PACIFIC JOURNAL OF MATHEMATICS
Vol. 58, No. 2, 1975

TRANSITIVE AFFINE TRANSFORMATIONS ON GROUPS

DAVID JONAH AND BERTRAM M. SCHREIBER

An affine transformation T on a group G is an automorphism followed by a translation; T is transitive if for each $x, y \in G$ there is an integer n such that $T^n(x) = y$. All groups with transitive affine transformations are determined: the infinite cyclic and infinite dihedral group are the only infinite examples; while the finite examples are semi-direct products of certain odd-order groups by a cyclic, dihedral or quaternion 2-group. The automorphism groups of the above groups are described, and the automorphisms which occur as parts of transitive affine transformations are given.

A bijective transformation T on a group G is called an *affine transformation* if there are an element s in G and an automorphism σ of G such that

$$T(x) = s\sigma(x), \quad \text{for all} \quad x \in G. \tag{1}$$

We are interested in determining those groups G on which there is defined a *transitive* affine transformation T, i.e., for each pair x and y of elements in G there is an integer n such that $T^n(x) = y$. Groups having transitive affine transformations we shall call *single orbit groups.*

We shall first show, in §5, that there exist only two infinite single orbit groups; namely, the infinite cyclic group and the infinite dihedral group. The structure of all finite single orbit groups as semi-direct products is then described in §6, and presentations of these groups in terms of generators and relations are given in §7. We shall show that any such group is the semi-direct product of an odd-order group whose Sylow subgroups are cyclic by a 2-group which is cyclic, dihedral or a generalized quaternion group. Moreover, the image of the action of the 2-Sylow subgroup on the odd-order part must be a cyclic group. All groups of the above type have transitive affine transformations. In §8 the automorphism groups of the finite single orbit groups are calculated; it is shown that, with two types of exceptions, these automorphism groups can all be expressed in the same simple form.

If T is an affine transformation given as in (1), the element s will be called the *initial value* of T and σ the *associated automorphism.* Both are uniquely determined by T: $s = T(1)$ and $\sigma(x) = (T(1))^{-1}T(x)$ for all x in G. Given a single orbit group G, we shall determine in §9 all the associated automorphisms of transitive affine transformations on G.

It is easy to see (Lemma 1.1 below) that the set of all affine transformations on a group G is a realization of the holomorph of G. However, we shall continue to speak of affine transformations since we are concerned here with elements of the holomorph that act transitively on G.

The topological analogs of the transitive affine transformations are continuous affine transformations on a locally compact topological group which are *ergodic* with respect to Haar measure. Ergodic affine transformations have been studied in a number of papers; see, for example, **[1; 2; 4; 10; 11]**, where necessary and sufficient conditions for ergodicity are found for affine transformations on compact groups of various types. Moreover, some effort has been put into determining which locally compact groups have ergodic affine transformations defined on them, and the discrete version of this very question represents one of the motivations for the study of single orbit groups. We refer here in this regard to **[5; 6; 7; 10]**, where some preliminary observations are made and where it is shown that the only locally compact, noncompact, abelian or connected group with an ergodic affine transformation is the infinite cyclic group (see Corollary 3.6 below).

Theorem 5.2 below was announced in **[4]**. A proof of most of Corollary 3.6 appears in **[8]**, and Example 2.3(i) was noticed by Thomas **[10]**.

1. Affine transformations.

LEMMA 1.1. (i) *The set* Aff(G) *of all affine transformations on a group G forms a subgroup of the symmetric group* Sym(G) *of the set G, namely the holomorph of G.*

(ii) *Let T in* Aff(G) *have associated automorphism σ and initial value s. Then T^k has associated automorphism σ^k and initial value $T^k(1)$. Furthermore*

$$T^k(1) = s\sigma(s)\cdots\sigma^{k-1}(s) \quad \text{if} \quad k>0, \tag{2}$$

$$T^k(1) = \sigma^{-1}(s^{-1})\sigma^{-2}(s^{-1})\cdots\sigma^{k}(s^{-1}) \quad \text{if} \quad k<0.$$

Proof. Let T_i have initial value s_i and associated automorphism σ_i for $i = 1,2$. Then T_1T_2 has initial value $s_1\sigma_1(s_2)$ and associated automorphism $\sigma_1\sigma_2$, for

$$T_1T_2(x) = s_1\sigma_1[s_2\sigma_2(x)] = s_1\sigma_1(s_2)[\sigma_1\sigma_2(x)]$$

by the definition of T_1 and T_2.

The identity transformation on G is clearly an affine transformation, and the inverse T^{-1} of the affine transformation T is affine with initial value $\sigma^{-1}(s^{-1})$ and associated automorphism σ^{-1}.

REMARKS 1.2. (i) Let T be transitive on a set X and let x be an element of X. Then $T^i(x) = T^j(x)$ if and only if $i \equiv j \bmod |X|$.

(ii) Let T in Aff(G) be left translation by an element $s \in G$. Then T is transitive on G if and only if G is a cyclic group with generator s.

BASIC LEMMA 1.3. *Let T be an affine transformation on a group G and let H be a nontrivial subgroup which is invariant under the associated automorphism σ. The transformation T induces a transformation $\bar{T}$ on the set $\bar{G} = G/H$ of left cosets of H given by $\bar{T}(\bar{x}) = \overline{T(x)}$. Then T is transitive on G if and only if $\bar{T}$ is transitive on G/H, the subgroup H has finite index n in G, and T^n is transitive on the subgroup H. If H is normal in G, then $\bar{T}$ is an affine transformation on the group G/H.*

Proof. Let T be transitive on G. Then $\bar{T}$ is transitive on G/H, for $\bar{T}^k = \overline{T^k}$ for every integer k. The set G/H must then be finite, for $\bar{T}$ is transitive on G/H and there is a positive integer m satisfying $\bar{T}^m(\bar{1}) = \bar{1}$; this m exists as T is transitive on G and H has a nonidentity element. The least positive integer n for which $T^n(1)$ is in H must then be the order of the set G/H, and if $T^m(1)$ is also in H then n divides m; these statements are direct consequences of Remark 1.2(i). T^n is then transitive on H as T is on G and as $T^n(x) = T^n(1)\sigma^n(x)$ is in H whenever x is.

Let $\bar{T}$ and T^n be transitive on G/H and H, respectively, and let x be an arbitrary element of G. Then, as $\bar{T}$ is transitive on G/H, $T^k(1)$ and x determine the same left coset of H for some integer k. Furthermore, as T^n is transitive on H and as $\sigma^{-k}[T^k(1)^{-1}x]$ is an element of H, there is an integer h such that

$$T^{nh}(1) = \sigma^{-k}[T^k(1)^{-1}x].$$

But this just says (by Lemma 1.1) that

$$T^{k+nh}(1) = T^k(1)\sigma^k[T^{nh}(1)] = x,$$

as needed to show T is transitive.

COROLLARY 1.4. *Let T_i be an affine transformation on the nontrivial group G_i, for $i = 1, 2$. Then the affine transformation $T = T_1 \times T_2$ is*

transitive on $G_1 \times G_2$ if and only if G_1, G_2 are finite groups with relatively prime orders.

Proof. If T is transitive on $G_1 \times G_2$, then by Lemma 1.3 G_i is finite and T_i is transitive on G_i. Furthermore

$$T^m(1) = (T_1^m(1),\ T_2^m(1)) = 1$$

where $m = \operatorname{lcm}(|G_1|, |G_2|)$. Thus by Remark 1.2(i) we have $m = |G_1 \times G_2| = |G_1|\,|G_2|$.

Let T_i be transitive on G_i for $i = 1, 2$, where G_1 and G_2 are finite groups with relatively prime orders. Then T is transitive, for $T^m(1) = 1$ means $T_i^m(1) = 1$ for $i = 1, 2$, which implies that both $|G_1|, |G_2|$, and so their product $|G_1 \times G_2|$, divide m.

COROLLARY 1.5. *An infinite nonabelian single orbit group is centerless.*

Proof. Let G be a nonabelian single orbit group with nontrivial center. The center would have finite index by Lemma 1.3, and the commutator subgroup would be finite by a theorem of Schur [**9**, p. 443] and would be of finite index by Lemma 1.3. Thus G would be finite.

2. Fixed points. For any endomorphism σ of a group G the set $F_\sigma = \{x \in G \mid \sigma(x) = x\}$ of fixed points of G is a subgroup of G. The endomorphism σ is called *fixed point free* if 1 is the only fixed point.

LEMMA 2.1. *Let T be a transitive affine transformation on a nontrivial finite group G. Then the fixed point group F_σ of the associated automorphism σ is a nontrivial cyclic subgroup of G with generator $T^m(1)$, where m is the index of F_σ in G.*

Proof. Let T be a transitive affine transformation on the finite group G, and suppose the associated automorphism σ is fixed point free. The initial value s must then be of the form $y^{-1}\sigma(y)$ for some y as the function $x \to x^{-1}\sigma(x)$ is a one-to-one, and so onto, function on the finite set G. The formula (2) telescopes to give $T^k(1) = y^{-1}\sigma^k(y)$ for all positive integers k. But as $y^{-1} = T^n(1)$ for some positive n, the element y, and so $s = y^{-1}\sigma(y)$, equals the identity of G. Hence $G = \{1\}$ for T is transitive on G. The group F_σ is cyclic with generator $T^m(1)$, $m = [G: F_\sigma]$, by Remark 1.2(ii) and Lemma 1.3.

COROLLARY 2.2. *Let G be a noncyclic group of order 4. Then an automorphism σ of G is the associated automorphism of a transitive*

affine transformation on G if and only if σ is not the square of an element in the automorphism group Aut(G).

Proof. The automorphism group Aut(G) is isomorphic to Sym(3), the symmetric group on three letters (the three nonidentity elements of G). The automorphisms of order 2 — the nonsquares — are the only automorphisms whose fixed point subgroup is cyclic of order 2.

Let σ be of order 2 and let s be a nonfixed point of σ. The product $s\sigma(s)$ is a nontrivial fixed point of σ; the affine transformation with initial value s and automorphism σ is transitive on G.

EXAMPLES 2.3. The following groups have transitive affine transformations.

(i) the infinite dihedral group D_∞
(ii) the finite dihedral groups D_m
(iii) the dicyclic groups DC_m

Proof. (i) The infinite dihedral group is generated by two elements x, y satisfying $y^2 = 1$ and $x^y = y^{-1}xy = x^{-1}$, and there is an automorphism α on D_∞ which takes y to yx and leaves x fixed. The fixed point set F_α has index 2 and generator $y\alpha(y) = x$. The affine transformation with automorphism α and initial value y is transitive by Remark 1.2(ii) and Lemma 1.3.

(ii) Each finite dihedral group D_m is a single orbit group for it is the factor group of the single orbit group D_∞ by the characteristic subgroup generated by x^m.

(iii) The dicyclic groups DC_m are generated by two elements x, y satisfying $x^{2m} = 1$, $y^2 = x^m$, and $x^y = x^{-1}$. Arguing as in (i), with α replaced by α^{m+1}, we see that DC_m is a single orbit group.

REMARK 2.4. Let T be transitive on the set X and let S by any element of Sym(X). Then $T^S = S^{-1}TS$ is also transitive on X.

LEMMA 2.5. *Let T be a transitive affine transformation on a group G and let T have initial value s and associated automorphism σ. Let C_s denote conjugation by s: $C_s(x) = sxs^{-1}$. Then the affine transformation with initial value $s' = s^{-1}$ and associated automorphism $\sigma' = C_s\sigma$ is also transitive on G. Furthermore, if G is finite, then*

$$[G: F_{\sigma'}] = |\sigma|,$$

and

$$[G: F_\sigma] = |\sigma'|.$$

Proof. Let θ be the inversion function: $\theta(x) = x^{-1}$. Then T^θ is transitive as T is, and

$$T^\theta(x) = [T(x^{-1})]^{-1} = [s\sigma(x^{-1})]^{-1} = \sigma(x)s^{-1}$$

for all x in G. Furthermore

$$\sigma(x)s^{-1} = s^{-1}s\sigma(x)s^{-1} = s^{-1}[C_s\sigma](x),$$

so that the affine transformation with initial value $s' = s^{-1}$ and associated automorphism $\sigma' = C_s\sigma$ is transitive on G.

Let $n = |\sigma|$. Then

$$\sigma T^k(1) = \sigma(s)\cdots\sigma^{k-1}(s)s = s^{-1}T^k(1)s$$

whenever n divides the positive integer k (see 1.2(i)). Conversely, if $\sigma T^k(1) = s^{-1}T^k(1)s$ where k is positive, then $\sigma^k(s) = s$ which, by the transitivity of T, implies that $\sigma^k = 1$. Thus $|\sigma|$ divides k if and only if $T^k(1)$ is in $F_{\sigma'}$ where $\sigma' = C_s\sigma$. Set $m = |F_{\sigma'}|$. As T is transitive there must be exactly m multiples of $|\sigma|$ which lie in the range $1 \leqq k \leqq |G|$; that is $[G: F_{\sigma'}] = |G|/|F_{\sigma'}| = |\sigma|$.

Because $T^{\theta\theta} = T$ the roles of (s, σ) and (s', σ') may be interchanged to deduce $[G: F_\sigma] = |\sigma'|$.

EXAMPLE 2.6. Let D_∞ be the infinite dihedral group. Then D_∞ has a fixed point free automorphism of order 2 which is part of a transitive affine transformation on D_∞.

Proof. Let x, y and α be as in the proof of Example 2.3 (i) and let β be the automorphism on D_∞ which takes x to x^{-1} and leaves y fixed. The composition $\beta\alpha = C_y\alpha$ is part of a transitive affine transformation by Example 2.3 (i) and Lemma 2.5. Furthermore, $\beta\alpha$ is of order 2 and is fixed point free. The latter follows as $\beta\alpha$ takes x to x^{-1} and yx^i to yx^{-i-1}.

3. *P*-Groups.

We shall determine the finite abelian single orbit groups and use the Burnside Basis Theorem for p-groups to determine all finite single orbit p-groups.

LEMMA 3.1. ([**5,** Lemma 2.3]) *Single orbit groups are finitely generated.*

Proof. Let the affine transformation T with initial value s and associated automorphism σ be transitive on a noncyclic group G. In

order to show that G is finitely generated we need only produce a finitely generated subgroup H which is invariant under σ, i.e. $\sigma(H) = H$, and which contains s; by the transitivity of T it follows that $H = G$.

As G is noncyclic and as T is transitive there is an integer $k \neq 0$ or 1 such that $T^k(1) = \sigma(s)$. If $k \geqq 2$, then from formula (2) we see that $H = \langle s, \sigma(s), \cdots, \sigma^{k-2}(s)\rangle$ is invariant under σ and contains s. If $k = -m$, with $m \geqq 1$ then from formula (2) we see that

$$[\sigma^{m+1}(s)]^{-1} = s\sigma(s)\cdots\sigma^{m-1}(s),$$

which implies that $H = \langle s, \sigma(s), \cdots, \sigma^m(s)\rangle$ is invariant under σ and contains s.

COROLLARY 3.2. *Abelian single orbit groups are either finite or finitely generated free.*

Proof. An abelian single orbit group G is of the form $G = t(G) \oplus F$ where $t(G)$ is the torsion subgroup of G and F is finitely generated free. If $t(G)$ is nontrivial, then $G = t(G)$ is finite, for F is the factor group of G by a nontrivial characteristic subgroup, so the free group F is finite by Lemma 1.3.

REMARK 3.3. Let G be an abelian single orbit group, written additively, and let p be a prime. Then the group G/pG is both a vector space over the integers mod p and a single orbit group.

We will denote a cyclic group of order n by $C(n)$.

LEMMA 3.4. *Let G be a nontrivial abelian single orbit group, written additively, which satisfies $pG = \{0\}$ for some prime p. Then*

(i) *$G = C(p)$ if p is odd,*

(ii) *$G = C(2)$ or $C(2) \times C(2)$ if $p = 2$.*

Proof. Let T be a transitive affine transformation on the group G where $pG = \{0\}$ for some prime p. The affine transformation is of the form $T(x) = s + \sigma(x)$ for x in G. By Corollary 3.2 G is of finite order $q = p^d$; as T is transitive, the integer q is the least positive integer such that

$$T^q(0) = s + \sigma(s) + \cdots + \sigma^{q-1}(s) = 0.$$

In fact q is the least positive integer such that the endomorphism $\tau_q = 1_G + \sigma + \cdots + \sigma^{q-1}$ is zero, as $\tau_q T = \sigma\tau_q$ since $\tau_q(s) = 0$, and as T is transitive on G. Thus the minimum polynomial $m(x)$ of σ divides

$$1+x+\cdots+x^{q-1}=\frac{1-x^q}{1-x}=(1-x)^{q-1}$$

over the integers mod p for q is a power of the prime p. Hence the minimum polynomial is of the form $m(x)=(1-x)^h$; furthermore $h \leqq d$ by the Cayley-Hamilton theorem.

The dimension d of G cannot satisfy

$$d < p^{d-1}, \tag{3}$$

for otherwise $m(x)$ would divide

$$(1-x)^{q'-1}=1+x+\cdots+x^{q'-1},$$

where $q'=p^{d-1}$, which in turn implies that

$$T^{q'}(0)=s+\sigma(s)+\cdots+\sigma^{q'-1}(s)=0,$$

in contradiction to T being transitive on a group of order q. Thus d must be 1 if p is odd and 1 or 2 if $p=2$, for otherwise equation (3) would be satisfied.

THEOREM 3.5. *Let G be a finite, single orbit p-group where p is a prime. Then*

(i) *G is cyclic whenever p is odd, and*

(ii) *G is a cyclic, dihedral, or quaternion group if $p=2$. Furthermore, all such p-groups are single orbit groups.*

Proof. Let $T(x)=s\sigma(x)$, x in G, be a transitive affine transformation on a finite p-group G. By the Burnside basis theorem there is a characteristic subgroup $\mathrm{Fr}(G)$ of G such that $G/\mathrm{Fr}(G)$ is a vector space over the integers mod p whose dimension is equal to the number of elements in a minimal generating set of G. Thus when p is odd, G is cyclic by Lemmas 1.3 and 3.4.

When p is 2, we shall first show that a subgroup H of G is cyclic if it is both proper and invariant under σ. By two applications of Lemma 1.3 the factor group $H/\mathrm{Fr}(H)$ has an automorphism whose square is the associated automorphism of a transitive affine transformation. By Lemma 3.4, Corollary 2.2 and the Burnside basis theorem, the groups $H/\mathrm{Fr}(H)$ and H must be cyclic.

If the 2-group G is noncyclic, then G has a cyclic subgroup H of index 2 which is invariant under σ. For σ induces an automorphism $\bar{\sigma}$ on $G/\mathrm{Fr}(G) \simeq C(2)\times C(2)$ which has a fixed point set $F_{\bar{\sigma}}$ of index 2 by Lemmas 1.3 and 2.1. The inverse image of $F_{\bar{\sigma}}$ under the natural

homomorphism from G to $G/\mathrm{Fr}(G)$ is the desired subgroup H of index 2. This group H is then cyclic by the preceding paragraph.

A 2-group with a cyclic subgroup of index 2 is known to either have a characteristic subgroup of type $C(2) \times C(2)$ or to be a cyclic, dihedral, semi-dihedral, or quaternion group; see for instance [3, p. 68]. The squares of the elements of a semi-dihedral group generate a characteristic subgroup isomorphic to a dihedral group. Such groups are, therefore, not single orbit groups.

The p-groups listed in the theorem are single orbit groups by Remark 1.2(ii) and Examples 2.3.

COROLLARY 3.6. *An abelian single orbit group is either cyclic or of the form $C(n) \times C(2) \times C(2)$ where n is odd. All such groups are single orbit groups.*

Proof. Such groups are single orbit by Remark 1.2(ii), Example 2.3(ii), and Corollary 1.4.

Let G be an abelian single orbit group written additively. G is either finitely generated free or finite by Corollary 3.2. If G were free with rank d and if p were a prime then G/pG would be a vector space of dimension d over the integers mod p. When p is odd, the dimension d is one by Lemmas 1.3 and 3.4. Hence the infinite cyclic group is the only infinite abelian single orbit group.

Each p-primary component of a finite abelian single orbit group G is either cyclic or of the form $C(2) \times C(2)$ by Lemmas 1.3 and 3.4. Such a group G is either cyclic or of the form $C(n) \times C(2) \times C(2)$ where n is odd.

4. Z-Groups. Finite groups whose p-Sylow subgroups are cyclic were shown by Burnside to be generated by two elements x and y which satisfy $x^m = 1$, $y^n = 1$, and $x^y = x^r$ where $n(r-1)$ is relatively prime to m; see for instance [3, pp. 104–107] where such groups are called *Z-groups*. Thus a Z-group is a semi-direct product $A \times_\theta B$ of two cyclic groups A, B of relatively prime orders where the structural homomorphism θ from A to $\mathrm{Aut}(B)$ takes a generator of A to a fixed point free automorphism of B.

THEOREM 4.1. *Let G be a finite group. Then there is a transitive affine transformation T on G of the form*

$$T(x) = axb \text{ for all } x \text{ in } G \tag{4}$$

if and only if G is a Z-group.

An affine transformation of the form (4) *is one whose associated automorphism is inner.*

Proof. Let T be of the form (4). Then T is transitive on G only if the order of G is the least common multiple of the orders of a and b. If this is the case and q is any prime power dividing the order of G, then q divides the order of either a or b. Thus all p-Sylow subgroups of G are cyclic.

Conversely, if G is a Z-group, let a and b be elements of G having relatively prime orders such that the order of G is the product of the orders of a and b. Then T, given by (4), is transitive.

The following lemma will be needed in §6.

LEMMA 4.2. *The outer automorphism group of a Z-group is abelian.*

Proof. Let G be a Z-group, and let x and y be generators of G as above. It is easy to see that the commutator subgroup G' is just $\langle x \rangle$ since $r - 1$ is relatively prime to m. Thus G' and G/G' are cyclic, so their automorphism groups are abelian. The kernel of the map

$$\mathrm{Aut}(G) \to \mathrm{Aut}(G') \times \mathrm{Aut}(G/G')$$

consists of maps of the form $\sigma(x) = x$, $\sigma(y) = yx^k$, and such a map σ is conjugation by a power of x.

5. Infinite groups. We now determine the infinite single orbit groups.

LEMMA 5.1. *A single orbit group G is isomorphic to a normal subgroup of a group H which is a product of two cyclic subgroups A and B. If G is finite, the cyclic group A has the same order as G, while the order of B divides the order of G.*

Proof. The set of all left translations of G by elements of G forms a normal subgroup of the group $\mathrm{Aff}(G)$ of all affine transformations on G; this subgroup is isomorphic to G. When T is an affine transformation on G with associated automorphism σ, let H be the subgroup of $\mathrm{Aff}(G)$ generated by the translations and T. This subgroup H consists of all affine transformations whose associated automorphism is a power of σ.

The transformation T is transitive on G if and only if the group A generated by T is a transitive permutation group on G. When this is

the case, the above group H is a product AB where B is the subgroup of elements of H leaving invariant a fixed element of G; see for instance [**3**, p. 25]. Choosing the fixed element of G to be the identity element of G makes B the subgroup generated by the automorphism σ. If G is finite the order of B divides that of G by Lemma 2.5.

THEOREM 5.2. *Let G be an infinite single orbit group. Then G is either the infinite cyclic group or the infinite dihedral group D_∞.*

Proof. By Corollary 3.6 we may restrict our attention to an infinite nonabelian single orbit group G. The commutator subgroup G' of G is abelian, for by Lemma 5.1 G is a subgroup of a group H which is a product AB of abelian subgroups, so $H'' = \{1\}$ by a theorem of N. Ito [**9**, p. 384]. The commutator subgroup G' is then infinite cyclic by Lemma 1.3 and Corollary 3.6.

The standard normalizer/centralizer theorem [**9**, p. 50] tells us there is a monomorphism $G/C \to \mathrm{Aut}(G') \simeq C(2)$ where C is the centralizer of G' in G. This characteristic subgroup C is a single orbit group, by Lemma 1.3, which has an infinite center. Hence C is infinite cyclic by Corollary 1.5 and $G/C \simeq C(2)$. Thus G must be isomorphic to D_∞ for D_∞ is the only nonabelian extension of an infinite cyclic group by the group $C(2)$.

6. Finite groups: characterization. We shall show that each finite single orbit group is a semidirect product of an odd-order Z-group by a 2-group which is a cyclic, dihedral, or quaternion group.

LEMMA 6.1. *Finite single orbit groups are supersolvable.*

Proof. By Lemma 5.1 a single orbit group G is a subgroup of a group H which is the product of two cyclic groups A and B. Such groups H are known to be supersolvable when B is finite [**9**, p. 383]. The group G, being a subgroup of a supersolvable group, is itself supersolvable.

THEOREM 6.2. *Let G be a finite single orbit group. Then G is a semi-direct product $G_0 \times_\theta G_2$, where*

(i) *G_0 is a Z-group and is the unique maximal subgroup of G of odd order;*

(ii) *G_2 is a 2-group which is either cyclic, dihedral, or a quaternion group;*

(iii) *the image of the action* $\theta\colon G_2 \to \mathrm{Aut}(G_0)$ *of* G_2 *on* G_0 *is a cyclic group*; *and*

(iv) *if* θ *is nontrivial, then* $\ker\theta$ *is cyclic.*

Conversely, all such semi-direct products are single orbit groups.

Proof. Let G be a finite single orbit group; it is supersolvable by Lemma 6.1 and so has a Sylow tower

$$G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = (1\}$$

of characteristic subgroups of G such that each factor group N_i/N_{i+1} is isomorphic to a p_i-Sylow subgroup of G where $p_1 < p_2 < \cdots < p_n$. (See for instance [**9**, p. 158]). By Lemma 1.3 each N_i and each p-Sylow subgroup of G is a single orbit group. Thus when p is odd each p-Sylow subgroup of G is cyclic by Theorem 3.5; when the order of G is even, then N_1 is a Z-group.

In any case, G is isomorphic to a semi-direct product $N\times_\theta P$ where N, a Z-group, is a characteristic subgroup and P is a 2-group which is a cyclic, dihedral, or quaternion group by Theorem 3.5.

Let σ be the associated automorphism of a transitive affine transformation on G. Set $\tau = \sigma \mid N$, let ρ be the automorphism on $P \simeq G/N$ induced by σ via the natural homomorphism from G to G/N, and let η be the natural homomoprhism from $\mathrm{Aut}(N)$ to $\mathrm{Out}(N) = \mathrm{Aut}(N)/\mathrm{Inn}(N)$. The diagram

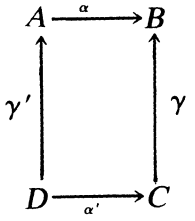
$$\begin{array}{ccccc} P & \xrightarrow{\theta} & \mathrm{Aut}(N) & \xrightarrow{\eta} & \mathrm{Out}(N) \\ \downarrow{\scriptstyle\rho} & & & & \downarrow{\scriptstyle\gamma} \\ P & \xrightarrow{\theta} & \mathrm{Aut}(N) & \longrightarrow & \mathrm{Out}(N) \end{array}$$

is commutative, where γ is induced by conjugation by τ. As P is a 2-group and as N, and so $\mathrm{Inn}(N)$, is of odd order it follows that $\ker\theta = \ker\eta\theta$. The image of θ is then a single orbit group by Lemma 1.3, for the kernel of θ is a ρ-invariant subgroup of P. But $\mathrm{Out}(N)$ is abelian — and so γ is the identity — as N is a Z-group (see Lemma 4.2). Thus σ on G induces the identity on $\mathrm{Im}\,\theta$ via the natural epimorphism $G \to P \to \mathrm{Im}\,\theta$ with σ-invariant kernel. Hence $\mathrm{Im}\,\theta$ must be cyclic by Remark 1.2(ii) and Lemma 1.3. Finally, if θ is nontrivial, then $\ker\theta$ is cyclic by the proof of Theorem 3.5.

The remainder of this section is primarily devoted to several diagram-chasing lemmas which will be used to give a noncomputational proof that groups of the type just exhibited are single orbit groups.

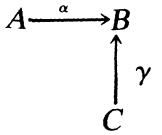
6.3. Recall that in a category a commutative diagram

(5)



is called a *pull-back* of

(6)

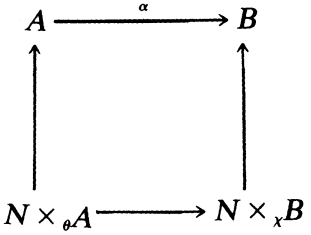


if for each pair of morphisms $f: X \to A$ and $g: X \to C$ satisfying $\alpha f = \gamma g$ there is a unique morphism $h: X \to D$ such that $\gamma' h = f$ and $\alpha' h = g$. We shall also say D is a pull-back of (6). For both sets and groups D can be taken as

$$\{(a, c) \in A \times C \mid \alpha(a) = \gamma(c)\}$$

where γ' and α' are induced by the projections. For groups γ' induces an isomorphism from $\ker \alpha'$ to $\ker \alpha$, and $|D| = (|A| \cdot |C|)/|B|$ when α and γ are epimorphims and A and C are finite.

LEMMA 6.4. *Let θ be the composition $\chi\alpha$ where α is a homomorphism from A to B and χ from B to* Aut(N). *Then*



is a pull-back diagram, where the vertical homomorphisms are the obvious projections and the other unlabeled homomorphism is induced by α and the identity on N.

Proof. Follows from the definitions and some diagram chasing.

6.5. Let α be a homomorphism from A to A' and let T and T' be affine transformations on A and A', respectively. Then $T'\alpha = \alpha T$ if and only if $\alpha(s) = s'$ and $\alpha\sigma = \sigma'\alpha$ when s and s' are the initial values and σ and σ' the associated automorphisms of T and T', respectively. The map α being fixed, we shall say T and T' are *compatible* if $\alpha T = T'\alpha$.

LEMMA 6.6. *Consider a pull-back* (5) *where A and C are finite and* α *and* γ *are epimorphisms. Let* T_A *and* T_C *be affine transformations on A and C, respectively, which are compatible with an affine transformation* T_B *on B. Then there is a unique affine transformation* T_D *compatible with both* T_A *and* T_C. T_D *is transitive on D if and only if* T_A *and* T_C *are transitive and the order of B is the greatest common divisor of the orders of A and C.*

Proof. The existence and uniqueness of T_D follow from the basic properties of the pull-back. As $T_D^n(1) = 1$ if only if both $T_A^n(1) = 1$ and $T_C^n(1) = 1$ and as the order of D is $(|A| \cdot |C|)/|B|$, the transformation T_D is transitive if and only if

$$\text{lcm}(|A|, |C|) = |D| = (|A| \cdot |C|)/|B|$$

which happens if and only if $|B| = \gcd(|A|, |C|)$.

Proof of Theorem 6.2 (*Completion*). Let $N \times_\theta A$ be a semi-direct product where N is an odd order Z-group, A is a 2-group which is cyclic, dihedral or quaternion, and θ has a cyclic image and has a cyclic kernel if it is nontrivial. We need to show that $N \times_\theta A$ is a single orbit group.

If A is cyclic, then we are done for $N \times_\theta A$ is a Z-group and so is single orbit by Theorem 4.1. If the 2-group A is dihedral or quaternion, then $\text{Im}\theta$, a cyclic group by assumption, is either trivial or $C(2)$ as $A/A' \simeq C(2) \times C(2)$. In both cases θ can be written as a composition $\chi\alpha$ where α takes A onto $C(2) = B$. The group $N \times_\chi B$ is also a Z-group as all of its Sylow subgroups are cyclic.

By the nature of A and its cyclic subgroups of index 2, there is a transitive affine transformation T_A on A which induces the identity on $B = C(2)$. (See Examples 2.3). Furthermore as N is a characteristic subgroup of the Z-group $N \times_\chi B = C$ there is also a transitive affine transformation T_C on C which induces the identity on $B = C(2)$. (See Theorem 4.1 and Lemma 1.3). The semi-direct product $N \times_\theta A$ is then a single orbit group by Lemmas 6.4 and 6.6.

COROLLARY 6.7. *Under the notation of Theorem* 6.2, $\ker\theta$ *is a characteristic subgroup of G.*

Proof. It is easy to see $\ker\theta$ is the set of elements in the centralizer $C_G(G_0)$ of G_0 of order a power of two. For if $x \in G_0$ and $y \in G_2$ such that $xy \in C_G(G_0)$, then $(xy)^n = x^n y^n$, $n = 1, 2, \cdots$. Since x has odd order and y has order a power of two, it follows that $y \in G_2 \cap C_G(G_0) = \ker\theta$ and that for xy to have order a power of two we must have $x = 1$.

7. Generators and relations. We shall show that all single orbit groups are extensions of cyclic groups by cyclic groups. Recall that an extension of $C(m)$ by $C(n)$ can be presented as

$$G(m, n, r, s) = \langle x, y \mid x^m = 1,\ x^y = x^r,\ y^n = x^s \rangle, \tag{7}$$

where the parameters m, n and r must satisfy $r^n \equiv 1$ and $(r-1)s \equiv 0 \bmod m$.

We know by Theorem 6.2 that the 2-Sylow subgroup of a finite single orbit group must be a cyclic, dihedral, or quaternion group; we shall call such single orbit groups *Z-groups*, *D-groups* or *Q-groups*, respectively.

THEOREM 7.1. (i) *Z-groups can be described as* $G(m, n, r, 0)$ *where* m *is relatively prime to* $n(r-1)$; *all such groups are Z-groups.*

(ii) *D-groups can be described as* $G(2^k m, 2n, r, 0)$ *where* m *and* n *are odd,* $k \geqq 1$, $n(r-1)$ *is relatively prime to* m, *and* $r \equiv -1 \bmod 2^k$; *all such groups are D-groups.*

(iii) *Q-groups can be described as* $G(2^k m, 2n, r, 2^{k-1}m)$ *where* m, n *and* r *satisfy the same conditions as in* (ii) *and where* $k \geqq 2$; *all such groups are Q-groups.*

Proof. (i) Follows from Theorem 6.2 and §4.

(ii) Let G be a D-group. Then by Theorem 6.2, G is a semi-direct product $N \times_\theta A$ where A is a dihedral 2-group, N an odd-order Z-group, and θ from A to $\mathrm{Aut}(N)$ has image which is either trivial or $C(2)$; in the latter case $\ker\theta$ is cyclic. Any semi-direct product $N \times_\chi C(2)$ is a Z-group. Hence by Lemma 6.4 G is the pull-back of

(8)
$$\begin{array}{ccc} A & \xrightarrow{\alpha} & C(2) \\ & & \uparrow{\scriptstyle \gamma} \\ & & C \end{array}$$

where A is a dihedral 2-group and C is a Z-group. The dihedral 2-group A has a presentation

$$\langle a, b \mid a^{2^k} = 1,\ b^2 = 1,\ a^b = a^{-1} \rangle \tag{9}$$

where $\theta(a) = 1$. The Z-group C has a presentation

$$\langle x_1, y_1 \mid x_1^m = 1,\ y_1^{2n} = 1,\ x_1^{y_1} = x_1^{r_1} \rangle \tag{10}$$

where m and n are odd and $2n(r_1 - 1)$ is relatively prime to m (in any Z-group $G(m', n', r', 0)$ the parameter m' must be odd).

By the Chinese Remainder Theorem there is an integer r satisfying both $r \equiv r_1 \bmod m$ and $r \equiv -1 \bmod 2^k$. A group $G(2^k m, 2n, r, 0)$ exists. For $r^{2n} \equiv (r^n)^2 \equiv 1 \bmod m$, as C was a Z-group, and $r^{2n} \equiv (-1)^{2n} \equiv 1 \bmod 2^k$, which gives $r^{2n} \equiv 1 \bmod 2^k m$. Clearly this group $D = G(2^k m, 2n, r, 0)$ is as described in (ii).

This group D also provides a pull-back of (8). For there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C(2^k) & \longrightarrow & A & \xrightarrow{\alpha} & C(2) & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle \gamma'} & & \uparrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & C(2^k) & \longrightarrow & D & \xrightarrow[\alpha']{} & C & \longrightarrow & 0 \end{array}$$

with exact rows where $\gamma'(x) = a$, $\gamma'(y) = b$, $\alpha'(x) = x_1$, and $\alpha'(y) = y_1$, the notation being as in (7), (9) and (10). By the uniqueness of the pull-back, the groups G and D are isomorphic.

Conversely, if $G = G(2^k m, 2n, r, 0)$ is as in (ii), then it is easily checked that its 2-Sylow subgroup is a dihedral group and that it fits into the commutative diagram (8), where $C = G(m, 2n, r, 0)$ is a Z-group. Thus G is a single orbit group, and so a D-group, by Lemma 6.6.

(iii) The proof for Q-groups is similar to that for D-groups and is omitted.

8. Automorphism groups. We shall determine the automorphism groups of finite single orbit groups.

Let G be a finite single orbit group with noncyclic 2-Sylow subgroup G_2. As was shown in §6, we have a pull-back diagram.

(11)
$$\begin{array}{ccc} G_2 & \xrightarrow{\alpha} & C(2) \\ \uparrow{\scriptstyle \gamma'} & & \uparrow{\scriptstyle \gamma} \\ G & \xrightarrow[\alpha']{} & G_1 \end{array}$$

where both α and γ are epimorphisms, G_1 is a Z-group, $\ker \gamma = G_0$ is the maximal odd-order subgroup of G, and $\ker \alpha$ is cyclic.

THEOREM 8.1. *Let G be a finite single orbit group with noncylic 2-Sylow subgroup.*

(i) *When G_2 is a direct summand of G, then*

$$\mathrm{Aut}(G) \simeq \mathrm{Aut}(G_0) \times \mathrm{Aut}(G_2) \simeq \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2).$$

(ii) *When G_2 is not a direct summand of G, then with two types of exceptions*

$$\mathrm{Aut}(G) \simeq \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2).$$

The two exceptions occur when G_2 is either $D_2 = C(2) \times C(2)$ or the classical quaternion group Q_4.

(iii) *When G_2 is either D_2 or Q_4, then*

$$\mathrm{Aut}(G) \simeq \mathrm{Aut}(G_1) \times C(2) \text{ or } \mathrm{Aut}(G_1) \times D_4,$$

respectively.

8.2. Before proceeding with the proof let us introduce some notation. When K is a subgroup of a group A, the group of all automorphisms of A leaving K invariant (as a set) will be denoted by $\mathrm{Aut}(A, K)$. When $\alpha: A \to B$ is an epimorphism, then for each σ_A in $\mathrm{Aut}(A, \ker \alpha)$ there is a unique automorphism σ_B on B satisfying $\alpha\sigma_A = \sigma_B\alpha$. The resulting homomorphism from $\mathrm{Aut}(A, \ker \alpha)$ to $\mathrm{Aut}(B)$ will be denoted by α_*.

LEMMA 8.3. *Let (5) be a pull-back where α and γ are epimorphisms and the kernels of α' and γ' are characteristic subgroups of D. Then there is a pull-back diagram*

$$\begin{array}{ccc} \mathrm{Aut}(A, \ker \alpha) & \xrightarrow{\alpha_*} & \mathrm{Aut}(B) \\ \uparrow{\scriptstyle \gamma'_*} & & \uparrow{\scriptstyle \gamma_*} \\ \mathrm{Aut}(D) & \xrightarrow{\alpha'_*} & \mathrm{Aut}(C, \ker \gamma) \end{array}$$

Proof. As (5) is a pull-back and as γ and α are epimorphisms, so are γ' and α'. When σ_A and σ_D are automorphisms on A and D

satisfying $\gamma'\sigma_D = \sigma_A\gamma'$, then $\sigma_D(\ker\alpha') = \ker\alpha'$ — meaning that γ_*' is as claimed. For since $\ker\alpha'$ is characteristic and the pull-back satisfies $\gamma'(\ker\alpha') = \ker\alpha$, we have

$$\begin{aligned}\alpha\sigma_A(\ker\alpha) &= \alpha\sigma_A\gamma'(\ker\alpha')\\ &= \alpha\gamma'\sigma_D(\ker\alpha')\\ &= \gamma\alpha'\sigma_D(\ker\alpha') = \{1\};\end{aligned}$$

and this same argument may be applied to both σ_D^{-1} and σ_A^{-1}. Similarly α' induces a homomorphism from $\mathrm{Aut}(D)$ to $\mathrm{Aut}(C, \ker\gamma)$; furthermore $\gamma_*\alpha_*' = \alpha_*\gamma_*'$.

Let σ_A, σ_B and σ_C be automorphisms on A, B and C respectively which satisfy $\sigma_A \in \mathrm{Aut}(A, \ker\alpha)$, $\sigma_C \in \mathrm{Aut}(C, \ker\gamma)$ and

$$\gamma_*(\sigma_C) = \sigma_B = \alpha_*(\sigma_A). \tag{12}$$

Then two applications of (12) and the commutativity of (5) yield $\alpha(\sigma_A\gamma') = \sigma_B\alpha\gamma' = \gamma(\sigma_C\alpha')$. Since (5) is a pull-back, there is a unique endomorphism — actually an automorphism — σ_D of D satisfying both $\gamma'\sigma_D = \sigma_A\gamma'$ and $\alpha'\sigma_D = \sigma_C\alpha'$; that is, $\gamma_*'(\sigma_D) = \sigma_A$ and $\alpha_*'(\sigma_D) = \sigma_C$, which makes the diagram involving the automorphism groups a pull-back diagram.

Proof of Theorem 8.1. Since (i) is obvious we assume G_2 is not a direct summand of G. Referring to (11), we have $\ker\gamma' = G_0$, a characteristic subgroup of G, while $\ker\alpha'$ is characteristic in G by Corollary 6.7. Hence, since $\mathrm{Aut}(C(2)) = 1$, Lemma 8.3 implies

$$\begin{aligned}\mathrm{Aut}(G) &= \mathrm{Aut}(G_1, G_0) \times \mathrm{Aut}(G_2, \ker\alpha)\\ &= \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2, \ker\alpha).\end{aligned} \tag{13}$$

If G_2 is neither D_2 nor Q_4, then $\ker\alpha$ is characteristic in G_2, so (13) gives (ii) of our theorem. If $G_2 = D_2$, then $\mathrm{Aut}(G_2, \ker\alpha) = \mathrm{Aut}(D_2, C(2)) = C(2)$. And if $G_2 = Q_4$, then $\ker\alpha = C(4)$, and a straightforward calculation shows $\mathrm{Aut}(Q_4, C(4)) = D_4$. Indeed Q_4 has a presentation

$$\langle a, b \mid a^4 = 1,\ a^2 = b^2,\ a^b = a^{-1}\rangle,$$

where $\langle a\rangle = \ker\alpha$. And $\mathrm{Aut}(Q_4, \langle a\rangle) = \langle\alpha, \beta_{-1}\rangle$, where $\alpha(a) = a$, $\alpha(b) = ba$, $\beta_{-1}(a) = a^{-1}$, and $\beta_{-1}(b) = b$.

8.4. For each positive integer m define

$$H(m) = \mathrm{Hol}(C(m)),$$

the holomorph of $C(m)$, and

$$U(m) = U(\mathbf{Z}/m\mathbf{Z}),$$

the group of units in the ring of integers modulo m; and for each positive integer t dividing m let

$$U(n;t) = \ker(U(n) \to U(t)) = \{i \in U(n) \mid i \equiv 1 \bmod t\}.$$

These groups have orders $m\phi(m)$, $\phi(m)$, and $\phi(m)/\phi(t)$, respectively, and $U(m) \simeq \mathrm{Aut}(C(m))$. When $r^n \equiv 1 \bmod m$ set $U(n;r,m) = U(n;t)$ where t is the multiplicative order of r mod m.

Observe that the groups $H(m)$ are "multiplicative" in the sense that $H(mn) = H(m) \times H(n)$ if m and n are relatively prime.

THEOREM 8.5. *Let G be a finite single orbit group, so that G is of the form $G(m,n,r,s)$ where the four parameters satisfy the conditions of one of the parts of Theorem* 7.1. *Then with two types of exceptions its automorphism group is given by*

$$\mathrm{Aut}(G) \simeq H(m) \times U(n;r,m).$$

The exceptions occur when the 2-Sylow subgroup of G is both a direct summand of G and either D_2 or Q_4. In these two cases G can be presented as $G(2m_0, 2n_0, r, 0)$ and $G(4m_0, 2n_0, r, 2m_0)$, respectively, where m_0 and n_0 are odd, and the respective automorphism groups are given by

$$\mathrm{Aut}(G) \simeq \mathrm{Sym}(3) \times H(m_0) \times U(n_0; r, m_0)$$

and

$$\mathrm{Aut}(G) \simeq \mathrm{Sym}(4) \times H(m_0) \times U(n_0; r, m_0).$$

In order to give the proof we need the following lemma.

LEMMA 8.6. *Let G be a Z-group presented as $G(m,n,r,0)$ with generators x and y as in* (7) *and Theorem* 7.1(*i*).

(i) *There is an automorphism α on G such that $\alpha(x) = x$ and $\alpha(y) = yx$. The order of α is m.*

(ii) *There is an automorphism* β_b *on* G *such that* $\beta_b(x) = x^b$ *and* $\beta_b(y) = y$ *if and only if* b *is relatively prime to* m. *We have* $\beta_{b_1}\beta_{b_2} = \beta_{b_1 b_2}$.

(iii) *There is an automorphism* γ_c *on* G *such that* $\gamma_c(x) = x$ *and* $\gamma_c(y) = y^c$ *if and only if* c *is relatively prime to* n *and* $r^c \equiv r \bmod m$. *We have* $\gamma_{c_1}\gamma_{c_2} = \gamma_{c_1 c_2}$.

Furthermore, every automorphism of G *is of the form* $\alpha^a\beta_b\gamma_c$ *for some suitable choices of* a, b, *and* c *which are unique modulo* m, m *and* n, *respectively. The* γ_c *are in the center of* Aut(G), *and* α *and the* β_b *satisfy*

$$\beta_b\alpha = \alpha^b\beta_b. \tag{14}$$

Thus $\mathrm{Aut}(G) \simeq H(m) \times U(n; r, m)$.

Proof. (i), (ii) and (14) may be verified by straightforward computations. It is also easy to see from the relation $x^y = x^r$ that a map of the form γ_c is an endomorphism if and only if $r^c \equiv r \bmod m$ and that such a γ_c is an automorphism if and only if c is relatively prime to n.

Let $\sigma \in \mathrm{Aut}(G)$. Since $\langle x \rangle$ is the commutator subgroup we must have $\sigma(x) = x^b$ for some b relatively prime to m and $\sigma(y) = y^c x^a$ where c is relatively prime to n. The composition $\tau = \sigma\beta_b^{-1}\alpha^{-a}$ then satisfies $\tau(x) = x$ and $\tau(y) = y^c$, i.e., $\sigma\beta_b^{-1}\alpha^{-a} = \gamma_c$. The asserted uniqueness is clear.

That γ_c is in the center of Aut(G) follows from $r^c \equiv r \bmod m$ and $(r-1)$ being relatively prime to m. For clearly γ_c commutes with the β_b, while a computation yields

$$\alpha\gamma_c = \gamma_c\alpha^{c[r]}$$

where

$$c[r] = 1 + r + \cdots + r^{c-1}. \tag{15}$$

And $(r-1)c[r] = r^c - 1 \equiv r - 1 \bmod m$, so $c[r] \equiv 1 \bmod m$.

The formula for Aut(G) now follows easily.

Proof of Theorem 8.5. The Z-group case is proved in Lemma 8.6. Thus let G be a D-group, and write $m = 2^k m_0$ and $n = 2n_0$ where m_0 and n_0 are odd. Then as shown in §7 G_0, G_1 and G_2 can be presented as $G(m_0, n_0, r, 0)$, $G(m_0, n, r, 0)$ and $G(2^k, 2, -1, 0)$ respectively.

Suppose first that $G = G_0 \times G_2$ and $k \geqq 2$. By an argument similar to the proof of Lemma 8.6 one obtains $\mathrm{Aut}(G_2) \simeq H(2^k)$. Also, if t is the multiplicative order of $r \bmod m_0$, so that t divides n_0, then it follows

from the fact that $r \equiv -1 \bmod 2^k$ that the order of r mod m is $2t$. Since $U(n_0; t) \simeq U(n; 2t)$, we have by Theorem 8.1(i), Lemma 8.6 and the observation in 8.4

$$\begin{aligned}\mathrm{Aut}(G) &\simeq \mathrm{Aut}(G_0) \times \mathrm{Aut}(G_2) \\ &\simeq H(m_0) \times U(n_0; r, m_0) \times H(2^k) \\ &\simeq H(m) \times U(n; r, m).\end{aligned}$$

If $G = G_0 \times D_2$, so that G can be presented as $G(2m_0, 2n_0, r, 0)$, then since it is known that $\mathrm{Aut}(D_2) \simeq \mathrm{Sym}(3)$ we have

$$\begin{aligned}\mathrm{Aut}(G) &\simeq \mathrm{Aut}(G_0) \times \mathrm{Aut}(D_2) \\ &\simeq H(m_0) \times U(n_0; r, m_0) \times \mathrm{Sym}(3).\end{aligned}$$

Now suppose G_2 is not a direct summand of G and that $k \geqq 2$. If t is the order of r mod m_0, then as above it follows that the order of r mod m is $2t$. Since $U(n; t) = U(n; 2t)$ we have by Theorem 8.1(ii) that

$$\begin{aligned}\mathrm{Aut}(G) &\simeq \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \\ &\simeq H(m_0) \times U(n; r, m_0) \times H(2^k) \\ &\simeq H(m) \times U(n; r, m).\end{aligned}$$

If $G_2 = D_2$, then as is easily seen the orders of r mod m_0 and m are the same. Since $H(2) = C(2)$ we have by Theorem 8.1(iii)

$$\begin{aligned}\mathrm{Aut}(G) &\simeq \mathrm{Aut}(G_1) \times C(2) \\ &\simeq H(m_0) \times U(n; r, m_0) \times C(2) \\ &\simeq H(m) \times U(n; r, m).\end{aligned}$$

The Q-groups may be dealt with similarly. It is only necessary to verify that for $k \geqq 3$ $\mathrm{Aut}(G_2) \simeq H(2^k)$; it is also known that $\mathrm{Aut}(Q_4) \simeq \mathrm{Sym}(4)$ [**12**, p. 148].

9. The set $\mathscr{A}(G)$. In this final section we deal with the problem of describing all transitive affine transformations on a single orbit group. Though this can be done, we have chosen not to burden the reader by carrying out these computations completely here. Rather, we shall limit ourselves to the determination of all associated automorphisms of such transformations. Thus, for G a single orbit group, let $\mathscr{A}(G)$ denote the set of all $\sigma \in \mathrm{Aut}(G)$ such that σ

is the associated automorphism of some transitive affine transformation on G. Since the infinite case is easy, and in view of the results in §§6 and 8, it suffices to describe $\mathscr{A}(G)$ when G is either cyclic, dihedral, a quaternion group or a Z-group. Let us preserve the notation established in §8. In particular, if $G = G(m, n, r, s)$ let α, β_b and γ_c be as defined in Lemma 8.6 if they exist. We begin with some general properties of the set $\mathscr{A}(G)$.

LEMMA 9.1. *Let G be a finite single orbit group of order n, and let $\sigma \in \mathscr{A}(G)$.*

(i) $\tau^{-1}\sigma\tau \in \mathscr{A}(G)$ *for all* $\tau \in \mathrm{Aut}(G)$.

(ii) $\sigma^k \in \mathscr{A}(G)$ *if k is relatively prime to n.*

(iii) *If the affine transformation with initial value s and associated automorphism σ is transitive, then $C_s\sigma \in \mathscr{A}(G)$, where C_s denotes conjugation by s.*

(iv) *If H is a normal subgroup of G invariant under σ and $\bar{\sigma}$ is the induced automorphism of G/H, then $\bar{\sigma} \in \mathscr{A}(G/H)$.*

Proof. Let $T(x) = s\sigma(x)$ be transitive on G.

(i) Let $\tau \in \mathrm{Aut}(G)$. Then the affine transformation

$$S(x) = \tau^{-1}T\tau(x) = \tau^{-1}(s)\tau^{-1}\sigma\tau(x)$$

is transitive by Remark 2.4.

(ii) If k is relatively prime to n and $S = T^k$, then S has associated automorphism σ^k by Lemma 1.1, and S is easily seen to be transitive.

(iii) and (iv) are implied by Lemmas 2.5 and 1.3, respectively.

We shall also need the following variant of Lemma 1.3.

LEMMA 9.2. *Let G be a finite group and H a subgroup of G of index n. Suppose that the affine transformation T on G with associated automorphism σ satisfies the following conditions.*

(i) $\sigma^n(H) = H$.

(ii) *n is the least positive integer such that $T^n(1) \in H$.*

(iii) *The restriction of T^n to H is transitive on H.*

Then T is transitive on G.

Proof. Recall that (iii) makes sense by (ii) of Lemma 1.1. Suppose $T^k(1) = 1$ for some positive integer k. Write $k = nq + r$, where $0 \leqq r < n$. Then

$$1 = T^k(1) = T^{nq}(T^r(1)) = T^{nq}(1)\sigma^{nq}(T^r(1)).$$

As $T^{nq}(1) \in H$, (i) implies that $T^r(1) \in H$, whence $r = 0$ by (ii). But (iii) then says $|H|$ divides q, so $|G|$ divides $nq = k$. Hence T is transitive on G.

9.3. For each positive integer n, let $\pi(n)$ denote the product of all the distinct primes dividing n if n is not divisible by 4. If 4 divides n let $\pi(n)$ be twice the product of the primes dividing n. Recall that for c and r positive integers, the symbol $c[r]$ was defined in (15).

THEOREM 9.4. *Let* $G = C(n)$. *Then* $\mathscr{A}(G) = \{\beta_b \in \mathrm{Aut}(G) \mid b \equiv 1 \bmod \pi(n)\}$.

Proof. In view of the observation in 8.4 and Corollary 1.4 it suffices to consider the case $n = p^k$ where p is a prime. If $\beta_b \in \mathscr{A}(G)$, then the automorphism β_b of $C(p)$ is in $\mathscr{A}(C(p))$ by (iv) of Lemma 9.1, whence this automorphism must have a nontrivial fixed point group by Lemma 2.1. It follows that $b \equiv 1 \bmod p$. If $p = 2$, $k > 1$ and $b \equiv 3 \bmod 4$, then the automorphism β_b of $C(4)$ is not in $\mathscr{A}(C(4))$. Indeed, in this case, for any $s \in C(4)$ $s\beta_b(s) = s^4 = 1$, so the affine transformation with initial value s and associated automorphism β_b is not transitive. Thus $\beta_b \in \mathscr{A}(G)$ implies that $b \equiv 1 \bmod \pi(n)$.

Conversely, if $b \equiv 1 \bmod \pi(n)$ and x is a generator of G, let us show that the map $T(y) = x\beta_b(y)$ is transitive by induction on k. If $k = 1$, then T is clearly transitive since $p[b] \equiv 0 \bmod p$. And for $k > 1$ observe that, since $j[b] \equiv j \bmod p$ for all j, p is the least positive integer such that $T^k(1) \in \langle x^p \rangle$. Clearly $\beta_b^p(x^p) = \beta_{b^p}(x^p) \in \langle x^p \rangle$, $b^p \equiv 1 \bmod p$ and $|\langle x^p \rangle| = p^{k-1}$. If $p > 2$ and $b = 1 + mp$ with $m \not\equiv 0$, then $b^p \equiv 1 + mp^2 \bmod p^3$. Thus

$$p[b] = \frac{b^p - 1}{b - 1} \equiv \frac{mp^2}{mp} = p \not\equiv 0 \bmod p^2, \tag{16}$$

while (16) is obvious if $p = 2$ and $b \equiv 1 \bmod 4$. Finally $T^p(1)$ is a generator of $\langle x^p \rangle$. Thus we may assume that the restriction of T^p to $\langle x^p \rangle$ is transitive. By Lemma 9.2 T is transitive on G, and the induction is complete.

THEOREM 9.5. (i) $\mathscr{A}(D_2) = \{\sigma \in \mathrm{Aut}(D_2) \mid \sigma$ *is not a square*$\}$.

(ii) $\mathscr{A}(Q_4) = \{\sigma \in \mathrm{Aut}(Q_4) \mid \sigma$ *corresponds to a transposition or a 4-cycle*$\}$.

Proof. (i) $\alpha \in \mathscr{A}(D_2)$ and α has order 2. Since all elements of Sym(3) of order 2 are conjugate, by Lemma 9.1 they all correspond to elements of $\mathscr{A}(D_2)$. On the other hand, the elements of order 3 in $\mathrm{Aut}(D_2)$ cannot be in $\mathscr{A}(D_2)$ since their order does not divide that of D_2. Finally, since D_2 is not cyclic, the identity is not in $\mathscr{A}(D_2)$.

(ii) $Q_4/Z(Q_4) \simeq D_2$. Hence by (i) and Lemma 1.3 no element of $\mathscr{A}(Q_4)$ is a square. Hence no element of $A(Q_4)$ corresponds to a permutation of order 3 or an even permutation of order 2 in Sym(4).

Now, $\alpha \in \mathscr{A}(Q_4)$ and has order 4, so by conjugation all elements of $\mathrm{Aut}(Q_4)$ of order 4 are in $\mathscr{A}(Q_4)$. And $\beta_{-1}\alpha = C_y\alpha \in \mathscr{A}(Q_4)$ by (iii) of Lemma 9.1 and has order 2; hence it must correspond to an odd permutation. Thus, by conjugation, all elements of $\mathrm{Aut}(Q_4)$ corresponding to odd permutations of order 2 in Sym(4) lie in $\mathscr{A}(Q_4)$.

THEOREM 9.6. *Let* $G = D_{2^k}$ *or* $Q_{2^{k+1}}$, $k \geqq 2$. *Then* $\mathscr{A}(G) = \{\beta_b\alpha^a \mid a \text{ is odd.}\}$

Proof. G has a presentation as in (7) as $G(2^k, 2, -1, s)$ where $s = 0$ if G is dihedral and $s = 2^{k-1}$ if G is a quaternion group. Factoring out by the characteristic subgroup $\langle x^2\rangle$ yields D_2. If $\beta_b\alpha^a \in \mathscr{A}(G)$ the induced automorphism on D_2, also denoted $\beta_b\alpha^a$, is in $\mathscr{A}(D_2)$. Since $\beta_b = id = \alpha^2$ on D_2, we conclude that a must be odd.

If T is the affine transformation on G with initial value y and associated automorphism $\beta_b\alpha^a$ with a odd, then direct calculation yields for $n = 1, 2, \cdots$

$$T^{2n}(1) = x^{(ab+s)n[b^2]}, \quad T^{2n+1}(1) = y[T^{2n}(1)]^b.$$

Now, since b must be odd for β_b to be an automorphism, $b^2 \equiv 1 \bmod 4$, so the affine transformation $S(y) = 1 + b^2y \bmod 2^k$ is transitive on $\mathbf{Z}/2^k\mathbf{Z}$ (Theorem 9.4) and satisfies $S^n(0) = n[b^2]$. It follows that if $T^m(1) = 1$ then m is even and, since $ab + s$ is odd, $(m/2)[b^2] \equiv 0 \bmod 2^k$, whence 2^k divides $\frac{1}{2}m$. Thus T is transitive on G.

The remainder of the section is devoted to the proof of the following theorem.

THEOREM 9.7. *Let G be a Z-group presented as $G(m, n, r, 0)$. The automorphism $\alpha^a\beta_b\gamma_c$ is in $\mathscr{A}(G)$ if and only if $c \equiv 1 \bmod \pi(n)$ and m may be written as the product of two relatively prime positive integers m_1 and m_2 such that*

(i) $b \equiv r^j \bmod \pi(m_1)$ *for some j relatively prime to n,*

(ii) $b \equiv 1 \bmod \pi(m_2)$, *and*

(iii) *a is relatively prime to m_2.*

LEMMA 9.8. *Let G be as in Theorem 9.7. Then $\beta_b\gamma_c \in \mathscr{A}(G)$ if and only if*

(i) $c \equiv 1 \bmod \pi(n)$, *and*

(ii) $b \equiv r^j \bmod \pi(m)$, *where*

(iii) *j is relatively prime to n.*

Proof. Let T be the affine transformation on G with initial value $y^j x^i$ and associated automorphism $\beta_b\gamma_c$. Direct calculation shows that

$$T^k(1) = y^{k[c]j} x^{k[r^j,b]i}, \qquad k = 1, 2, \cdots,$$

where

$$k[a,b] = a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1} = \frac{a^k - b^k}{a - b}.$$

Hence

$$T^n(1) = x^{n[r^j,b]i}.$$

By Lemma 1.3 T is transitive if and only if the induced affine transformation $\bar{T}$ on $G/G' = G/\langle x\rangle$ and the restriction of T^n to $\langle x\rangle$ are transitive. Whence Theorem 9.4 implies T is transitive if and only if (i) and (iii) are satisfied as well as

(17) $b^n \equiv 1 \bmod \pi(m)$, and $n[r^j, b]i$ is relatively prime to m.

Thus if T is transitive, then

(iv) i is relatively prime to m,

and (17) along with the fact that $r^n \equiv 1 \bmod m$ gives

$$(r^j - b)n[r^j, b] = r^{jn} - b^n \equiv 0 \bmod \pi(m),$$

so (17) implies that (ii) follows. Conversely, if (i)–(iv) are satisfied, then by (ii)

$$r^j n[r^j, b] \equiv r^j n[r^j, r^j] = nr^{jn} \equiv n \bmod \pi(m).$$

Hence (17) holds and we conclude that T is transitive.

LEMMA 9.9. *Let b, c and j be as in (i)–(iii) of Lemma 9.8. Then $\alpha^a\beta_b\gamma_c$ is conjugate to $\beta_b\gamma_c$ for all $a = 1, 2, \cdots, m-1$.*

Proof. First note that $b - 1$ is relatively prime to m. Indeed, if $r^j \equiv 1 \bmod p$ for some prime p dividing m, then since $r^n \equiv 1 \bmod p$ and j and n are relatively prime, we would have $r \equiv 1 \bmod p$. But $r - 1$ is relatively prime to m as G is a Z-group. Thus, for any choice of a, we may choose a positive integer i such that $(b-1)i \equiv a \bmod m$. Then

$$\alpha^a\beta_b\gamma_c = \alpha^{(b-1)i}\beta_b\gamma_c = \alpha^{-i}\alpha^{bi}\beta_b\gamma_c = \alpha^{-i}\beta_b\gamma_c\alpha^i.$$

LEMMA 9.10. *Let G be as above and suppose that*
(i) *a is relatively prime to m,*
(ii) *$b \equiv 1 \bmod \pi(m)$, and*
(iii) *$c \equiv 1 \bmod \pi(n)$.*
Then $\alpha^a\beta_b\gamma_c \in \mathcal{A}(G)$.

Proof. Set $t = r^k b$ for any k relatively prime to n. Then t is relatively prime to m and $\beta_t\gamma_c \in \mathcal{A}(G)$ by Lemma 9.8. In fact, the affine transformation with associated automorphism $\beta_t\gamma_c$ and initial value $y^k x^i$ is transitive for any i relatively prime to m. Given a relatively prime to m, choose i such that $a \equiv i(1-r) \bmod m$, and set $s = x^i y^k = y^k x^{ir^k}$. Observe that $C_x = \alpha^{r-1}$ and $C_y = \beta_r^{-1}$. Thus by Lemma 9.1

$$\begin{aligned}\alpha^a\beta_b\gamma_c &= \alpha^{i(r-1)}\beta_r^{-k}\beta_{r^k b}\gamma_c \\ &= C_x^i C_y^k \beta_t\gamma_c = C_s\beta_t\gamma_c \in \mathcal{A}(G).\end{aligned}$$

LEMMA 9.11. *Let G, b and c be as in Lemma 9.10, and suppose $\alpha^a\beta_b\gamma_c \in \mathcal{A}(G)$. Then a must be relatively prime to m.*

Proof. Suppose that the prime p divides both a and m. Since the automorphism α on the group $H = G/\langle x^p\rangle$ has order p and $b \equiv 1 \bmod p$, the automorphism on H induced by $\alpha^a\beta_b\gamma_c$ is γ_c and is in $\mathcal{A}(H)$, which is impossible by Lemma 9.8.

Proof of Theorem 9.7. Sufficiency. Consider the pull-back diagram

$$\begin{array}{ccc} G_1 & \longrightarrow & C(n) \\ \uparrow & & \uparrow \\ G & \longrightarrow & G_2 \end{array}$$

where $G_i = G/\langle x^{m_i}\rangle = G(m_i, n, r, 0)$, $i = 1, 2$. For $i = 1, 2$ let σ_i denote the automorphism of the form $\alpha^a\beta_b\gamma_c$ on G_i and let x_i and y_i be the canonical generators of G_i. Then $\sigma_1 \in \mathcal{A}(G_1)$ by Lemmas 9.1, 9.8 and 9.9 and $\sigma_2 \in \mathcal{A}(G_2)$ by Lemma 9.10. Moreover, inspection of the proofs of these lemmas shows that if we take k in the proof of Lemma 9.10 such that $k \equiv -j \bmod n$, then for $i = 1, 2$ σ_i is the associated automorphism of a transitive affine transformation T_i on G_i with initial value of the form $s_i = y_i^j x_i^{k_i}$. The details will be left to the reader. Thus the images of s_1 and s_2 in $C(n)$ coincide, so there is an element $s = y^j x^k \in G$ whose image in G_i is s_i, $i = 1, 2$. Hence if T is

the affine transformation on G with initial value s and associated automorphism $\alpha^a\beta_b\gamma_c$, then T is compatible with both T_1 and T_2 in the sense of 6.5, whence T is transitive by Lemma 6.6.

Necessity. Since m is odd, we may write $m = m_1m_2$ such that $b - 1$ is relatively prime to m_1 and $b \equiv 1 \bmod \pi(m_2)$. Let G_1, G_2, σ_1 and σ_2 be as above with respect to this choice of m_1 and m_2. Since $\sigma_1 \in \mathcal{A}(G_1)$ and is conjugate to the automorphism $\beta_b\gamma_c$ of G_1 by the choice of m_1 (see the proof of Lemma 9.9), condition (i) of the theorem as well as the condition on c must hold by Lemmas 9.1 and 9.8. Condition (iii) follows from Lemma 9.11 applied to σ_2.

REFERENCES

1. F. J. Hahn, *On affine transformations of compact abelian groups*, Amer. J. Math., **85** (1963), 428–446.
2. A. H. M. Hoare, W. Parry, *Semi-groups of affine transformations*, Quart. J. Math. Oxford Ser., (2) **17** (1966), 106–111.
3. D. S. Passman, *Permutation Groups*, New York — Amsterdam: W. A. Benjamin 1968.
4. M. Rajagopalan, B. M. Schreiber, *Ergodic automorphisms and affine transformations*, Proc. Japan Acad., **46** (1970), 633–636.
5. ———, *Ergodic automorphisms and affine transformations of locally compact groups*, Pacific J. Math., **38** (1971), 167–176.
6. R. Sato, *On locally compact abelian groups with dense orbits under continuous affine transformations*, Proc. Japan Acad., **46** (1970), 147–150.
7. ———, *Properties of ergodic affine transformations of locally compact groups, II*, Proc. Japan Acad., **46** (1970), 236–238.
8. ———, *Properties of ergodic affine transformations of locally compact groups, III*, Proc. Japan Acad., **47** (1971), 163–166.
9. W. R. Scott, *Group Theory*, Englewood Cliffs, N. J.: Prentice-Hall 1964.
10. R. K. Thomas, *On affine transformations of locally compact groups*, J. London Math. Soc., (2) **4** (1972), 599–610.
11. P. Walters, *Topological conjugacy of affine transformations of tori*, Trans. Amer. Math. Soc., **131** (1968), 40–50.
12. H. Zassenhaus, *The Theory of Groups* (2nd ed.), New York: Chelsea 1958.

Received May 22, 1974. Research of the first author was partially supported by a Wayne State University Faculty Research Award and that of the second author by the National Science Foundation under Grants GP–13741 and GP–20150.

WAYNE STATE UNIVERSITY