SOLVABLE PRIMITIVE PERMUTATION GROUPS OF LOW RANK(1)

BY
DAVID A. FOULSER

1. **Introduction.** B. Huppert [14] has classified all finite solvable doubly transitive permutation groups. It is possible to generalize Huppert's theorem to the class of two-dimensional solvable flag-transitive affine groups [8]. However, a more natural generalization is the class of permutation groups of low rank. Let G be a finite transitive permutation group of degree n on a set S, and let G_0 be the subgroup of G fixing a point 0 in S. Define $r(G)$, the rank of G, to be the number of orbits of G_0 in S (including the orbit $\{0\}$) (cf. [11], [12]). Thus, Huppert's theorem is concerned with groups of rank 2.

In this paper, we consider the finite solvable primitive permutation groups of rank >2 (the primitivity of G assures that G_0 is a linear group). Using techniques similar to Huppert's, it is possible to classify the maximal solvable primitive permutation groups of rank 3, and to restrict the possibilities for rank 4 groups to a small set. Moreover, certain results for groups of rank less than 10 and 20 are possible. On the basis of these results, it would be relatively easy, but tedious, to determine all the groups of rank 3 (or 4) by examining the subgroups of the maximal groups of rank $\leqq 3$ (or $\leqq 4$).

Moreover, these techniques when applied to rank 2 groups produce a new proof of Huppert's theorem, as follows(2).

The standard analysis of the class of solvable linear groups [5], [13], [17] divides this class roughly into 3 subclasses, $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{L}$. $\mathfrak{A}$ consists of collineation groups of affine lines; $\mathfrak{B}$ consists of the remaining groups which are vector space primitive, and $\mathfrak{L}$ of those which are imprimitive. If $H \in \mathfrak{B}$, then H has a minimal normal nonabelian subgroup N which is a q-group (in fact, N is usually an extra-special q-group), for some prime q, such that $|N/Z(N)| = q^{2m}$, for some m. $\mathfrak{B}$ can be subdivided into two subclasses $\mathfrak{B}_I$ and $\mathfrak{B}_R$ according as H contains, or does not contain, respectively, such an N which is irreducible.

Huppert's theorem states that if G is a solvable doubly transitive permutation group, then $G_0 \in \mathfrak{A}$ with the exception of 13 groups which are in $\mathfrak{B}$ (for an analysis of the doubly transitive groups of $\mathfrak{A}$, see [9, Theorem 15.3]). To prove Huppert's

Received by the editors July 7, 1966.

(1) I gratefully acknowledge the support of the U.S. Army Research Office, Durham, and the National Science Foundation, through the University of Chicago.

(2) See D. S. Passman, *Permutation groups* (Benjamin, New York, 1968), p. 228 for a simplified proof of Huppert's theorem.

theorem, let $G_0 \in \mathfrak{B}$. Then the stabilizers N_x in N of points $x \neq 0$ in S are abelian subgroups of N. Since N is normal in G_0, 2 points x and y lie in the same orbit under G_0 only if N_x and N_y are conjugate in G_0. Hence the number of nonisomorphic stabilizers in N yields a lower bound for $r(G)$. When this bound is applied to Huppert's theorem, it eliminates all the possibilities in $\mathfrak{B}$ except those cases in which doubly transitive groups actually occur (see (3.13) and (3.15)). This proof seems preferable to the proof of Huppert's theorem in [8, Theorem 2.3], which depends on a number-theoretic lemma of Artin-Birkhoff-Vandiver, in that the present proof depends only on the permutation properties of G.

Now let G be a maximal solvable primitive permutation group of degree n on a set S. Then G_0 is a semilinear group on a vector space V over a field $GF(p^k)$.

1.1 THEOREM. *Let $r(G)=3$. Let (a, b) be the lengths of the nontrivial orbits of G_0. Then G satisfies one of the following conditions.*

1. $G \in \mathfrak{A}$;
2. $G \in \mathfrak{B}_1$, *and one of the following cases applies.*
   (a) $q^m=3$, $p^k=4$, $n=4^3$, $|G|=4^3(2^4 \cdot 3^4)$, *and* $(a, b)=(27, 36)$;
   (b) $q^m=2$, $n=p^{2k}$, $|G|=p^{2k}(24k(p^k-1))$, *for p^k and (a, b) as follows.*

p^k	3^2	13	17	19	3^3	29	31	47
(a, b)	(32, 48)	(72, 96)	(96, 192)	(144, 216)	(104, 624)	(168, 672)	(240, 720)	(1104, 1104)

   (c) $q^m=4$, $p^k=3$, $n=3^4$, $|G|=3^4(2^8 \cdot 3^2)$, *and* $(a, b)=(32, 48)$;
   (d) $q^m=4$, $p^k=7$, $n=7^4$, $|G|=7^4(2^7 \cdot 3 \cdot 5)$, *and* $(a, b)=(480, 1920)$.
3. $G \in \mathfrak{L}$; *then there exists a decomposition $V=V_1 \oplus V_2$ of V into minimal imprimitivity subspaces for G_0, and $G_0|V_i$ is transitive on the nonzero elements of V_i $(i=1, 2)$ (hence $G_0|V_i$ is determined by Huppert's theorem). Moreover, the nontrivial orbits of G_0 are $V_1 \cup V_2 - \{0\}$ and $V-(V_1 \cup V_2)$.*

REMARK. All the cases in part 2 exist. The two cases with $n=3^4$ in 2(b) and 2(c) are distinct, from the structure of N and A.

The groups of part 2 are all maximal solvable groups. Certain of these groups contain proper rank 3 subgroups (e.g., the group G in 2(c), for $n=3^4$, contains rank 3 subgroups which are in the class $\mathfrak{B}_R$; see Proposition 9.10).

Moreover, there exist two cases in which exceptional doubly transitive groups have proper rank 3 subgroups (this information can be derived from [9, p. 457, Table II]). These cases are as follows (for G a maximal rank 3 group):

2(b'). $G \in \mathfrak{B}_1$, $q^m=2$, $n=p^{2k}$, where either
   (i) $p^k=7$, $|G|=7^2(2^3 \cdot 3^2)$, and $(a, b)=(24, 24)$; or
   (ii) $p^k=23$, $|G|=23^2(2^3 \cdot 3 \cdot 11)$, and $(a, b)=(264, 264)$.

1.2 THEOREM. $r(G) \geqq 5$ *except possibly in the following cases*:

1. $G \in \mathfrak{A}$;
2. $G \in \mathfrak{B}_I$ *and one of the following cases applies.*
   (a) $q^m = 3$, $p^k = 4$ *or* 7, *and* $n = p^{3k}$;
   (b) $q^m = 2$, $p^k \leqq 71$, *and* $n = p^{2k}$;
   (c) $q^m = 4$, $p^k = 3$, 5, *or* 7, *and* $n = p^{4k}$.
3. $G \in \mathfrak{B}_R$ *and one of the following cases applies.*
   (a) $q^m = 2$, $p^k \leqq 7$, *and* $n = p^{4k}$;
   (b) $q^m = 2$, $p^k = 3$, *and* $n = 3^6$;
   (c) $q^m = 2$, $p^k = 3$, *and* $n = 3^{10}$.
4. $G \in \mathfrak{L}$, *there exists an imprimitivity decomposition* $V = \sum_{i=1}^{r} \oplus V_i$ *for* $r = 2$ *or* 3, *and* $G_0 | V_i$ *is transitive on* $V_i - \{0\}$, *for* $1 \leqq i \leqq r$.

Moreover, if $r(G) < 10$ *or if* $r(G) < 20$, *then certain results are possible if* $G_0 \in \mathfrak{B}_I \cup \mathfrak{L}$ (*see* (2.5) *and* (5.1); *also* (6.34), (8.1), (8.5), *and* (8.7)). *It is clear from* §9 *how these results could be extended to* $\mathfrak{B}_R$.

Proof of Theorem 1.1. 2(a) from Theorem 6.34, Corollary 6.35, and Proposition 4.6; 2(b) from Corollary 8.2; 2(c) and 2(d) from Corollary 8.6 (also see Theorem 5.1); and (3) from Proposition 2.5. For the class $\mathfrak{B}_R$, see Proposition 9.10. Theorem 1.1 has been obtained recently independently by Larry Dornhoff, using work of D. S. Passman (ibid). Related papers of Professor Dornhoff include: *On imprimitive solvable rank* 3 *permutation groups*, and *The rank of primitive solvable permutation groups*, (to appear).

Proof of Theorem 1.2. Property 2 from Theorem 5.1, 3 from Proposition 9.10, and 4 from Proposition 2.5.

§§2 and 3 below contain the standard analysis of solvable linear groups; §2 contains the discussion of the class $\mathfrak{L}$, §§3–8 discuss $\mathfrak{B}_I$, and §9 analyzes $\mathfrak{B}_R$. The proof of Huppert's theorem is given in §3 along with the required analysis of the abelian subgroups of N. §5 contains a lower bound for $r(G)$ which eliminates all but a relatively few cases of $\mathfrak{B}_I$. The remaining cases of $\mathfrak{B}_I$ are discussed in §§6–8. In particular, §6 contains an analysis of the case $q > 2$, $m = 1$, which is complete if $q = 3$ (see (6.34) and (6.35)).

1.3 NOTATION. Let V be a vector space over a field F, and let H be a group of linear transformations of V. It often is necessary to discuss the corresponding projective space PV determined by V and F, and the induced projective group $PH \simeq H/F$. We will try to avoid the explicit introduction of the projective situation, and the resultant additional notation and complications, as follows. Define a *point* of V (as opposed to an element of V) to be a one-dimensional subspace of V, i.e., a point of PV. Moreover, let H denote both the linear group H and the projective group PH, depending on the context.

If x is a point or an element of V, let H_x denote the subgroup of H fixing x, and let x^H denote the orbit of H containing x. If b is a matrix acting on V, let b^T denote the transpose of b.

Let $GL(V)$, $SL(V)$, $\Gamma L(V)$, and $Sp(V)$ denote the general, special, semilinear and symplectic groups of V, respectively (also $GL_n(p^k)$, etc.). Let $PGL(V)$, etc. denote the corresponding projective groups. If $V_1 \subset V$, let $H|V_1$ denote the restriction of H to V_1. Finally let Σ_n denote the symmetric group of degree n.

If N is a subgroup of H, let $\mathfrak{N}_H(N)$, $\mathfrak{C}_H(N)$, $\mathfrak{Z}(N)$, and N' denote the normalizer and centralizer of N in H, and the center and commutator subgroup of N, respectively. Let $\mathrm{Aut}(N)$ and $\mathrm{Aut}_Z(N)$ denote the group of automorphisms of N and the group of automorphisms which fix $\mathfrak{Z}(N)$ element-wise, respectively. If $\alpha, \beta, \ldots \in H$ (or in V) then $\langle \alpha, \beta, \ldots \rangle$ denotes the subgroup of H (subspace of V) generated by $\alpha, \beta, \ldots$.

Let a and b be integers. Then $a|b$ and $a\nmid b$ denotes that $b \equiv 0 \pmod{a}$ and $b \not\equiv 0 \pmod{a}$, respectively; and (a, b) is the g.c.d. of a and b. Let $|H|$ denote the order of H.

2. **Solvable primitive permutation groups.** In the following section, the standard analysis of maximal solvable linear groups is applied to primitive permutation groups (cf. [13], [17]). The various cases which arise lead to three classes of groups, $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{L}$. The groups of low rank in $\mathfrak{L}$ are discussed below in this section, and the groups in $\mathfrak{B}$ are discussed in §§3–9.

Let G be a maximal solvable primitive permutation group of a finite set V. Let T be a minimal normal abelian subgroup of G, so that T is an elementary abelian group of order p^f, for some prime p and integer f. Since G is primitive, then T is unique, T is transitive on V, and $|T| = |V| = p^f$. Thus $G = T \cdot G_0$ is the split extension of T by G_0, the subgroup of G fixing a point of V. Moreover, it is possible to make V into a vector space of dimension f over $GF(p)$ by inducing the group addition of T in V. Then T and G_0 act as the group of translations of V, and as an irreducible group of linear transformations of V over $GF(p)$, respectively.

2.1 Definition [11], [12]. If G is a transitive permutation group on a finite set V, define *the rank of* G, $r(G)$, to be *the number of orbits of* G_0 *in* V. The trivial orbit, (0), is counted in determining $r(G)$. Thus if G is a k-fold transitive group for $k \geqq 2$, then $r(G) = 2$. Further, $r(G) = 3$ if G_0 has exactly two orbits in addition to (0).

If H is a group of linear transformations of a vector space V, then it is convenient to define $r^*(H)$, the r^*-rank of H, to be *the number of nontrivial* (i.e., $\neq(0)$) *orbits of* H. If $G = T \cdot H$, with $H = G_0$, let $r^*(G) = r^*(H) = r(G) - 1$.

Now for the moment, let H be a maximal solvable linear (or semilinear) group on V over F. Then H contains the subgroup F^* of all scalar transformations of V. Thus H is transitive on the nonzero elements of any one-dimensional subspace of V. Hence, $r^*(H)$ is equal to the number of orbits among the points of the projective space PV under the projective group PH. Therefore, the study of the rank of the maximal solvable primitive permutation groups G can be reduced to the study of the number of orbits of certain solvable projective groups. As we explained in (1.3), a point x of V is defined to be a one-dimensional subspace of V (i.e., $x = Fv$,

for $v \neq 0$ in x), and H denotes both the linear group H and the projective group PH, depending on the context. This avoids the explicit introduction of the projective situation.

To continue the analysis of a solvable, primitive permutation group G with $G_0 = H$, let A be a maximal normal abelian subgroup of H.

2.2 LEMMA. *If A is irreducible, then $G = T \cdot H$ is a subgroup of the affine group of dimension* 1 *over $GF(p^f)$. I.e.,*

$$G \subseteq \{x \to ax^{p^b} + c: \quad x, a, c \in GF(p^f), 1 \leqq b \leqq f\}.$$

Proof. [14, Hilfssatz 2], [8, 3.2].

2.3 DEFINITION. *Let $\mathfrak{A}$ be the class of primitive permutation groups which are subgroups of finite one-dimensional affine groups.* Now let $G = T \cdot H$ be a solvable primitive permutation group which is not in $\mathfrak{A}$. *Let $G \in \mathfrak{B}$ if H is vector space primitive on V over $GF(p)$, and let $G \in \mathfrak{L}$ if H is imprimitive* [13]. The definitions of $\mathfrak{B}$ and $\mathfrak{L}$ do not depend on the choice of A. However, if $H \notin \mathfrak{A}$ then every A is reducible; and if any A has inequivalent irreducible representations on V, then $H \in \mathfrak{L}$ [13, Satz 2, p. 481].

Let $G \in \mathfrak{B}$, and let A decompose V into t equivalent irreducible subspaces $V_1, \ldots, V_t$, where $t > 1$ and $t \mid f$. Then A acts faithfully on each V_i as scalar multiplication by elements of $F = GF(p^k)$, where $k = f/t$. Thus in particular, A is cyclic and $|A| \mid p^k - 1$. Moreover, A is contained in no proper subfield of $GF(p^k)$. Therefore, each V_i and hence V is a vector space over $GF(p^k)$, under the action of A. It follows that $\mathfrak{C}_H(A)$ and $H = \mathfrak{N}_H(A)$ operate on V as groups of linear and semilinear transformations, respectively, over $GF(p^k)$; hence $[H : \mathfrak{C}_H(A)]$ divides k. Since G is maximal, $A = F^*$. Moreover A is unique. For if A_1 is another maximal normal abelian subgroup of H which determines $F_1 = GF(p^{k_1})$, then $|A : A \cap A_1| \mid k_1$ and hence $|A| \mid k_1(p^{k_1} - 1)$. Therefore, $k \leqq k_1$ by a number-theoretic lemma [8, 3.1], [9, 2.4]. Similarly, $k_1 \leqq k$, so $k = k_1$. Therefore, $(p^k - 1) \mid k|A_1 \cap A|$, so $A \cap A_1$ generates both F and F_1. Thus $A = A_1$.

Next, suppose $G \in \mathfrak{L}$. Let $V = V_1 \oplus \cdots \oplus V_r$ $(r > 1)$ be a decomposition of V into minimal imprimitivity components of H. Since H is irreducible, H acts transitively on the set $\{V_i\}$ $(1 \leqq i \leqq r)$. For H in $\mathfrak{L}$, A is not unique; in fact, A depends on the decomposition of V, $V = V_1 \oplus \cdots \oplus V_r$.

2.4 LEMMA [14, Hilfssatz 3, p. 131]. *Let G be a solvable doubly transitive permutation group. Then $G \in \mathfrak{A} \cup \mathfrak{B}$.*

Proof. If $G \in \mathfrak{L}$, then a point of V_1 and a point of $V - \bigcup_1^r V_i$ never lie in the same orbit, so $r^*(H) \geqq 2$.

Since $H|V_i$ is primitive, the remarks above concerning $\mathfrak{B}$ can be applied to $V_1, \ldots, V_r$. Since H is transitive on $\{V_i\}$, it follows that each V_i is a vector space of

dimension t over $GF(p^k)$, for some integers k and t such that $ktr=f$. Let $H_i=H|_{V_i}$, $1\leqq i\leqq r$; and let $H_{V_1,\ldots,V_r}=\overline{H}$ be the subgroup of H fixing each V_i. Then $H_1\simeq H_2\simeq\cdots\simeq H_r$, $\overline{H}\lhd H$, $\overline{H}\subseteq H_1\times\cdots\times H_r$, and $H/\overline{H}$ is a subgroup of Σ_r by its action on $\{V_i\}$ $(1\leqq i\leqq r)$. For example, $h\in\overline{H}$ has the form $h=\operatorname{diag}(h_1,\ldots,h_r)$, for h_i acting on V_i. Finally, there is a 1-1 correspondence between the orbits of V_i under H_i and the orbits of V_j under H_j $(1\leqq i,j\leqq r)$, determined by $H/\overline{H}$. For let x_i and $y_i\in V_i$, with $h(x_i)=y_i$ for some $h\in H_i$. Suppose a and $b\in H$, $a(x_i)=x_j$, $b(y_i)=y_j$, with x_j and $y_j\in V_j$. Then $bha^{-1}(x_j)=y_j$, and since elements of H permute the subspaces $V_1,\ldots,V_r$, it follows that $bha^{-1}\in H_j$. Hence x_j and y_j are in the same orbit in V_j and this orbit is the image of the orbit $\{\ldots x_i,\ldots,y_i,\ldots\}$ of V_i under every element of H which maps V_i onto V_j.

2.5 PROPOSITION. *Let $G=T\cdot H\in\mathfrak{L}$, let $V=V_1\oplus\cdots\oplus V_r$ be an imprimitive decomposition of V determined by H, and let $n=r^*(H|V_1)$. The following table lists lower bounds for $r^*(H)$ for certain values of (n,r). For all other values, $r^*(H)\geqq 5$; and for all other values with $n>1$, $r^*(H)\geqq 10$. In addition, $r^*(H)\geqq 20$ if either $n\geqq 5$, or $r\geqq 5$ and $n\geqq 2$, or $r\geqq 11$.*

n \ r	2	3	4	5
1	2	3	4	9
2	5	9		
3	9			

2.6 LEMMA. *Let H satisfy the following conditions: $\overline{H}=H_1\times H_2\times\cdots\times H_r$, and $H/\overline{H}=\Sigma_r$. Then $r^*(H)=C_{n+r,r}-1$.*

Proof. H_i has $n+1$ orbits (including $\{0\}$) in V_i $(1\leqq i\leqq r)$. As we mentioned, the orbits of H_i and H_j $(1\leqq i,j\leqq r)$ are in one-to-one correspondence under H. Since $\overline{H}=\overline{H}_1\times\cdots\times H_r$, the points of V_i can be permuted independently of the points of V_j. Since $H/\overline{H}\simeq\Sigma_r$, then the number of orbits in V under H is equal to the number of unordered r-tuples with entries from the set $\{0,1,\ldots,n\}$, namely $C_{n+r,r}$. Excluding the trivial orbit, $r^*(H)=C_{n+r,r}-1$, as required.

Proof of Proposition 2.5. Since $\overline{H}\subseteq H_1\times\cdots\times H_r$ and $H/\overline{H}\subseteq\Sigma_r$, it follows from (2.6) that $r^*(H)\geqq C_{n+r,r}-1$. In addition, note that $C_{n+r,r}-1\geqq 20$ for $n\geqq 5$, or for $n\geqq 2$ and $r\geqq 5$.

Let us return to the class $\mathfrak{B}$. Let $G=T\cdot H$ be a maximal element of $\mathfrak{B}$, with $f=kt$ and $A\simeq F^*$ as before. Since H is maximal, it follows from [17, Theorem 10, p. 21], that $\mathfrak{C}_H(A)\neq A$. Let N be a minimal normal nonabelian subgroup of H contained in $\mathfrak{C}_H(A)$.

2.9 DEFINITION. Let $\mathfrak{B}_I$ and $\mathfrak{B}_R$ be the subclasses of $\mathfrak{B}$ for which a minimal group N (above) is irreducible, and for which no minimal group N is irreducible, respectively.

The subclasses $\mathfrak{B}_I$ and $\mathfrak{B}_R$ are discussed in §§3–8, and 9, respectively.

2.10 LEMMA. *Let $G=T\cdot H$ be a solvable doubly transitive permutation group, and let $G\in\mathfrak{B}$. Then $G\in\mathfrak{B}_I$.*

Proof. First, $\mathfrak{C}_H(A)\neq A$, since $p^f-1\nmid k(p^k-1)$, for $k<f$. Second, if N is a minimal subgroup of H as above, then N is irreducible (see [14, Hilfssatz 1, p. 129] and [3, p. 199]).

3. **Huppert's theorem.** We continue to study the class $\mathfrak{B}$ (Definition 2.3). Let the groups H and N satisfy the following hypothesis:

3.1. H is a maximal solvable irreducible, primitive, semilinear group acting on the vector space V over $F=GF(p^k)$. A, a maximal abelian normal subgroup of H, is the group of all scalar transformations of V. And N is a minimal normal non-abelian subgroup of H which is contained in $\mathfrak{C}_H(A)$.

A study of the abelian subgroups of N leads to a new proof of Huppert's theorem (3.15), and some information concerning the groups of low rank in the class $\mathfrak{B}_I$, for which N is irreducible (§§6–8). The class $\mathfrak{B}_R$, for which N is reducible, is treated in §9.

If H and N satisfy 3.1, then [13, Hilfssätzen I and II, pp. 486, 488] shows that H and N also satisfy the following conditions:

3.2. (1) N is a q-group, for some prime q.

(2) $|N'|=q$, and $N'\subseteq\mathfrak{Z}(N)\subseteq A$. Thus, $q\mid|\mathfrak{Z}(N)|\mid p^k-1$.

(3) The exponent of N is q or 4, as $q>2$ or $q=2$, respectively.

(4) $W=N/\mathfrak{Z}(N)$ is an elementary abelian group.

(5) $H/\mathfrak{C}_H(W)$ acts irreducibly on W, over $GF(q)$.

(6) $\mathfrak{C}_H(Z)/\mathfrak{C}_H(Z)\cap\mathfrak{C}_H(W)$ is isomorphic to a subgroup of $Sp(W)$, the symplectic group of W, where $Z=\mathfrak{Z}(N)$. Hence $|W|=q^{2m}$, for some integer m.

In fact, from 3.2, N belongs to one of the following classes of groups:

3.3. (1) N is an extra-special q-group (i.e., $\mathfrak{Z}(N)=N'=\Phi(N)$, the Frattini subgroup of N, and $|N'|=q$; see [10, p. 15]), and the exponent of N is q or 4 as $q>2$ or $q=2$, respectively; or

(2) $q=2$, $|\mathfrak{Z}(N)|=4$, and $N=N^*\cdot\mathfrak{Z}(N)$, for N^* an extra-special 2-group contained in N such that $N^*\cap\mathfrak{Z}(N)=N'$.

However, not all of the groups which satisfy 3.3 also satisfy 3.1 or 3.2. Nonetheless, it is convenient to study the groups of 3.3 and then to restrict the results to the original groups of 3.1.

3.4 DEFINITION. Let $\mathfrak{H}$ be the set consisting of all q-groups which satisfy 3.3 (1) or (2). Let $N\in\mathfrak{H}$ and $|N/\mathfrak{Z}(N)|=q^{2m}$. Define m to be the *length* of N.

3.5 LEMMA. *Let $N\in\mathfrak{H}$ be a q-group of length m. Then*

1. *$N=N_1\dot\times\cdots\dot\times N_m$, the central product of m q-groups N_i of length 1 in $\mathfrak{H}$. Moreover, $\mathfrak{C}_N(N_i)=N_1\dot\times\cdots\bigwedge^i\cdots\dot\times N_m$, for $1\leqq i\leqq m$.*

2. (a) *If $q>2$, then each N_i $(1\leqq i\leqq m)$ is isomorphic to the unique nonabelian group of order q^3 and exponent q.*

(b) *Let $q=2$ and $|\mathfrak{Z}(N)|=2$. Then one can assume that $N_1, \ldots, N_{m-1}$ are isomorphic to D, and that N_m is isomorphic either to D or to Q, where D and Q are the dihedral and quaternion groups of order 8, respectively.*

(c) *Let $q=2$ and let $|\mathfrak{Z}(N)|=4$. Then N_i is isomorphic to $\langle D, z\rangle$, where D is the dihedral group of order 8, z has order 4, z centralizes D, and $\langle z^2\rangle=\mathfrak{Z}(D)$.*

Proof. 1. (Cf. [10, p. 17].) By definition, N is the central product, $N=N_1\times N_2$, of 2 normal subgroups N_1 and N_2, if $\mathfrak{Z}(N_1)=\mathfrak{Z}(N_2)$, and if N is equal to the direct product of N_1 and N_2 in which $\mathfrak{Z}(N_1)$ and $\mathfrak{Z}(N_2)$ have been identified. Let $Z=\mathfrak{Z}(N)$. Let $x\in N-\mathfrak{Z}(N)$. Then there exists $y\in N-Z$ such that the commutator $[x, y]\neq 1$. Hence $\langle x, y, Z\rangle=N_1$ is a q-group of length 1 in $\mathfrak{H}$. Let $\{x, y, x_3, \ldots, x_{q^m}\}$ be a base for $N/\mathfrak{Z}(N)$. For each u, $3\leqq u\leqq q^m$, there exist integers i_u, j_u such that $x'_u=x^{i_u}y^{j_u}x_u$ centralizes $\langle x, y\rangle$, since $|N'|=q$. Then $\langle x'_3, \ldots, x'_{q^m}, Z\rangle=\mathfrak{C}_N(N_1)$ is a q-group of length $m-1$ in $\mathfrak{H}$, and N is the central product, $N=N_1\times\mathfrak{C}_N(N_1)$. Continue.

2. There exists one extra-special q-group of order q^3 and exponent q, for $q>2$ (see 3.8 or [19, p. 151]). There exist two extra-special 2-groups of order 8 and exponent 4, namely D and Q.

Next, note that $D\times D\simeq Q\times Q$. For let $D_i=\langle a_i, b_i\rangle$, where $a_i^4=b_i^2$ and $a_i^{-1}b_ia_i=a_i^2b_i$, so that $D_i\simeq D$, for $i=1, 2$. In $D_1\times D_2$, let $c_i=a_i$ $(i=1, 2)$, $d_1=a_2b_1$, $d_2=a_1b_2$, and $Q_i=\langle c_i, d_i\rangle$, $i=1, 2$. Then $Q_i\simeq Q$, $i=1, 2$; and $D_1\times D_2=Q_1\times Q_2$.

To prove 2(b), let $N=N_1\times\cdots\times N_m$, where $N_i\simeq D$ or $N_i\simeq Q$, for each i. Thus $N\simeq D\times\cdots\times D\times Q\times\cdots\times Q$, and (2b) follows by replacing $Q\times Q$ by $D\times D$ as many times as possible.

2(c). From (3.2), $N_1=\langle N_1^*, z\rangle$, where $\langle z\rangle=\mathfrak{Z}(N)$. Moreover, $N_1^*\simeq D$ or Q. However, $\langle D, z\rangle\simeq\langle Q, z\rangle$, since $x\in N-\mathfrak{Z}(N)$ and $|x|=2$ or 4 implies $|xz|=4$ or 2, respectively.

3.6 NOTATION. Let N be a q-group of length m in $\mathfrak{H}$. If $q\neq 2$, write $N=N(q^m)$. If $q=2$ and $|\mathfrak{Z}(N)|=2$, write $N=N^i(2^m)$ with $i=1$ if $N\simeq D\times\cdots\times D$ (*type* 1), and $i=2$ if $N\simeq D\times\cdots\times D\times Q$ (*type* 2). If $|\mathfrak{Z}(N)|=4$, then write $N=N^3(2^m)$ (*type* 3).

Note that $D\simeq N^1(2)$ and $N^3(2)$ do not satisfy 3.1; D contains a characteristic subgroup of order 4, and so violates 3.2(5); and $N^3(2)$ contains a characteristic subgroup isomorphic to Q.

3.7 LEMMA. *Let $N=N(q)$ be a q-group of length 1 in $\mathfrak{H}$, and let $|\mathfrak{Z}(N)|\mid p^k-1$. Then N has a faithful, absolutely irreducible representation of degree q over $GF(p^k)$.*

Proof. Let $\lambda\in GF(p^k)$ have order $|\mathfrak{Z}(N)|$. If $q>2$, then N has generators $\bar a$, $\bar b$, $\bar c$, subject to the relations

$$\bar a^q=\bar b^q=\bar c^q=1,\quad \overline{ba}=\overline{abc},\quad \langle\bar c\rangle=\mathfrak{Z}(N),\qquad [19, \text{p. } 151].$$

Let a, b, c be the following $q \times q$ matrices:

$$a = \begin{pmatrix} 1 & & & \mathbf{0} \\ & \lambda & & \\ & & \lambda^2 & \\ & & & \ddots \\ & \mathbf{0} & & & \lambda^{q-1} \end{pmatrix}, \quad b = \begin{pmatrix} 010 & \cdots & \\ 001 & \cdots & \\ \vdots & & \\ 0 & \cdots & 01 \\ 10 & \cdots & 0 \end{pmatrix}, \tag{3.8}$$

$$c = \begin{pmatrix} \lambda & & \mathbf{0} \\ & \lambda & \\ & & \ddots \\ \mathbf{0} & & & \lambda \end{pmatrix}$$

Then $\theta: \bar{a} \to a$, $\bar{b} \to b$, $\bar{c} \to c$ is a faithful, absolutely irreducible representation of N. For suppose that θ is reducible over a finite extension field K, and let $\theta = \sum \theta_i$ be the complete reduction of θ over K. From the order of $GL_t(K)$, for $t < q$, the group of $t \times t$ diagonal matrices

$$S = \{\text{diag}\,(\lambda_1, \ldots, \lambda_t): \quad |\lambda_i| = q^{u_i},\ 1 \leqq i \leqq t\}$$

is a Sylow q-subgroup of $GL_t(K)$, and S is abelian. Hence $\theta_1(N)$ is abelian for each i, so $\theta(N)$ is abelian, which is false. Hence θ is absolutely irreducible.

If $q=2$, let $\theta(D)=\langle a, b\rangle$ and $\theta(Q)=\langle c, d\rangle$, where

$$a = c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad d = \begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix}, \tag{3.9}$$

λ and $\mu \in GF(p)$ such that $\lambda^2+\mu^2=-1$, [14, Hilfssatz 4]. Note that if $4 | p^k-1$, we can let $\theta(Q)=\langle a, \sqrt{(-1)}b\rangle$. Hence if $|\mathfrak{Z}(N)|=4$, let $\theta(N)=\langle a, b, \sqrt{-1}\rangle$.

Note that in each case, θ corresponds to a faithful representation of $\mathfrak{Z}(N)$ of degree 1.

3.10 LEMMA. *Let $N=N(q^m)$ be a q-group of length m in $\mathfrak{H}$, and let $|\mathfrak{Z}(N)| \mid p^k-1$. Then there exist exactly $\phi(|\mathfrak{Z}(N)|)$ faithful, absolutely irreducible representations of N over $GF(p^k)$ (where ϕ is Euler's function), one for each faithful representation of $\mathfrak{Z}(N)$ of degree 1 over $GF(p^k)$. Each such representation of N has degree q^m.*

Proof. Let $N=N_1 \times \cdots \times N_m$, as in Lemma 3.5, and let θ_i be a faithful, absolutely irreducible representation of N_i on the q-dimensional space V_i, for $1 \leqq i \leqq m$. Finally, let all the θ_i's agree on $\mathfrak{Z}(N)=\mathfrak{Z}(N_i)$. Let $\theta=\theta_1 \otimes \cdots \otimes \theta_m$ be the representation of N of degree q^m on $V=V_1 \otimes \cdots \otimes V_m$, as explained in the following diagram.

$$\begin{array}{ccccccccc} N & = & N_1 & \times & N_2 & \times \cdots \times & N_m \\ \theta \downarrow & & \theta_1 \downarrow & & \theta_2 \downarrow & & \theta_m \downarrow \\ \theta(N) & = & \theta_1(N_1) & \otimes & \theta_2(N_2) & \otimes \cdots \otimes & \theta_m(N_m) \\ V & = & V_1 & \otimes & V_2 & \otimes \cdots \otimes & V_m \end{array} \tag{3.11}$$

Then θ is a faithful, absolutely irreducible representation of N [10, pp. 17, 18]. For $\theta(N_1)$ is irreducible and nonabelian of prime degree q on V_1 over $GF(p^k)$, so the group ring of $\theta(N_1)$ over $GF(p^k)$ is isomorphic to $GL(V_1)$. Since $GL(V_1) \otimes GL(V_2) \simeq GL(V_1 \otimes V_2)$ [15, p. 212], it follows that $\theta(N_1) \otimes \theta(N_2)$, and similarly $\theta(N)$, is irreducible. Similarly, θ is absolutely irreducible.

Moreover, since there are $\phi(|\mathfrak{Z}(N)|)$ choices of λ (or $\sqrt{-1}$) in (3.8) and (3.9), there exist at least $\phi(|\mathfrak{Z}(N)|)$ inequivalent representations of this type, corresponding to the $\phi(|\mathfrak{Z}(N)|)$ inequivalent faithful representations of $\mathfrak{Z}(N)$ of degree 1. Finally, these are the only possible faithful, absolutely irreducible representations of N, as follows [13, p. 490]. Let $|\mathfrak{Z}(N)| = q^\tau$, for $\tau = 1$ or 2, so that $|N| = q^{2m+\tau}$. There exist $|N/N'| = q^{2m+\tau-1}$ absolutely irreducible representations of N of degree 1. If $\{\rho_i\}$ is the set of degrees of the absolutely irreducible representations of N, then $\sum \rho_i^2 = |N|$. The representations of degree 1 and degree q^m listed above yield:

$$q^{2m+\tau-1} + \phi(|\mathfrak{Z}(N)|)q^{2m} = q^{2m}(q^{\tau-1} + q + \tau - 2) = q^{2m+\tau} = |N|.$$

Hence no further absolutely irreducible representations exist.

3.12 COROLLARY. *Let $N = N(q^m)$ be a q-group of length m in $\mathfrak{H}$, and let $|\mathfrak{Z}(N)| \mid p^k - 1$. Then every faithful, irreducible representation of N over $GF(p^k)$ is absolutely irreducible, and hence has degree q^m.*

Proof. Cf. [13]. Let θ be equivalent to $\theta' = \sum_1^r \theta_i$ over a finite extension field K of $GF(p^k)$, where each θ_i is absolutely irreducible. Since N is nilpotent (or directly), $J \cap \mathfrak{Z}(N) \neq 1$ for every normal subgroup J of N. Since θ' is faithful, then each θ_i is faithful on $\mathfrak{Z}(N)$ and hence on N. Each θ_i agrees with θ' on $\mathfrak{Z}(N)$. Let θ^* be the (unique) faithful, absolutely irreducible representation of N over $GF(p^k)$, which agrees with θ' on $\mathfrak{Z}(N)$, and let $\psi = r\theta^*$. Then θ^* is equivalent to each θ_i over K, and hence ψ is equivalent to θ over K. But θ and ψ are both representations over $GF(p^k)$. Hence [6, p. 200], θ and ψ are equivalent over $GF(p^k)$, and $r = 1$. Therefore θ is absolutely irreducible, and has degree q^m.

Let H and $N = N^i(q^m)$ satisfy hypothesis 3.1. For the remainder of §2 we assume N is irreducible ($H \in \mathfrak{B}_I$). The following lemma gives a lower bound for $r^*(H)$, the r^*-rank of H.

3.13 PROPOSITION. *If N is irreducible, then $r^*(H) \geqq t$, for t as listed in the following table.*

Cases	$q>2$	$N=N^1(2^m)$, $m>1$		$N=N^2(2^m)$		$N=N^3(2^m)$, $m>1$	
		$p^k>5$	$p^k \leqq 5$	$p^k>5$	$p^k \leqq 5$	$p^k>5$	$p^k=5$
t	$m+1$	$*\mu m+1$	$\mu(m-1)+1$	μm	$\mu(m-1)$	$m+1$	m

* $\mu = (2, (p^k-1)/2)$ *for* $q=2$.

3.14 COROLLARY. *$r^*(H) \geqq 2$ except possibly in the following cases.*

1. *$q=2$, $m=1$, $N \simeq Q$, and $p^k=5$ or $p^k \equiv 3 \pmod 4$;*

2. $q=2$, $m=2$, $N\simeq D\times Q$, *and* $p^k=3$, *where* D *and* Q *are the dihedral and quaternion groups of order* 8, *respectively.*

Proof. Apply 3.13. If $q=2$ and N has type 1 or 3, then $m>1$ (see remark following 3.6).

Huppert's theorem is an immediate consequence of Corollary 3.14.

3.15 THEOREM (HUPPERT). *Let* G *be a finite solvable doubly transitive permutation group. Then* G *satisfies one of the following conditions.*

1. G *is a collineation group of a Desarguesian affine line*;

2. $G_0=H$ *contains a normal subgroup isomorphic to the quaternion group* Q, *and* H *is a linear group of degree* 2 *over* $GF(p^k)$, *where* $p^k=3$, 5, 7, 11, or 23;

3. $G_0=H$ *contains a normal subgroup isomorphic to* $D\times Q$ ($D=$ *dihedral group*), *and* H *is a linear group of degree* 4 *over* $GF(3)$.

Proof of Huppert's theorem. If G is not the collineation group of a Desarguesian affine line ($G\notin\mathfrak{A}$), then $H=G_0$ contains a maximum abelian normal subgroup A which is reducible. Since G is doubly transitive, then $\mathfrak{C}_H(A)\neq A$, H is primitive (Lemma 2.4), and so H contains a minimal normal nonabelian subgroup N such that $N\subset\mathfrak{C}_H(A)$. Again since G is doubly transitive, then N is irreducible (Lemma 2.10), so the analysis of this section and in particular Corollary 3.14 applies. In case 1 of the corollary, $p^{2k}-1\mid|H|\mid 24k(p^k-1)$ from (4.6), so $p^k=3$, 5, 7, 11, or 23. The existence of solvable groups H such that $r^*(H)=1$ in cases 2 and 3 of Corollary 3.14 follows as in [14] and [8].

From the preceding lemmas on the representations of N, it is easy to see that any stabilizer N_x of N (where the point x is a one-dimensional subspace of V) is an abelian group which contains $\mathfrak{Z}(N)$. Moreover, if two points x and y are in the same orbit under H, then clearly N_x and N_y are conjugate in H. Hence the number of nonisomorphic abelian subgroups of N which contain $\mathfrak{Z}(N)$ and are stabilizers in N, is a lower bound for $r^*(H)$. It is this bound which is computed in Proposition 3.13. Hence the proof of 3.13 depends on a study of the abelian subgroups of N.

3.16 DEFINITION. Let S be an abelian subgroup of N such that $S\supseteq\mathfrak{Z}(N)$, and let $|S/\mathfrak{Z}(N)|=q^r$, for $0\leqq r\leqq m$. Define r to be the *length* of S. If q^j is the exponent of S, for $j=1$ or 2, define S to be of *type* j, and write $S=S_r^j$.

3.17 LEMMA. *Let* $S=S_r^j$ *be an abelian subgroup of* N *of type* j *and length* r ($j=1$ *or* 2, $0\leqq r\leqq m$), *which contains* $\mathfrak{Z}(N)$. *Then*:

1. *There exist elements* $x_1,\ldots,x_r\in N-\mathfrak{Z}(N)$ *such that* $S=\langle x_1,\ldots,x_r,\mathfrak{Z}(N)\rangle$, *where* $|x_i|=q$, $1\leqq i\leqq r-1$, *and* $|x_r|=q^j$.

2. *Moreover, there exist subgroups* $N_1,\ldots,N_m$ *of* N (*each* N_i *is a* q*-group of length* 1 *in* H) *such that* $x_i\in N_i$ *for* $1\leqq i\leqq r$, *and* $N=N_1\times\cdots\times N_m$. *In particular, if* $q=2$ *and* N *has type* 1 *or* 2, *then we can assume* $N_i\simeq D$, $1\leqq i\leqq m-1$, *and* $N_m\simeq D$ *or* Q *as* N *has type* 1 *or* 2, *respectively.*

Proof. Part 1 is obvious except in the following case: $N=N^i(2^m)$, $i=1$ or 2, and $r>1$. In this case, $S-\mathfrak{Z}(N)$ contains elements of order 2 (e.g., the product of two independent elements of order 4), so we can choose $r-1$ independent elements (mod $\mathfrak{Z}(N)$) of order 2. Then the rth independent element, x_r, must satisfy $|x_r|$ = exponent of $S=2^j$.

For part 2, assume $S=\langle x_1, \ldots, x_r, \mathfrak{Z}(N)\rangle$ as in (1), and suppose there exist $N_1, \ldots, N_s$, $s<r$, such that $x_i \in N_i$ $(1 \leqq i \leqq s)$, $N_i \simeq \langle D, \mathfrak{Z}(N)\rangle$ $(1 \leqq i \leqq s)$ if $q=2$, $\langle N_1, \ldots, N_s\rangle = N_1 \times \cdots \times N_s$, and each N_i centralizes each x_u for $i \neq u$ $(1 \leqq i \leqq s, 1 \leqq u \leqq r)$. Proceed as follows. There exists $a_{s+1} \in N-\mathfrak{Z}(N)$ such that the commutator $[x_{s+1}, a_{s+1}] \neq 1$. We can assume a_{s+1} centralizes $N_1 \times \cdots \times N_s$ (if not, multiply a_{s+1} by an appropriate element from $N_1 \times \cdots \times N_s$). Let $N_{s+1}=\langle x_{s+1}, a_{s+1}, \mathfrak{Z}(N)\rangle$. If $[a_{s+1}, x_u] \neq 1$, $u>s+1$, then let $\bar{x}_u = x_{s+1}^t x_u$, for appropriate t such that $[a_{s+1}, \bar{x}_u]=1$. Let

$$S = \langle x_1, \ldots, x_{s+1}, \bar{x}_{s+2}, \ldots, \bar{x}_r, \mathfrak{Z}(N)\rangle,$$

and note that $|x_u| = |\bar{x}_u|$, $u>s+1$. Finally if $q=2$ and $s+1<m$, then it is possible to choose a_{s+1} such that $|a_{s+1}|=2$; hence $N_{s+1} \simeq D$. If $q=2$ and $s+1=r=m$, then $N_m \simeq D$ or Q as N has type 1 or 2, respectively.

3.18 LEMMA. *Two abelian subgroups of N which contain $\mathfrak{Z}(N)$ and have the same length and type, are conjugate in $\mathfrak{N}_{GL(V)}(N)$.*

Proof. Let $N=N_1 \times \cdots \times N_m$, $S=\langle x_1, \ldots, x_r, \mathfrak{Z}(N)\rangle$ with $x_i \in N_i$ $(1 \leqq i \leqq r)$, and $N=\bar{N}_1 \times \cdots \times \bar{N}_m$, $\bar{S}=\langle \bar{x}_1, \ldots, \bar{x}_r, \mathfrak{Z}(N)\rangle$ with $\bar{x}_i \in \bar{N}_i$ $(1 \leqq i \leqq r)$, as in Lemma 3.17. There exists an element $\alpha \in \mathrm{Aut}_Z(N)$ such that $\alpha: N_i \to N_i$ $(1 \leqq i \leqq m)$; by examining Aut (N_i), we can assume $a: x_i \to \bar{x}_i$ $(1 \leqq i \leqq s)$. Therefore $\alpha: S \to \bar{S}$. As before, N and $\alpha(N)$ are two faithful irreducible representations of N which agree on $\mathfrak{Z}(N)$. Hence these representations are equivalent from Lemma 3.10, and so α is induced by conjugation in $\mathfrak{N}_{GL(V)}(N)$, as required.

Before deciding which abelian subgroups are stabilizers in N (Lemma 3.22), we determine the number of distinct abelian subgroups of each length and type and their fixed points.

3.19 DEFINITION. Let $N=N^j(q^m)$ (for $j=1$, 2, or 3 if $q=2$). Let the number of abelian subgroups of N which contain $\mathfrak{Z}(N)$ and which have length r and type i $(1 \leqq r \leqq m$, $i=1$ or 2), be denoted by

$C_{r,m}$ if $q>2$;

$C^3_{r,m}$ if $q=2$ and $N=N^3(2^m)$;

$C^{i\ j}_{r,m}$ if $q=2$ and $N=N^j(2^m)$, $j=1$ or 2.

Note that $C_{1,m}$ and $C^3_{1,m}$ are the number of one-dimensional subspaces in a space of dimension $2m$ over $GF(q)$. Similarly, $2 \cdot C^{i\ j}_{1,m}$ is the number of elements in $N-\mathfrak{Z}(N)$ of order 2^i ($i=1$ or 2).

3.20 LEMMA. 1. *Let $q>2$. Then* $C_{r,m} = \prod_{u=0}^{r-1} [(q^{2(m-u)}-1)/(q^{u+1}-1)]$, for $1 \leqq r \leqq m$.

2. *Let* $q=2$ *and let* $f(r, m)=\prod_{u=1}^{r-1}(2^{2(m-u)}-1)/(2^u-1)$, *for* $1\leqq r\leqq m$, *with the convention that* $f(1, m)=1$. *Then*

$C^3_{r,m}=(2^{2m}-1)f(r, m)/(2^r-1)$,

$C^{1\,j}_{r,m}=(2^m+(-1)^j)(2^{m-r}-(-1)^j)f(r, m)/(2^r-1)$, *and*

$C^{2\,j}_{r,m}=(2^m+(-1)^j)(2^{m-r})f(r, m)$, *for* $j=1$ *or* 2 *and* $1\leqq r\leqq m$.

Proof. 1. Let $S_r=\langle x_1, \ldots, x_r, \mathfrak{Z}(N)\rangle$ be an abelian subgroup of N, and let $N=N_1\otimes\cdots\otimes N_m$, with $x_u\in N_u$ $(1\leqq u\leqq r)$. There exist $q^{2m}-1$ choices for x_1 (mod $\mathfrak{Z}(N)$), i.e., any nonidentity element in $N/\mathfrak{Z}(N)$. Since $\mathfrak{C}_N(\langle x_1\rangle)=\langle x_1, N_2\otimes\cdots\otimes N_m\rangle$, there exist $q(q^{2(m-1)}-1)$ choices for x_2 (mod $\mathfrak{Z}(N)$). Continuing, there exist $\prod_{u=0}^{r-1}q^u(q^{2(m-1)}-1)$ ordered sequences $x_1, \ldots, x_r$ of elements which generate abelian subgroups of order q^r. Given such a sequence, there exist $(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})$ ordered sequences which generate the same subgroup. Hence, $C_{r,m}=\prod_{u=0}^{r-1}(q^{2(m-u)}-1)/(q^{u+1}-1)$, for $1\leqq r\leqq m$.

2. A similar argument proves $C^3_{r,m}=(2^{2m}-1)f(r, m)/(2^r-1)$.

Now let $S=S^i_r\subseteq N=N^j(2^m)$ for $j=1$ or 2. The proof consists of induction on r and m.

Let $r=1$ and apply induction to m. Clearly, the formulas for C^{ij}_{11} $(i, j=1, 2)$ are correct. Assume that $m>1$ and that the formulas hold for $m-1$; let $N=N_1\otimes\cdots\otimes N_m$, as in Lemma 3.17. Any subgroup S^i_1 of N has the form $S^i_1=\langle x_1\otimes x_2, \mathfrak{Z}(N)\rangle$, for $x_1\mathfrak{Z}$ unique in $N_1/\mathfrak{Z}(N)$ and x_2 unique in $N_2\otimes\cdots\otimes N_m/\mathfrak{Z}(N)$. Further, $i=1$ if and only if either (i) $|x_1|=1$ or 2, $|x_2|=1$ or 2, but not $|x_1|=|x_2|=1$; or (ii) $|x_1|=|x_2|=4$. Similarly, $i=2$ if and only if either (i) $|x_1|=4$ and $|x_2|=1$ or 2, or (ii) $|x_1|=1$ or 2 and $|x_2|=4$. Hence,

$$C^{1j}_{1m} = (C^{11}_{11}+1)(C^{1\,j}_{1,m-1}+1)-1+C^{21}_{11}C^{2\,j}_{1,m-1}$$

and

$$C^{2j}_{1m} = C^{21}_{11}(C^{1\,j}_{1,m-1}+1)+(C^{11}_{11}+1)C^{2\,j}_{1,m-1},$$

for $j=1$ or 2, and these equations lead to the correct formulas for C^{ij}_{1m} $(i, j=1, 2$ and $m>1)$.

Applying induction to r, we assume that $r>1$ and that the formulas are correct for $r-1$ and all m. Let $S^i_r=\langle x_1, \ldots, x_r, \mathfrak{Z}(N)\rangle$, where $x_u\in N_u$ $(1\leqq u\leqq r)$ and $|x_1|=\cdots=|x_{r-1}|=2$. Since $|x_1|=2$, there exist C^{1j}_{1m} choices for $\langle x_1, \mathfrak{Z}(N)\rangle$ in N. Having fixed x_1, S^i_r is uniquely determined by S^i_{r-1} in $N_2\otimes\cdots\otimes N_m=N^j(2^{m-1})$. Hence, there exist $C^{1j}_{1m}\cdot C^{i\,j}_{r-1,m-1}$ choices for S^i_r with a distinguished element x_1 of order 2. But x_1 can be chosen arbitrarily within the unique maximal subgroup of S^i_r of exponent 2, namely S^i_r itself if $i=1$, or $\langle x_1, \ldots, x_{r-1}, \mathfrak{Z}(N)\rangle$ if $i=2$. Hence, $C^{ij}_{rm}=C^{ij}_{1m}C^{i\,j}_{r-1,m-1}/(2^\varepsilon-1)$, where $\varepsilon=r$ or $r-1$ as $i=1$ or 2, respectively. Moreover, this equation leads to the correct formulas for C^{ij}_{rm}, for $i, j=1, 2$, and $1<r\leqq m$.

Let $N=N^j(q^m)=N_1\otimes\cdots\otimes N_m$ act irreducibly on $V=V_1\otimes\cdots\otimes V_m$. Let $S^i_r=\langle x_1, \ldots, x_r, \mathfrak{Z}(N)\rangle$ be an abelian subgroup of N, with $x_u\in N_u$ $(1\leqq u\leqq r)$, where N_u is a q-group of length 1 in $\mathfrak{H}$ acting on V_u $(1\leqq u\leqq m)$.

3.21 LEMMA. 1. *There exist points* (1-*dimensional spaces*) Fv *for* $v \in V$ *fixed by* S_r^i, *except in case* $q=2$, $i=2$, *and* $4 \nmid p^k-1$.

2. *If there exist fixed points for* S_r^i, *then there exist exactly* $q^r(p^{kg^{m-r}}-1)/(p^k-1)$ *fixed points distributed in* q^r *vector subspaces of dimension* q^{m-r}. *These* q^r *vector spaces are permuted transititively by* N.

Proof. By suitable change of the representation of each N_u, each x_u can be put in diagonal form as in (3.8) and (3.9) ($1 \leqq u \leqq r$), except in case $|x_r|=4$ and $4 \nmid p^k-1$. In this case, since every irreducible representation of N_r on V is faithful, x_r fixes no element of V. Otherwise, x_u fixes exactly q points of V_u, say $Fv_{u,t}$ ($1 \leqq u \leqq r$, $1 \leqq t \leqq q$). Then S_r^i fixes every point of V of the form $F(v_{1,t_1} \otimes \cdots \otimes v_{r,t_r} \otimes w)$, for $w \in V_{r+1} \otimes \cdots \otimes V_m$, and these points are distributed in q^r vector subspaces of dimension q^{m-r}. Since q is a prime, and since N_u fixes no point of V_u, the q fixed points in V_u of x_u are permuted transitively by N_u ($1 \leqq u \leqq r$) (also directly from (3.8) and (3.9)). Hence by induction, the q^r vector spaces of fixed points of S_r^i are permuted transitively by $N_1 \otimes \cdots \otimes N_r$.

On the other hand, suppose v is an element in V which does not have the form $v=v_{1t_1} \otimes \cdots \otimes w$ above. Then we can assume $v=\sum_t v_{vt} \otimes w_t$, for some fixed ν ($i \leqq \nu \leqq r$) with $w_t \in V_1 \otimes \cdots \bigwedge^{\nu} \cdots \otimes V_m$, and at least 2 w_t's (say w_{t_1} and w_{t_2}) nonzero. Then $x_\nu: v \to \sum_t \lambda^{t-1} v_{vt} \otimes w_t = v'$, and $Fv \neq Fv'$ since $\lambda^{t_1-1} \neq \lambda^{t_2-1}$. Therefore, Fv is not fixed by S_r^i.

The proof of Proposition 3.13 follows by counting the number of nonisomorphic stabilizers of N listed below. Note that $N^1(2)$ and $N^3(2)$ can be excluded from Proposition 3.13 since they do not satisfy the hypothesis 3.1.

3.22 LEMMA. *The following tables list the stabilizer subgroups of* N, *for* N *an element of* H *acting irreducibly on* V.

N	$N(q^m)$, $q>2$	$N^1(2^m)$	
		$p^k>5$	$p^k \leqq 5$
S_r^1	$0 \leqq r \leqq m$	$0 \leqq r \leqq m$	$0 \leqq r \leqq m$, $r \neq m-1$
$*S_r^2$	*not defined*	$1 \leqq r \leqq m$	$1 \leqq r \leqq m$, $r \neq m-1$

N	$N^2(2^m)$			$N^3(2^m)$	
	$p^k>5$	$p^k=3$	$p^k=5$	$p^k>5$	$p^k=5$
S_r^1	$0 \leqq r \leqq m-1$	$0 \leqq r \leqq m-1$, $r \neq m-2$	$0 \leqq r \leqq m-2$	$0 \leqq r \leqq m$	$0 \leqq r \leqq m$, $r \neq m-1$
$*S_r^2$	$1 \leqq r \leqq m$	*none*	$1 \leqq r \leqq m$, $r \neq m-1$	*not defined*	

* S_r^2 *is a stabilizer subgroup only if* $4 \mid p^k-1$.

Proof. From the description of the fixed points of S_r^t, it is clear that S_r^t is a stabilizer subgroup of $N=N^j(q^m)$ exactly when $\mathfrak{Z}(N)$ is a stabilizer subgroup of $N_{r+1}\otimes\cdots\otimes N_m=N^j(q^{m-r})$. In particular, it would be sufficient to show that N_u has $\mathfrak{Z}(N_u)$ as a stabilizer subgroup for $r+1\leqq u\leqq m$. In the few cases for which this is false, we determine whether or not $\mathfrak{Z}(N)$ is a stabilizer for $N=N^j(q^t)$, where $t=2$ and 3.

Let $q>2$. Then there exist $q+1$ abelian subgroups of $N(q)$ which contain $\mathfrak{Z}(N)$, each fixing q points. Hence there exist $(p^{kq}-1)/(p^k-1)-q(q+1)$ points with $\mathfrak{Z}(N)$ as stabilizer. Since $q|p^k-1$ and $q>2$, $(p^{kq}-1)/(p^k-1)\geqq p^{2k}+p^k+1>q(q+1)$. Therefore, every subgroup S_r of $N(q^m)$ is a stabilizer subgroup for $q>2$.

Let $q=2$. If $N_u\simeq D$, then there are 2 abelian subgroups of type 1 and one of type 2 in N_u. Hence, there exist p^k-3, or p^k-5 points with stabilizer $\mathfrak{Z}(N_u)$, as $p^k\equiv 3$ or 1, (mod 4), respectively. Hence, $\mathfrak{Z}(N_u)$ is a stabilizer subgroup if and only if $p^k>5$. Similarly, if $N_u=N^2(2)$ or $N^3(2)$, then $\mathfrak{Z}(N_u)$ is a stabilizer subgroup exactly if $p^k\neq 5$. Hence, if $p^k>5$, then S_r^1 is a stabilizer subgroup of N whenever it exists, and S_r^2 is a stabilizer subgroup of N whenever $4|p^k-1$. If $p^k=5$, then S_m^i is a stabilizer subgroup whenever it exists ($i=1, 2$), and S_{m-1}^i is not a stabilizer subgroup. If $p^k=3$, then S_m^1 is a stabilizer whenever it exists, and S_{m-1}^1 is not a stabilizer unless $N=N^2(2^m)$.

To complete the proof, it is sufficient to prove the following facts.

1. If $N=N^1(2^m)$, $m=2$ or 3 and $p^k=3$ or 5, then $\mathfrak{Z}(N)$ is a stabilizer subgroup of N.

2. If $N=N^2(2^m)$, $m=2$ or 3 and $p^k=5$, then $\mathfrak{Z}(N)$ is a stabilizer subgroup of N.

3. If $N=N^2(2^m)$ and $p^k=3$, then $\mathfrak{Z}(N)$ is not a stabilizer subgroup if $m=2$ ($N\simeq D\times Q$), but $\mathfrak{Z}(N)$ is a stabilizer subgroup if $m=3$.

As an example of the application of 1–3, let $p^k=3$ or 5 and $N^1(2^m)\simeq D\times\cdots\times D$. From (1), $\mathfrak{Z}(N)$ is a stabilizer in $D\times D$ and in $D\times D\times D$. Hence S_r^1 is a stabilizer for $0\leqq r\leqq m-2$. The other cases for $p^k=3$ or 5 can be handled similarly.

Proof of 1–3. 1. Let $N=N^1(2^2)\simeq D\times D$. The nontrivial stabilizers of N have length 2, and fix exactly 4 points each. Hence from Lemma 3.20, there exist $4(C_{22}^{11}+\delta C_{22}^{21})=4(6+9\delta)$ points with nontrivial stabilizers, where $\delta=0$ or 1 as $p^k\equiv 3$ or 1 (mod 4), respectively. It is easily checked that $(p^{4k}-1)/(p^k-1)>4(6+9\delta)$ for $p^k=3$ or 5, as required.

Let $N=N^1(2^3)\simeq D\times D\times D$. N contains $C_{13}^{11}=35$ and $C_{13}^{21}=28$ abelian subgroups of length 1 and type 1 or 2, respectively. Let $p^k=5$. Then each of these 63 subgroups fixes $2(5^4-1)/4$ points. Hence, there exist at least $(5^8-1)/4-126(5^4-1)/4=(5^4+1-126)(5^4-1)/4>0$ points with stabilizer $\mathfrak{Z}(N)$. Let $p^k=3$. Then the 28 subgroups of type 2 fix no points, so there exist at least $(3^8-1)/2-2\cdot 35\cdot(3^4-1)/2=40(82-70)>0$ points with stabilizer $\mathfrak{Z}(N)$.

2. Let $N=N^2(2^2)\simeq D\times Q$ and $p^k=5$. The nontrivial stabilizer subgroups have length 2 and hence type 2, and there exist $C_{22}^{22}=15$ of them, each fixing 4 points. Hence, there exist $(5^4-1)/4-4\cdot 15>0$ points with stabilizer $\mathfrak{Z}(N)$.

Let $N=N^2(2^3)$ and $p^k=5$. There exist $2^{2m}-1=63$ subgroups S_1^i ($i=1$ or 2) in N, each fixing $2\cdot(5^4-1)/4$ points. Hence there exist $((5^4-1)/4)(5^4+1-126)>0$ points with stabilizer $\mathfrak{Z}(N)$.

3. If $p^k=3$ and $N=N^2(2^2)\simeq D\times Q$, then $U=\mathfrak{N}_{GL(V)}(N)$ is transitive on the points of V, and hence $\mathfrak{Z}(N)$ is not a stabilizer [1], [8], [14]. If $N\simeq(D\times D)\times Q$, then $\mathfrak{Z}(N)$ is a stabilizer, since $\mathfrak{Z}(N)$ is a stabilizer in $D\times D$ from (1), and in Q since $p^k=3$. This completes the proof of 3.22.

If S_r^i is a stabilizer subgroup of $N=N^j(q^m)$ acting on V over $GF(p^k)$, then there may exist fixed points x of S_r^i such that $N_x\supsetneqq S_r^i$. The following lemma discusses the number of points y such that $N_y=S_r^i$.

3.23 DEFINITION. Let $s_{r,m}^j$ be the total number of stabilizer subgroups of $N=N^j(q^m)$ of length r ($r\leqq m$); let $v_{r,m}$ be the number of points fixed by a stabilizer of N of length r; let g_m^j be the number of points x such that $N_x=\mathfrak{Z}(N)$. Finally, let $w_{r,m}$ be the number of subgroups of order q^r in an elementary abelian group of order q^m ($r\leqq m$). These definitions may depend on q and p^k, as well as on j and m, the type and length of N.

Note that if $q>2$, then $j=1$ and $s_{r,m}^1=C_{r,m}$. If $q=2$, $p^k\equiv 1 \pmod 4$, and $p^k>5$, then $s_{r,m}^j=(2^{2m}-1)f(r,m)/(2^r-1)$ is independent of j. Moreover,

$$v_{r,m}=q^r(p^{kq^{m-r}}-1)/(p^k-1), \quad \text{and} \quad w_{r,m}=\prod_{v=0}^{r-1}(q^{m-v}-1)/(q^{v+1}-1).$$

Finally, from the proof of Lemma 3.21, the number of points stabilized by the stabilizer S_r^i is $q^r\cdot g_{m-r}^j$. Therefore,

$$g_m^j=(p^{kq^m}-1)/(p^k-1)-\sum_{r=1}^{m}s_{r,m}^j q^r g_{m-r}^j. \tag{3.24}$$

If $q=2$, $p^k\equiv 1 \pmod 4$ and $p^k>5$, then by induction g_m^j is independent of j.

3.25 LEMMA. *In the following equation, g_m^j is determined from m, j, $s_{r,m}^j$ ($1\leqq r\leqq m$), q, and p^k:*

$$g_m^j=(p^{kq^m}-1)/(p^k-1)-\sum_{r=1}^{m}\mu_r s_{r,m}^j v_{r,m},$$

where $\mu_r=\sum(-1)^{t+1}w_{i_1i_2}w_{i_2i_3}\cdots w_{i_{t-1}i_t}$, summed over all sequences $1\leqq i_1<i_2<\cdots i_t=r$, for $1\leqq t\leqq r$.

Proof. Clearly $s_{r,m}^j v_{r,m}=\sum_{v=r}^{m}w_{r,v}s_{v,m}^j q^v g_{m-v}^j$. The proof follows from (3.24), noting that $\sum_{r=1}^{m}s_{r,m}^j q^r g_{m-r}^j=\sum_{r=1}^{m}\mu_r s_{r,m}^j v_{r,m}$.

4. **The order of H.** Let H, A and $N=N(q^m)$ be transformation groups of V which satisfy hypotheses 3.1. We continue to study the properties of N, without at first assuming N is irreducible. Let the dimension of V be tq^m, let V_1 be an N-irreducible subspace of V, and let A_1 be the group of scalar transformations of V_1. Finally, let X be a vector space of dimension t.

4.1 LEMMA. 1. $\mathfrak{N}_{GL(V)}(N) \simeq \mathfrak{N}_{GL(V_1)}(N) \otimes GL(X)$, *acting on* $V \simeq V_1 \otimes X$; $\mathfrak{C}_{GL(V)}(N) \simeq A_1 \otimes GL(X)$.

2. $[\mathfrak{N}_{\Gamma L(V)}(N) : \mathfrak{N}_{GL(V)}(N)] = k$.

Proof. 1. See [13, Satz III, p. 482, Hilfssatz II (1), p. 488].

2. Let N be represented as in (3.8), (3.9) and (3.11); with respect to the given basis for V, let σ be defined by $\sigma\colon (x_i) \to (x_i^p)$ $(1 \leqq i \leqq q^m)$. Then $[\Gamma L(V) : GL(V)] = k$, $|\sigma| = k$, and σ normalizes N.

Now let N be irreducible on V, so that $t=1$, $V_1 = V$, $A_1 = A$, and $X = 0$.

4.2 NOTATION. For N irreducible on V, let $U = \mathfrak{N}_{GL(V)}(N)$ and $U^* = \mathfrak{N}_{\Gamma L(V)}(N)$. Recall that $W = N/\mathfrak{Z}(N)$. Further, let N be represented as in (3.8), (3.9), and (3.11). With respect to this basis for V, let σ be defined by $\sigma\colon (x_i) \to (x_i^p)$, $1 \leqq i \leqq q^m$. Finally, let $\hat{k}$ be the least integer such that $|\mathfrak{Z}(N)| \mid p^{\hat{k}} - 1$ (hence $\hat{k} | k$).

4.3 LEMMA. *Let N be irreducible and represented on V by* (3.8), (3.9), *and* (3.11); *and let σ be defined as above. Then*

1. $U^* = \langle U, \sigma \rangle$;

2. (i) $\mathfrak{C}_{U^*}(\mathfrak{Z}(N)) = \langle U, \sigma^{\hat{k}} \rangle$, (ii) $\mathfrak{C}_{U^*}(N) = \langle A, \sigma^{\hat{k}} \rangle$, (iii) $\mathfrak{C}_{U^*}(W) = \langle N, A, \sigma^{\delta} \rangle$, *where* $\delta = \hat{k}$ *if* $q > 2$ *and* $\delta = 1$ *if* $q = 2$.

3. $U/A \simeq \mathrm{Aut}_Z(N)$, *the group of automorphisms of N which fix each element of* $\mathfrak{Z}(N)$.

Proof. 1. Lemma 4.1 (2).

2. (i) Apply (1), the definition of $\hat{k}$, and the fact $\mathfrak{Z}(N) \subseteq A$.

(ii) $\mathfrak{C}_U(N) = A$ from Lemma 4.1 (1). Moreover, $\sigma^{\hat{k}} \in \mathfrak{C}_{U^*}(N)$ from (3.8), (3.9) and (3.11). Now apply 2(i).

(iii) Applying [13, Hilfssatz II.2, p. 488], but replacing in Huppert's lemma the direct product $\mathfrak{Z}(N) \times \cdots \times \mathfrak{Z}(N)$ by $N' \times \cdots \times N'$, we see that $\mathfrak{C}_U(W) = \langle N, A \rangle$. Further, $\sigma^{\hat{k}}$ centralizes N and hence W.

(α) Let $q = 2$. Then σ centralizes W from (3.9).

(β) Let $q > 2$, let $N_1 = \langle a, b \rangle \subset N$, as in (3.8), and let $y = \sigma^i x$ centralize W, where $x \in U$ and $0 < i < \hat{k}$. From (3.8), $x\colon aZ \to a^{p^{-i}}Z$ and $bZ \to bZ$, where $Z = \mathfrak{Z}(N)$. Moreover, x induces a central automorphism in N_1, which corresponds to conjugation by some element u in $U_1 = \mathfrak{N}_{GL(V_1)}(N_1)$ from (3) below. However, since u fixes $\langle aZ \rangle$ and bZ in N_1/Z, it follows from (6.5) below that $\theta(u) = 1$; i.e., x, and hence σ^i, centralize W, so $i = 0 \pmod{\hat{k}}$ which is a contradiction. Therefore, $\mathfrak{C}_{U^*}(W) = \langle N, A, \sigma^{\hat{k}} \rangle$.

3. Let ν be the natural homomorphism of U into $\mathrm{Aut}_Z(N)$. The kernel of ν is $A = \mathfrak{C}_U(N)$. Moreover, if $\alpha \in \mathrm{Aut}_Z(N)$, then N and $\alpha(N)$ are two irreducible representations of N which are equivalent, since they agree on $\mathfrak{Z}(N)$ (Lemma 3.10). Hence $\nu(U) = \mathrm{Aut}_Z(N)$.

4.4 COROLLARY. $|U^*| = k(p^k - 1) \cdot |\mathrm{Aut}_Z(N)|$.

We determine $|\mathrm{Aut}_Z(N)|$ by counting the number of subgroups of N which are q-groups of length 1 in $\mathfrak{H}$.

4.5 LEMMA. 1. *Let $q>2$ and $N=N(q^m)\in\mathfrak{H}$. Then N contains $q^{2(m-1)}(q^{2m}-1)/(q^2-1)$ subgroups which are in $\mathfrak{H}$ and have length* 1.

2. *Let $q=2$, $|\mathfrak{Z}(N)|=2$, and $N=N^j(2^m)$ ($j=1$ or 2). The following table lists the numbers of subgroups of N isomorphic to D and Q, the dihedral and quaternion groups of order* 8, *respectively.*

	D	Q
$N^j(2^m)$ $j=1$ *or* 2	$2^{2m-3}(2^m+(-1)^j)(2^{m-1}-(-1)^j)$	$2^{2m-3}(2^m+(-1)^j)(2^{m-1}+(-1)^j)/3$

3. *Let $q=2$, $|\mathfrak{Z}(N)|=4$, and $N=N^3(2^m)$. The following table lists the numbers of $\mathfrak{H}$-subgroups of N of various types and lengths.*

sub-group	$N^1(2^m)$	$N^2(2^m)$	$N^1(2)\simeq D$	$N^2(2)\simeq Q$	$N^3(2)$
number	$2^{m-1}(2^m+1)$	$2^{m-1}(2^m-1)$	$2^{2(m-1)}(2^{2m}-1)$	$2^{2(m-1)}(2^{2m}-1)/3$	$2^{2(m-1)}(2^{2m}-1)/3$

Proof. 1. There exist $C_{1,m}$ abelian subgroups $\langle x, \mathfrak{Z}(N)\rangle$ of length 1 in N. For each such subgroup, there exists $y\in N-\mathfrak{Z}(N)$ such that $\langle x, y, \mathfrak{Z}(N)\rangle=N_1$ has length 1 in $\mathfrak{H}$. Further, every other nonabelian subgroup of length 1 of N containing x has the form $\langle x, yw, \mathfrak{Z}(N)\rangle$, for w uniquely determined in $N_2/\mathfrak{Z}(N)$, where $N_2=\mathfrak{C}_N(N_1)$ has length $m-1$. Thus, there exist $(q^{2m}-1)q^{2(m-1)}/(q-1)$ subgroups isomorphic to $N_1=N(q)$ with a distinguished subgroup $\langle x, \mathfrak{Z}(N)\rangle$. Hence, each N_1 is counted $C_{11}=q+1$ times, so there exist $q^{2(m-1)}(q^{2m}-1)/(q^2-1)$ such subgroups of N.

2. If $m=1$, the formulas are correct. Let $m>1$. There exist C_{1m}^{2j} abelian subgroups $\langle x, \mathfrak{Z}(N)\rangle$ of N of length 1 and exponent 4, and for such an x, there exists y such that $N_1=\langle x, y, \mathfrak{Z}(N)\rangle\simeq D$ or Q. Then every other subgroup isomorphic to D or Q has the form $\langle x, yw, \mathfrak{Z}(N)\rangle$, for w of order 1 or 2 in $\mathfrak{C}_N(N_1)$. If $N_1\simeq D$, then $\mathfrak{C}_N(N_1)$ has the same type as N, namely j ($=1$ or 2), and the number of subgroups isomorphic to D is $C_{1m}^{2j}\cdot(C_{1,m-1}^{1\,j}+1)$, as required. However, if $N_1\simeq Q$, then $\mathfrak{C}_N(N_1)$ has type $j'=1$ or 2 as $j=2$ or 1, respectively. Moreover, in this case Q has three subgroups of order 4, so each N_1 is counted three times. Hence, the number of subgroups of N isomorphic to Q is $C_{1m}^{2j}\cdot(C_{1,m-1}^{1\,j'}+1)/3$, as required.

3. The number of subgroups $N^3(2)$ in $N^3(2^m)$ is given by the formula in part 1. Moreover, $N^3(2)\simeq\langle Q, z\rangle$, where $|z|=4$, as in (3.9), and it is easily checked that $N^3(2)$ contains one subgroup isomorphic to Q and 3 subgroups isomorphic to D. Finally, one can verify the formulas for $N^i(2^m)$ ($i=1, 2$) by induction. For example, let $i=2$. There exist $2^{2(m-1)}(2^{2m}-1)/3$ subgroups $N_1\simeq Q$ in N and $2^{m-2}(2^{m-1}+1)$ subgroups of $\mathfrak{C}_N(N_1)=N^3(2^{m-1})$ isomorphic to $N^1(2^{m-1})$. Further, there exist

$2^{2m-3}(2^m+1)(2^{m-1}+1)/3$ subgroups isomorphic to Q in $N^2(2^m)$. Hence, there exist

$$[2^{2(m-1)}(2^{2m}-1)/3]2^{m-2}(2^{m-1}+1)/[2^{2m-3}(2^m+1)(2^{m-1}+1)/3] = 2^{m-1}(2^m-1)$$

subgroups of $N^3(2^m)$ isomorphic to $N^2(2^m)$, as required.

4.6 PROPOSITION. *Let $N=N^i(q^m) \in \mathfrak{H}$, (for $i=1$, 2, or 3 if $q=2$) act irreducibly on V, and let $U^*=\mathfrak{N}_{\Gamma L(V)}(N)$.*

1. *Let $q>2$, or $q=2$ and $N=N^3(2^m)$. Then*

$$|U^*| = k(p^k-1)\cdot q^{m^2+2m}\prod_{u=1}^{m}(q^{2u}-1).$$

2. *Let $q=2$ and $N=N^i(2^m)$, for $i=1$ or 2. Then*

$$|U^*| = k(p^k-1)\cdot 2^{m^2+m+1}(2^m+(-1)^i)\prod_{u=1}^{m-1}(2^{2u}-1).$$

Proof. It is sufficient by Corollary 4.4 to show that

$$|\mathrm{Aut}_Z(N)| = q^{m^2+2m}\prod_{u=1}^{m}(q^{2u}-1)$$

in case 1 and

$$|\mathrm{Aut}_Z(N)| = 2^{m^2+m+1}(2^m+(-1)^i)\prod_{u=1}^{m-1}(2^{2u}-1)$$

in case 2, where $\mathrm{Aut}_Z(N)$ is the group of automorphisms of N which fix each element of $\mathfrak{Z}(N)$. If N_1 is an $\mathfrak{H}$-subgroup of N of length 1, then $N=N_1 \times \mathfrak{C}_N(N_1)$. Hence it is clear that $\mathrm{Aut}_Z(N)$ is transitive on the set of subgroups isomorphic to N_1, and the subgroup of $\mathrm{Aut}_Z(N)$ fixing N_1 is the direct product $\mathrm{Aut}_Z(N_1) \times \mathrm{Aut}_Z(\mathfrak{C}_N(N_1))$. Now apply induction, noting that $|\mathrm{Aut}_Z(N_1)|=q^3(q^2-1)$, 8, or 24, in case 1, case 2 ($i=1$), and case 2 ($i=2$) respectively (e.g., see (6.5)).

4.7 COROLLARY. *Let $I(N)$ be the group of inner automorphisms of N; let $U=\mathfrak{N}_{GL(V)}(N)$. Then $\mathrm{Aut}_Z(N)/I(N) \simeq U/\langle N, A\rangle$ is isomorphic to a subgroup B of $Sp(2m, q)$, the symplectic group of degree $2m$ over $GF(q)$. In case 1, $B=Sp(2m, q)$.*

Proof. Use Lemma 3.2 (6), Lemma 4.3, Proposition 4.6, and $|Sp(2m, q)| = q^{m^2}\prod_{u=1}^{m}(q^{2u}-1)$, [2, p. 147].

5. **An estimate for $r^*(H)$, $H \in \mathfrak{B}_I$.** Let H, $N=N(q^m)$, and A be transformation groups of V which satisfy hypothesis 3.1, and let N be irreducible on V. Further, let N be represented as in (3.8), (3.9), and (3.11), and let σ, $\hat{k}$, U and U^* be defined as in 4.2. In §3, we derived a crude lower bound for $r^*(U^*)$ which depended on a study of the abelian subgroups of N. In this section, another type of estimate for $r^*(U^*)$ is discussed. This estimate shows that the groups of low rank occur in relatively few cases, and these cases are discussed in detail in §§6–8. The results of §§5–8 can be summarized in the following theorem.

5.1 THEOREM. *Let H and N satisfy* 3.1, *and N be irreducible. Let* $U^* = \mathfrak{N}_{\Gamma L(V)}(N)$. *Then*

1. $r^*(U^*) \geqq 100$, *except possibly in the following cases*:

q	2	2	2	3	3	5, 7
m	1, 2	3	4	1	2	1
p^k	*all*	$\leqq 9$	3	*all*	4, 7	$\leqq 16$

2. $r^*(H) \geqq 9$, *except possibly in the following cases*:

q	2	2	2	3
m	1	2	3	1
p^k	$\leqq 6^3$	$\leqq 13$	3, 5	$\leqq 25$

3. $r^*(H) \geqq 4$, *except possibly in the following cases*:

q	2	2	3
m	1	2	1
p^k	$\leqq 71$	$\leqq 7$	4, 7

4. $r^*(H) \geqq 3$, *except possibly in the following cases*:

q	2	2	3
m	1	2	1
p^k	$\leqq 47$	3, 7	4

5.2 LEMMA. *If N is irreducible, then*

$$r^*(U^*) > p^{k(q^m-2)}/q^{2m^2+3m} > p^{k(q^m-(2m^2+3m+2))} > q^{q^m-(2m^2+3m+2)},$$

whenever $q^m \geqq 2m^2+3m+2$.

Proof. There exist $(p^{kq^m}-1)/(p^k-1)$ points (i.e., one-dimensional subspaces) in V, and every orbit of U^* has length at most $|U^*|/(p^k-1)$. Hence, $r^*(U^*) \geqq (p^{kq^m}-1)/|U^*|$. From Proposition 4.6, $|U^*| \mid k(p^k-1)q^{m^2+2m}\prod_{u=1}^{m}(q^{2u}-1)$. Since $(p^{kq^m}-1)/(p^k-1) > p^{k(q^m-1)}$, it follows that:

$$r^*(U^*) > p^{k(q^m-1)}/kq^{m^2+2m}\prod_{u=1}^{m}(q^{2u}-1). \tag{5.3}$$

The proof follows by using the estimates $k<p^k$, $q<p^k$, and $\prod_{u=1}^{m}(q^{2u}-1)<q^{m(m+1)}$, in (5.3).

The final estimate, $r^*(U^*)>q^{q^m-(2m^2+3m+2)}$ gives good results for $q\geqq 11$ and $m\geqq 1$. For example, if $q^m=11$, then $r^*(U^*)>11^4$. In fact, the lemma shows that $r^*(U^*)$ is very large, except in a relatively few cases. These cases will be discussed in §§6–8.

5.4 COROLLARY. $r^*(U^*)\geqq 100$ *except in the following cases.*

A. $m=1$, $q<11$,

B. $q=3$, $m=2$, *and* $p^k=4$ *or* 7,

C. $q=2$, $m\leqq 4$,

D. $q=2$, $m=5$, *and* $p^k=3$ *or* 5.

Proof. First, $q^{q^m-(2m^2+3m+2)}>100$ in the following cases: $q\geqq 11$, $m\geqq 1$; $q\geqq 5$, $m\geqq 2$; $q\geqq 3$, $m\geqq 4$; and $q\geqq 2$, $m\geqq 7$. Next, applying (5.3) to the case $q=3$ and $m=3$ yields: $r^*(U^*)>p^{26k}/k\cdot 2^7\cdot 3^{21}\cdot 5$. Since $p^k\geqq 4$ and $p^k/k\geqq 2$, $r^*(U^*)>4^{25}/2^6 3^{21}5$ $=(4/3)^{3\cdot 7}(4/5)>2^9/5>102$. For $q=3$, $m=2$, and $p^k\geqq 16$, then $p^k/k\geqq 2^4/4=4$. So (5.3) implies $r^*(U^*)>(16^7\cdot 4)/(2^7\cdot 3^8\cdot 5)=2^{23}/3^8\cdot 5>(2^8/3^5)^2\cdot 2^7>100$. For $p^k=13$, and $k=1$, (5.3) implies $r^*(U^*)>(13/6)^8\cdot(2/5)>2^9/5>100$.

Finally let $q=2$. If $m=6$, then from Lemma 5.2

$$r^*(U^*) > p^{k(62)}/2^{90} \geqq 3^{62}/2^{90} > (9/8)^{30}\cdot 9 > [(1+\tfrac{1}{8})^8]^{7/2}\cdot 9 > 100.$$

If $q=2$, $m=5$, and $p^k\geqq 7$, then Lemma 5.2 implies

$$r^*(U^*) > 7^{30}/2^{65} > (7/4)^{30}/2^5 > 3^{15}/2^5 > 3^{10} > 100.$$

The estimates of Lemma 5.2 can be improved in various ways. For example the orbits of the points for the various stabilizers in N could be estimated separately. Lemmas 5.5–5.7 are one result in this direction. Another possibility is to restrict H to be a solvable subgroup of U^*, in which case Huppert's analysis can be applied to H/N acting on $N/\mathfrak{Z}(N)$ (see Lemmas 5.8 and 5.9).

For $N=N^j(q^r)$ in $\mathfrak{H}$ acting irreducibly on the vector space V ($j=1$, 2, or 3 if $q=2$), let T be the set of points (i.e., 1-spaces) x of V such that $N_x=\mathfrak{Z}(N)$; and let $|T|=g_r^j$ as in Definition 3.23. Further, let $U^*(N^j)=\mathfrak{N}_{\Gamma L(V)}(N^j(q^r))$ permute the elements of T in u_r^j orbits (let $u_0=1$). Let S_n^i be a stabilizer subgroup of N of length $n\leqq r$, and type i, for $i=1$, 2, or 3 (if $q=2$).

5.5 LEMMA. $U^*=U^*(N^j(q^m))$ *permutes the set of points of* V *which have stabilizers isomorphic to* S_n^i *(for* $1\leqq n\leqq m$*) in* u_{m-n}^j *orbits.*

5.6 COROLLARY. $r^*(U^*)=\sum_{n=0}^{m}\gamma_n u_{m-n}^j$, *where* γ_n *is the number of nonisomorphic stabilizer subgroups of length* n *in* N.

Proof. The lemma is true for $n=m$, from Lemma 3.21. Now let $n<m$. Let $N=N_1\otimes\cdots\otimes N_m$, $V=V_1\otimes\cdots\otimes V_m$,where N_μ acts on V_μ, the dimension of V_μ is q ($1\leqq\mu\leqq m$) and $N_1\simeq\cdots\simeq N_{m-1}\simeq D$ if $q=2$ and $j\neq 3$. Let $M_1=N_1\otimes\cdots$

$\otimes N_n$ act on $W_1 = V_1 \otimes \cdots \otimes V_n$, and let $M_2 = N_{n+1} \otimes \cdots \otimes N_m$ act on $W_2 = V_{n+1} \otimes \cdots \otimes V_m$. Let $U_\mu^* = \mathfrak{N}_{\Gamma L(W_\mu)}(M_\mu)$, $\mu = 1, 2$.

Let $S_n^i = \langle a_1, \ldots, a_n \rangle \subset M_1$, and for $1 \leqq \mu \leqq n < m$ let $N_\mu = \langle a_\mu, b_\mu, \mathfrak{Z}(N) \rangle$ where a_μ and b_μ are $q \times q$ matrices whose entries are qth-roots of 1 in F (this is possible from (3.8) and (3.9), noting that $N_\mu \simeq D$ if $q = 2$ and $j \neq 3$). For each μ, $1 \leqq \mu \leqq n$, there is a base $\{\eta_{\nu,\mu}\}$, $1 \leqq \nu \leqq q$, for V_μ such that a_μ fixes the points $F\eta_{\nu,\mu}$ $(1 \leqq \nu \leqq q)$, and the elements in this base are permuted transitively by b (Lemma 3.21). Hence W_1 has a base $\{\varepsilon_\nu\}$, $1 \leqq \nu \leqq q^n$, such that $F\varepsilon_\nu$ is a fixed point of S_n^i. Moreover, the fixed points of S_n^i in $V = W_1 \otimes W_2$ are distributed in the set of subspaces $\{X_\nu\}$ where $X_\nu = \varepsilon_\nu \otimes W_2$ for $1 \leqq \nu \leqq q^n$; and this set is permuted transitively by $\mathfrak{N}_{U^*}(S_n^i)$. Since S_n^i is conjugate in U^* to every other stabilizer subgroup J of N of length n and type i from Lemma 3.18, it follows that every fixed point of J in V occurs in an orbit with one of the points of X_1.

Let $T_\nu = \{\text{points } x \in X_\nu : N_x = S_n^i\}$ for $1 \leqq \nu \leqq q^n$; i.e., $x \in T_\nu$ if and only if $x = \varepsilon_\nu \otimes y$ for some point $y \in W_2$ such that $(M_2)_y = \mathfrak{Z}(N)$. Since $\mathfrak{N}_{U^*}(S_n^i)$ permutes the set $\{T_\nu\}$ $(1 \leqq \nu \leqq q^n)$ transitively, then the number of orbits under U^* in which points of $\bigcup T_\nu$ occur is equal to the number of orbits in T_1 under $\mathfrak{N}_{U^*}(S_n^i) \cap U_{T_1}^* = U_{T_1}^* = (\mathfrak{N}_{U^*}(S_n^i))_{X_1}$ from Lemma 6.1 below. For let $c \in U^*$ such that $c(x) = x'$, for x and $x' \in T_1$. Then $c \in \mathfrak{N}_{U^*}(S_n^i)$, and since $\mathfrak{N}_{U^*}(S_n^i)$ permutes the set of disjoint subspaces $\{X_\nu\}$, then $c \in U_{X_1}$.

To prove the Lemma 5.5, it is sufficient to prove the following lemma.

5.7 LEMMA. *If* $c \in (\mathfrak{N}(S_n^i))_{X_1}$ *then* $c|X_1 \in U_2^*$.

Proof. With respect to the decomposition $V = X_1 \oplus \cdots \oplus X_{q^n}$, let

$$c = \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix},$$

where $C = c|X_1$ and c is a monomial semilinear matrix in $q \times q$ blocks since $\mathfrak{N}(S_n^i)$ permutes the subspaces $\{X_\nu\}$. Let

$$1 \otimes h = \begin{pmatrix} H & 0 \\ 0 & * \end{pmatrix}, \quad \text{for } h \in M_2.$$

Then $c \in U^*$ implies

$$chc^{-1} = \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix}\begin{pmatrix} H & 0 \\ 0 & * \end{pmatrix}\begin{pmatrix} C^{-1} & 0 \\ 0 & D^{-1} \end{pmatrix} = \begin{pmatrix} CHC^{-1} & 0 \\ 0 & * \end{pmatrix} \in M_1 \otimes M_2.$$

Hence there exists $\mu \in F$ such that $\mu^{-1}CHC^{-1} \in M_2$. Since μ is an entry in a matrix in M_1, then $\mu^q = 1$ (or $\mu^4 = 1$ if $q = 2$ and $j = 3$), so $\mu I \in \mathfrak{Z}(M_2)$ and $CHC^{-1} \in M_2$. Since h was arbitrary in M_2, therefore $C \in U_2^*$ as required.

Note that $\mathfrak{N}(S_n^i)_{X_1} \not\subseteq U_1^* \otimes U_2^*$. For example, let $q > 2$, $m = 3$, $n = 1$, and let $M_1 = M_2 = \langle a, b \rangle$, as in (3.8). Let

$$h_1 = \operatorname{diag}(1, a, a^2, \ldots, a^{q-1}) \quad \text{and} \quad h_2 = \operatorname{diag}(1, b, \ldots, b^{q-1}).$$

Then

$$h_1 : a \otimes 1 \to a \otimes 1, \quad b \otimes 1 \to b \otimes a^{-1}, \quad 1 \otimes a \to 1 \otimes a, \quad 1 \otimes b \to a \otimes b,$$

and

$$h_2: a \otimes 1 \to a \otimes 1, \quad b \otimes 1 \to b \otimes b^{-1}, \quad 1 \otimes a \to a \otimes a, \quad 1 \otimes b \to 1 \otimes b,$$

so $h_1, h_2 \in \mathfrak{N}(S_n^i)_{X_1}$, but $h_1, h_2 \notin U_1^* \otimes U_2^*$.

Also note that if $q=2$ then M_2 must be the same type as N. For example, let $q=2$, $N=N^2(2^m)$, $r=1<m$, and $p^k \equiv 1 \pmod 4$. Then S_1^2 is a stabilizer subgroup of N. It is possible to imbed S_1^2 in $M_1 \simeq Q$, so $M_2 \simeq D \otimes \cdots \otimes D$ has type 1. But Q cannot be represented by matrices with entries ± 1 and 0. Hence, the proof of Lemma 5.7 fails because μ is not necessarily in $\mathfrak{Z}(N)$, so CHC^{-1} is not necessarily in M_2.

Next, let H be a solvable subgroup of U^*. Let $W=N/\mathfrak{Z}(N)$ and $H_1=H/\mathfrak{C}_H(W)$. Then from Lemma 3.2 W is a $2m$-dimensional vector space over $GF(q)$, and H_1 is a solvable irreducible group of linear transformations of W.

5.8 LEMMA. 1. $|H_1| \mid \delta|\mathrm{Aut}_Z(N)|/q^{2m}$, *where* $\delta=1$ *if* $q=2$ *and* $\delta=\hat{k}$ *if* $q>2$.
2. $|H| \mid (k/\delta)(p^k-1)q^{2m}|H_1|$.

Proof. Lemma 4.3.

Let A_1 be a maximal normal abelian subgroup of H_1. We apply the analysis of §2 to H_1 on W, in order to estimate $|H_1|$. Three cases arise. In case 1, A_1 is irreducible, so that $|H_1| \mid 2m(q^{2m}-1)$. In case 2, A_1 is reducible and H_1 is vector space imprimitive relative to some decomposition of W, $W=W_1 \oplus \cdots \oplus W_{r_1}$, where $(H_1)_{W_i}$ is an irreducible group of semilinear transformations on the t_1-dimensional vector space W_i over $GF(q^k)$, $1 \leqq i \leqq r_1$, for $k_1 t_1 r_1 = 2m$. Moreover, H_1 permutes the subspaces $\{W_i\}$ transitively. In this case, $|H_1| \mid r_1! \, |\Gamma L_{t_1}(q^{k_1})|^{r_1}$. In case 3, A_1 is reducible but H_1 is primitive. Let $|A_1|=p^{k_1}-1$, where $k_1 | 2m$, so that W is a t_1-dimensional space over $GF(q^{k_1})$, where $t_1 k_1 = 2m$. If $\mathfrak{C}_{H_1}(A_1)=A_1$ (case 3(a)), then $|H_1| \mid k_1(q^{k_1}-1)$.

If $\mathfrak{C}_{H_1}(A_1) \neq A_1$, let M be a minimal nonabelian normal subgroup of H_1 contained in $\mathfrak{C}_{H_1}(A_1)$. Since H_1 is primitive, either M is irreducible over $GF(q^{k_1})$, or M reduces W to a sum of equivalent and hence faithful, irreducible subspaces. In either case, $M \in \mathfrak{H}$ and M satisfies the condition of Lemma 3.2, for some prime p_1, such that $p_1 | q^{k_1}-1$. Moreover $p_1 | t_1$, and $p_1^3 \mid |H_1|$.

5.9 LEMMA. *Let H be a solvable subgroup of U^*, containing a normal irreducible $\mathfrak{H}$-group $N(q^m)$. Let $H_1=H/\mathfrak{C}(W)$ act irreducibly on $W=N/\mathfrak{Z}(N)$. Then one of the following cases applies.*

I. $|H_1| \mid 2m(q^{2m}-1)$,

II. $|H_1| \mid r_1! \, |\Gamma L_{t_1}(q^{k_1})|^{r_1}$, *for* $k_1 t_1 r_1 = 2m$, *and* $r_1 > 1$,

III. *There exists a prime p_1 such that $p_1 | ((q^{k_1}-1), t_1)$, for $k_1 t_1 = 2m$; and $p_1^3 \mid |H_1|$.*

Note that I *includes cases* 1 *and* 3(a). *Moreover,* $k_1 > 1$ *in* II *and* III *if* $q=2$.

6. **Case A** ($q>2$, $m=1$). In this paragraph and the next, the cases A–D of Corollary 5.4 will be analyzed. In fact, §§6 and 7 furnish the proof for Theorem 5.1.

Let $N=N(q^m)\in\mathfrak{H}$ be an irreducible linear group of length m acting on a vector space V of dimension q^m over the field $F=GF(p^k)$, where $q|p^k-1$. Let $U=\mathfrak{N}_{GL(V)}(N)$ and $U^*=\mathfrak{N}_{\Gamma L(V)}(N)$. Further let $N=N_1\otimes\cdots\otimes N_m$ and $V=V_1\otimes\cdots\otimes V_m$, where $N_i\in\mathfrak{H}$ is an irreducible group of degree q acting on V_i for $1\leqq i\leqq m$. Let $U_i=\mathfrak{N}_{GL(V_i)}(N_i)$, so that $U_1\otimes\cdots\otimes U_m\subseteq U$. Let A be the group of nonzero scalar operators of V, so that $A\simeq F^*$. Let θ be the homomorphism from U^* into $\Gamma L_{2m}(q)$ defined by the action of U^* on $N/\mathfrak{Z}(N)$. Then $\theta(U)\subseteq Sp_{2m}(q)$ and the kernel of θ in U is $\langle N, A\rangle$ from Lemma 4.3. Further, let ψ be the homomorphism from $\Gamma L_{2m}(q)$ onto $P\Gamma L_{2m}(q)$, and let $\rho=\psi\theta$.

The following permutation lemma will be helpful in the subsequent analysis.

6.1 LEMMA. *Let $\mathfrak{G}$ be a permutation group acting on a set S. Let G be a subgroup of $\mathfrak{G}$ which permutes the subset $T\subset S$. Let H be a normal subgroup of $\mathfrak{G}$. For fixed $x\in T$, let $T_x=\{y\in T: H_x=H_y\}$. Finally, let $J=\mathfrak{N}_G(H_x)$. Then:*

1. *the number of orbits in $(T_x)^G$ under G is equal to the number of orbits in T_x under J.*
2. *$|x^G|=|x^J|\cdot[G:J]$, and hence $|T_x^G|=|T_x|[G:J]$. In particular*
3. *if $H=G$, then the number of orbits under G in $(T_x)^G$ is $|T_x|/[J:G_x]$.*

Proof. 1. Let $\{x_1\},\ldots,\{x_n\}$ be the disjoint orbits in T under G containing points of T_x (for fixed x). Let the $x_i\in T_x$. The elements of $\{x_i\}$ in T_x form suborbits under J, for each i, since $J\subset G$. It is sufficient to prove that in each $\{x_i\}$, only one such suborbit exists. I.e., if $y\in\{x_i\}$, $y\in T_x$, show that $y\sim x_i$ under J. Now there exists $g\in G$ such that $g(x_i)=y$, and $H_{x_i}=H_y=H_x$, so $g\in\mathfrak{N}_G(H_x)=J$, as required.

2. $|x^G|=[G:G_x]=[G:J][J:G_x]=|x^J|[G:J]$, since $H\lhd\mathfrak{G}$ implies $G_x\subset J$ and hence $G_x=J_x$.

3. J/G_x acts regularly on T_x.

Case A: $q>2$, $m=1$. Let $q>1$ and $m=1$. The following is a specific representation of U^* (unique up to conjugacy in $\Gamma L(V)$), with respect to a basis $B=\{\varepsilon_1,\ldots,\varepsilon_q\}$ for V. Let $\lambda\in F$ be such that $\lambda^q=1$, and $\lambda\neq 1$. Define a, b, c, d, f, and g to be $q\times q$ matrices acting as left operators on V with respect to the base B, as follows (let a matrix m have entries m_{ij}, $1\leqq i, j\leqq q$; let $\delta_{ij}=1$ if $i\equiv j \pmod q$, otherwise let $\delta_{ij}=0$).

$$a_{ij}=\delta_{ij}\lambda^{j-1};\quad b_{ij}=\delta_{i+1,j};\quad c_{ij}=\lambda\delta_{ij};\quad d_{ij}=\delta_{ij}d_j, \tag{6.2}$$

where $d_j=\lambda^{(j-1)(q+j-1)/2}$ so that $d_i=d_j$ if and only if $i=j$ or $i=q-j+2$, for $1\leqq i, j\leqq q$; $f_{ij}=\lambda^{(i-1)(j-1)}$; $g_{ij}=\delta_{(i-1)t+1,j}$, so that $(g^u)_{ij}=\delta_{(i-1)t^u+1,j}$, where t is a fixed primitive $(q-1)$th-root of unity $(\bmod q)$. Finally, let σ be the semilinear transformation of V defined by $\sigma\colon(x_1,\ldots,x_q)\to(x_1^p,\ldots,x_q^p)$.

From the definitions (6.2), the following relations hold.

$$a^q=b^q=c^q=d^q=I,\quad g^{q-1}=I,\quad f^2=qg^{(q-1)/2}, \tag{6.3}$$

so $f^4=q^2I\in A$; $\sigma^k=1$. Further, $ba=abc$, $dad^{-1}=a$, $dbd^{-1}=a^{-1}bc^{-(q+1)/2}$; gag^{-1}

$=a^t$, $gbg^{-1}=b^{t^{-1}}$; $faf^{-1}=b$, $fbf^{-1}=a^{-1}$; and $\sigma a\sigma^{-1}=a^p$, $\sigma b\sigma^{-1}=b$. In particular, note that if $g^u\neq 1$ for some u, then

$$\mathfrak{N}_U(\langle g^u\rangle)\cap N\subset A, \tag{6.4}$$

and hence $\langle g^u\rangle$ is conjugate to $\langle a^ib^jg^u\rangle$ under N, for $1\leqq i,j\leqq q$.

Let $N=\langle a, b, c\rangle$, where $\langle c\rangle=\mathfrak{Z}(N)\subset A$. With respect to the basis $(10)=\langle a\rangle$ and $(01)=\langle b\rangle$ of N/A, it follows that

$$\theta(d)=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix},\ \theta(f)=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\ \theta(g)=\begin{pmatrix}t & 0\\ 0 & t^{-1}\end{pmatrix} \text{ and } \theta(\sigma)=\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}. \tag{6.5}$$

Hence, $U=\langle a, b, d, f, g, A\rangle$ and $\langle U, \sigma\rangle=U^*$. Since $m=1$, then $Sp_2(q)=SL_2(q)$. Note that $\rho(U^*)=PSL_2(q)$ or $PGL_2(q)$ according as p is or is not a square (mod q), respectively. In addition, $\theta(U^*)$ contains the scalars (mod q) generated by $\{\sqrt{p}, -1\}$, or by $\{p, -1\}$, respectively. Since $g^{q-1}=1$, let $\hat{g}=g^{(q-1)/2}$. Then $\theta(\hat{g})=-1$ is the unique element of order 2 in $SL_2(q)$.

The following information concerning U is helpful:

$$b^idb^{-i}=c^{i(q+1)/2+i(i+1)/2}a^id \quad\text{and}\quad (b^id)^j=c^{\zeta(j)}a^{-ij(j-1)/2}b^{ij}d^j, \tag{6.6}$$

for $1\leqq i, j\leqq q$, where

$$\zeta(j)=-[3j(j-1)i(i-1)+2i^2j(j-1)(2j-1)]/12.$$

Hence (b^id) has order q, except in the case $q=3$ and $i=1$ or 2, in which case (b^id) has order 9. In addition, $g^idg^{-i}=d^{t^{2i}}$, so that $\hat{g}d=d\hat{g}$, (where $\hat{g}=g^{(q-1)/2}$).

6.7 LEMMA. *Let $x\in U$ and $y\in N$ fix a point $v\in V$. Then $\rho(x)$ fixes the projective point $\langle y\rangle$.*

Proof. N is irreducible.

The subgroups $U^*\supset U\supset\langle N, A\rangle\supset A$ are all normal in U^*, so it is natural to ask what splitting occurs in this chain.

6.8 LEMMA. 1. *The group U/A splits over $\langle N, A\rangle/A$, with complement K/A, where $K=\langle d, f, g, A\rangle$. Any two complements of $\langle N, A\rangle/A$ are conjugate.*

2. *$K=\langle d, f, g, A\rangle$ splits over A if and only if $q\equiv -1$ (mod 4) or $p=2$. In fact, let $\bar{K}=\langle d, \varepsilon g, \beta f\rangle$, where $\beta=(\text{trace }(d^{-1}))^{-1}$ and $\varepsilon=\pm 1$ as $q\equiv\pm 1$ (mod 4), respectively. Then $K=\bar{K}A$ and $\bar{K}\cap A=\langle -\varepsilon\rangle$.*

Proof. 1. It is sufficient to note that K normalizes $\hat{g}=g^{(q-1)/2}$ and to use Lemma 4.1. If $\bar{K}$ is another complement of N (mod A), then $\bar{K}/A\simeq SL_2(q)$, and hence $\bar{K}$ contains a normal involution of the form $x\hat{g}$, for $x\in\langle N, A\rangle$, since $\theta(\hat{g})=-I\in SL_2(q)$. Therefore, $\bar{K}=\mathfrak{N}_U(\langle x\hat{g}\rangle)$ is conjugate to K since $\langle x\hat{g}\rangle$ is conjugate to $\langle\hat{g}\rangle$.

A similar proof shows that $\mathfrak{N}_{GL(V)}(N)/A$ splits for $N=N(q^m)\in\mathfrak{H}$, if $q>2$.

2. $SL_2(q)$ can be generated by three elements, S, V, T, subject to the relations $S^q=1$, $V^{-1}SV=S^{t^2}$, $V^{(q-1)/2}=T^2=(ST)^3=(TV)^2=z$, with the extra relation $(S^tTV)^3=z$ when $q\equiv 1$ (mod 4), where $z^2=1$ and $\langle z\rangle$ is the center of $\langle S, V, T\rangle$

[5, p. 95]. Moreover, $\theta(d^{-1})$, $\theta(g^{-1})$ and $\theta(f)$ satisfy these relations for S, V, and T, respectively, with $z=\theta(\hat{g})$. Therefore, $K=\langle d, f, g, A\rangle$ splits over A if and only if there exist elements a_1, a_2, a_3, and a_4 in $GF(p^k)$ such that $S=a_1d^{-1}$, $V=a_2g^{-1}$, $T=a_3f$, and $z=a_4\hat{g}$ satisfy the above relations. However, $gd^{-1}g^{-1}=(d^{-1})^{t^2}$ and $f^2=(fg^{-1})^2=q\hat{g}$. In addition, $(d^{-1}f)^3=\gamma\hat{g}$, so

$$\gamma = [(d^{-1}f)^3]_{1,1} = \sum_{0\leqq i,j\leqq q-1} \lambda^{-(i-j)^2/2} = q\sum_{j=0}^{q-1} \lambda^{-j^2/2} = q\cdot\text{trace}\,(d^{-1}).$$

Similarly, $(d^{-t}fg^{-1})^3=q\cdot\text{trace}\,(d^t)\cdot\hat{g}$. Therefore, $a_1,\ldots,a_4$ must satisfy: $a_1^q=1$, $a_1=a_1^{t^2}$ (and hence $a_1=1$ if $q>3$, from the definition of t), $a_2^{(q-1)/2}=a_3^2q=a_2^2a_3^2q$ $=a_3^3q\cdot\text{trace}\,(d^{-1})=a_4$, and $(a_2a_3)^3q\cdot\text{trace}\,(d^t)=a_4$ if $p^k\equiv 1 \pmod 4$. Hence, a_3 $=(\text{trace}\,(d^{-1}))^{-1}$ and $a_2^2=a_4^2=1$. Moreover by computation

$$(\text{trace}\,(d^t))^2 = \left(\sum_{j=0}^{q-1}\lambda^{-tj^2/2}\right)^2 = \sum_{0\leqq j,k\leqq q-1}\lambda^{-t(j^2+k^2)/2}.$$

From [7, Theorem 64, p. 46], with $\varepsilon=\pm 1$ as $q\equiv\pm 1 \pmod 4$, respectively, the number of solutions (j, k) in $GF(q)$ for the equation $-t(j^2+k^2)/2=x$ is $q-\varepsilon$ or $q+(q-1)\varepsilon$ as $x\neq 0$ or $x=0$, respectively. Thus, $(\text{trace}\,(d^t))^2=q\varepsilon$ (for $0<t<q$), since $(1+\lambda+\cdots+\lambda^{q-1})=0$.

Returning to the a's, it follows that $a_4=\varepsilon$, $a_2^2=1$ and so $a_2=\varepsilon$. Hence for these values of $a_1,\ldots,a_4$, S, V, and T generate $SL_2(q)$ if $q\equiv -1 \pmod 4$, since $z=\varepsilon\hat{q}$ centralizes S, V, and T. However, if $q\equiv 1 \pmod 4$ and $p\neq 2$ then $\varepsilon=1$, and the extra relation $(S^tTV)^3=z$ is not satisfied, since $(a_2a_3)^3q\ \text{tr}\,(d^t)=\text{tr}\,(d^t)/\text{tr}\,(d^{-1})$. The equation $t^2/2=-j^2t/2$ has $q+(q-1)(-1)=1$ solution (namely $t=j=0$) in $GF(q)$ from [7, p. 46], since $-t$ is a nonsquare. It follows that $\text{trace}\,(d^{-1})=-\text{trace}\,(d^t)$. Therefore, K does not split over A if $q\equiv 1 \pmod 4$ and $p\neq 2$ but $\langle S, V, T\rangle \cap A$ $=\langle -1\rangle$.

In the following paragraphs, various stabilizer subgroups of U for points (i.e., one-dimensional suspaces) of V are determined, and the corresponding orbital structure is discussed. In the remainder of §6 and in §7, all groups will be understood to be factor groups (mod A), and group elements will be cosets (mod A). As usual points denote 1-spaces of V.

1. Let $J=\langle a\rangle$, (i.e., $J=\langle a, A\rangle/A$). Then J fixes exactly the points of the base $B=\{\varepsilon_1,\ldots,\varepsilon_q\}$, (i.e., J fixes the 1-spaces $F\varepsilon_1,\ldots,F\varepsilon_q$). Let $J_1=\langle a^ib^j\rangle$. Then J_1 is conjugate to J in U (for J and J_1 correspond to points of the projective line on which $\rho(U)=PSL_2(q)$ operates transitively), and so J_1 fixes exactly q points. Moreover, if $J\neq J_1$, then J and J_1 fix no point in common since $N=\langle J, J_1\rangle$ is irreducible. Hence, there are $q(q+1)$ points which have nontrivial stabilizer subgroups in N. Since b permutes $\{\varepsilon_1,\ldots,\varepsilon_q\}$ transitively, these $q(q+1)$ points lie in one orbit under U. The stabilizer of one such point, say ε_1, is $U_{\varepsilon_1}=\langle a, d, g\rangle$.

2. The fixed points of $\langle d\rangle$ are ε_1 and the points of the $(q-1)/2$ two-dimensional spaces $\langle\varepsilon_i, \varepsilon_{q-i+2}\rangle$, for $i=2, 3,\ldots,(q+1)/2$.

6.9 LEMMA. *Let $J=\langle d, g^u\rangle$, where $u|q-1$ but $u\neq q-1$. Then J fixes only the points ε_1, except in case $u=(q-1)/2$, i.e., $g^u=\hat{g}$. In this case, J fixes the additional $(2, p-1)(q-1)/2$ points $\varepsilon_1 \pm \varepsilon_{q-i+2}$, for $i=2, \ldots, (q+1)/2$.*

Proof. Suppose g^u fixes $v=\nu_1\varepsilon_i+\nu_2\varepsilon_{q-i+2}$, for $\nu_1, \nu_2 \in F$. Since $g^u=(\delta_{(i-1)t^u+1,j})$ $\neq 1$, g^u has no nonzero diagonal terms except the first. Hence it follows that $\nu_1=\pm\nu_2$ and that g^u interchanges the two components of v, i.e., that

$$(g^u)_{i,q-i+2} = \delta_{(i-1)t^u+1,q-i+2} \neq 0 \quad \text{and} \quad (g^u)_{q-i+2,i} = \delta_{(q-i+1)t^u+1,i} \neq 0.$$

These conditions imply that $(i-1)(t^u+1)=0 \pmod q$. Since $i-1\not\equiv 0 \pmod q$, it follows that $t^u\equiv -1 \pmod q$ and hence $u=(q-1)/2$.

6.10 COROLLARY. *Let $K=\langle d, g, f\rangle$. Then K fixes a point of V if and only if $q=3$. If $q=3$, then K fixes exactly the point $v=\varepsilon_2-\varepsilon_3$. Moreover, $K=U_v$ and $|v^U|=9$.*

Proof. If $q>3$, then $g\neq\hat{g}$ and hence $\langle d, g\rangle$ fixes only ε_1. But ε_1 is not fixed by f, and hence not by K. If $q=3$, then $\langle d, g\rangle$ fixes ε_1 and $\varepsilon_2\pm\varepsilon_3$. Of these, f fixes only $v=\varepsilon_2-\varepsilon_3$. Moreover, $K=U_v$, since any subgroup of U which properly contains K also contains N, and N is irreducible.

6.11 COROLLARY. 1. *Let $q>3$. Then the group $\langle d, \hat{g}\rangle$ is the stabilizer subgroup for the points $\varepsilon_i\pm\varepsilon_{q-i+2}$, $2\leqq i\leqq(q+1)/2$. These points occur in $(2, p-1)$ orbits of length $q^2(q^2-1)/2$.*

2. *Let $q=3$. Then the group $\langle d, g\rangle$ is the stabilizer subgroup for the point $\varepsilon_2+\varepsilon_3$ if and only if $p\neq 2$. If $p\neq 2$, then $\varepsilon_2+\varepsilon_3$ occurs in an orbit of length* 36.

Proof. Let $x\in\{\varepsilon_1\pm\varepsilon_{q-i+2}\}$, for $2\leqq i\leqq(q+1)/2$, and let $J=U_x$. Then $J\supseteq\langle d, g\rangle$. Since $\rho(\langle d, g\rangle)$ is the maximal subgroup of $PSL_2(q)$ containing $\rho(d)$, then $\rho(J)=\langle d\rangle$ from Lemma 6.9. Suppose $J\cap N=\langle a^ib^j\rangle$ for some i, j. Then $\langle a^ib^j\rangle=\langle a\rangle$ from (6.5). Therefore, $U_x=\langle d, \hat{g}\rangle$, except in the case $q=3$. In this case, $U_v=K$, for $v=\varepsilon_2-\varepsilon_3$. To complete the proof, note that $\mathfrak{N}_U(\langle d, \hat{g}\rangle)=\langle d, g\rangle$.

3. Next we determine the points x for which $U_x=\langle d\rangle$. We have considered the stabilizer conjugacy classes containing $K=\langle d, f, g\rangle$, $\langle a, d, g\rangle$, and $\langle d, \hat{g}\rangle$. Note that q groups from each of these classes contain $\langle d\rangle$, namely the conjugates under $\langle a\rangle$. The only other possibilities for stabilizer subgroups containing $\langle d\rangle$ are the groups $J=\langle d, a^ib^jg^u\rangle$, for some integers i, j, u, with $u\neq 0$. If $j\neq 0$, then the commutator $[d, (a^ib^jg^u)^{-1}]=a^{jt^{2u}}d^{t^{2u}-1} \pmod A$ implies $a\in J$, so that $J=\langle a, d, g\rangle$. If $j=0$, then J is conjugate to $\langle d, g^u\rangle$ under $\langle a\rangle$, and hence J fixes some point only if $g^u=\hat{g}$.

If $q=3$, then (1) and (2) above account for $3+3(2, p-1)$ fixed points of $\langle d\rangle$, whose stabilizers are conjugate to K, $\langle a, d, g\rangle$, or $\langle d, \hat{g}\rangle$. The remaining $p^k+2-(3+3(2, p-1))=p^k-1-3(2, p-1)$ fixed points of $\langle d\rangle$ must have $\langle d\rangle$ as stabilizer. These points occur in $[p^k-1-3(2, p-1)]/6$ orbits of length 72, since $[\mathfrak{N}_U(\langle d\rangle) : \langle d\rangle]=6$. This proves the first part of the following lemma.

6.12 LEMMA. *The following tables summarize the structure of the orbits under U which contain fixed points of $\langle d\rangle$.*

$q=3$	U_x	$\lvert x^U\rvert$	*number of orbits*
	$K=\langle d,f,g\rangle$	9	1
	$\mathfrak{N}(\langle d\rangle)=\langle a,d,g\rangle$	12	1
	$\langle d,g\rangle$	$36\gamma^*$	γ^*
	$\langle d\rangle$	72	$[p^k-1-3(2,p-1)]/6$

* $\gamma=(2,p-1)-1$, *so* $\gamma=1$ *if* $p\neq 2$, *and* $\gamma=0$ *if* $p=2$.

$q>3$	U_x	$\lvert x^U\rvert$	*number of orbits*
	$\mathfrak{N}(\langle d\rangle)=\langle a,d,g\rangle$	$q(q+1)$	1
	$\langle d,\hat{g}\rangle$	$q^2(q^2-1)/2$	$(2,p-1)$
	$\langle d\rangle$	$q^2(q^2-1)$	$[p^k-1-q(2,p-1)]/2q$

Proof. The proof for $q>3$ is similar to that for $q=3$. As above, the possible choices for U_x which contain d are $\langle d\rangle$, $\langle d,\hat{g}\rangle$, $\langle a,d,g\rangle$, and their conjugates. The groups $\langle d,\hat{g}\rangle$ and $\langle a,d,g\rangle$ are stabilizer groups from 1 and 2. They and their conjugates account for $q+(2,p-1)q(q-1)/2$ of the fixed points of $\langle d\rangle$. The remaining points have $\langle d\rangle$ as stabilizer.

6.13 COROLLARY. 1. *If* $U_x\supsetneq\langle d\rangle$, *then* $x^{U^*}=x^U$.

2. *The points x for which $U_x=\langle d\rangle$ occur in at least $[p^k-1-q(2,p-1)]/2kq$ orbits under U^*.*

Proof. The element σ fixes the points ε_1 and $\varepsilon_i\pm\varepsilon_{q-i+2}$, for $i\leqq 2\leqq(q+1)/2$, for which the stabilizers in U are $\langle a,d,b\rangle$ and $\langle d,\hat{g}\rangle$ (or K if $q=3$), respectively.

Let $v=\varepsilon_2+\nu^i\varepsilon_q$, for ν a primitive root of F, satisfy $U_v=\langle d\rangle$. Then $a^j\colon v\to\varepsilon_2+\nu^i\lambda^{-2j}\varepsilon_q$, $\langle g\rangle/\langle\hat{g}\rangle$ sends v into the $(q-1)/2$ fixed 2-spaces of $\langle d\rangle$, and $\hat{g}\colon v\to\varepsilon_2+\nu^{-1}\varepsilon_q$. Hence the orbits with $\langle d\rangle$ as stabilizer are in one-to-one correspondence with the classes $\{i,-i\}\pmod{(p^k-1)/q}$, for $1\leqq i\leqq[p^k-1-q(2,p-1)]/2q$, under the mapping $\xi\colon(\varepsilon_2+\nu^i\varepsilon_q)\to\{i',-i'\}$, where $i'\equiv i\pmod{(p^k-1)/q}$. The element σ permutes these classes, $\sigma\colon\{i,-i\}\to\{pi,-pi\}\pmod{(p^k-1)/q}$, and σ performs the corresponding permutation of the orbits having $\langle d\rangle$ as stabilizer.

4. Having determined the stabilizers for the fixed points of $\langle d\rangle$ and its conjugates, including $\langle a^id\rangle$ for $1\leqq i\leqq q$, we now investigate the fixed points of the remaining elements, a^ib^jd with $j\neq 0$, of dN.

6.14 LEMMA. *Let $J=\langle bd\rangle$. Then $\mathfrak{N}_U(J)=\langle a,bd,xg^\tau\rangle$, where $\tau=(q-1)/(3,q-1)$ and x is some element in $\langle b\rangle$.*

6.15 COROLLARY. 1. *The subgroups $\langle a^ib^jd\rangle$, for $1\leqq i,j\leqq q$, form $1+(3,q-1)$ conjugacy classes under U, with representatives $\langle d\rangle$, and $\langle b^{t^j\tau}d\rangle$, for $j=1,2,3$.*

2. *Groups* $\langle b^{t^j\tau}d\rangle$ *for* $j=1, 2, 3$, *are conjugate in* U^* (*under* σ), *unless* $3|q-1$ *and* $q|p^{(q-1)/3}-1$, *in which case these groups represent three distinct classes.*

Proof of Lemma 6.14. $\mathfrak{N}_U(J)\subseteq\langle a, b, g, d\rangle$, and $\mathfrak{N}_U(J)\cap N=\langle a\rangle$ from (6.5). Hence $\mathfrak{N}_U(J)=\langle a, bd, xg^\tau\rangle$ for some $x\in\langle b\rangle$ and some integer τ. From the relations satisfied by b, d, and g, $b^ig^j(bd)g^{-j}b^{-i}=b^{i+t^{-j}}d^{t^{2j}}b^{-i}=a^{it^{2j}}b^{t^{-j}}d^{t^{2j}}$. On the other hand, $(bd)^{t^{2j}}=a^{-t^{2j}(t^{2j}-1)/2}b^{t^{2j}}d^{t^{2j}}$, so that $b^ig^j\in\mathfrak{N}_U(J)$, if and only if $3j\equiv 0 \pmod{q-1}$ and $i\equiv -(t^{2j}-1)/2 \pmod q$. Hence in the above description of $\mathfrak{N}_U(J)$, $\tau=(q-1)/(3, q-1)$.

Proof of Corollary 6.15. The subgroups $\langle a^id\rangle$, for $1\leqq i\leqq q$, form one conjugacy class in U, and the remaining subgroups form $(3, q-1)$ classes, as in the proof of Lemma 6.14. If $3|q-1$, then it is easily checked that the groups $\langle b^{t^j\tau}d\rangle$, $j=1, 2, 3$ are not conjugate under $\langle b, g\rangle$, and hence represent distinct classes in U.

2. Exactly as in Lemma 6.14, $b^ig^j\sigma^r\in\mathfrak{N}(J)$ for some i, j and r if and only if $p^r\equiv t^{3u} \pmod q$ for some u. Clearly solutions for i and j exist if $3|r$. If $3|q-1$ and if $p^{(q-1)/3}\equiv 1 \pmod q$, then $b^ig^j\sigma\in\mathfrak{N}(J)$ for some i and j, and hence the three classes represented by $\langle b^{t^j\tau}d\rangle$, $j=1, 2, 3$, are preserved by U^*. Otherwise, these classes collapse to one class under U^*.

6.16 LEMMA. *Let* $J=\langle bd\rangle$. *Then*: 1. J *fixes* q *points, unless* $q=3$ *and* $9\nmid p^k-1$, *in which case* J *fixes no points.*

2. *If* J *has fixed points, then these fixed points lie in one orbit of length* $q^2(q^2-1)/(3, q-1)$ *under* U.

3. *The fixed points of the groups* $\langle b^id\rangle$, $1\leqq i\leqq q$, *occur in the following number of orbits under* U^*:

(i) *no orbits if* $q=3$ *and* $9\nmid p^k-1$;

(ii) *at least* 3 *orbits if* $3|q-1$ *and* $q|p^{(q-1)/3}-1$;

(iii) *otherwise, one orbit.*

Proof. 1. Let $x=\sum_{i=1}^q x_i\varepsilon_i\neq 0$ in V_1 and let $y=bd(x)=\sum_{i=1}^q x_{i+1}d_{i+1}\varepsilon_i$. Then $y=\mu x$ for some μ in F if and only if

$$\mu x_i = x_{i+1}d_{i+1} \quad \text{for } 1\leqq i\leqq q. \tag{6.17}$$

There exist solutions for (6.17), namely

$$x_{i+1} = \mu^i \prod_{j=2}^{i+1} d_j^{-1}x_1 \quad \text{for } 1\leqq i<q, \text{ and } x_1 = 1, \tag{6.18}$$

if and only if $\mu^q=\prod_{j=2}^q d_j$. From (4.2),

$$\prod_{j=2}^{q} d_j = \prod_{j=2}^{(q+1)/2} \lambda^{2(j-1)(q+j-1)/2} = \lambda^r,$$

for $r=q(q^2-1)/24$. If $q\neq 3$, then $r\equiv 0 \pmod q$, and (6.18) defines the q fixed points of $\langle bd\rangle$, for $\mu\in\langle\lambda\rangle$. If $q=3$, then $r\equiv 1 \pmod 3$, and hence (6.18) defines the 0 or

3 fixed points of $\langle bd\rangle$, as $\mu^3=\lambda$ has no solutions, or 3 solutions, respectively, for μ in F.

2. Now suppose $\langle bd\rangle$ has q fixed points, one of which is x. Then U_x is conjugate to $\langle bd, xg^\tau\rangle$. First, $U_x \cap N \subset A$, since $\langle a\rangle$ permutes the q fixed points of $\langle bd\rangle$ transitively, and from Lemma 6.7. Next, $\langle bd\rangle$ is contained in no complement $\bar{K}$ of N; for if so, then $\bar{K}$ is conjugate to $K=\langle d, f, g\rangle$, and hence $\langle bd\rangle$ is conjugate to $\langle d\rangle$, which is false. Finally, $U_x \subseteq \mathfrak{N}(\langle bd\rangle)$ since $\mathfrak{N}(\rho\langle d\rangle)$ is the unique maximal proper subgroup of $PSL_2(q)$ containing $\rho(d)$. Hence U_x is conjugate to $\langle bd, xg^\tau\rangle$ under $\langle a\rangle$. It follows that the fixed points of $\langle bd\rangle$ lie in one orbit of length $q^2(q^2-1)/(3, q-1)$.

3. If $3|q-1$, then $(b^id)^q=1$, for $1\leqq i\leqq q$ from (6.6). Hence each group $\langle b^id\rangle$ is completely reducible, and so fixes at least q points of V. Further, the fixed points of each conjugacy class of these groups contribute at least one orbit under U^*. The number of classes under U^* is determined in Corollary (6.15).

5. Now consider stabilizers of the fixed points of $\langle g\rangle$ and $\langle \hat{g}\rangle$, where $\hat{g}=g^{(q-1)/2}$.

6.19 LEMMA. 1. *The group $\langle g\rangle$ fixes the points of the two-dimensional space $W_1=\langle \varepsilon_1, \varepsilon_2+\cdots+\varepsilon_q\rangle$, and the following additional points: $v=\sum_{i=2}^{q} \nu_i\varepsilon_i$, for $\nu_{t^i+1}=\mu^i$, $1\leqq i\leqq q-1$, where $\mu^{q-1}=1$ and $\mu\neq 1$.*

2. *The group $\langle \hat{g}\rangle$ fixes the points of the $(q+1)/2$-dimensional space*

$$\langle \varepsilon_1, \varepsilon_{i+1}+\varepsilon_{q-i+1} : 1 \leqq i \leqq (q-1)/2\rangle.$$

And if $p\neq 2$, then $\langle \hat{g}\rangle$ fixes the points of the $(q-1)/2$-dimensional subspace

$$\langle \varepsilon_{i+1}-\varepsilon_{q-i+1} : 1 \leqq i \leqq (q-1)/2\rangle.$$

Proof. From the definitions (6.2).

6.20 LEMMA. *The group $\langle f\rangle$ fixes exactly $(2, p-1)$ or 0 of the fixed points of g in $W_1=\langle \varepsilon_1, \varepsilon_2+\cdots+\varepsilon_q\rangle$, as q is or is not a square in F, respectively.*

Proof. Let $x=\nu_1\varepsilon_1+\nu_2\sum_2^q \varepsilon_i$, for ν_1 and $\nu_2\in F$. Then $f: x\to y$, where $y=(\nu_1+(q-1)\nu_2)\varepsilon_1+(\nu_1-\nu_2)\sum_2^q \varepsilon_i$. Since f fixes no points of $\langle a\rangle$ or of $\langle b\rangle$ from (6.5) and Lemma 6.7, then $\nu_2\neq 0$, and $\nu_2\neq\nu_1$. Let $\nu_2=1$. Then f fixes x if and only if $\nu_1/\nu_2=\nu_1=(\nu_1+(q-1))/(\nu_1-1)$, if and only if $\nu_1^2-2\nu_1-(q-1)=0$ in F. If $p=2$, then $\nu_1=0$ is the unique solution. If $p\neq 2$, then from the quadratic formula there exist 2 or 0 solutions as q is or is not, a square in F. If solutions exist, they are $\nu_1=1\pm q^{1/2}$.

6.21 LEMMA. *Let $q=3$. If 3 is a square in F and if $p\neq 2$, then $\langle f\rangle$ is the stabilizer subgroup in U for exactly two points of V and these two points occur in one orbit of length 54. Otherwise, $\langle f\rangle$ is the stabilizer for no point of V.*

Proof. From Corollary 6.10, $\langle f\rangle$ always fixes $x=\varepsilon_2-\varepsilon_3$, if $q=3$, and $U_x=K$. If $p=2$, then f fixes no further points of V.

If $p \neq 2$, then from Lemma 6.20, f fixes 2 or 0 additional points, as 3 is or is not a square in F, respectively. If 3 is a square, let x_1 and x_2 be the two additional fixed points. Then $U_{x_i} \cap N = 1$, for $i = 1$, or 2 from Lemma (6.7). Moreover, $f^2 = g$ implies $U_{x_i} \subsetneq K$, so either $U_{x_i} = \langle f \rangle$, or $|U_{x_i}| = 8$, for $i = 1$ and 2. The latter case is impossible, because $\mathfrak{N}(U_{x_i})/U_{x_i}$ must act nontrivially on the set $\{x_1, x_2\}$. Hence $U_{x_1} = U_{x_2} = \langle f \rangle$. Further, $\mathfrak{N}_K(\langle f \rangle)$ has order 8, and hence interchanges x_1 and x_2. Therefore, x_1 and x_2 occur in one orbit of length 54.

Since $\mathfrak{N}(\langle f \rangle) \cap N \subset A$, $\langle f \rangle$ is conjugate to every subgroup of order 4 in U. Hence, no subgroup of order 8 is a stabilizer subgroup. Therefore, in the case $q = 3$, the only stabilizer subgroups J such that $4 \mid |J|$, are $\langle f \rangle$, K, and their conjugates.

6.22 LEMMA. *Let $q > 11$. If x is fixed by g, then either $U_x = \langle g \rangle$, $U_x = \langle f, g \rangle$, or U_x is conjugate to $\langle a, d, g \rangle$.*

Proof. Since $q > 11$, the maximal subgroups of $PSL_2(q)$ which contain $\rho(g)$ are $\langle f, g \rangle^\rho$ and $\langle d, g \rangle^\rho$. If $q \leqq 11$, then $\rho(g)$ may be contained in subgroups isomorphic to A_4, Σ_4, or A_5, the alternating and symmetric groups.

Hence, in addition to the groups mentioned in the lemma, only groups of the form $J_1 = \langle a^i b^j d, g \rangle$ and $J_2 = \langle a^i b^j f, g \rangle$, for $1 \leqq i, j \leqq q$, need be considered. It is easily checked from (6.2)–(6.6) that either $J_\nu \cap N \neq 1$ and so J_ν is conjugate to $\langle a, d, g \rangle$, for $\nu = 1$ and 2, or that $J_2 = \langle f, g \rangle$.

6.23 LEMMA. *Let $q > 11$. The following table summarizes the orbital structure under U of the fixed points of $\langle g \rangle$ which lie in V_1, the unique two-dimensional subspace of fixed points of g.*

	U_x	$\lvert x^U \rvert$	*number of orbits*
$q > 11$	$\langle a, d, g \rangle$	$q(q+1)$	1
	$\langle f, g \rangle$	$\eta \cdot q^3(q+1)/2$*	$\eta(2, p-1)$*
	$\langle g \rangle$	$q^3(q+1)$	$[p^k - 1 - \eta(2, p-1)]/2$

* $\eta = 1$ *if q is a square in F, $\eta = 0$ otherwise.*

6.24 COROLLARY. 1. *Let $\langle f, g \rangle$ be a stabilizer subgroup and $p \neq 2$. Then σ combines the 2 orbits for which $\langle f, g \rangle$ is the stabilizer into one orbit, if and only if $\sqrt{q} \notin GF(p)$.*

2. *There exist at least $[p^k - 1 - \eta(2, p-1)]/2k$ orbits in U^* with stabilizer $\langle g \rangle$.*

Proof of Lemma 6.23. Of the fixed points of g, one each is fixed by $\langle a \rangle$ and $\langle b \rangle$, and $\eta(2, p-1)$ are fixed by f. The remaining fixed points are permuted in orbits of length 2 by $\mathfrak{N}_U(\langle g \rangle) = \langle g, f \rangle$.

Proof of Corollary 6.24. 1. Let $x_i = (1 + (-1)^i q^{1/2})\varepsilon_1 + \sum_{j=2}^{q} \varepsilon_j$, for $i = 1$ and 2, be the points fixed by $\langle f, g \rangle$, as in Lemma 6.20. Then $(1 + (-1)^i q^{1/2})^p = 1 + (-1)^i q^{p/2}$, and $q^{p/2} = \pm q^{1/2}$ according as $q^{1/2} \in GF(p)$ or $q^{1/2} \notin GF(p)$, respectively. Hence σ fixes or interchanges x_1 and x_2, respectively, in these two cases.

2. At worst, σ permutes the orbits with stabilizer $\langle g\rangle$ in cycles of length k.

Next, if $q>3$, Lemma 6.1 is used to estimate the number of orbits among the fixed points of $\langle \hat{g}\rangle$ which have not been accounted for above. In Lemma 6.1, let $G=K$, let $H=\langle N, \hat{g}\rangle$, and let T be the set of fixed points of $\hat{g}$. Let $|T|=r_1$. Then

$$r_1 = \frac{p^{k(q+1)/2}-1}{p^k-1} + \gamma\frac{p^{k(q-1)/2}-1}{p^k-1}, \tag{6.25}$$

from Lemma 6.19, where $\gamma=(2, p-1)-1$. Of these r_1 points, $r_2=q+1$ are fixed by the $q+1$ conjugates of $\langle a\rangle$, and $r_3=(2, p-1)(q^2-1)/2$ additional points are fixed by the $q+1$ conjugates (in K) of $\langle d\rangle$. The fixed points of $\langle b^i d\rangle$ are not fixed by g, $1\leqq i\leqq q$. However, if $q>11$ then Lemmas 6.22 and 6.23 account for the p^k-1 additional points in the two-dimensional space W_1 of fixed points of g. Thus the $q(q+1)/2$ conjugates of $\langle g\rangle$ in K account for $r_4=(p^k-1)q(q+1)/2$ additional points. Thus r fixed points of $\langle \hat{g}\rangle$ have not been accounted for, where $r=r_1-(r_2+r_3)$ if $3<q\leqq 11$, and $r=r_1-(r_2+r_3+r_4)$ if $q>11$.

6.26 LEMMA. *Let $q>3$. Then the r fixed points of $\hat{g}$ which have not been considered in the previous lemmas, occur in at least*

$$\frac{2p^{k(q-1)/2}}{kq(q^2-1)} > 2p^{k(q-9)/2} > 2q^{k(q-9)/2}$$

orbits under U^*.

Proof. If x is one of the r remaining fixed points of $\langle \hat{g}\rangle$, then $U_x\subseteq K$. For otherwise, $U_x\cap N\neq 1$, and x is one of the r_2 excluded points. Hence, the number of orbits in which these r points occur under U is determined by K. Since at least $\hat{g}$ fixes each point, it follows that these points occur in at least $2r/|K|=2r/q(q^2-1)$ orbits under U, and at least $2r/kq(q^2-1)$ orbits under U^*. It is now sufficient to show that:

$$p^{k(q-3)/2} \geqq r_2+r_3+r_4 \quad \text{if } q > 11, \tag{6.27}$$

or

$$p^{k(q-3)/2} \geqq r_2+r_3 \quad \text{if } 3 < q \leqq 11. \tag{6.28}$$

For $q>11$, $r_2+r_3+r_4\leqq(q+1)+(q^2-1)+(p^k-1)q(q+1)/2=q(q+1)(p^k+1)/2$ $<p^{3k}$. Since $q>11$, $p^{k(q-3)/2}>p^{3k}$, so (6.27) is proved.

If $3<q\leqq 11$, then $r_2+r_3\leqq q(q+1)$; moreover, $p^{k(q-3)/2}\geqq q(q+1)$, and hence (6.28) is proved, if $q=7$ or 11. If $q=5$, then $r_2+r_3=6+(2, p-1)12$, and $p^{k(q-3)/2}=p^k$. In this case, $p^k>16$ implies (6.28), but (6.28) is false for $p^k=11$ or 16. However, the lemma is still true even if (6.28) is false, as follows.

If $q=5$ and $p^k=11$ or 16, then the lemma states that the r remaining fixed points of $\langle \hat{g}\rangle$ occur in at least 3 or 2 orbits, respectively, under U^*. The original estimate of at least $2r/kq(q^2-1)$ orbits is sufficient to prove the lemma if $p^k=16$, but not if $p^k=11$. If $p^k=11$, then since 5 is a square (mod 11), Lemma 6.20 implies that

there exist three fixed points of $\langle g\rangle$ in V_1, x_i for $i=1, 2, 3$, such that $\langle f, g\rangle \subseteq U_{x_1} \cap U_{x_2}$, but $\langle f, g\rangle \nsubseteq U_{x_3}$, and such that $U_{x_i} \cap N \subset A$ $(i=1, 2, 3)$. This last fact implies that $U_{x_i}=K_{x_i}$ $(i=1, 2, 3)$, since $K=\mathfrak{N}_U(\langle \hat{g}\rangle)$.

Suppose that K_{x_1} is isomorphic to K_{x_3}. Then K_{x_3} contains a subgroup J of order 8 which contains $\langle g\rangle$, and hence $J=\langle f, g\rangle=\mathfrak{N}_U(\langle g\rangle)$, which is false. Therefore, x_1 and x_3, and similarly x_2 and x_3, occur in distinct orbits. Finally, suppose x_1 and x_2 occur in the same orbit. Since $\langle f, g\rangle \subset K_{x_1}$, then $K_{x_1}=K_{x_2}$ and $|K_{x_1}|=8$ or 24. In either case, $\mathfrak{N}_U(K_{x_1})=K_{x_1}$, yet $\mathfrak{N}(K_{x_1})$ must interchange x_1 and x_2, which is impossible. Therefore, x_1, x_2, and x_3 occur in three distinct orbits under U.

6. Finally, let us consider the points which are fixed by none of the stabilizer subgroups discussed above.

6.29 LEMMA. *Let $q>3$. Then the s points of V which are fixed by none of the groups $\langle a\rangle$, $\langle d\rangle$, $\langle bd\rangle$, $\langle \hat{g}\rangle$ or their conjugates occur in at least*

$$p^{k(q-1)}/kq^5 > p^{k(q-7)} > q^{q-7} \tag{6.30}$$

orbits under U^*, except in the case $q=5$ and $p^k=11$. In this case, the s points of V form at least 4 orbits under U^*.

Proof. Let $s=(p^{kq}-1)/(p^k-1)-s_1$, where s_1 is the number of points fixed by $\langle a\rangle$, $\langle bd\rangle$, $\langle \hat{g}\rangle$, and their conjugates. From Lemma 6.1, these s_1 points consist of the following: (1) $q(q+1)$ points with stabilizer conjugate to $\langle a, d, g\rangle$; (2) $r_1-(q+1)$ points fixed by $\langle \hat{g}\rangle$ but not by any element of N (where r_1 is the number of points fixed by $\hat{g}$, as in Lemma 6.26); hence $q^2(r_1-(q+1))$ points in addition to those of (1), fixed by one of the q^2 conjugates of $\langle \hat{g}\rangle$; (3) similarly,

$$[p^k-1-q(2, p-1)]q(q^2-1)/2$$

points having as stabilizer one of the $q(q+1)$ conjugates of $\langle d\rangle$ (see Lemma 6.12); (4) finally, $q^2(q^2-1)/(3, q-1)$ points with stabilizer conjugate to $\langle bd\rangle$.

Hence

$$\begin{aligned} s_1 &= q(q+1)+q^2(r_1-(q+1))+[p^k-1-q(2, p-1)]q(q^2-1)/2 \\ &\quad +q^2(q^2-1)/(3, q-1) \leqq q(q^2-1)[p^k+q-3]/2+q^2r_1 \leqq p^{4k}+q^2r_1. \end{aligned} \tag{6.31}$$

First assume $q\geqq 7$. Then (6.31) and (6.25) imply

$$\begin{aligned} s &= (p^{kq}-1)/(p^k-1)-s_1 \\ &\geqq p^{k(q-1)}+p^{k(q-1)/2}(p^{k(q-3)/2}-q^2) \\ &\quad +\left(\frac{p^{k(q-1)/2}-1}{(p^k-1)}\right)(p^{k(q-3)/2}-q^2(2, p-1))-p^{4k} \\ &= p^{k(q-1)}-p^{4k}+\sum_{i=0}^{(q-1)/2} a_i p^{ki}, \end{aligned} \tag{6.32}$$

where

$$a_{(q-1)/2} = p^{k(q-3)/2}-q^2 \quad \text{and} \quad a_j = p^{k(q-3)/2}-q^2(2, p-1),$$

for $0 \leqq j < (q-1)/2$. Since $|U^*| = kq^3(q^2-1) < kq^5$, in order to prove (6.30), it is sufficient to show that $s \geqq p^{k(q-1)}$. From (6.32), it is sufficient to prove that $a_i \geqq 0$, for $0 \leqq i \leqq (q-1)/2$, and that $a_3 \geqq p^k$ (this takes care of the term $(-p^{4k})$). Since $a_{(q-1)/2} \geqq a_0$, and $a_j = a_0$ for $0 \leqq j < (q-1)/2$, it is sufficient to prove that $a_0 - p^k \geqq 0$, i.e., that

$$p^{k(q-3)/2} - q^2(2, p-1) - p^k \geqq 0. \tag{6.33}$$

This is clear for $q > 7$, since $q < p^k$. If $q = 7$, first let $p^k = 8$. Then (6.33) becomes: $8^2 - 7^2 - 8 \geqq 0$. Next, if $p^k \neq 8$, then $p^k > 4q$, and (6.33) becomes: $p^k(p^k-1) - q^2(2, p-1) \geqq 16q^2 - 2q^2 > 0$ as required.

Finally, let $q = 5$. Returning to (6.31), $s_1 \leqq 60(p^k+2) + 25(p^{2k} + (2, p-1)(p^k+1)) \leqq 25p^{2k} + 110p^k + 170$. It is easily checked that $s \geqq p^{4k}$ for $p^k \geqq 31$, as required. If $p^k = 11$, then $s = 12{,}000$ and $s/kq^3(q^2-1) = 4$. If $p^k = 16$, then $s = (16^5 - 1)/(16-1) - s_1 \geqq 15 \cdot 16^3$. Hence, $s/kq^3(q^2-1) = s/4 \cdot 5^3 \cdot 24 \geqq 15 \cdot 16^3/15 \cdot 16 \cdot 50 = 256/50 > 5$, as required.

6.34 THEOREM. *Let $q = 3$, $m = 1$. The following table summarizes the orbital structure under U.*

$p = 2$

Stabilizer	*Number of Orbits*	*Length of orbits*
$\langle a, d, g \rangle$	1	12
$K = \langle g, d, f \rangle$	1	9
$\langle d \rangle$	$(p^k - 4)/6$	72
$\langle bd \rangle$	ν^*	$72\nu^*$
$\langle g \rangle$	$(p^k - 4)/12$	108
1	$(p^{2k} - 20p^k + 64 - 72\nu)/216$	216

* $\nu = 1$ *if* $9 \mid p^k - 1$, $\nu = 0$ *if* $9 \nmid p^k - 1$.

$p \neq 2$

Stabilizer	*Number of Orbits*	*Length of orbits*
$\langle a, d, g \rangle$	1	12
$K = \langle d, g, f \rangle$	1	9
$\langle g, d \rangle$	1	36
$\langle d \rangle$	$(p^k - 7)/6$	72
$\langle bd \rangle$	ν^*	$72\nu^*$
$\langle f \rangle$	τ^{**}	$54\tau^{**}$
$\langle g \rangle$	$(p^k - 7 - 6\tau)/12$	108
1	$(p^{2k} - 20p^k + 91 - 72\nu)/216$	216

* $\nu = 1$ *if* $9 \mid p^k - 1$, $\nu = 0$ *if* $9 \nmid p^k - 1$; **$\tau = 1$ *or* 0 *as* 3 *is or is not a square in* F, *respectively.*

Proof. Since $q=3$, then $g=\hat{g}$. The information about the stabilizers $\langle a, d, g\rangle$, $K=\langle d, g, f\rangle$, $\langle d, g\rangle$, $\langle d\rangle$, $\langle bd\rangle$, and $\langle f\rangle$ comes from Lemmas 6.12, 6.16, and 6.21. As in the proof of Lemma 6.26, of the $p^k+(2, p-1)$ fixed points of $\langle g\rangle$, $q+1=4$ have stabilizers conjugate (in K) to $\langle a, d, g\rangle$; similarly, 1 point for K, $4((2, p-1)-1)$ points for $\langle d, g\rangle$, and 6τ points for $\langle f\rangle$ (if $p\neq 2$). From the proof of Lemma 6.21, no subgroup of U of order 8 is a stabilizer subgroup, since $q=3$. Hence the remaining $(p^k-1-3(2, p-1)-6\tau)$ fixed points of $\langle g\rangle$ have $\langle g\rangle$ as stabilizer. These points are permuted in orbits of length 12 by $K=\mathfrak{N}(\langle g\rangle)$. Finally, the remaining points of V have stabilizer 1, and occur in orbits of length $|U|=216$.

Incidentally, if $p\neq 2$, then $\tau=1$ if and only if either k is even or $p\equiv 1$ or 11 (mod 12) (e.g., [16, (5-4), p. 69]).

6.35 COROLLARY. *Let $q=3$ and $m=1$. The following table summarizes the orbital structure of U^*, for $p^k\leqq 67$. The table includes all cases for which U^* has less than 20 orbits.*

$q = 3, m = 1.$

p^k	4	7	13	16	19	25	31	37	43	49	61	64	67
number of orbits under $U^*(U)$	2	3	5	4(5)	7	8(9)	11	15	17	15*(21)	29	11*(31)	33

* *indicates the lower estimates for the number of orbits under U^*.*

Proof. The number of orbits under U and U^* differ in case $k>1$, due to the action of σ. The figures in the table are exact, except for $p^k=49$ and 64, in which case the estimates for $r^*(U^*)$ are calculated as follows. E.g., if $p^k=64$, then the orbital structure under U is as follows:

number of orbits	1	1	10	1	5	13	*total* 31
stabilizer	$\langle a, d, g\rangle$	K	$\langle d\rangle$	$\langle bd\rangle$	$\langle g\rangle$	1	

Since $k=6$, the points with stabilizer $\langle d\rangle$, in U occur in at least 3 orbits under U^* (the smallest partition of 10 into a sum of terms each of which divides 6 has 3 terms). Similarly, the points with stabilizer $\langle g\rangle$ or 1 in U occur in at least 2 orbits or 3 orbits under U^*, respectively. Hence, U^* has at least 11 orbits.

Finally, if $p^k>67$, the number of orbits under U^* is at least

$$\frac{p^{2k}}{2^3\cdot 3^3\cdot k}\geqq\frac{p^k}{k}\cdot\frac{p^k}{2^3\cdot 3^3}.$$

Since $3|(p^k-1)$ and $p^k>64$, then $p^k/k\geqq 2^8/8=2^5$; hence, $p^{2k}/3^3\cdot 8\cdot k\geqq 4p^k/3^3$. Moreover, $4p^k/3^3>20$ if $p^k>3^3\cdot 5=135$. If $67<p^k<135$ and $3|p^k-1$, then $k=1$. In this case, $r^*(U^*)>p^{2k}/2^3\cdot 3^3>20$, since $p^k\geqq 73$.

6.36 THEOREM. *Let $q>3$ and $m=1$ and let H be a solvable subgroup of U^*. The following table lists lower estimates for $r^*(U^*)$ and $r^*(H)$, in the cases $q=5$ and $p^k=11$ or 16, and $q=7$ and $p^k=8$. In all other cases $r^*(U^*)\geqq 200$ and $r^*(H)\geqq 600$.*

Case	$q=5$, $p^k=11$	$q=5$, $p^k=16$	$q=7$, $p^k=8$	*all other cases*
$r^*(U^*)\geqq$	12	12	11	200
$r^*(H)\geqq$	19	20	26	600

Proof. The information in the special cases for U^* follow from Lemmas 6.12, 6.16, 6.26, and 6.29. In these cases, by the estimate of Lemma 6.29, there exist at least $p^k(q-1)/kq^5$ orbits under U^*. For $q\geqq 11$, $p^{k(q-1)}/kq^5>q^4>10^4$. For $q=7$ and $p^k\geqq 29$, $p^{k(q-1)}/kq^5\geqq p^{5k}/7^5>4^5=2^{10}$. Finally if $q=5$, let $p^k\geqq 31$ but $p^k\neq 81$. Then $p^k/k\geqq$ minimum $(2^8/8, 31/1)=31$, and $p^{k(q-1)}/kq^5>31^4/5^5>(30/5)^3=216$. If $p^k=81$, then $p^{k(q-1)}/kq^5>80^4/4\cdot 5^5=2^{14}/5>2^{11}$.

To estimate $r^*(H)$, we refine the estimates of $r^*(U^*)$ contained in Lemmas 6.12, 6.16, 6.26, and 6.29. As above, Lemmas 6.12 and 6.16 account for at least 4, 4, 3 orbits in the estimate of $r^*(H)$ for the three special cases of the table, respectively. Next replace the estimate of Lemma 6.29, $s/k\cdot q^3(q^2-1)$, by the estimate $s/kq^2|H_1|$, where

I: $|H_1|\mid 2(q^2-1)$, II: $|H_1|\mid 2(q-1)^2$, III: $|H_1|\mid 48$, from Lemma 5.8 (in case III, $M\cong Q$, the group of quaternions, and $H_1\subseteq \mathfrak{N}_{GL_2(q)}(Q)$). Hence, $|H_1|\leqq 2(q^2-1)$. For the 3 cases in the table, $s=12{,}000$, $s\geqq 15\cdot 16^3$, and $s\geqq 8^6$, respectively, and $s/2kq^2(q^2-1)\geqq 10$, 13, 19, respectively.

A similar improvement results from replacing the estimate $2r/|K|$ of Lemma 6.26 by $2r/|H_1|\geqq r/k(q^2-1)$ (note that $\hat{g}\in H_1$ if H_1 is maximal, hence the extra factor 2). For the 3 cases of the table, $r_1=145$, 273, 585; $r_2=6$, 6, 8; $r_3=24$, 12, 24; $r=115$, 255, 553; and hence the r points occur in at least 5, 3, 4 orbits, respectively.

Finally, the entries in the table are the sums of the above estimates.

For the remaining cases, not listed in the table, $r^*(H)\geqq p^{k(q-1)}/2kq^4$ implies $r^*(H)\geqq 600$.

6.37 THEOREM. *Let $q>2$ and $m=1$, and let H be a solvable subgroup of U^*. Then $r^*(U^*)\leqq 10$ only if $q=3$ and $p^k\leqq 25$; and $r^*(H)\leqq 20$ only if $q=3$ and $p^k\leqq 64$, or $q=5$ and $p^k\leqq 16$.*

7. **Case B** ($q=3$, $m=2$). Let $q=3$, and $m=2$, so that $N=N(3^2)$, acting on V of dimension 9 over F. Let $V=V_1\otimes V_2$ and let B_i be a basis for V_i ($i=1,2$), where $B_1=\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ and $B_2=\{\eta_1, \eta_2, \eta_3\}$. Further, let $B=\{\varepsilon_i\otimes\eta_j\}$, $1\leqq i,j\leqq 3$, be a basis for V. Let $N=N_1\otimes N_2$, where N_i is represented on V_i with respect to B_i by $N_i=\langle a, b, c\rangle$, as defined in (6.2) above, for $i=1, 2$. Similarly, let $U_i=\langle N_i, d, f, g\rangle$, $i=1, 2$. For $x\in\langle a, b, c, d, f, g\rangle$, let $x_1=x\otimes 1$ and $x_2=1\otimes x$ in $U=\mathfrak{N}_{GL(V)}(N)$. Let $g^*=g_1\cdot g_2=g\otimes g$, recalling that $g=\hat{g}$ since $q=3$. To simplify the notation,

we drop the * and denote g^* simply by g. Finally, let $L=\langle N, g\rangle$. We continue to assume that the groups under discussion are factor groups (mod A), and we neglect the distinction between a point $v=F\varepsilon$ in V and the generating element ε of V.

If $x\in N$, then $gxg^{-1}=x^{-1}$ (mod A), so that $\theta(g)=-1$ in $Sp(4, 3)$. Hence, $L=\langle N, g\rangle$ is normal in U, and $\langle g\rangle$ is normal in $U/N\cong Sp(4, 3)$. Let $K=\mathfrak{N}_U(\langle g\rangle)$. Then $K\cap N=1$ (mod A) and hence K is a complement for N in U (mod A), so that $K\simeq Sp(4, 3)$. In this section, Lemma 6.1 is applied to L in order to exhibit at least four orbits which have nontrivial stabilizers in L.

7.1 LEMMA. *The fixed points of g comprise the five-dimensional space (with respect to B) spanned by*

$$(100)\otimes(100),\quad (100)\otimes(011),\quad (011)\otimes(100),\quad (010)\otimes(010)+(001)\otimes(001),$$
$$(010)\otimes(001)+(001)\otimes(010);$$

and, if $p\neq 2$, the four-dimensional space spanned by

$$(100)\otimes(01-1),\quad (01-1)\otimes(100),\quad (010)\otimes(010)-(001)\otimes(001),$$
$$(010)\otimes(001)-(001)\otimes(010).$$

7.2 LEMMA. (1) *There exists one point, $x=(100)\otimes(100)$, in V such that $L_x=\langle R_2, g\rangle$, for $R_2=\langle a_1, a_2\rangle$.*

(2) *There exist $(p^k-4+(2, p-1))$ points x in V such that $L_x=\langle R_1, g\rangle$, for $R_1=\langle a_1\rangle$. These points occur in $s-1$ orbits under U, where s is the number of orbits in V_2 among the fixed points of g_2 under U_2.*

(3) *Let $v=(01-1)\otimes(01-1)\in V$. Then $L_v=\langle g\rangle$, and $|v^K|=45$, for $K=\mathfrak{N}_U(\langle g\rangle)$.*

(4) *There exist points y such that $L_y=\langle g\rangle$ and $y\notin v^L$, for v as defined in* (3).

(5) *The points x in V such that $L_x\subseteq N$, form at least $p^{8k}/3^{14}\cdot k$ orbits under U^*. If $p^k=4$, these points form at least 2 orbits under U^*.*

Proof. (1) $R_2=\langle a_1, a_2\rangle$ fixes the points $\varepsilon_i\otimes\eta_j$, $1\leqq i, j\leqq 3$. Of these, g fixes only $\varepsilon_1\otimes\eta_1$.

(2) Let $R_1=\langle a_1\rangle$, and let $S=\{x\in V : L_x=\langle R_1, g\rangle\}$. Then $x\in S$ if and only if $x=(100)\otimes x_2$, for $x_2\in V_2$ such that $\langle N_2, g_2\rangle_{x_2}=\langle g_2\rangle$. From Lemma 6.1, the number of orbits in S^U under U is equal to the number of orbits in S under $\mathfrak{N}_U(\langle R_1, g\rangle)$. By Lemma 5.6, this number is equal to the number of orbits in S under $\mathfrak{N}_{U_2}(\langle g_2\rangle)$. Finally, this number is equal to $s-1$, by the definition of s (the remaining orbit in V_2 of points fixed by g_2 is counted in (1)). Moreover, $|S|=p^k+(2, p-1)-4$.

(3) Recalling that $(01-1)$ has stabilizer $K_i=\langle d_i, f_i, g_i\rangle$ in U_i $(i=1, 2)$, (Corollary 6.10), it follows that $\langle d_1, d_2, f_1, f_2, g_1, g_2, e\rangle\subset K_v$, for e defined by $e: \varepsilon_i\otimes\eta_j\to\varepsilon_j\otimes\eta_i$, $1\leqq i, j\leqq 3$. Hence, $2^7\cdot 3^2 \mid |K_v|$ and so $|v^K|=|K|/|K_v|$ divides $3^2\cdot 5$, since $|Sp(4, 3)|=2^7\cdot 3^4\cdot 5$. The group $\langle h_1, h_2, d_1, d_2\rangle$ is a Sylow 3-subgroup of K (for h_1 and h_2 defined following Lemma 5.7). For $h_2h_1=d_1^2h_1h_2$ since $q=3$, so $\langle h_1, h_2\rangle$ has order 27 and contains d_1; moreover, $\langle h_1, h_2\rangle$ is normal under d_2. It is easily checked that

$v^{\langle h_1,h_2\rangle}$ consists of 9 distinct vectors, each with 0 for the first three coordinates (recall $v=(000\ 01-1\ 0-11)$). For example, $h_2v=(000\ 1-10\ 10-1)$. Next, $f_1(h_2v)=-(211\ 1\lambda\lambda^2\ 1\lambda^2\lambda)$. It follows that $(f_1h_2v)^{\langle h_1,h_2\rangle}$ is a set of 9 distinct vectors, such that $v^{\langle h_1,h_2\rangle}\cap(f_1h_2v)^{\langle h_1,h_2\rangle}=\varnothing$ (because $|(1\lambda\lambda^2)^{\langle a,b,c\rangle}|=9$). Hence, $|v^K|\geqq 18$, so $|v^K|=45$. Moreover $L_v=\langle g\rangle$, since no element of N_1 fixes $(01-1)$.

(4) Let $T=\{x\in V : g\in U_x\}$. Apply Lemma 6.1 with $G=K$, and $H=N$ in order to count the points of T accounted for in (1)–(3).

(i) Let $x=(100)\otimes(100)$. Then $|x^K|=|x^J|\cdot[K:J]$, where $J=\mathfrak{N}_K(R_2)=\mathfrak{N}_U(\langle R_2,g\rangle)$. But $|x^J|=1$ from (1); and since $K\cong U/N$, it follows that $[K:J]=C_{22}=2^3\cdot 5$, from Lemma 3.20.

(ii) Similarly, the $(p^k-4+(2,p-1))$ points $x\in T$ for which $L_x=\langle R_1,g\rangle$ contribute $C_{12}(p^k-4+(2,p-1))$ points under K, where $C_{12}=2^3\cdot 5$.

Therefore, the orbits discussed in (1)–(3) account for

$$2^3\cdot 5+2^3\cdot 5(p^k-4+(2,p-1))+3^2\cdot 5$$

points of T under K. Since

$$|T|=\frac{p^{5k}-1}{p^k-1}+[(2,p-1)-1]\left(\frac{p^{4k}-1}{p^k-1}\right)$$

from Lemma 7.1, it is easy to check that there exist points $y\in T$ not contained in the orbits of (1)–(3). Moreover, since $K=U/N$ and from Lemma 3.18, it follows that $L_y=\langle g\rangle$, for these points y.

(5) The number of points $x\in V$ such that $L_x\subset N$ is

$$(p^{9k}-1)/(p^k-1)-|T^U|.$$

We determine $|T^U|$ by applying Lemma 6.1 to the set T with $G=U$ and $H=L$. Thus each point $x\in T$ with $L_x=\langle R_2,g\rangle$ accounts for $[U:J]$ points in T^U, where $J=\mathfrak{N}_U(L_x)$. In this case, $J=\mathfrak{N}_K(R_2)\cdot R_2$ is a semidirect product, and hence $[U:J]=C_{22}[N:R_2]$. Similarly, T^U consists of $9\cdot 40$ points from (1),

$$27\cdot 40\cdot(p^k-4+(2,p-1))$$

points from (2), and

$$81\cdot[p^{4k}+(2,p-1)(p^{4k}-1)/(p^k-1)-40p^k+120-40(2,p-1)]$$

points from (3) and (4).

Let $p^k>4$. Since $(2,p-1)(p^{4k}-1)/(p^k-1)<2p^{4k}$, it follows that $|T^U|<3^5p^{4k}$, and hence

$$(p^{9k}-1)/(p^k-1)-|T^U|\ >\ p^{8k}+p^{4k}(p^{4k}-1)/(p^k-1)-3^5>p^{8k}.$$

Therefore, there exist at least p^{8k} remaining points x, distributed in at least $p^{8k}/k\cdot 3^8(3^2-1)(3^4-1)>p^{8k}/k\cdot 3^{14}$ orbits under U^*. If $p^k=4$, then $(p^{9k}-1)/(p^k-1)-|T^U|=2^5\cdot 3^4\cdot 5^2$. Since $|U^*|/(p^k-1)=2^8\cdot 3^8\cdot 5$ for $p^k=4$ $(k=2)$, it follows that $2^5\cdot 3^4\cdot 5^2\nmid|U^*|$, so the points of (5) occur in at least 2 orbits, as required.

7.3 COROLLARY. *Let $q=3$ and $m=2$; let H be a solvable subgroup of U^*. The following table lists lower bounds for $r^*(U^*)$ and $r^*(H)$ for $p^k=4$ and 7. For $p^k>7$, $r^*(U^*)\geqq 100$.*

Case	$p^k = 4$	$p^k = 7$	$p^k > 7$
$r^*(U^*) \geqq$	6	7	100
$r^*(H) \geqq$	9	67	

Proof. The orbits of parts (1)–(5) of the lemma are all distinct under U^*. For example, the orbits of (1), (2), and (3) are distinct, since their stabilizer subgroups in L have distinct orders and since $L \triangleleft U^*$. The orbits of (4) and (5) are distinct under U by construction. Moreover, since $\sigma(v)=v$, for v of (4), $v^U=v^{U^*}$, so v^{U^*} is distinct from the orbits of (5).

If $p^k=4$, then $s=2$ in part (2), from Theorem 6.34, and hence (1)–(5) prove the existence of at least 6 orbits under U^*. If $p^k=7$ then $s=3$, so that (1)–(4) account for at least 5 orbits. Finally, from (5), $7^8/3^{14} > 7^8/28^4 \cdot 3^2 = 7^4/2^8 \cdot 3^2 > 2^8 \cdot 3^2/2^8 \cdot 3^2 = 1$, implies the existence of at least 2 more orbits. Hence U^* has at least 7 orbits in V. If $p^k>7$, then $r^*(U^*)\geqq 100$ from Corollary 5.3.

Next, by applying to H the various cases of Lemma 5.8, one can see that, in each case, either $|H_1| \mid 2^7 \cdot 3^2 \cdot \hat{k}$, or $|H_1| \mid 2^7 \cdot 5 \cdot \hat{k}$, since $\delta=\hat{k}$. For example, in case III, $p_1=2$ and $t_1=2$ or 4. If $t_1=4$, then W is four-dimensional over $GF(3)$, and M, a minimal, nonabelian normal subgroup of H_1, has order 2^{2n} for $n=1$ or 2. If $n=1$, then $M \cong Q$, and M acts reducibly on W, so that $|H_1| \mid 48 \cdot |GL_2(3)| = 2^8 \cdot 3^2$, whether H_1 is primitive or imprimitive on W. However, $|H_1| \mid \hat{k}|\mathrm{Aut}_Z(N)|/q^{2m}$ implies $|H_1| \mid 2^7 \cdot 3^4 \cdot 5\hat{k}$; so if $n=1$, then $|H_1| \mid 2^7 \cdot 3^2 \cdot \hat{k}$. If $n=2$, then $M=N^1(2^2)$ or $N^2(2^2)$. In these cases, $|H_1| \mid 2^7 \cdot 3^2 \cdot \hat{k}$, and $|H_1| \mid 2^7 \cdot 3 \cdot 5 \cdot \hat{k}$, respectively. However, in the latter case $15 \nmid |H_1|$, since H_1 is solvable and $U/N \simeq \Sigma_5$ [1], [14]. The other cases are similar.

Let $H^*=\mathfrak{N}_H(\langle g \rangle)$, so that H^* splits H over N (mod A), and $H^* \cong H_1$, if $k=\hat{k}$.

1. Let $p^k=4$, so that $k=\hat{k}=2$. If $|H^*| \mid 2^8 \cdot 3^2$, then each of the 2 orbits of 40 points under K, of parts (1) and (2) of Lemma 7.2, decompose into at least 2 orbits under H^*, since $40 \nmid 2^8 \cdot 3^2$. Similarly, the 45 points of v^K, part (3) of Lemma 7.2, occur in at least 2 orbits under H^*. On the other hand, if $|H^*| \mid 2^8 \cdot 5$, then the points of (1) and (2) might occur in one orbit each under H^*, but the points of part (3) of Lemma 7.2 must form at least 2 orbits. There remain $341-125=216$ points in T which do not occur in (1)–(3) (see proof of part (4) of Lemma 7.2). It is easy to check that there are no solutions for $2^{i_1} \cdot 5^{j_1} + 2^{i_2} \cdot 5^{j_2} = 216$, $0 \leqq i_1, i_2 \leqq 8$, $0 \leqq j_1, j_2 \leqq 1$; hence these 216 points occur in at least 3 orbits under H^*.

Therefore, in each of the two cases, H^* has at least 3 more orbits than the estimate for U^* above.

2. Let $p^k=7$. From (5) of Lemma 7.2, there exist at least 7^8 points x such that $L_x \subseteq N$. Since $|H_1| \mid 2^7 \cdot 5$ or $2^7 \cdot 3^2$, then $|H|/(p^k-1) \leqq 2^7 \cdot 3^6$. Hence the points of

(5) occur in at least $7^8/2^7 \cdot 3^6 = (7/6)^6(49/2) > 61$ orbits under H. Parts (1)–(4) contribute at least 5 orbits under H, so $r^*(H) \geqq 67$.

8. **Cases C_1–C_4, D ($q=2$).** We continue to assume that the groups under discussion are factor groups (mod A).

Case C_1: $q=2$, $m=1$. In this case, $N \simeq Q$ (type 2), since otherwise Lemma 3.2 (5) is violated. Hence $|U^*| = 24k$ (mod A), and $r^*(U^*) \geqq (p^k+1)/24k$. The exact situation is as follows.

8.1 LEMMA. *Let $N \simeq Q$. Define integers $\nu_1, \ldots, \nu_5$ as follows: $\nu_1, \ldots, \nu_4$ are* 0 *except that $\nu_1 = 1$ if $p^k \equiv 1$* (mod 4), $\nu_2 = 1$ *if $p = 3$, $\nu_3 = 1$ if $p^k \equiv 1$* (mod 3), *and $\nu_4 = 1$ if $p \neq 3$ and $p^k \equiv 1$ or* 3 (mod 8). *Last, $\nu_5 = [(p^k+1) - (6\nu_1 + 4\nu_2 + 8\nu_3 + 12\nu_4)]/24$.*

Then $r^*(U^*) = \sum_1^5 \nu_i$, and $r^*(U^*) \geqq (\nu_5/k) + \sum_1^4 \nu_i$.

8.2 COROLLARY. *Let $N \simeq Q$. The following table gives the exact orbital structure of U, for the first few cases of p^k.*

p^k	3	5	7	9	11	13	17	19	23	25
$(\nu_1, \nu_2, \nu_3, \nu_4, \nu_5)$	01000	10000	00100	11000	00010	10100	10010	00110	00001	10110
$r^*(U)$	1	1	1	2	1	2	2	2	1	3

p^k	27	29	31	37	41	43	47	49	53	59
$(\nu_1, \nu_2, \nu_3, \nu_4, \nu_5)$	01001	10001	00101	10101	10011	00111	00002	10111	10002	00012
$r^*(U)$	2	2	2	3	3	3	2	4	3	3

Proof. The proof depends upon the following facts about $PSL_2(p^k)$, and $PGL_2(p^k)$ as permutation groups of the projective line L_∞ (see [7], [8]). First, $\psi(Q)$ is a noncyclic group of order 4, $\psi(U) \simeq \Sigma_4$, and $\psi(U) \subseteq PGL$ (where ψ: $GL_2(p^k) \to PGL_2(p^k)$). Further, $\psi(U) \subseteq PSL$ if and only if $p^k \equiv \pm 1$ (mod 8). Each element of PGL has a regular cycle structure (i.e., all nontrivial cycles have the same length), and each element fixes 0, 1, or 2 points of L_∞ as it belongs to a cyclic subgroup of PGL of order p^k-1, p, or p^k+1, respectively. PSL consists of the even permutations of PGL.

Further, $\psi(U)$ consists of $\psi(Q)$, 4 conjugate Sylow 3-subgroups, 3 conjugate cyclic groups of order 4 (which intersect $\psi(Q)$ nontrivially), and 6 conjugate groups of order 2, disjoint from $\psi(Q)$. The normalizer of a Sylow 3-subgroup in $\psi(U)$ is noncyclic of order 6, and every element of order 2 in $\psi(U) - \psi(Q)$ normalizes two Sylow 3-subgroups.

The elements of $\psi(Q)$ have a total of 0 or 6 fixed points occuring in $\nu_1 = 0$ or 1 orbits, as $p^k \equiv 3$ or 1 (mod 4), respectively. In the latter case, U_x is cyclic of order 4, for such a fixed point x.

A Sylow 3-subgroup of $\psi(U)$ fixes no point in common with an element of $\psi(Q)$ or another Sylow 3-subgroup. Hence, there exist 0, 4, or 8 points fixed by each Sylow 3-subgroup, as $p^k \equiv -1$, 0, or 1 (mod 3), respectively. These points occur in 0, $\nu_2 = 1$, or $\nu_3 = 1$ orbits, respectively, by conjugacy (in the last case, an element of order 2 in $\psi(U) - \psi(Q)$ normalizes two Sylow 3-subgroups, and hence must permute the two fixed points of at least one of them). In the last two cases, $|U_x| = 6$ or 3, respectively.

Next, let $f \in \psi(U) - \psi(Q)$ with $f^2 = 1$. Then f fixes two points if and only if either: 1. $f \in PSL$ and $p^k \equiv 1 \pmod 4$, i.e., $p^k \equiv 1 \pmod 8$; or 2. $f \notin PSL$ and $p^k \equiv 3 \pmod 4$, i.e. $p^k \equiv 3 \pmod 8$. If f fixes two points, then these are interchanged by the element of $\psi(Q)$ commuting with f. Further, if f and a conjugate f' fix a common point, then $\langle f, f' \rangle$ has order 6 (since $\langle f, f' \rangle \cap \psi(Q) \neq 1$), and from above $p = 3$. Therefore, if $p \neq 3$ and $p^k \equiv 1$ or 3 (mod 8), then the conjugates of f fix a total of 12 points which occur in $\nu_4 = 1$ orbit.

Finally, the remaining points are fixed by no element of $\psi(Q)$ and so occur in ν_5 orbits of length 24. It is only these orbits which can be consolidated by elements of U^*/U.

Although $N \simeq D$ (type 1) does not satisfy (3.1), it is helpful to know the structure of U in order to apply Lemma 5.7 to the case C_2 ($q = 2$, $m = 2$).

8.3 LEMMA. *Let $N \simeq D$. Define the integers $\nu_1, \ldots, \nu_4$ as follows*: $\nu_1 = 1$; ν_2 *and* $\nu_3 = 0$, *except that* $\nu_2 = 1$ *if* $p^k \equiv 1 \pmod 4$, *and* $\nu_3 = 1$ *if* $p^k \equiv \pm 1 \pmod 8$; *and* $\nu_4 = [(p^k + 1) - (4\nu_1 + 2\nu_2 + 4\nu_3)]/8$.

Then $r^*(U) = \sum_1^4 \nu_i$, *and* $r^*(U^*) \geqq \nu_1 + \nu_2 + \nu_3 + (\nu_4/k)$.

Proof. Since $\psi(U)$ is a nonabelian group of order 8, it is clear that $\psi(U)$ is a dihedral group. Let $\psi(U) = \langle a, b \rangle$, $a^4 = b^2 = 1$, $bab = a^{-1}$; and let $\psi(D) = \langle a^2, b \rangle$. Then b and a^2b each have 2 fixed points, which lie in $\nu_1 = 1$ orbit under U. Next, a and a^2 have a total of 0 or 2 fixed points as $p^k \equiv 3$ or 1 (mod 4) occurring in ν_2 orbits. Further, $a^2 \in PSL$; and $a \in PSL$ if and only if $p^k \equiv \pm 1 \pmod 8$. Since ab and a^3b have order 2, and since b always has fixed points, then ab and a^3b have fixed points exactly in case ab and b are either both in PSL or both not in PSL, i.e., exactly in case $a \in PSL$, or $p^k \equiv \pm 1 \pmod 8$. The 0 or 4 points fixed by ab and a^3b occur in ν_3 orbits. Finally, the remaining points occur in ν_4 orbits of length 8.

8.4 COROLLARY. *The points x for which $D_x = 1$, occur under U^* in at least* 2 *orbits if $p^k \geqq 17$ and $p^k \neq 27$.*

Proof. Use the inequality $(p^k - 5)/8k \geqq 2$, and check the cases $p^k = 17$, 19, and 25 individually.

Case C_2: $q = 2$, $m = 2$. For a discussion of splittings in the chain $U \supset \langle N, A \rangle \supset A$, see the end of this section.

8.5 PROPOSITION. *Let $q=2$, $m=2$, and $N=N^j(2^2)$, for $j=1, 2, 3$, be irreducible. Let H be a maximal solvable subgroup of U which satisfies* 3.1. *The following table gives a lower bound for $r^*(H)$ for certain values of p^k.*

type \ p^k	3	5	7	9	11	13	17	19	23	25	27	$p^k > 17$
$j=1$	2	3	4	6	4	6	11	10	15	13	9	9
$j=2$	1	4	2	5	6	11	19	23	40	29	23	23
$j=3$		3		6		6	9			11		11

8.6 COROLLARY. *The maximal solvable subgroups H of U for which $r^*(H)\leqq 2$ are as follows:*

1. *$p^k=3$, $N=N^1(2^2)$; U is solvable and $r^*(U)=2$, where $|U|=2^8\cdot 3^2$ by* (4.6).

2. *$p^k=3$, $N=N^2(2^2)$. Let H be a subgroup of order $2^6\cdot 5$ (mod A) (case* I). *Then $r^*(H)=1$ (Huppert). H contains two proper subgroups, of orders $2^5\cdot 5$ and $2^4\cdot 5$ for which the r^*-rank is* 1. *U contains no subgroup satisfying* (3.1) *with r^*-rank* 2.

3. *$p^k=7$, $N=N^2(2^2)$. Let $|H|=2^6\cdot 5$ (mod A), (case* I). *Then $r^*(H)=2$. Moreover, each proper subgroup of H has r^*-rank at least* 4.

Proof. It is convenient to consolidate in the following table the available information about these cases, according to the type of N. Let $T=\{x : N_x=1\}$.

Type		1	2	3
$\|H_1\|$ divides: (case)		$2^3\cdot 3^2$, (II)	$2^2\cdot 5$, (I)	$2^2\cdot 5$, (I); $2^3\cdot 3^2$, (II)
C_{r2}^{ij}		$C_{12}^{11}=9$, $C_{22}^{11}=6$ $C_{12}^{21}=6$, $C_{22}^{21}=9$	$C_{12}^{12}=5$, $C_{22}^{12}=0$ $C_{12}^{22}=10$, $C_{22}^{22}=15$	$C_{12}^{3}=15$, $C_{22}^{3}=15$
for $p^k>5$ $\|T\|$	$p^k\equiv 3$ (mod 4)	$(p^{2k}-17)(p^k+1)+48$	$(p^{2k}-9)(p^k+1)$	—
	$p^k\equiv 1$ (mod 4)	$(p^{2k}-29)(p^k+1)+120$	$(p^{2k}-29)(p^k+1)+120$	$(p^{2k}-29)(p^k+1)+120$
$p^k=3$	N-Stabilizers	S_2^1	S_2^1	—
	$\|T\|$	16	0	—
$p^k=5$	N-Stabilizers	S_2^1, S_2^2	S_2^2	S_2
	$\|T\|$	96	96	96

Most of this information is immediately available. For example, the values for C_{rm}^{ij} are computed in Lemma 3.20; moreover, the number of fixed points for each S_r^i is computed in Lemma 3.21, the N-stabilizers are discussed in Lemma 3.22, and from this information and Lemma 3.25 one can compute the number of points with trivial N-stabilizer in each case.

Finally, 3 cases I, II, III must be considered to determine $|H_1|$ (Lemma 5.9). Case III is impossible since $m=2$ and $q=2$. In case I, $|H_1| \mid 2^2 \cdot 3 \cdot 5$, and in case II, $|H_1| \mid 2^3 \cdot 3^2$. However, $|H_1| \mid |\mathrm{Aut}_Z(N)|/2^4 = 2^3 \cdot 3^2, 2^3 \cdot 3 \cdot 5, 2^4 \cdot 3^2 \cdot 5$ as the type j of N is 1, 2, 3, respectively (Lemma 5.9 and Proposition 4.6). Therefore:

Type		1	2	3
$\lvert H_1\rvert$	*case* I	$2^2 \cdot 3$	$2^2 \cdot 3 \cdot 5$	$2^2 \cdot 3 \cdot 5$
divides:	*case* II	$2^3 \cdot 3^2$	$2^3 \cdot 3$	$2^3 \cdot 3^2$

However, type 1, case I and type 2, case II cannot occur, and in case I of types 2 and 3, $3 \nmid |H_1|$, as follows.

Type 1, *case* I. Let $N = Q_1 \otimes Q_2$, where $Q_i = \langle c_i, d_i \rangle \simeq Q$, $i=1, 2$. Let $\mathfrak{N}(Q_i) = \langle Q_i, e_i, f_i \rangle$, where $e_i: c_i \to d_i \to c_i d_i$, and $f_i: c_i \to d_i$, with $e_i^3 = f_i^2 = 1$, $i=1, 2$. Let $\delta: Q_1 \to Q_2$ by $\delta: c_1 \to c_2, d_1 \to d_2$, with $\delta^2 = 1$. Then $U = \langle N, e_1, e_2, f_1, f_2, \delta \rangle$ from $|U|$, or from the fact that there exist $2Q$'s in N (Lemma 4.5). In case I, H_1 consists of the normalizer of an element e of order 3 which fixes no point of W. Hence $e = e_1 e_2$ or $e_1^2 e_2$ (which are conjugate). Let $e = e_1 e_2$. Then $H_1 \subseteq \langle N, e_1 e_2, f_1 f_2, \delta \rangle / N$, but H_1 reduces W, since H_1 fixes the subspace $\langle c_1 c_2, d_1 d_2 \rangle / \mathfrak{Z}(N)$ of W. This contradicts Lemma 3.2, so case I is impossible. Note that $e = e_1 e_2$ fixes the following abelian subgroups of N: $\langle c_1 c_2, d_1 d_2 \rangle$, $\langle c_1 d_1 d_2, c_1 c_2 d_2 \rangle$, $\langle c_1 d_2, c_1 d_1 c_2 \rangle$. It can be checked that none other of the 12 abelian subgroups of length 2 is fixed by e.

Type 2, *case* II. Since $C_{12}^{12} = 5$ and $|H_1| \mid 2^7 \cdot 3$, H_1 must permute the subgroups S_1^1 of N in at least 2 orbits. One orbit must generate an H_1-invariant subspace of W of dimension $\leqq 2$, which is impossible by Lemma 3.2. Hence case II is impossible.

Types 2 *and* 3, *case* I. A similar argument as above shows that in types 2 and 3 case I, $|H| \nmid 2^6 \cdot 3 \cdot k$. For example, if $N = N^3$, then $N^1 \subset N^3$, and a Sylow 3-subgroup of N^1 is also a Sylow 3-subgroup of N^3. Hence, we can assume (in case I, type 3, with $|H_1| \mid 2^2 \cdot 3$) that $\langle e \rangle$ is the subgroup of H_1 of order 3. Since $\langle e \rangle$ fixes exactly 3 of the 15 S_2's of N^3 (from above), it is clear from the order of H_1 that H_1 fixes at least one of the S_2's, thus violating Lemma 3.2. Hence, this situation is impossible. Finally, $3 \cdot 5 \nmid |H_1|$ in case I, because if so then H_1 is the normalizer of an element h of order 15. But $Sp(4, 2)$ contains no element of order 15, as follows. Let

$$h = \begin{bmatrix} 0011 \\ 1100 \\ 0111 \\ 0110 \end{bmatrix} \quad \text{and} \quad f = \begin{bmatrix} 0110 \\ 1110 \\ 1001 \\ 0010 \end{bmatrix}$$

be elements of $GL(4, 2)$, represented as left operators. Then $h^{15} = 1$ and $h^3 = f$.

Hence $\langle h\rangle = \mathfrak{S}_{GL(4,2)}(\langle f\rangle)$. Moreover, $f \in Sp(4, 2)$, with respect to the alternating form with matrix

$$M = \begin{pmatrix} 0100 \\ 1000 \\ 0001 \\ 0010 \end{pmatrix}.$$

Further $\langle f\rangle$ is a Sylow 5-subgroup of $Sp(4, 2)$. Hence $Sp(4, 2)$, has an element of order 15 if and only if $h \in Sp(4, 2)$, but $h^T M h \neq M$ so $h \notin Sp(4, 2)$. This fact also follows by examining the permutation of the 15 abelian subgroups of length 2 in N induced by h. To do this, identify h^5 with the appropriate element of order 3 in the Sylow 3-subgroup discussed above (for type 1). Then h^5 fixes exactly 3 of the abelian subgroups, while h^3 fixes none. This is impossible so $h \notin Sp(4, 2)$.

The proof of Proposition 8.5 follows by considering the various values for p^k and types for N separately.

$p^k = 3$, *type* 1. Since H is maximal then $H = U$. Therefore, the $4 \cdot C_{22}^{11} = 24$ points with nontrivial N-stabilizer lie in one orbit (from Lemma 3.21). From the representation of U (for $N = Q_1 \otimes Q_2$) given above, clearly the 16 points of the form $x = x_1 \otimes x_2$ form one orbit under U. These points have trivial N-stabilizer, and hence $r^*(U) = 2$.

$p^k = 3$, *type* 2. Huppert has shown that for case I, there exist 3 groups H_i with orders $2^4 \cdot 5$, $2^5 \cdot 5$, $2^6 \cdot 5$, such that $r^*(H) = 1$. There are subgroups $\overline{H}$ of U with r^*-rank 2, but these occur in a different context; i.e., none of the groups $\overline{H}$ satisfy the hypotheses (3.1). Incidentally, it is known that for $p^k = 3$ and $N = N^2(2^2)$, $U/N \simeq \Sigma_5$ by the action of U on certain pairs of lines of the nearfield plane of order 9 [1], [8, §5]. Such a pair of lines constitute the fixed points of a stabilizer subgroup S_1^1. Hence U/N acts on the set of 5 subgroups $\{S_1^1\}$ as Σ_5.

$p^k = 5$, *type* 1. There exist 3 types of stabilizer subgroups of N (including 1). Hence, $r^*(U) \geqq 3$.

$p^k = 5$, *type* 2. Since $|H| \mid 2^6 \cdot 5$, then $C_{22}^{22} = 15 \nmid |H|$, so there exist at least 2 orbits of points with nontrivial N-stabilizer. The 96 remaining points form at least two orbits, similarly. Hence $r^*(H) \geqq 4$.

$p^k = 5$, *type* 3. If $|H| \mid 2^6 \cdot 5$, then exactly as above, $r^*(H) \geqq 4$. If $|H| \mid 2^7 \cdot 3^2$, then there exist 2 classes of N-stabilizers, so $r^*(H) \geqq 3$.

$p^k = 7$, *type* 2. If $|H| = 2^6 \cdot 5$, then $r^*(H) = 2$, as follows. Let

$$a_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad b_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad c_1 = \begin{pmatrix} 3 & 5 \\ 5 & 4 \end{pmatrix},$$

with entries in $GF(7)$. Let $a = a_1 \otimes I$, $b = b_1 \otimes I$, $c = I \otimes c_1$, $d = I \otimes a_1$. Then $N^2 = \langle a, b, c, d\rangle \simeq D \otimes Q$. Further let

$$g = \begin{pmatrix} 25 & & \\ 22 & & \mathbf{0} \\ & & 24 \\ \mathbf{0} & & 45 \end{pmatrix}, \quad \text{and} \quad f = 5\begin{bmatrix} 1 & -1 & 1 & 1 \\ 2 & -1 & 1 & 2 \\ 1 & -1 & -1 & -1 \\ 2 & -1 & -1 & 5 \end{bmatrix}.$$

Then f and g normalize N, $g^4 = -b, f^5 = I$, and $gfg^{-1} \in \langle f, N\rangle$. Hence we may take $H = \langle N, f, g, A\rangle$. One orbit of H consists of the 80 points with some nontrivial N-stabilizer, S_1^1. For f can fix no element of W and hence must permute the 5 S_1^1's transitively. And the 16 fixed points $(10) \otimes x$ and $(01) \otimes x$ for the stabilizer subgroup $S_1^1 = \langle a, \mathfrak{Z}(N)\rangle$ lie in one orbit under $\langle b, c, d, g\rangle$. Hence, since $|H| = |\{x : N_x = 1\}|$, it is sufficient to show that if $N_x = 1$ then $H_x = 1$. Since $p^k = 7$, every element of order 5 fixes no point of V, so it is sufficient to examine the elements of the form g^2y, with $y \in N$, such that $(g^2y)^2 \in \mathfrak{Z}(N)$. Since $g^4 = -b$, y must satisfy: $g^2yg^{-2} = \pm by$. Now g^2 has the following action on N; $g: a \to abd$, $b \to b$, $c \to bc$, $d \to d$. Hence $y \in \{c, bc, cd, bcd\}$. Therefore,

$$g^2y = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix},$$

where X_i are 2×2 blocks ($i = 1, 2$), and $X_1, X_2 \in \langle c_1, d_1\rangle \simeq Q$. Hence, if g^2y fixes $v = (v_i)$, then either $v = (v_1v_200)$ and $X_1 = \pm 1$, or $v = (00v_3v_4)$ and $X_2 = \pm 1$, in which cases $N_v = \langle a, \mathfrak{Z}(N)\rangle$ as above: or $g^2y = \pm I$. Therefore, the 320 points $x \in V$ such that $N_x = 1$ lie in one orbit under H, and $r^*(H) = 2$.

For the remaining cases, similar techniques are used. To get the best results, it is necessary to treat the subcases $p^k \equiv 1$ and $p^k \equiv 3 \pmod 4$ separately. In addition, to prove the results for $p^k \geqq 19$, it is necessary to treat the cases $k = 1$ and $k > 1$ separately (e.g., $p^k \equiv 3 \pmod 4$: $p^k \geqq 19$, $k = 1$; $p^k \geqq 27$, $k > 1$; similarly for $p^k \equiv 1 \pmod 4$). Finally, for $p^k \geqq 19$, one must use Lemmas 8.4 and 5.7 to improve the estimates. E.g., for $p^k \geqq 19$ and $p^k \neq 27$, $\mathfrak{N}(D)$ has at least two orbits with trivial D-stabilizer. Hence, every class of stabilizers of length 1 in $N^1(2^2)$ has at least two orbits, from Lemma 5.7.

In case $N = N^2(2^2)$ is represented over an arbitrary field $F = GF(p^k)$, what splitting occurs in the chain $U \supset \langle N, A\rangle \supset A$?

PROPOSITION. 1. *U/A splits over $\langle N, A\rangle/A$, (possibly several conjugacy classes of complements exist).*

2. *If $\overline{U}/A$ is a complement of $\langle N, A\rangle/A$, then $\overline{U}$ does not split over A, but $\overline{U}/\langle -1\rangle$ splits over $A/\langle -1\rangle$.*

3. *There is a subgroup $\hat{U}$ of U such that $N \subset \hat{U}$, $\hat{U} \cap A = \langle -1\rangle$, $\hat{U}/N \simeq U/\langle N, A\rangle$ and $\hat{U}/\langle -1\rangle$ splits over $N/\langle -1\rangle$.*

Proof. To prove (3), let $\hat{U} = \overline{U}^- \cdot N$, where $\overline{U}^-/\langle -1\rangle$ is a complement of $A/\langle -1\rangle$ in $\overline{U}/\langle -1\rangle$.

To prove (1), it is sufficient to show that a Sylow 2-subgroup S of U/A splits over $\langle N, A\rangle/A$ [Theorem 6.9, p. 26, Proc. Sympos. Pure Math., Vol. 6, Amer. Math. Soc., Providence, R. I., 1960]. Let

$$a_1 = d_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad b_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{and} \quad c = \begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix}$$

where $\lambda^2+\mu^2=-1$ in $GF(p^k)$, as in the case above for $p^k=7$ (also see (3.9)). Let $a=a\otimes I$, $b=b_1\otimes I$, $c=I\otimes c_1$ and $d=I\otimes d_1$. Then $Q\simeq\langle c, d\rangle$ and $N=N^2(2^2)=\langle a, b, c, d\rangle\simeq D\otimes Q$. Let g_1 be a 2×2 matrix with determinant ± 1 normalizing $Q=\langle c, d\rangle$ and inducing the following automorphism of Q: $c\to cd\to -c\to -cd$, $d\to d$. Thus $g_1^2=\varepsilon d\in Q$, where $\varepsilon=\pm 1$. Let

$$g = \begin{pmatrix} 0 & -cg_1 \\ g_1 & 0 \end{pmatrix} \quad \text{and} \quad s = \begin{pmatrix} d & 0 \\ 0 & cd \end{pmatrix}.$$

Then $g^4=s^2=-1$, $sgs^{-1}=\varepsilon g^3$, $\langle g, s\rangle\subset U$, and in fact $\langle g, s, A\rangle/A$ is a complement of $\langle N, A\rangle/A$ in the Sylow 2-subgroup $S=\langle g, s, N, A\rangle/A$ of U/A.

However, $\langle g, bs, A\rangle/A$ is another complement in S, which is not conjugate to $\langle g, s, A\rangle/A$ (conjugacy would have to occur in $\mathfrak{N}_N(\langle g\rangle)=\langle b, -1\rangle$). Hence, two complements of $\langle N, A\rangle/A$ may not be conjugate.

Finally, if $\overline{U}/A$ is a complement of $\langle N, A\rangle/A$, then we can assume that either $\langle g, s\rangle$ or $\langle g, bs\rangle\subset\overline{U}$ ($\langle g\rangle$ and $\langle ag\rangle$ each have 8 conjugates under N, but $\langle a, g\rangle$ does not split over N since $(ag)^4=-b$). In either case, splitting does not occur over A.

To show $\overline{U}/\langle -1\rangle$ splits over $A/\langle -1\rangle$, it is sufficient to examine the Sylow subgroups of $\overline{U}/\langle -1\rangle$, where $|\overline{U}/\langle -1\rangle|=2^7\cdot 3\cdot 5\cdot(p^k-1)/2$. If $5^i\| p^k-1$ for $i>0$, then $5^{4i}\parallel |GL_4(p^k)|$ and a Sylow 5-subgroup of $GL_4(p^k)$ is an abelian group which splits as required. The Sylow 3-subgroups of U split over A, since

$$h = \begin{pmatrix} h_1 & 0 \\ 0 & h_1 \end{pmatrix} \in U,$$

where h_1 is a 2×2 matrix of order 3 which induces an automorphism of Q of order 3. Finally either $\langle s, g\rangle/\langle -1\rangle$ or $\langle bs, g\rangle/\langle -1\rangle$ is a complement in a Sylow 2-subgroup of $\overline{U}/\langle -1\rangle$.

Case C_3: $(q=2, m=3)$.

8.7 LEMMA. *Let $m=3$, $q=2$, and let H be a solvable subgroup of U^*. The following table lists lower bounds for $r^*(H)$ for special cases of p^k.*

p^k	3	5	7	$9\geqq 11$
$r^*(H)^{\geqq}$	4	6	15	31 200

Proof. Applying the Cases I–III to $N=N^i$ $(1\leqq i\leqq 3)$, and keeping in mind that $|H_1| \mid 2^9\cdot 3^4\cdot 5\cdot 7$ from Lemma 5.8, the following possibilities arise.

Cases I and II: $|H_1| \mid 2\cdot 3^3\cdot 7$ or $2^4\cdot 3^4$ (since $7^2\nmid |H_1|$);

Case III: $k_1=2$, $t_1=3$, $p_1=(2^{k_1}-1,\ t_1)=3$, $M=M(3^1)\in \mathfrak{P}$ has length 1 and is irreducible, so that $|H_1| \mid k_1(q^{k_1}-1)\cdot p_1^2\cdot |SL_2(p_1)|=2^4\cdot 3^4$.

In Cases I–III, $|H_1|\leqq 2^4\cdot 3^4$, so from Lemma 5.8

$$r^*(H) \geqq (p^{8k}-1)/k(p^k-1)2^{10}\cdot 3^4 \geqq p^{6k}(p^k+1)/2^{10}\cdot 3^4\cdot k.$$

If $p^k\geqq 11$, then $p^k/k\geqq 3^3/3=9$, so

$$r^*(H) \geqq 3^2\cdot 11^5/2^8\cdot 3^3 \geqq 11\cdot(120)^2/2^8\cdot 3 = 3\cdot 5^2\cdot 11/4 > 200.$$

If $p^k=9$, then

$$r^*(H) \geqq 2\cdot 3^{12}\cdot 5/2^{11}\cdot 3^4 = 3^8\cdot 5/2^{10} \geqq (9/8)^3(45/2) > 30.$$

If $p^k=7$ then N has type 1 or 2. Moreover, Lemma 3.22 and the fact that $5|C_{23}^{1j}$ $(j=1, 2)$ but $5\nmid |H|$, imply that the points x such that $N_x\neq 1$ occur in at least 3 orbits. From Lemma 3.20, $C_{13}^{11}=35$ and $C_{13}^{12}=27$. Since each stabilizer subgroup of length 1 fixes $2\cdot(7^4-1)/6$ points from Lemma 3.21, it follows from Lemma 3.23 that there exist at least $[(7^8-1)-70(7^4-1)]/6$ points x such that $N_x=1$ (mod A). Since $|H|\leqq 2^{10}3^4$, then these points contribute at least

$$(7^4+1-70)(7^4-1)/2^{11}\cdot 3^5 \geqq 2^7\cdot 3\cdot 5^2\cdot 583/2^{11}\cdot 3^5 > 5^2\cdot 2^6\cdot 3^2/2^4\cdot 3^4 = 100/9 > 11$$

orbits under H. Therefore, $r^*(H)\geqq 15$.

Let $p^k=5$. 1. Let $N=N^1$ (type 1). From Lemma 3.22, the stabilizer subgroups of N are S_1^i, S_3^i $(i=1, 2)$. But $C_{s3}^{i1}\nmid |H_1|$, for $i=1, 2$ and $s=1, 3$. Hence, each of the four stabilizer subgroups in N contributes at least 2 orbits, so $r^*(H)\geqq 8$.

2. Let $N=N^2$ (type 2). First, the stabilizers are S_1^1, S_1^2, and S_3^2. Next, estimate the number t of points x with $N_x=1$ (mod A). Each S_1^i $(i=1, 2)$ fixes $2(5^4-1)/(5-2)$ points, so

$$t \geqq (5^8-1)/4-(63)\cdot 2\cdot(5^4-1)/4.$$

However, each of the C_{33}^{22} stabilizers S_3^2 fixes 8 distinct points, and each such set of 8 points is counted 6 times too often in the above estimate. Since $C_{33}^{22}=3^3\cdot 5$, then

$$t \geqq (5^8-1)/4-2\cdot 3^2\cdot 7\cdot(5^4-1)/4+2^4\cdot 3^4\cdot 5 = 2^9\cdot 3\cdot 5\cdot 11.$$

Therefore, these t points contribute at least $2^9\cdot 3\cdot 5\cdot 11/2^{10}\cdot 3^4>1$ orbits.

Finally, since $C_{33}^{22}\nmid |H_1|$, the stabilizers S_3^2 contribute at least 2 orbits. Moreover, from Proposition 8.5, in case $q=2$, $m=2$, $p^k=5$, and $\overline{N}=\overline{N}^2(2^2)$ has type 2, the points with trivial $\overline{N}$-stabilizer occur in at least 2 orbits. Lemma 5.7 implies the stabilizers S_1^1 and S_1^2 of N contribute at least 2 orbits each.

Therefore, $r^*(H)\geqq 8$.

3. Let $N=N^3$ (type 3). The stabilizers are S_1 and S_3, and $C_{13}^3=63$ and $C_{33}^3=3^3\cdot 5$. If $|H_1| \mid 2^4\cdot 3^4$ then the t points with N-stabilizer 1 contribute at least 2 orbits, as in 2 above. In this case, $C_{13}^3 \nmid |H_1|$ and $C_{33}^3 \nmid |H_1|$ imply $r^*(H)\geqq 6$. If $|H_1| \mid 2\cdot 3^3\cdot 7$, then the t nonfixed points form at least $2^9\cdot 3\cdot 5\cdot 11/2^7\cdot 3^3\cdot 7=220/63>3$ orbits; and since $C_{33}^3 \nmid |H_1|$, then $r^*(H)\geqq 7$.

Finally, let $p^k=3$. 1. Let $N=N^1$. Then S_1^1 and S_3^1 are the stabilizers in N, and $C_{13}^{11}=5\cdot 7$, $C_{33}^{11}=2\cdot 3\cdot 5$. Since $5 \nmid |H_1|$, the stabilizers of N contribute at least 4 orbits.

There exist $(3^8-1)/2-2\cdot 5\cdot 7((3^4-1)/2)+2\cdot 3\cdot 5(6\cdot 8)=2^7\cdot 3\cdot 5$ points with trivial stabilizer. Since $5 \nmid |H_1|$, these points contribute at least 2 orbits. Hence $r^*(H)\geqq 6$.

2. $N=N^2$. Then S_2^1 is the only stabilizer subgroup of N, and $C_{23}^{12}=3^2\cdot 5$. Since $5 \nmid |H_1|$, the stabilizers in N contribute at least 2 orbits. Moreover, there exist $((3^8-1)/2)-45\cdot 16=2^9\cdot 5$ points with trivial stabilizer. Since $5 \nmid |H|$, these points contribute at least 2 orbits. Hence $r^*(H)\geqq 4$.

Case C_4 ($q=2$, $m=4$).

8.8 LEMMA. *Let $m=4$, $q=2$, and let H be a solvable subgroup of U^*. Then $r^*(H)\geqq 11$ if $p^k=3$, and $r^*(H)\geqq 3{,}000$ if $p^k\geqq 5$.*

Proof. As before, $r^*(H)\geqq p^{15k}/2^8k|H_1|$. Now apply Lemma 5.9.

I. $|H_1| \mid 8(2^8-1)=2^3\cdot 3\cdot 5\cdot 17$.

II. (i) $r_1=k_1=t_1=2$, $|H_1| \mid 2|(H_1)_{w_1}|^2$, where $(H_1)_{w_1}$ is a solvable irreducible subgroup of $\Gamma L_2(4)$. Hence, $|(H_1)_{w_1}|\leqq 72$ from [7, p. 286 (261, 262)], $|H_1|\leqq 2^7\cdot 3^4$. Moreover, $|H_1| \mid 2^7\cdot 3^4\cdot 5^2$.

(ii) $r_1=4$, $k_1=2$, $t_1=1$, $|H_1| \mid 4!\,(2\cdot 3)^4=2^7\cdot 3^5$.

(iii) $r_1=2$, $k_1=4$, $t_1=1$, $|H_1| \mid 2(4\cdot 3\cdot 5)^2=2^5\cdot 3^2\cdot 5^2$.

III. There is no prime p_1 such that $p_1|(2^{k_1}-1, t_1)$, with $k_1t_1=8$.

Therefore $|H_1|\leqq 2^7\cdot 3^5$, and $r^*(H)\geqq p^{15k}/2^{15}\cdot 3^5\cdot k$.

If $p^k\geqq 5$, then $p^k/k\geqq 9/2$, so

$$r^*(H) \geqq 3^2\cdot 5^{14}/2^{16}\cdot 3^5 = (5/4)^8\cdot(25/3)^3 > (45/8)\cdot(8^3+8^2) > 3000.$$

Next let $p^k=3$. From Lemma 3.20, $C_{14}^{11}=3^3\cdot 5$, $C_{24}^{11}=3^2\cdot 5^2\cdot 7$, $C_{44}^{11}=2\cdot 3^3\cdot 5$, $C_{14}^{12}=17\cdot 7$, and $C_{34}^{12}=3^2\cdot 5\cdot 17$.

Each of the C_{14}^{1j} subgroups S_1^1 of $N=N^j(2^4)$ fixes $2(p^{8k}-1)/(p^k-1)$ points of V from Lemma 3.21. Hence there are at least

$$(3^{16}-1)/2-C_{14}^{1j}\cdot 2(3^8-1)/2 \geqq (3^{16}-1)/2-3^3\cdot 5(3^8-1)$$

points x such that $N_x=1$. Now $(3^{14}-1)/2\geqq 3^3\cdot 5\cdot(3^8-1)$, since $3^{14}>2\cdot 3^{11}\cdot 5$. Therefore, there are at least $3^{15}+3^{14}=4\cdot 3^{14}$ such points x.

Case 1. Let $3^5 \mid |H_1|$, so that $|H_1| \mid 2^7\cdot 3^5$ (II-ii). From Lemmas 4.6 and 5.8,

$$|H_1| \mid \mathrm{Aut}_Z(N)/q^{2m} = 2^{13}\cdot(2^4\pm 1)(2^2-1)(2^4-1)(2^6-1) = 2^{13}\cdot 3^4\cdot 5\cdot 7\cdot(16+(-1)^i),$$

where N has type i. Since $3^5 \mid |H_1|$, it follows that $N=N^1(2^4)$ has type 1. From

Lemma 3.22, the subgroups S_i^1 of N are stabilizer subgroups, for $i=1, 2, 4$. Moreover, since $C_{i4}^{11} \nmid |H_1|$ $(i=1, 2, 4)$, each stabilizer subgroup contributes at least 2 orbits. In addition, each class of S_1^1's contributes at least 2 orbits from Lemma 3.23, since if $\bar{N}=\bar{N}^1(2^3)$ then the points with $\bar{N}_x=1$ occur in at least 2 orbits under $U(\bar{N})$ from the proof of Lemma 8.7. Hence, the points with nontrivial N-stabilizers occur in at least 8 orbits. In addition, the points x with $N_x=1$ (mod A) contribute at least $4\cdot 3^{14}/2^{15}\cdot 3^5=(9/8)^4\cdot(3/2)>2$ orbits. Therefore, $r^*(H)\geqq 11$.

Case 2. Let $|H_1|\leqq 2^7\cdot 3^4$. The points x with $N_x=1$ (mod A) contribute at least $3^{10}/2^{13}=(9/8)^5\cdot 4>57/8>7$ orbits. From Lemma 3.22, S_i^1 is a stabilizer subgroup of $N^j(2^4)$ for $i=1, 2, 4$ and $j=1$, and for $i=1, 3$ and $j=2$. In case $j=2$, then since $C_{14}^{12}=7\cdot 17 \nmid |H|$, there exist at least 2 classes of stabilizer subgroups S_1^1 under H. Hence whether $j=1$ or 2, there exist at least 3 orbits of points with nontrivial N-stabilizer. Therefore, $r^*(H)\geqq 11$.

Case D $(q=2, m=5)$.

8.9 LEMMA. *Let* $m=5$, $q=2$, *and let* H *be a solvable subgroup of* U^*. *Then* $r^*(H)\geqq 3^{11}$.

Proof. $r^*(H)\geqq p^{32k}/2^{10}k|H_1|\geqq 3^{31}/2^{10}|H_1|$ from Lemma 5.8, since $p^k\geqq 3$, and $p^k/k\geqq 3$.

Now consider the cases I–III of Lemma 5.9.

I. $|H_1| \mid 10(2^{10}-1)$. II. Since $q=2$, then $k_1>1$. (i) $r_1=2$, $k_1=5$, $t_1=1$, and $|H_1| \mid 2(5\cdot 31)^2$. (ii) $r_1=5$, $t_1=1$, $k_1=2$, and $|H_1| \mid 5!\,(2\cdot 3)^5=2^8\cdot 3^6\cdot 5$. III. No case is possible since $(2^{k_1}-1, t_1)=1$ if $k_1t_1=10$. Hence in cases I–III, $|H_1|\leqq 2^8\cdot 3^6\cdot 5$ and $r^*(H)\geqq 3^{31}/2^{18}\cdot 3^6\cdot 5\geqq 3^{25}/2^{18}\cdot 5>3^{13}/5>3^{11}$.

9. **The class** $\mathfrak{B}_R$. Let $H\in\mathfrak{B}_R$ (Definition 2.9). From 3.1, H is a maximal solvable, irreducible primitive semilinear group acting on a vector space V over $F=GF(p^k)$; H contains A, the group of all scalar transformations of V; H contains a minimal normal nonabelian subgroup $N=N^i(q^m)\in\mathfrak{H}$, (Definitions 3.4 and 3.6), and $N\subseteq\mathfrak{C}_H(A)$; and N is reducible. Since H is primitive, N reduces V to a sum of s equivalent irreducible representations of degree q^m, so dim $V=sq^m$. Let T be a subspace of V which is irreducible under N, and let $\hat{N}$ be the representation of N on T; let X be a vector space of dimension s. Let $\bar{H}$ denote $\mathfrak{C}_H(A)$ and recall that $[H:\bar{H}]|k$ (Lemma 4.1). Moreover, from Lemma 4.1 we can assume that $\bar{H}\subseteq\mathfrak{N}_{GL(T)}(\hat{N})\otimes_F GL(X)$ acting on $V=T\otimes X$. There are mappings (mod F) $\alpha\otimes\beta\to\alpha$ and $\alpha\otimes\beta\to\beta$ from $\bar{H}$ into $\mathfrak{N}_{GL(T)}(\hat{N})$ and $GL(X)$, respectively. Let $\bar{H}_T$ and $\bar{H}_X$ be the images of these mappings. Then $\bar{H}\subseteq\bar{H}_T\otimes\bar{H}_X$. Let $\{\eta_i\}$, $\{x_i\}$, and $\{\eta_i\otimes x_j\}$ be bases of T, X, and $T\otimes X$, respectively, and let σ_1, σ_2, and σ be the semilinear mappings $(a_1, \ldots)\to(a_1^p, \ldots)$ of T, X, and $T\otimes X$. Thus $\sigma=\sigma_1\otimes\sigma_2$. Let $H=\langle\bar{H}, \gamma\sigma^u\rangle$, for $\gamma\in GL(V)$, and $u|k$, and let $\gamma\sigma^u=\gamma_1\sigma_1^u\otimes\gamma_2\sigma_2^u$ (as in [13, p. 482]). Then $\gamma_1\sigma_1^u$ normalizes $\bar{H}_T$ and $\gamma_2\sigma_2^u$ normalizes $\bar{H}_X$. Since H is maximal, this implies that $\bar{H}=\bar{H}_T\otimes\bar{H}_X$, and $|H| \mid k|\bar{H}_T|\,|\bar{H}_X|$. In decomposing H, it will also be necessary to consider the groups $H_T=\langle\bar{H}_T, \gamma_1\sigma_1^u\rangle$ and $H_X=\langle\bar{H}_X, \gamma_2\sigma_2^u\rangle$.

Finally note that H_T acts irreducibly on $W=N|\mathfrak{Z}(N)$ from (3.2; 5) and (4.1); and since $H\in\mathfrak{B}_R$ then H_T is primitive so $H_T\in\mathfrak{B}_I$.

As before, the discussion of $\mathfrak{B}_R$ is conducted modulo F. That is, all groups are factor groups (mod A) acting on the points (i.e., one-dimensional subspaces) of V. We continue to neglect the distinction between a point $x=Fv$ and a generating element $v\in V$.

9.1 DEFINITION. Let v be a point (i.e., a one-dimensional subspace) of V. Define $\tau(v)$ to be the N-dimension of $FN(v)$, i.e., $\tau(v)=(\dim_F FN(v))/q^m$. If $\tau(v)=d$, we will call v a d-point of V.

9.2 LEMMA. *Let $v=\sum_{i=1}^{d}\eta_i\otimes x_i$, where $\{\eta_i\}$ and $\{x_i\}$ are linearly independent sets of T and X, respectively. Then $\tau(v)=d$.*

Proof. First note that $F\hat{N}=GL(T)$. For $F\hat{N}$ is a simple algebra since T is irreducible; hence $F\hat{N}$ is a complete matrix algebra over an extension K of F. Therefore, $F\hat{N}$ affords an irreducible representation of $N=N(q^m)$ over K, and hence $\dim F\hat{N}=q^{2m}=q^{2m}[K:F]$, from (3.12). Hence $K=F$ and $F\hat{N}=GL(T)$.

Next, $FN(v)\simeq FN/A(v)$, where $A(v)$ is the annihilator of v in FN. Hence $\tau(v)=(\dim FN-\dim A(v))/q^m$. Let $\alpha=\alpha_1\otimes 1\in FN$, where $\alpha_1\in F\hat{N}$. Then $\alpha(v)=\sum\alpha_1(\eta_i)\otimes x_i$, and hence $\alpha(v)=0$ if and only if $\alpha_1(\eta_i)=0$, $1\leqq i\leqq d$, since $\{x_i\}_{1\leqq i\leqq d}$ is a linearly independent set. Let $R=\langle\eta_1,\ldots,\eta_d\rangle\subset T$ where $\dim R=d$. Then $A(v)\simeq A(R)$, the annihilator of R in $F\hat{N}$. Since $F\hat{N}=GL(T)$, $A(R)$ is the set of $q^m\times q^m$ matrices with zeros in columns 1 through d, and hence $\dim A(R)=(q^m-d)q^m$. Finally, $\dim FN=q^{2m}$, so $\tau(v)=(q^{2m}-q^m(q^m-d))/q^m=d$.

9.3 COROLLARY. $r^*(H)\geqq\min(s,q^m)$.

Proof. Since N is normal in H, clearly τ is the constant function on each orbit of H. From the proof of 9.2, there exist points v_i with $\tau(v_i)=i$, for

$$1\leqq i\leqq\min(\dim T,\dim X)=\min(q^m,s).$$

It is also clear that $1\leqq\tau(v)\leqq\min(s,q^m)$ for all $v\neq 0$ in V.

9.4 LEMMA. *Let H_T and H_X have c_1 and c_2 orbits on the sets of d-dimensional subspaces of T and X, respectively, where $d\leqq\min(s,q^m)$. Then H has at least $c_1\cdot c_2$ orbits among the d-points of V.*

Proof. Let $v=\sum_{i=1}^{d}\eta_i\otimes x_i$, where $\{\eta_i\}$ and $\{x_i\}$ are linearly independent elements of T and X, respectively. Let $R=\langle\eta_1,\ldots,\eta_d\rangle\subset T$ and $Y=\langle x_1,\ldots,x_d\rangle\subset X$. If $v'=\sum_{i=1}^{d}\eta_i'\otimes x_i'$ is another d-point, with associated subspaces R' and Y', and if $\alpha\otimes\beta\in H$ such that $\alpha\otimes\beta: v\to v'$, then clearly $\alpha\otimes\beta: R\otimes Y\to R'\otimes Y'$ and hence $\alpha(R)=R'$, $\beta(Y)=Y'$.

9.5 COROLLARY. *If $r^*(\bar{H}_T)=r^*(\bar{H}_X)=1$, then H is transitive on the 1-points of V.*

Proof. In this case, the proof of 9.4 implies that $\bar{H}$ $(=\bar{H}_T\otimes\bar{H}_X)$ is transitive on the 1-points of V.

9.6 LEMMA. *Let d be an integer, $1 \leqq d \leqq \min(s, q^m)$. Since the s-dimensional space X has*

$$\prod_{i=0}^{d-1} (p^{k(s-i)}-1)/(p^{k(i+1)}-1) \tag{9.7}$$

subspaces of dimension d, it follows that V has

$$\frac{p^{kd(d-1)/2}}{(p^k-1)} \prod_{i=0}^{d-1} \frac{(p^{k(s-i)}-1)(p^{k(q^m-i)}-1)}{(p^{k(i+1)}-1)} \tag{9.8}$$

d-points.

Proof. Let $v=\sum_{i=1}^{d} \eta_i \otimes x_i$ be a d-point with $Y=\langle x_1, \ldots, x_d\rangle \subset X$. Since $F\hat{N} = GL(T)$, $FN(v)=T \otimes Y$. Moreover, for every d-dimensional space Y' of X, $T \otimes Y'$ is generated by some d-point v' of V. If $Y \neq Y'$, then $T \otimes Y$ and $T \otimes Y'$ have no d-points in common. Therefore, it is sufficient to compute the number of d-points in $T \otimes Y$. If $\{x_i\}$ is a fixed ordered base of Y, then for each ordered linearly independent set $\{\eta_1', \ldots, \eta_d'\}$ of d elements of T, there is a unique d-point $\sum \eta_i' \otimes x_i$ in $T \otimes Y$, and each d-point of $T \otimes Y$ has this form. However, since a "point" is a one-dimensional space, each d-point arises from (p^k-1) distinct proportional ordered sets, $\lambda_i(\eta_1', \ldots, \eta_d')$, $1 \leqq i \leqq p^k-1$. Therefore, there exist

$$(p^{kq^m}-1)(p^{kq^m}-p^k)\cdots(p^{kq^m}-p^{k(d-1)})/(p^k-1) = \frac{p^{kd(d-1)/2}}{(p^k-1)} \prod_{i=0}^{d-1} (p^{k(q^m-i)}-1)$$

d-points in $T \otimes Y$.

Let $v=\sum_{i=1}^{d} \eta_i \otimes x_i$ be a d-point of V, and let $R=\langle \eta_1, \ldots, \eta_d\rangle$ and $Y=\langle x_1, \ldots, x_d\rangle$ as before. Let $\overline{H}_v$ be the subgroup of $\overline{H}$ fixing v. To determine $\overline{H}_v$, let $\overline{H}_R$ (K_R) and $\overline{H}_Y$ (K_Y) be the subgroups of $\overline{H}_T$ and $\overline{H}_X$ which fix (fix point-wise) R and Y, respectively. Let $\hat{H}_R=\overline{H}_R/K_R$, $\hat{H}_Y=\overline{H}_Y/K_Y$, and $K=K_R \otimes K_Y$.

9.9 LEMMA. *$K \subset \overline{H}_v$. Moreover, there exist isomorphic subgroups $B \subset \hat{H}_R$ and $C \subset \hat{H}_Y$ such that $(\hat{H}_R \otimes \hat{H}_Y)_v \simeq B$.*

Therefore, $|\overline{H}_v| = |K| \cdot |B|$.

Proof. Clearly, $K \subset \overline{H}_v \subset \overline{H}_R \otimes \overline{H}_Y$. Let $\beta \otimes \gamma \in \overline{H}_R \otimes \overline{H}_Y$, and let β and γ be represented on R and Y with respect to $\{\eta_i\}$ and $\{x_i\}$ by $d \times d$ matrices $b=(b_{ij})$ and $c=(c_{ij})$, respectively. Then $b \otimes c \in (\hat{H}_R \otimes \hat{H}_Y)_v$ if and only if $b^T=c^{-1} \pmod F$, where b^T is the transpose of b. Hence, there exist isomorphisms $b \otimes c \to b$ and $b \otimes c \to c$ from $(\hat{H}_R \otimes \hat{H}_Y)_v$ onto subgroups B and C of $\hat{H}_R$ and $\hat{H}_Y$, respectively, as required.

Conversely, if B and C are subgroups of $\hat{H}_R$ and $\hat{H}_Y$ respectively, such that $B^T=C^{-1}$, then the subgroup $\{b \otimes c : b^T=c^{-1}\}$ of $B \otimes C$ is in $(\hat{H}_R \otimes \hat{H}_Y)_v$, and this subgroup is isomorphic to B.

9.10 PROPOSITION. *Let* $H \in \mathfrak{B}_R$, *with* $N = N(q^m)$ *a minimal normal nonabelian subgroup of* H, *and let* $\dim_F(V) = sq^m$, *where* $F = GF(p^k)$. *Then*:

1. $r^*(H) = 2$ *only in the following cases*:

(a) $q^m = 2$, $p^k = 3$, $s = 3$, $H \subseteq GL_2(3) \otimes H_X$, *where* H_X *is the full group of the affine line of order* 3^3; *in this case* 3 *nonconjugate groups occur, whose orders are* $2^3 \cdot 3^2 \cdot 13$, $2^3 \cdot 3 \cdot 13$, *and* $2^3 \cdot 3 \cdot 13$. *However,* H_X *has a normal subgroup of order* 13 *so that a maximal abelian normal subgroup has order* 26 *instead of* 2. *Therefore the groups listed here are subgroups of* U^* *in Case* C_1 ($q = 2$, $m = 1$) *for* $p^k = 3^3$ (*see Corollary* 8.2).

(b) $q^m = 2$, $p^k = 3$, $s = 2$, *and* $H \subseteq GL_2(3) \otimes GL_2(3)$. *In this case* 5 *nonconjugate groups occur whose orders are* $2^6 \cdot 3^2$, $2^5 \cdot 3^2$, $2^6 \cdot 3$, $2^5 \cdot 3$ *and* $2^5 \cdot 3$. *However, these groups occur as subgroups of* U *in Corollary* 8.6(1), *for* $p^k = 3$ *and* $N = N^1(2^2) = Q_1 \times Q_2 \subseteq GL_2(3) \otimes GL_2(3)$. *The groups listed here normalize one or both of* Q_1, Q_2, *so that* $N^1(2^2)$ *is no longer a minimal normal nonabelian subgroup.*

2. $r^*(H) \geqq 4$ *except possibly in the following cases*:

$q^m = 2$	s	2	3	5
	p^k	$\leqq 7$	3	3

Proof. For convenience, let $r_i^*(H)$ denote the number of orbits of H among the i-points of V, for $1 \leqq i \leqq \min(s, q^m)$. In order that $r^*(H) \leqq 3$, it is sufficient to consider the following cases (9.3, 9.4):

I. $r^*(H_T) = r^*(H_X) = 1$; II. $r^*(H_T) = 2$ and $r^*(H_X) = 1$; III. $r^*(H_T) = 1$ and $r^*(H_X) = 2$. In I, H must have at most two orbits among all the d-points for $d > 1$, so $\min(s, q^m) \leqq 3$. Similarly, in II and III, $r_2^*(H) = 1$ and $\min(s, q^m) = 2$.

Some subcases are covered by Cases C_3–C_5 and D, §8. For example, let $q = 2$ and $H_X \in \mathfrak{B}_1$; let M be an irreducible minimal normal nonabelian subgroup of H_X and let M be a $\bar{q}$-group of length $\bar{m}$ in H. If $\bar{q} = 2$, then $N \otimes M$ is an irreducible H-group. If $m + \bar{m} \geqq 3$, then $r^*(H) \geqq 4$ from Cases C_3–C_5 (the proofs in Cases C_3–C_5 do not require that H act irreducibly on $(N \otimes M)/Z$).

Case I. Let $r^*(H_T) = r^*(H_X) = 1$, and apply Huppert's theorem (3.15) to H_X and H_T.

(a) Let $q^m = 2$, $p^k = 3$, 5, 7, 11, or 23, and $|H_T| = 24$.

(i) Let $H_X \in \mathfrak{A}$, so that $|H_X| = s(p^{ks} - 1)/(p^k - 1)$. Hence $r_2^*(H) \geqq$ (number of 2-points)$/|H| = p^k(p^{k(s-1)} - 1)/24s > 2$, except in the following cases:

(α) $s = 2$, $p^k \leqq 7$; (β) $s = 3$, $p^k \leqq 5$; (γ) $s = 4$ or 5, $p^k = 3$. If $r_2^*(H) = 1$, then $s = 2$ or 3 and $p^k = 3$. These cases will be discussed further, below.

(ii) Let $H_X \in \mathfrak{B}$, so $s = 2$ or 4. If $s = 4$, then $Q \otimes Q \otimes D \lhd H$ so Case C_3 applies. If $s = 2$, then $|H| = 24^2$, and $r_2^*(H) \geqq p^k(p^{2k} - 1)/(24)^2 > 2$ if $p^k \geqq 11$. If $r_2^*(H) = 1$, then $p^k | 24$ so $p^k = 3$.

(b) Let $q^m = 4$, $p^k = 3$, and $|H_T| = 2^6 \cdot 5$. If $H_X \in \mathfrak{B}$, then Cases C_3–C_5 apply. So assume $H_X \in \mathfrak{A}$. Then $r_2^*(H) \geqq 3 \cdot 5 \cdot 13(3^{s-1} - 1)/2^5 \cdot 5 \cdot s > 2$ for $s \geqq 3$.

Case II. Let $r^*(H_T)=2$ and $r^*(H_X)=1$. Then one of the following subcases applies:

(a) $q^m=2$, $p^k\geqq 9$, and $|\bar{H}_T|=24$ (from Case C_1, §8),

(b) $q^m=4$, $p^k=3$ or 7, $|H_T|=2^6\cdot 5$, and $s=2$ (from Case C_2),

(c) $q^m=3$, $p^k=4$, $|H_T|=2^3\cdot 3^3$, and $s=2$ (from Corollary 6.35).

In cases (a) and (b), $|H| \mid 24^2k$ or $|H| \mid 24ks(p^{ks}-1)/(p^k-1)$, as $H_X\in\mathfrak{B}$ or $\mathfrak{A}$ respectively. Since $r_2^*(H)=1$, then $p^k \mid |H|$ so $p=3$. In case (a), $p=3$ implies $r_2^*(H)>1$. In (b), $p^k=3$ and Case C_3 applies. In (c), $7\nmid |H|$ but $7|\#$ (2-points), so $r_2^*(H)>1$.

Case III. Let $r^*(H_T)=1$, $r^*(H_X)=2$. Since $H_T\in\mathfrak{B}_I$, Huppert's theorem implies $q^m=2$ or 4 and $k=1$; also $\min(q^m, s)=2$.

(i) Let $H_X\in\mathfrak{A}$. Then since H is maximal, $|\bar{H}_X|=(p^{sk}-1)/(p^k-1)$ and $r^*(H_X)=1$; this case is discussed in I.

(ii) If $H_X\in\mathfrak{B}_I$ and $r^*(H_X)=2$, then see II.

(iii) Let $H_X\in\mathfrak{B}_R$ and $r^*(H_X)=2$. From Case I (a)(i) and (a)(ii), $p^k=3$, $s=\bar{q}^{\bar{m}}\bar{s}$ for $\bar{q}^{\bar{m}}=2$ and $\bar{s}=2$ or 3. If $\bar{s}=2$, then C_3 applies. If $\bar{s}=3$, then $s=6$ and $r_2^*(H)\geqq 3(3^6-1)(3^5-1)/2(24)^2\cdot 13>1$.

(iv) Let $H_X\in\mathfrak{L}$. From Proposition 2.5 X has a decomposition $X=X_1\oplus X_2$ into imprimitivity subspaces of H_X. Since $r_2^*(H)=1$, H_X must be transitive on the two-dimensional subspaces of X, which is impossible unless $\dim(X_1)=\dim(X_2)=1$. But then $|H_X| \mid 2(p^k-1)$. Further, $p^k \mid |H|$ so $p^k=3$. If $q^m=4$, then H_T is not transitive on the two-dimensional subspaces of T, so $r_2^*(H)\neq 1$. Hence, $q^m=2$, $s=2$, and $p^k=3$.

Returning to I (a)(i) and (a)(ii), let us determine whether groups with $r^*(H)=2$ actually occur.

Let $q^m=2$, $p^k=3$, and $s=3$. Then $|H_T|=2^3\cdot 3$, $|H_X|=3\cdot 13$, and there exist $2^3\cdot 3\cdot 13$ 2-points. Further, $K_1=1$ and $K_2=1$ so that $|H_v| \mid 3$, for v a 2-point, from Lemma 9.9. Therefore, $r_2^*(H)=1$, and $r^*(H)=2$. Moreover, $r^*(H)=2$ if $|H_T|=8$ and $|H_X|=3\cdot 13$, or if $|H_T|=24$ and $|H_X|=13$.

Next, let $q^m=2$, $p^k=3$, and $s=2$, so $H=GL_2(3)\otimes GL_2(3)$, $|H|=24^2$, and V has 24 2-points. Since H_T and H_X are $GL_2(3)$, then $(H_T)^T=(H_X)^{-1}$, so there exists a 2-point v with $|H_v|=24$. Thus $r_2^*(H)=1$, and $r^*(H)=2$. Now let H be a subgroup of $GL_2(3)\otimes GL_2(3)$. In order for $r^*(H)=2$, $r^*(H_T)=r^*(H_X)=1$ (so $|H_T|=24$, 12, 8, or 4 and if $|H_T|=4$ then $H_T\subseteq SL_2(4)$); moreover, if B is maximal subgroup of H_T such that $B^T\subset H_X$, then $|H_T|\,|H_X|/|B|=24$. These conditions are satisfied for $|H_T|$, $|H_X|$ the following pairs: (4, 24), (8, 24), (12, 24), (24, 24) and (8, 12).

Finally, from Case I, there are no further groups for which $r^*(H)=2$.

To complete part 2 of Proposition 9.10, it is sufficient to show that no group H has $r^*(H)=3$ if $q^m=2$, $s=4$, and $p^k=3$ (I(a)(ii)(γ)), or if $q^m=2$, $s=3$, and $p^k=5$ (I(a)(ii)(β)).

Let $q^m=2$, $s=4$, and $p^k=3$. Then $|H_T|=24$, and $|H_X|=2^5\cdot 5$, and V has $2^4\cdot 3\cdot 5\cdot 13$ 2-points. Then $|K_1|=1$ and $5\nmid |K_2|$, so $|H_v| \mid 2^5$, for v a 2-point. If $r_2^*(H)=2$ with

orbit lengths $2^3 \cdot 3 \cdot 5a$ and, $2^3 \cdot 3 \cdot 5b$, then $a+b=26$ where a and b divide 2^5. This is impossible, so $r^*(H) \geqq 4$.

Let $q^m=2$, $s=3$, and $p^k=5$. Then $|H_T|=24$, $|H_X|=3 \cdot 31$, and V has $2^3 \cdot 3 \cdot 5 \cdot 31$ 2-points. Hence $|H_v| \mid 3$, for v a 2-point; and $r_2^*(H)=2$ implies there exist a and b such that $a+b=5$, $a|3$ and $b|3$. This is impossible, so $r^*(H) \geqq 4$.

Finally, let $q^m=2$, $s=5$, and $p^k=3$. Then $|H_T|=24$, $|H_X|=5 \cdot 11^2$, and V has $2^4 \cdot 3 \cdot 5 \cdot 11^2$ 2-points. Then $|H_v| \mid 5$ for v a 2-point; but the mapping $x \to x^3$ does not fix a two-dimensional space of X point-wise (mod $GF(3)$), so $|H_v| \neq 5$. Hence $r_2^*(H)=2$, and $r^*(H)=3$.

References

1. J. André, *Projektive Ebenen über Fastkörpern*, Math. Z. **62** (1955), 137–160.
2. E. Artin, *Geometric algebra*, Interscience, New York, 1957.
3. W. Burnside, *Theory of groups of finite order*, Dover, New York, 1955.
4. W. H. Bussey, *Galois field tables for* $p^n < 169$, Bull. Amer. Math. Soc. **12** (1905), 22–38.
5. H. S. M. Coxeter and W. O. Moser, *Generators and relations for discrete groups*, Springer-Verlag, New York, 1965.
6. C. W. Curtis and I. Reiner, *Representation theory of finite groups*, Interscience, New York, 1962.
7. L. Dickson, *Linear groups*, Dover, New York, 1958.
8. D. A. Foulser, *Solvable flag transitive affine groups*, Math. Z. **86** (1964), 191–204.
9. ———, *The flag transitive collineation groups of the finite Desarguesian affine planes*, Canad. J. Math. **16** (1964), 443–472.
10. P. Hall and G. Higman, *On the p-length of p-solvable groups*, Proc. London Math. Soc. (3) **6** (1956), 1–42.
11. D. G. Higman, *Finite permutation groups of rank* 3, Math. Z. **86** (1964), 145–156.
12. D. G. Higman and J. E. McLaughlin, *Rank* 3 *subgroups of the finite symplectic and unitary groups*, J. Reine Angew. Math. **218** (1965), 174–189.
13. B. Huppert, *Lineare auflösbare Gruppen*, Math. Z. **67** (1957), 479–518.
14. ———, *Zweifach transitive, auflösbare Permutationsgruppen*, Math. Z. **68** (1957), 126–150.
15. N. Jacobson, *Lectures in abstract algebra*, Vol. II, Van Nostrand, New York, 1953.
16. W. J. LeVeque, *Topics in number theory*, Vol. 1, Addison-Wesley, Reading, Mass., 1956.
17. D. Suprunenko, *Soluble and nilpotent linear groups*, Transl. Math. Monographs, Vol. 9, Amer. Math. Soc., Providence, R. I., 1963.
18. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.
19. H. J. Zassenhaus, *The theory of groups*, 2nd ed., Chelsea, New York, 1958.

University of Illinois at Chicago Circle,
Chicago, Illinois