $F=F_7$ and $I=I_7$).

Now form the matrix $\hat{A}$ by replacing each of the indicated blocks of A by its row sum:

$$A=\left(\begin{array}{cc|ccc} 0 & 7 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 1 \\ \hline 0 & 1 & \beta_{11} & \cdots & \beta_{16} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \beta_{61} & \dots & \beta_{66} \end{array}\right)$$

Since $D(\pi)$ commutes with A, each block B_{ij} of B is a sum of powers $\neq I$ of C. Hence the symmetric matrix $b=(\beta_{ij})$ has non-negative integral entries, and since B is symmetric with all diagonal entries 0, the diagonal entries β_{ii} are even. The row sum of b is 6,

$$\sum_j \beta_{ij}=6. \tag{4}$$

There is a similarity transformation reducing A to the form diag $\{\hat{A}, A_1, \dots, A_6\}$ where the A_i are algebraically conjugate 7×7 matrices, and reducing F to the form diag $\{\hat{F}, 0, \dots, 0\}$, where

$$\hat{F}=\begin{pmatrix} 1 & 7 & \dots & 7 \\ 1 & 7 & \dots & 7 \\ & & \dots & \\ 1 & 7 & \dots & 7 \end{pmatrix}$$

comes from F in the same way as $\hat{A}$ comes from A. Hence $\hat{A}^2+\hat{A}=\hat{F}+6I$ by (1), and trace $\hat{A}=-6$ trace A_1. Hence $b^2+b=6(F+I)$, i.e.,

$$\sum \beta_{ij}\beta_{jk}+\beta_{ik}=\begin{cases} 12 & \text{for} \quad i=k \\ 6 & \text{for} \quad i\neq k. \end{cases} \tag{5}$$

From (4) and (5) we see easily that $\beta_{ii}=0$ or 2 for each i, and that the cases $\beta_{ii}=0$ for all i and $\beta_{ii}=2$ for all i are impossible. Hence b has trace 6, which means that we can assume that $\beta_{11}=\beta_{22}=\beta_{33}=0$ and $\beta_{44}=\beta_{55}=\beta_{66}=2$. Then by (4) and (5) we see that (disregarding order) the set of off diagonal entries in each of the first three rows (columns) must be either

$$\{2, 2, 2, 0, 0\} \tag{I}$$

or

$$\{3, 1, 1, 1, 0\} \tag{II}$$

while the set of off diagonal entries in each of the last three rows (columns) must be $\{2, 1, 1, 0, 0\}$. A straightforward analysis of the possible cases (say, according to the possible values of β_{12} and β_{13}) shows that (up to row and column permutations) exactly two matrices b exist, namely

$$b_1=\left(\begin{array}{ccc|ccc} 0&2&2&2&0&0\\ 2&0&2&0&0&2\\ 2&2&0&0&2&0\\ \hline 2&0&0&2&1&1\\ 0&0&2&1&2&1\\ 0&2&0&1&1&2 \end{array}\right), \quad b_2=\left(\begin{array}{ccc|ccc} 0&0&0&2&2&2\\ 0&0&3&1&1&1\\ 0&3&0&1&1&1\\ \hline 2&1&1&2&0&0\\ 2&1&1&0&2&0\\ 2&1&1&0&0&2 \end{array}\right).$$

Now we determine the matrices A, or what is the same thing, the matrices $B=(B_{ij})$, corresponding to b_1 and b_2.

First suppose that b_1 arises from B. Then with ρ a suitable power of C we have $B_{16}=0$, $B_{26}=\rho^k+\rho^l$, $B_{36}=0$, $B_{46}=\rho^j$, $B_{56}=\rho$ and $B_{66}=\rho^i+\rho^{-i}$, so that $B_{61}=0$, $B_{62}=\rho^{-k}+\rho^{-l}$, $B_{63}=0$, $B_{64}=\rho^{-j}$ and $B_{65}=\rho^6$. Applying (2) and (3) we see that $\{1, i, -i, j, k, l\}$ and $\{k-l, l-k, 2i, -2i, i, -i\}$ are complete residue systems modulo 7. There are exactly two possibilities

i	j	k	l
2	6	3	4
5	6	3	4

each of which gives $B_{26}=\rho^3+\rho^4$, $B_{46}=\rho^6$, $B_{54}=\rho$ and $B_{66}=\rho^2+\rho^5$. Putting $B_{15}=B_{25}=0$, $B_{35}=\rho^u+\rho^v$, $B_{45}=\rho^m$ and $B_{55}=\rho^s+\rho^{-s}$ and applying (2) and (3) again we see that $\{s, -s, m, u, v, 6\}$, $\{u-v, v-u, 2s, -2s, s, -s\}$ and $\{m+1, s+6, -s+6, 1, 4, 6\}$ are complete residue systems modulo 7, which is impossible.

Now assume that b_2 arises from B. Just as for b_1 we have $B_{16}=\rho^3+\rho^4$, $B_{26}=\rho^6$, $B_{36}=\rho$, $B_{46}=B_{56}=0$ and $B_{66}=\rho^2+\rho^5$. Putting $B_{15}=\rho^a+\rho^b$, $B_{25}=\rho^s$, $B_{35}=\rho^m$, $B_{45}=0$ and $B_{55}=\rho^u+\rho^{-u}$ and applying (2) and (3) we see that $\{u, -u, m, s, a, b\}$, $\{a-b, b-a, 2u, -2u, u, -u\}$ and $\{a+3, b+3, a+4, b+4, s+1, m+6\}$ are complete residue systems modulo 7. We need only consider the two possibilities

a	b	s	u	m
1	6	5	3	2
2	5	3	1	4

By repeated application of (2) and (3) we see that the first of these arises from exactly one matrix B, namely

$$\begin{array}{cccccc} 0 & 0 & 0 & \rho^2+\rho^5 & \rho+\rho^6 & \rho^3+\rho^4\\ 0 & 0 & \rho+\rho^2+\rho^4 & \rho^3 & \rho^5 & \rho^6\\ 0 & \rho^3+\rho^5+\rho^6 & 0 & \rho^4 & \rho^2 & \rho\\ \rho^2+\rho^5 & \rho^4 & \rho^3 & \rho+\rho^6 & 0 & 0\\ \rho+\rho^6 & \rho^2 & \rho^5 & 0 & \rho^3+\rho^4 & 0\\ \rho^3+\rho^4 & \rho & \rho^6 & 0 & 0 & \rho^2+\rho^5. \end{array}$$

In the same way we see that the second possibility arises from exactly one matrix B, which differs from this one only by the transposition (4, 5) applied to the rows and columns. Since the resulting matrix A is clearly independent of the choice of ρ as a power $\neq 1$ of C, we obtain exactly one matrix A (up to row and column permutations).

Assume that G is the full collineation group of the corresponding block design A. Then G has a rank 3 subgroup Γ isomorphic with $\hat{U}_3(5)$, and $\Gamma_a \approx S_7$, $G_a = T(a) \cdot \Gamma_a$, where $T(a)$ is the kernel of the action of G_a on $\Delta(a)$. We want to show first that $G = \Gamma$, i.e., that $T(a) = 1$.

For $x \in \Delta(a)$, $T(a) \lhd G_{a,x}$ and $G_{a,x}$ acts as S_6 on $\Sigma(x) = \Delta(x) - \{a\}$. If $T(a)$ acts trivially on $\Sigma(x)$ then $T(a) = T(a) \cap T(x)$ and this holds for all $x \in \Delta(a)$. Hence $T(a) = 1$ by (2.7). Hence if $T(a) \neq 1$ it acts as A_6 or S_6 on $\Sigma(x)$.

Now list the points of A as follows: a, the points of $\Delta(a) = \{b, c, \ldots, d\}$ in some order, the points of $\Delta(b) - \{a\}$, the points of $\Delta(c) - \{a\}$, ..., the points of $\Delta(d) - \{a\}$. For suitable arrangement of the points in each of the sets $\Delta(x) - \{a\}$, $x \in \Delta(a)$, A takes the form

$$
\begin{array}{c|c|c|c|c|c|c|c|}
0 & 1111111 & 0 & 0 & 0 & \cdots & 0 & 0 \\
\hline
\begin{matrix}1\\1\\1\\1\\1\\1\\1\end{matrix} & 0 & E_1 & E_2 & E_3 & \cdots & E_6 & E_7 \\
\hline
 & & 0 & I & * & \cdots & * & * \\
\cline{3-8}
 & & & 0 & I & \cdots & * & * \\
\cline{4-8}
 & & & & 0 & \cdots & * & * \\
\cline{5-8}
 & & & & & \cdots & \cdots & \cdots \\
\cline{7-8}
 & & & & & \cdots & 0 & I \\
\cline{7-8}
 & & & & & & & 0 \\
\cline{8-8}
\end{array}
$$

where E_i has 1's in the i-th row and all other entries 0. Then for $\tau \in T(a)$, $D(\tau)$ has the form $\operatorname{diag}\{1, I_7, X, \ldots, X\}$ where X is a 6×6 permutation matrix. Under our assumptions every 6×6 permutation matrix X occurs for some $\tau \in T(a)$. Thus each of the 6×6 blocks $*$ commutes with every even 6×6 permutation matrix and hence must be the identity, which is impossible. Hence $T(a) = 1$ and $G = \Gamma$.

Consider finally a rank 3 subgroup H of G, $H \neq G$. If $H_a \approx S_7$ or A_7 then $H \approx \hat{U}_3(5)$ or $U_3(5)$. We must therefore have that either H_a is solvable and contained in the normalizer of an element of order 7, or $H_a \approx$ the simple group of order 168. The minimal normal subgroup M of H is a transitive, nonregular simple group, so M is isomorphic with a subgroup of $U = U_3(5)$, and we regard M as a subgroup of U. If $M = 7 \cdot 50$, M would be a Frobenius group, so we have two cases: $|M| = 21 \cdot 50$ and $|M| = 168 \cdot 50$. To dispose of these we consider U as it acts transitively on the 126 absolute points of the projective plane over the field of 25 elements. Let P be an absolute point and suppose that $|M| = 21 \cdot 50$. Then $U : M = 120$ and we have $M : M_P = 21x \leqq 126$ and $|M_P| = 50/x$. If $5 | x$ then $M : M_P = 105$, i.e., there is an M-orbit of absolute points of length 105, and hence there must be one of length 21, i.e., $M : M_Q = 21$ for some absolute point Q. But then $25 \,|\, |M_Q|$ so M_Q contains an element $\sigma \neq 1$ of the center of the 5-Sylow subgroup of U_Q. Then σ is an elation with center Q and has for its orbits $\{Q\}$ and the sets of 5 absolute points $\neq Q$ and collinear with Q. Hence the M-orbit of length 21 consists of the absolute points on 4 nonabsolute lines through Q, and this must be true for each of its points Q, which is clearly impossible. Hence $25 \,|\, |M_P|$ for all absolute points P, so M contains an elation with center P for all P and therefore $M = U$. If $|M| = 168 \cdot 50$ we have at once that $25 \,|\, |M_P|$ for all P, and hence that $M = U$. Thus both cases are impossible.

References

[1] BRAUER, R.: On groups whose order contains a prime number p to the first power. I. Amer. J. Math. **54**, 401—420 (1942).
[2] —, and W. F. REYNOLDS: On a problem of E. ARTIN. Ann. Math. **68**, 713—720 (1958).
[3] BURNSIDE, W.: Theory of groups of finite order. 2nd edition. Cambridge: Univ. Press 1911, republished in 1955 by Dover Publications, Inc., Oxford.
[4] HIGMAN, D. G.: Finite permutation groups of rank 3. Math. Z. **86**, 145—156 (1964).
[5] —, and J. E. MCLAUGHLIN: Some properties of finite unitary groups. (In preparation.)
[6] WIELANDT, H.: Eine Verallgemeinerung der invarianten Untergruppen. Math. Z. **45**, 209—244 (1939).
[7] — Finite permutation groups. New York: Academic Press 1964.

Department of Mathematics, University of Michigan, Ann Arbor, Michigan, USA

(Received July 5, 1965)