J. Austral. Math. Soc. (*Series A*) 27 (1979), 189–198

A CLASS OF POLYNOMIAL PERMUTATIONS ON GROUPS

G. KOWOL

(Received 23 June; revised 28 August 1978)

Communicated by H. Lausch

Abstract

Let G be a finite group and $u(G)$ the group of all invertible transformations (polynomial permutations) of the form $x \to a_1 x^{k_1} a_2 \ldots a_r x^{k_r} a_{r+1}$ ($a_i \in G$, x runs through G). Continuing investigations of H. Lausch of groups satisfying $u(G) = \{x \to ax^k b\}$ we show here that this condition implies that G is the direct product of its $\{2, 3\}$-Hall subgroup and its $\{2, 3\}'$-Hall subgroup H where H is nilpotent of class $\leqslant 2$. Essentially all non-nilpotent groups G of order $2^m 3^n$ are described having the property $u(G) = \{x \to ax^k b\}$.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): primary 20 F 15; secondary 20 B 99.

1. Introduction

In this paper we consider the following problem of H. Lausch. Let G be a finite group, then the set of all transformations (polynomial functions) of the form

$$x \to a_1 x^{k_1} a_2 \ldots a_r x^{k_r} a_{r+1}$$

($a_i \in G$, x runs through G) forms a semigroup with identity id: $x \to x$. Thus the invertible transformations (polynomial permutations) form a group $u(G)$. We are here concerned with groups for which $u(G) \subseteq \{x \to ax^k b\}$. Lausch (1966) showed that for $(o(G), 2) = 1$ the condition $u(G) \subseteq \{x \to ax^k b\}$ implies that G is nilpotent with Sylow-3-subgroup of class $\leqslant 3$ and Sylow-p-subgroup ($p > 3$) of class $\leqslant 2$. Conversely, if $(o(G), 6) = 1$ and G is nilpotent of class $\leqslant 2$ then all polynomial permutations are of the form $x \to ax^k b$. The case $o(G) = 3^n$ was solved in Kowol (1978): $u(G) \subseteq \{x \to ax^k b\}$ holds if and only if G satisfies the second Engel condition or equivalently if and only if G is a homomorphic image of a subgroup of $P \times H$, where $\exp P = 3$ and H is a 3-group of class $\leqslant 2$.

Therefore the case $2|o(G)$ remained unsolved. One result in this direction was derived in Kowol (1977), where it is shown that G has to be supersolvable. Here we are able to give a more detailed answer to this problem: First, $u(G) \subseteq \{x \to ax^k b\}$ implies that G is a direct product of a (supersolvable) group M of order $2^m 3^n$ and a nilpotent group $N, (o(N), 6) = 1$, of class $\leqslant 2$. Therefore one only has to study (non-nilpotent) groups of order $2^m 3^n$ fulfilling the above condition. Under certain trivial restrictions we can describe all such groups G, namely

$$G = \langle a, b_1, \ldots, b_s | a^2 = b_i^3 = e, b_i b_j = b_j b_i, (ab_i)^2 = e \text{ for all } i, j \rangle.$$

All groups considered are finite.

2. General results

First we show a general group theoretical lemma. Let G be a group and $H(G)$ the subgroup

$$H(G) = \{g \in G, g^{-1}hg = h^{n(g)} \text{ for all } h \in G, n(g) \text{ suitable in } \mathbb{N}\}.$$

In Lausch *et al.* (1966) is proved that $H(G)$ is an abelian characteristic subgroup of G which contains the centre $Z(G)$ of G.

LEMMA 1. *$H(G) = E$ if and only if $Z(G) = E$.*

PROOF. Because of $H(G) \supseteq Z(G)$ one direction is trivial. Conversely, let $Z(G) = E$ and suppose indirectly that there exists a $g \in H(G)$, $g \neq e$. Fix this g. Writing n instead of $n(g)$ we have $g^{-1}hg = h^n$ for all $h \in G$ and thus the function $x \to x^n$ is an automorphism of G. Using a result of Baer (1951/52), p. 173, Folgerung 2, we get $h^n k^{n-1} = k^{n-1} h^n$ for all $h, k \in G$, which means $k^{n-1} \in Z(G)$ for all $k \in G$. Now $Z(G) = E$ implies $\exp G | n-1$ and thus the relation $g^{-1}hg = h^n$ becomes $g^{-1}hg = h$ for all $h \in G$ and therefore $g \in Z(G)$, $g \neq e$, a contradiction.

Groups which do not belong to the class considered here, are the following—a result which we shall need later:

LEMMA 2. *Let G be a dihedral group of order $o(G) = 2n$, $(n, 2) = 1$. Then all polynomial permutations on G are of the form $x \to ax^k b$ if and only if $n = 3$.*

PROOF. Under the conditions of Lemma 2 it is shown in Schumacher (1970), §I.5 that $o(u(G)) = 2(n\varphi(n))^2$ where $\varphi(n)$ denotes Euler's φ-function. If we assume, on the other hand, that $u(G) \subseteq \{x \to ax^k b\}$, then the proof of Zusatz zu Satz 4 in

Lausch *et al.* (1966) implies $o(u(G)) = (o(G))^2\varphi(\exp G)/o(H(G))$. Now

$$o(G) = \exp G = 2n$$

for dihedral groups with $(n,2) = 1$, and $\varphi(2n) = \varphi(n)$. Furthermore, $H(G) = E$ by Lemma 1 since $Z(G) = E$ for dihedral groups with $(n,2) = 1$. Using all these facts we get the equality $2(n\varphi(n))^2 = (2n)^2\varphi(n)$ or $\varphi(n) = 2$. $(n,2) = 1$ implies the assertion $n = 3$.

If conversely, G is the dihedral group of order 6, then G is the symmetric group S_3; it is known (see Lausch *et al.* (1966)) that in this case $u(G) \subseteq \{x \to ax^k b\}$ holds.

The next theorem already establishes an important property of certain groups belonging to our class. For its proof we need the notion of semi-n-abelian groups (Kowol (1977)). A group G is called semi-n-abelian if for every $g \in G$ there exists at least one element $a(g) \in G$, depending only on g, such that

$$(gh)^n = a^{-1}(g)\, g^n h^n a(g)$$

for all $h \in G$. As shown in Kowol (1977), there is a close connection between groups satisfying $u(G) \subseteq \{x \to ax^k b\}$ and semi-n-abelian groups.

THEOREM 1. *Let G be a group such that* $3 \nmid o(G)$ *and let* $u(G) \subseteq \{x \to ax^k b\}$. *Then G is nilpotent.*

PROOF. First note that the conditions on G are hereditary to homomorphic images of G (see Lausch and Nöbauer (1973), chapter 5). Using induction, we can therefore assume indirectly that all homomorphic images of G are nilpotent, G itself is supersolvable (Satz 18 in Kowol (1977)), but not nilpotent (particularly $2 \mid o(G)$ by the above-mentioned result of H. Lausch (1966)). Such a group has the following properties:

(a) $Z(G) = E$—this is trivial; thus $H(G) = E$ by Lemma 1;

(b) there exists a unique minimal normal subgroup N of G, which by the supersolvability of G has order p (>2), where p is the greatest prime divisor of $o(G)$;

(c) if M is a maximal non-normal subgroup of G, then $\bigcap_{g \in G} M^g = E$, evidently; $C_G(N) = N$ by Lemma 2, p. 119 of Baer (1957) and (b).

Now $u(G) \subseteq \{x \to ax^k b\}$ implies by Lemma 16(b) in Kowol (1977) with $m = 3$:

$$(g^2h)^3 = g^4h^3g^2 \quad \text{and} \quad (hg^2)^3 = g^2h^3g^4 \quad \text{for all } g, h \in G.$$

If we compare Lemma 4(d) of Kowol (1977) with these equalities we get $[G^4, G^2] \subseteq C_G(G^3) = Z(G) = E$, where $G^n = \langle g^n, g \in G\rangle$. Particularly we have $[N^4, G^2] = [N, G^2] = E$ or $G^2 \subseteq C_G(N) = N$. Thus $\exp G/N = 2$, $o(G) = 2^n p$ and G has elementary abelian Sylow-2-subgroups G_2. Now G_2 is a maximal subgroup of G and thus (c) above and Theorem 1, p. 183, of Baer (1957) imply $o(G) = 2p$ and G is a dihedral group. Since $p > 3$ by assumption the conditions of Lemma 2 are satisfied, which shows that not all elements of $u(G)$ are of the form $x \to ax^k b$, a contradiction.

For the next proof we recall the following notations: if G is a group, G_π will denote an arbitrary Hall π-subgroup (particularly we write G_p for a Sylow-p-subgroup of G) and if π is a set of primes, π' means all primes dividing $o(G)$ which are not elements of π.

THEOREM 2. *Let G be a group with $u(G) \subseteq \{x \to ax^k b\}$. Then for the hypercentre $Z_\infty(G)$ we have $Z_\infty(G) \supseteq G_{\{2,3\}'}$—particularly $G = G_{\{2,3\}} \times G_{\{2,3\}'}$ where $G_{\{2,3\}'}$ is nilpotent of class $\leqslant 2$.*

PROOF. We first prove the second assertion of the theorem. Assume that $Z_\infty(G) \supseteq G_{\{2,3\}'}$ is already shown. Then by Hilfssatz VI.12.9 in Huppert (1967), $G = H \times G_p$ for some subgroup H of G with $p > 3$. Continuing in this way with H we get $G = G_{\{2,3\}} \times G_{\{2,3\}'}$; the last assertion of the theorem then follows by the theorem of H. Lausch (1966).

To show $Z_\infty(G) \supseteq G_{\{2,3\}'}$ we can assume by the theorem of Lausch (1966) and Theorem 1 that $6 \mid o(G/Z_\infty(G))$. Considering $G/Z_\infty(G)$ instead of G we also can assume without loss of generality that $Z(G) = E$. Finally we suppose indirectly that $o(G) = 2^m 3^n p_3^{k_3} \ldots p_r^{k_r}$ with $r \geqslant 3$, $k_i > 0$. We take $l = 3p_3 \ldots p_r + 2$. l satisfies $l < \exp G$ and $(l, \exp G) = 1$, since l is odd and $l \equiv 2 \pmod 3$. Now G is supersolvable, thus $G_{2'}$ is a normal subgroup of G. Lemma 16(b) of Kowol (1977) implies $(g^2 h)^l = g^{l+1} h^l g^{l-1}$ for all $g, h \in G$ and Lemma 4(d) of the same paper further on implies

$$(1) \qquad [G^{m+1}, G^{m-1}] \subseteq C_G(G^l) = Z(G) = E.$$

On the one hand, we get $G_3 = G_3^{l-1} \subseteq G_{2'}^{l-1}$, since $l - 1 \equiv 1 \pmod 3$, for all Sylow-3-subgroups of G; on the other hand, by the supersolvability of G we have $G_{\{2,3\}'} \lhd G$, thus $G_{\{2,3\}'} = (G_{\{2,3\}'})^{l+1} \subseteq (G_{2'})^{l+1}$, because $l + 1 \not\equiv 0 \pmod{p_3 \ldots p_r}$ and thus $l + 1 \not\equiv 0 \pmod{\exp G_{\{2,3\}'}}$. Using both results in (1) we obtain $[G_3, G_{\{2,3\}'}] = E$ for all Sylow-3-subgroups of G. This means in particular that $G_{\{2,3\}'}$ normalizes G_3. Now $G_{2'} = G_3 G_{\{2,3\}'}$ by the supersolvability of G. Thus G_3 is normal hence characteristic in G_2, and therefore $G_3 \lhd G$. Theorem 1 implies G/G_3 is nilpotent (since condition $u(G) = \{x \to ax^k b\}$ is hereditary to homomorphic images) and so $G_{\{2,3\}} \lhd G$. But since G is supersolvable, $G_{\{2,3\}'}\lhd G$ holds too and $G = G_{\{2,3\}} \times G_{\{2,3\}'}$ is proved. Considering $G/G_{\{2,3\}} \cong G_{\{2,3\}'}$ we obtain by using Theorem 1 once more that $G_{\{2,3\}'} \neq E$ is nilpotent and therefore $Z(G) \neq E$, in contrast to the assumption.

Theorem 2 allows us to restrict the investigation of groups G with

$$u(G) \subseteq \{x \to ax^k b\}$$

to the case $o(G) = 2^m 3^n$, which will be treated in the next section.

3. The case $o(G) = 2^m 3^n$

We now investigate those groups of order $o(G) = 2^m 3^n$ having the property $u(G) \subseteq \{x \to ax^k b\}$. By Satz 18 of Kowol (1977) these groups are necessarily supersolvable. To get a coherent description of these groups satisfying the above condition we make the additional assumption $Z(G) = E$. An example will illustrate the significance of this restriction; for this we need some results of Scott (1969), which we recall in the following:

Let $p(x) = a_1 x^{k_1} a_2 \dots a_r x^{k_r} a_{r+1}$ be an arbitrary polynomial over G. Then $\sum_{i=1}^r k_i = l(p(x))$ is called the length of $p(x)$. Finally, let $\lambda(G)$ be the uniquely determined positive integer $\lambda(G) = \min l(q(x))$, the minimum taken over all polynomials $q(x)$ of positive length having the property $q(g) = e$ for all $g \in G$. Now the following results hold:

(1) Let N be a normal subgroup of G, then (a) $\lambda(G/N) \mid \lambda(G)$ and (b) $\lambda(G) \mid \lambda(G/N)\,\lambda(N)$ (Proposition 2.3 of Scott (1969)).

(2) Let $G = G_1 \times G_2$, then $u(G) = u(G_1) \times u(G_2)$ if and only if $(\lambda(G_1), \lambda(G_2)) \mid 2$ (Theorem 2.2 of the same paper).

We now return to the announced example: Let G be a group of order $o(G) = 2 \cdot 3^n$ satisfying $u(G) \subseteq \{x \to ax^k b\}$—it will be shown below that infinitely many (not nilpotent) groups have this property—and let K be a 2-group of class $\leqslant 2$. Evidently $\lambda(K) = 2^m$, m suitable. To calculate $\lambda(G)$ we choose $N \lhd G$ of index 2—N exists because of the supersolvability of G. Now $\lambda(G/N) = 2$ and $\lambda(N) = 3^s$, since N is a 3-group. Thus by the result (1) mentioned above $\lambda(G) \mid 2 \cdot 3^s$. Therefore $(\lambda(G), \lambda(K)) \mid 2$ and we get by (2) $u(G \times K) = u(G) \times u(K)$.

Now $u(G)$ and $u(K)$ satisfy the condition that all permutation polynomials have the form $x \to ax^k b$ by assumption and Satz 4 of Lausch *et al.* (1966), respectively. We claim the same for $u(G \times K)$; trivially $Z(G \times K) \neq E$ for $K \neq E$. Now $\{p\colon x \to ax^k b,\, p \text{ invertible}\} \subseteq u(G \times K)$ and thus

$$o(u(G \times K)) \geqslant (o(G \times K))^2 \varphi(\exp G \times K)/o(H(G \times K))$$

by Lausch *et al.* (1966). On the other hand,

$$o(u(G)) = (o(G))^2\varphi(\exp G)/o(H(G))$$

and

$$o(u(K)) = (o(K))^2\varphi(\exp K)/o(H(K)).$$

Here it is easily seen that $\varphi(\exp G\times K) = \varphi(\exp G)\cdot\varphi(\exp K)$. Furthermore, take an element $h\in H(G\times K)$, thus $h = gk$ with $g\in G$, $k\in K$ and $h^{-1}xh = x^{r(h)}$ for all $x\in G\times K$. Writing $x = yz$, $y\in G$, $z\in K$ we obtain $g^{-1}ygk^{-1}zk = y^r z^r$ for all $y\in G$, $z\in K$ which means $g\in H(G)$ and $k\in H(K)$ and thus $h = gk\in H(G)\times H(K)$. It follows $o(H(G\times K))\leqslant o(H(G))\cdot o(H(K))$. Combining these formulas we get

$$\begin{aligned} o(u(G\times K)) = o(u(G)\times u(K)) = o(u(G))\cdot o(u(K)) \\ \leqslant (o(G\times K))^2\varphi(\exp G\times K)/o(H(G\times K)). \end{aligned}$$

Consequently we have equality. Thus $u(G\times K) = \{p\colon x\to ax^k b, p \text{ invertible}\}$ actually. Note besides that in this case we have shown also

$$H(G\times K) = H(G)\times H(K),$$

a formula which is not trivial at all.

We thus have proved that one can construct to every group G with $Z(G) = E$ and $u(G)\subseteq\{x\to ax^k b\}$—we shall see below that such a group necessarily has order $2\cdot 3^n$—new ones satisfying the last condition but having a non-trivial centre.

THEOREM 3. *Let G be a group with order $o(G) = 2^m 3^n$, $m\geqslant 2$, and $u(G)\subseteq\{x\to ax^k b\}$. Then $2\,|\,o(Z(G))$.*

PROOF by induction on n. The case $n = 0$ is trivial thus we assume $n\geqslant 1$. Since G is supersolvable there exists a normal subgroup N of G with $o(N) = 3$. Considering G/N we obtain by induction that there exists a normal subgroup $M/N\lhd G/N$ with $o(M/N) = 2$. Thus there is a $K\lhd G$ with $o(K) = 6$. If, on the one hand, K is abelian, then the Sylow-2-subgroup K_2 is characteristic in $K\lhd G$. Therefore $K_2\lhd G$ and $K_2\subseteq Z(G)$ trivially.

If, on the other hand, $K = S_3$, the symmetric group, then $G = S_3\times F$, since S_3 is a complete group (see, for example, p. 278 in Kurosch (1970)). We claim $u(G) = u(S_3)\times u(F)$. For this purpose it suffices to show $\lambda(S_3) = 2$ because of the result (2) mentioned above. Now $2\,|\,\lambda(S_3)\,|\,6$ using the same argument as in the above example. According to Theorem 3.3 in Scott (1969), 3 divides $\lambda(G)$ if and only if $3\,|\,o(D)$, where D is a system normalizer of G. But this is not true and so really $\lambda(S_3) = 2$ and $u(G) = u(S_3)\times u(F)$. Since G fulfils the condition

$$u(G)\subseteq\{x\to ax^k b\},$$

so F does, since it is a homomorphic image of G. We get

$$\begin{aligned} o(u(G)) &= (o(G))^2\varphi(\exp G)/o(H(G)) \\ &= (o(S_3))^2(o(F))^2\varphi(\exp F)/o(H(G)) \end{aligned}$$

($\exp G = \exp F$, since $o(F) = 2^{m-1}3^{n-1}$ $(m \geqslant 2)$—if $n = 1$ we have $o(F) = 2^{m-1} \geqslant 2$ and $2 \mid o(Z(F)) = o(Z(G))$). On the other hand, we have $o(u(S_3)) = 72$,

$$o(u(F)) = (o(F))^2\varphi(\exp F)/o(H(F)).$$

The equality $u(G) = u(S_3) \times u(F)$ thus yields $o(H(F)) = 2 \cdot o(H(G))$. In particular $2 \mid o(H(F))$. Now $H(F)$ is an abelian characteristic subgroup of F and therefore

$$(H(F))_2 \operatorname{char} H(F) \operatorname{char} F \lhd G,$$

since F is a direct factor of G. We thus have obtained a normal subgroup S of G of order $o(S) = 2^t$, $t \geqslant 1$. The supersolvability now implies the existence of $T \lhd G$, $o(T) = 2$, which means $T \subseteq Z(G)$.

THEOREM 4. *Let G be a group with $o(G) = 2\cdot 3^n$ and let $u(G) \subseteq \{x \to ax^k b\}$. Furthermore, let $Z(G) = E$. Then the Sylow-3-subgroup G_3 of G is abelian.*

PROOF. First we show that $p(x) = x^2cx^{-1}c^{-1}$ is an element of $u(G)$ for every $c \in G_3$. Assume $p(g) = p(h)$ for $g, h \in G$. Now $p(x) \in u(G_3)$ by Satz 11 of Lausch *et al.* (1965), and thus if $g, h \in G_3$ it follows $g = h$. On the other hand, $G = \langle d \rangle \cdot G_3$ with $d^2 = e$ and so if $g \in G_3$ and $h \in dG_3$ a simple calculation would give $d \in G_3$, a contradiction. Therefore we can assume $g, h \in dG_3$, which means $g = dr$, $h = ds$ with $r, s \in G_3$ and $p(g) = p(h)$. This implies the equation

$$rdrcr^{-1} = sdscs^{-1} \quad \text{or equivalently} \quad s^{-1}d^{-1}s^{-1}rdr = cs^{-1}rc^{-1}.$$

Multiplying the last equation with $r^{-1}s$ on the left we get

$$r^{-1}d^{-1}(s^{-1}r)dr = [s^{-1}r, c^{-1}],$$

which means $s^{-1}r$ is conjugate to $[s^{-1}r, c^{-1}]$. First this implies $s^{-1}r \in (G_3)' = K_2(G_3)$ and using this we have $s^{-1}r \in K_3(G_3)$, since every $K_i(G_3)$ is normal (even characteristic) in G. By induction we derive $s^{-1}r \in K_i(G_3)$ for all $i \in \mathbb{N}$. The nilpotency of G_3 finally gives $s^{-1}r = e$, and thus $s = r$ what had to be shown.

By assumption $u(G) \subseteq \{x \to ax^k b\}$ and therefore every function $x \to x^2cx^{-1}c^{-1}$ $(c \in G_3)$ can be written in the form $x \to ax^k b$. Thus we can associate with every $c \in G_3$ elements $a_c, b_c \in G$ and an element $k_c \in \mathbb{N}$ satisfying

$$p(x) = x^2cx^{-1}c^{-1} = a_c x^{k_c} b_c.$$

Choosing $x = e$ we get $b_c = a_c^{-1}$, which implies $x^2 c x^{-1} c^{-1} = a_c x^{k_c} a_c^{-1}$. We prove $k_c \equiv 1 \pmod 6$ and $a_c \in G_3$ for all $c \in G_3$. For this we choose $N \lhd G$ with $o(G/N) = 6$ ($n = 0$, that is $o(G) = 2$, is impossible since $Z(G) = E$ by hypothesis)—such an N exists since G is supersolvable. Then Theorem 5.3.3 in Lausch and Nöbauer (1973) yields the equation

$$x^2 \nu(c) x^{-1} (\nu(c))^{-1} = \nu(a_c) x^{k_c} (\nu(a_c))^{-1},$$

where ν is the natural homomorphism of G onto G/N. If, on the one hand, $G/N \cong Z_6$ (the cyclic group of order 6) we obtain $x = x^{k_c}$ and thus $k_c \equiv 1 \pmod 6$ for all $c \in G_3$. If, on the other hand, $G/N \cong S_3$, a simple calculation implies $k_c \equiv 1 \pmod 6$ for all $c \in G_3$ too—note that $\nu(c) \in A_3$, the alternating group.

To show $a_c \in G_3$ for all $c \in G_3$ we assume that there exists an element $c \in G_3$ with $a_c = dt$, $t \in G_3$—we fix such a c and omit the index c in t_c. Choose $w \in Z(G_3)$ with $w^3 = e$, $w \neq e$. We obtain $w = d w^{k_c} d^{-1} = d w d^{-1}$ since $k_c \equiv 1 \pmod 6$, which means $w \in Z(G) = E$, a contradiction.

Summarizing we have shown: to every $c \in G_3$ there exists an element $a_c \in G_3$ and an element $k_c \in \mathbf{N}$, $k_c \equiv 1 \pmod 6$ such that

$$x^2 c x^{-1} c^{-1} = a_c x^{k_c} a_c^{-1}. \tag{2}$$

Next we prove that $c a_c \in H(G_3)$ for all $c \in G_3$. We put $x = y^{-1}$ and note that y runs through all elements of G if x does. We obtain $y^{-2} c y c^{-1} = a_c y^{-k_c} a_c^{-1}$ for all $y \in G$. On the other hand, inverting equality (2) and putting $x = y$ we get $c y c^{-1} y^{-2} = a_c y^{-k_c} a_c^{-1}$ for all $y \in G$. Combining both equalities we derive

$$y^{-2} c y c^{-1} = c y c^{-1} y^{-2},$$

that is,

$$y^2 (c y c^{-1}) = (c y c^{-1}) y^2 \quad \text{for all } y \in G.$$

This at once gives $y^{2\alpha}(c y c^{-1}) = (c y c^{-1}) y^{2\alpha}$ for arbitrary $\alpha \in \mathbf{N}$. Restricting our considerations to $y \in G_3$ we get

$$y^{\beta}(c y c^{-1}) = (c y c^{-1}) y^{\beta} \tag{3}$$

for all $c, y \in G_3$ and $\beta \in \mathbf{N}$, since $2\alpha \equiv \beta \pmod{o(y)}$ always has a solution ($y \in G_3$!). In particular this means that every element of G_3 is commutable with its conjugates, which by Satz III.6.5 of Huppert (1967) implies $\gamma(G_3) \leqslant 3$ where $\gamma(G)$ denotes the class of a group G.

Returning to equality (2) we restrict ourselves to the case $x \in G_3$. Then we can use equality (3) to calculate the term $x^2 c x^{-1} c^{-1}$:

$$a_c x^{k_c} a_c^{-1} = x^2 c x^{-1} c^{-1} = x[x(c x^{-1} c^{-1})] \overset{(3)}{=} x[c(x^{-1} c^{-1} x)]$$
$$\overset{(3)}{=} x x^{-1} c^{-1} x c = c^{-1} x c.$$

This implies $a_c^{-1}c^{-1}\in H(G_3)$ for every $c\in G_3$ and thus $a_c=c^{-1}h_c$, $h_c\in H(G_3)$, what we have claimed. Therefore (2) becomes

$$x^2cx^{-1}c^{-1}=c^{-1}h_cx^{k_c}h_c^{-1}c,\quad c\in G_3,\quad h_c\in H(G_3),\quad k_c\equiv 1\ (\mathrm{mod}\,6),\quad x\in G.$$

Putting here $x=d\,(d^2=e)$ we obtain $c^2dc^{-2}=h_cdh_c^{-1}$ and thus

$$d^{-1}c^2dc^{-2}=d^{-1}h_cdh_c^{-1}$$

for every $c\in G_3$. Now $H(G_3)\,\mathrm{char}\,G_3\,\mathrm{char}\,G$ and so $d^{-1}hd$ (and h^{-1}) is an element of G_3 for every $h\in H(G_3)$. We assert that $d^{-1}hdh^{-1}\in Z(G_3)$ for all $h\in H(G_3)$. Let $z\in G_3$ and $h^{-1}zh=z^{k_h}$ with a certain $k_h\in\mathrm{N}$. Then evidently $hzh^{-1}=z^{l_h}$ where $l_hk_h\equiv 1\ (\mathrm{mod}\,o(G_3))$. Noting that $d^{-1}xd\in G_3$ for all $x\in G_3$ we obtain:

$$d^{-1}hd(h^{-1}zh)d^{-1}h^{-1}d=d^{-1}h(dz^{k_h}d^{-1})h^{-1}d=d^{-1}dz^{k_hl_h}d^{-1}d=z,$$

which means $d^{-1}hdh^{-1}\in Z(G_3)$ for all $h\in H(G_3)$.

Concluding the proof of Theorem 4 we note that for every $c\in G_3$ we have shown the existence of an element $\xi_c\in Z(G_3)$ such that $d^{-1}c^2dc^{-2}=\xi_c$. This is equivalent to $d^{-1}yd=\xi_y y$ for all $y\in G_3$ since every element $y\in G_3$ can be written as c^2 for a certain $c\in G_3$. We now get

$$d^{-1}[y,z]d=\xi_y^{-1}y^{-1}\xi_z^{-1}z^{-1}\xi_y y\xi_z z=[y,z]\quad\text{for all } y,z\in G_3.$$

Taking here $y\in G_3'=K_2(G_3)$ and using $\gamma(G_3)\leqslant 3$ thus $K_3(G_3)\subseteq Z(G_3)$ we first obtain $[y,z]\in Z(G)=E$ and so $K_3(G_3)=E$. If y is arbitrary in G_3 we have $[y,z]\in G_3'\subseteq Z(G_3)$ and once more $[y,z]\in Z(G)=E$ for all $y,z\in G_3$—that is, G_3 is abelian, what we have claimed.

Now we are able to characterize all groups G with $o(G)=2^m\cdot 3^n$, $Z(G)=E$ having the property $u(G)=\{x\to ax^kb\}$.

THEOREM 5. *Let G be a group with $o(G)=2^m\cdot 3^n$, $Z(G)=E$. Then $u(G)\subseteq\{x\to ax^kb\}$ if and only if $m=1$, G_3 is abelian and* $\exp G_3=3$. *In this case G can be described by*

$$G=\langle d,g_1,\dots g_s\,|\,d^2=g_i^3=e,\ g_ig_j=g_jg_i,(dg_i)^2=e \text{ for all } i,j\rangle.$$

PROOF. If G satisfies $u(G)\subseteq\{x\to ax^kb\}$ and the assumptions of the theorem, then by Theorems 3 and 4 we have $m=1$, that is $G=\langle d\rangle\cdot G_3$ with $d^2=e$ and G_3 abelian. We prove $d^{-1}gd=g^{-1}$ for all $g\in G_3$. In fact if $d^{-1}gd=h$ we obtain $g=d^{-1}hd$ and therefore $d^{-1}ghd=hg=gh$ with $gh\in G_3$ since $G_3\lhd G$ by the supersolvability of G. Thus gh is centralized by d and lies therefore in $Z(G)=E$ since G_3 is abelian. We get $h=g^{-1}$ which was claimed.

Suppose now that $\exp G>3$. Then we can write $G_3=\langle z\rangle\times N$ where $o(z)>3$. The relation $d^{-1}gd=g^{-1}$ for all $g\in G_3$ implies $N\lhd G$ and we obtain G/N is a dihedral group of order $2 \cdot 3^l$ with $l > 1$. Now $u(G) \subseteq \{x \to ax^k b\}$ and so G/N has the same property, contradicting Lemma 2.

The converse statement of the theorem will not be proved here. The proof is only technical and runs completely analogous to that given in Schumacher (1970) for dihedral groups. To give an idea we summarize the method used there. Take an arbitrary polynomial function $p(x)$ (invertible or not) with coefficients written in terms of d and g_i. Analogously write x in this function in terms of d and g_i. Then use the rules which hold in G to calculate $p(x)$. After a terrible computation one can derive conditions for $p(x)$ to be invertible, which after tedious calculations yield the exact order of $u(G)$. This order coincides with the number of distinct invertible polynomial functions of the form $x \to ax^k b$. It should be mentioned that all these calculations can only be performed in such simple semi-direct products as G is.

PROBLEM. We mention that the case $o(G) = 2^n$, $u(G) \subseteq \{x \to ax^k b\}$ still remains unsolved.

References

R. Baer (1951/52), 'Endlichkeitskriterien für Kommutatorgruppen', *Math. Ann.* **124**, 161–177.

R. Baer (1957), 'Classes of finite groups and their properties', *Illinois J. Math.* **1**, 115–187.

B. Huppert (1967), *Endliche Gruppen I* (Springer, Berlin–Heidelberg–New York).

G. Kowol (1977), 'Fast-n-abelsche Gruppen', *Arch. Math.* **29**, 55–66.

G. Kowol (1978), 'Polynomfunktionen auf 3-Gruppen', *Contributions to General Algebra*, Klagenfurt, edited by H. Kautschitsch, W. Müller and W. Nöbauer (J. Heyn, Klagenfurt), in print.

A. G. Kurosch (1970), *Gruppentheorie I*, 2nd ed. (Akademie-Verlag, Berlin).

H. Lausch (1966), 'Eine Charakterisierung nilpotenter Gruppen der Klasse 2', *Math. Z.* **93**, 206–209.

H. Lausch and W. Nöbauer (1973), *Algebra of polynomials* (North-Holland, Amsterdam–London; American Elsevier, New York).

H. Lausch, W. Nöbauer and F. Schweiger (1965), 'Polynompermutationen auf Gruppen I', *Monatsh. Math.* **69**, 410–423.

H. Lautsch, W. Nöbauer and F. Schweiger (1966), 'Polynompermutationen auf Gruppen II', *Monatsh. Math.* **70**, 118–126.

F. Schumacher (1970), *Über die Polynompermutationen der endlichen Gruppen* (Thesis, Wien).

S. D. Scott (1969), 'The arithmetic of polynomial maps over a group and the structure of certain permutational polynomial groups I', *Monatsh. Math.* **73**, 250–267.

University of Vienna
1090 Vienna
Austria