ON COMMUTATION SEMIGROUPS OF A GROUP

N. D. GUPTA

(Received 28 June 1964, revised 3 March 1965)

1. Introduction

Let G be a group. With each element a in G we associate the mappings $\rho(a)$ and $\lambda(a)$ of G into itself defined as follows,

1.1 $$g\rho(a) = [g, a] \text{ for all } g \in G$$

1.2 $$g\lambda(a) = [a, g] \text{ for all } g \in G.$$

The product of mappings is defined as usual. Let $P(G)$ and $\Lambda(G)$ denote respectively the semigroups generated by the set of all ρ's and λ's. These semigroups will be called the *commutation semigroups* of G.

One naturally raises the following two questions:

(i) Are the commutation semigroups of a group isomorphic?

(ii) If not, how are these two semigroups related to each other?

The answer to both the questions depends upon the group G. For instance it can be observed easily that if G is the symmetric group on 3 letters, then $|P(G)| = 6$ and $|\Lambda(G)| = 9$; and also in this case $P(G)$ is properly contained in $\Lambda(G)$.

The purpose of this paper is to give a complete answer to question (i) for dihedral groups and for nilpotent groups which are not of class 4. The paper is in two parts, dealing with the commutation semigroups of dihedral groups and of nilpotent groups, respectively. For dihedral groups we give criteria for isomorphism of $P(G)$ and $\Lambda(G)$. For nilpotent groups we construct an example of a group of class 5 and prove that for nilpotent groups of class $\geqq 5$, the commutation semigroups are not in general isomorphic. Also we prove that these semigroups are always isomorphic for groups of class 2 and 3. For groups of class 4 we prove, however, that the two semigroups are of the same cardinality.

I thank my supervisor Professor B. H. Neumann F.A.A., F.R.S. for suggesting the study of commutation semigroups and for his general guidance. I also thank the referee for his many useful suggestions which in particular have considerably simplified the proof of theorem 1.

2. Notations and definitions

For any two elements a and b of a group G, we write

2.1 $$a^b = b^{-1}ab.$$

The commutator of a and b is defined as,

2.2 $$[a, b] = a^{-1}b^{-1}ab;$$

and for $n > 2$, the left normed commutator of weight n is defined inductively as

2.3 $$[a_1, a_2, \cdots, a_n] = [[a_1, a_2, \cdots, a_{n-1}], a_n].$$

The following commutator identities are standard and are used repeatedly without reference,

2.4 $$[a, b] = [b^{-1}, a]^b = [b, a^{-1}]^a$$

2.5 $$[a, bc] = [a, c][a, b]^c$$

2.6 $$[ab, c] = [a, c]^b[b, c].$$

If A and B are subgroups of a group G, then $[A, B]$ is the subgroup of G generated by all the commutators of the form $[a, b]$ where $a \in A$ and $b \in B$. In particular $[G, G]$ is the commutator subgroup of G and is denoted by G'. If G' is abelian, then G is called metabelian. If G is metabelian and if $[a, b] = 1$ for $a, b \in G$, then it can be verified that for any $g \in G$,

2.7 $$[g, a, b] = [g, b, a].$$

For a given group G, the commutation semigroups $P(G)$ and $\Lambda(G)$ may also be written as P and Λ respectively. Both $P(G)$ and $\Lambda(G)$ possess zero elements, namely $\rho(1)$ and $\lambda(1)$, respectively; and $\rho(1) = \lambda(1)$. We denote the zero element of P and Λ by 0. For all elements z in the centre of G, we have $\rho(z) = \lambda(z) = 0$.

An element $\alpha \in P(G)(\Lambda(G))$ is called prime if it cannot be expressed as a product of two or more elements of $P(G)(\Lambda(G))$.

PART I

Commutation semigroups of dihedral groups

Let $n = 2^r m$ be a positive integer where m is odd and $r \geqq 0$. Consider the dihedral group G of order $2n$ given as:

$$G = \text{gp}\{a, b | a^2 = 1 = b^n, aba = b^{-1}\}.$$

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

Let N denote the set of residue classes (mod n). For each pair of elements $i, j \in N$, define a mapping $\mu(i, j)$ of G into itself as,

$$b^k\mu(i,j) = b^{ki},\ ab^k\mu(i,j) = b^{ki+j}. \tag{1}$$

Then it is easy to see that

$$\mu(i,j) = \mu(i',j') \text{ if and only if } i = i',\ j = j' \tag{2}$$

and

$$\mu(i,j)\mu(i',j') = \mu(ii', ji'). \tag{3}$$

Thus the set of all $\mu(i, j)$ form a semigroup S of order n^2. Further it can be directly verified that

$$\rho(b^{-j}) = \mu(0, -2j),\ \rho(ab^{-j}) = \mu(-2, -2j) \tag{4}$$

and

$$\lambda(b^{-j}) = \mu(0, 2j),\ \lambda(ab^{-j}) = \mu(2, 2j). \tag{5}$$

Thus by (2), (3), (4), (5) it follows that $P(G)$ is the subsemigroup of S consisting of all elements of the form $\mu(0, -2j)$ and $\mu((-2)^i, (-2)^i j)$; and $\Lambda(G)$ is the subsemigroup of S consisting of all elements of the form $\mu(0, 2j)$ and $\mu(2^i, 2^i j)$.

If u, v are relatively prime integers, let $\text{ind}_u v$ denote the least positive integer t such that $v^t \equiv 1 \pmod{u}$. Then we prove the following theorem:

THEOREM 1. *$P(G) \cong \Lambda(G)$ if and only if $\text{ind}_p 2 \equiv 0 \pmod 4$ for every prime divisor p of m.*

PROOF. Let $\text{ind}_p 2 \equiv 0 \pmod 4$ for each prime divisor p of m. Let $0 \neq k \in N$ and let $d = (k, m)$ be the greatest common divisor of k and m. Let $d < m$. The residue classes (mod m/d) which are prime to m/d form a multiplicative group H of order $\varphi(m/d)$, the Euler's function of m/d. Let C_1 and C_2 denote the cyclic subgroups of H generated by the residue classes of 2 and -2 respectively. By hypothesis both C_1 and C_2 are of the same even order. Then clearly either $C_1 = C_2$ or $C_1C_2 = C_1 \cup -4C_1 = C_2 \cup -4C_2$ and in the latter case if $\{m_1(= 1), m_2, \cdots, m_s\}$ is a set of coset representatives of C_1C_2 in H, then $\{m_1, m_2, \ldots, m_s, -4m_1, -4m_2, \ldots, -4m_s\}$ is a set of common coset representatives of C_1 and C_2 in H. Let M denote the set of common coset representatives of C_1 and C_2 in H. Then,

$$k = (-2)^{t_1}l_1 = 2^{t_2}l_2, \tag{6}$$

for some $l_1, l_2 \in M$, where l_1, l_2, t_1, t_2 are uniquely determined.

Now, for each $k \in N$ we define integers $\alpha(k), \beta(k) \in N$ as follows:

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

(7) $$\alpha(0) = \beta(0) = 0;$$

$\alpha(k) = \beta(k) = (-1)^t k$ if $d = m$, where $k \neq 0$ and t is the largest power of 2 dividing k; $\alpha(k) = (-1)^{t_1} k$, $\beta(k) = (-1)^{t_2} k$ if $d < m$, where $k \neq 0$ and t_1, t_2 are given by (6). The following properties can be easily verified:

(8) $k = k$ if and only if $\alpha(k) = \alpha(k')$ and $\beta(k) = \beta(k')$.

(9) $\alpha(1) = \beta(1) = 1$

(10) $\alpha\big((-2)^t k\big) = 2^t \alpha(k)$, $\beta(2^t k) = (-2)^t \beta(k)$

(11) $\alpha\big(\beta(k)\big) = \beta\big(\alpha(k)\big) = k$.

We now define the mappings η_1 and η_2 of $P(G)$ into $\Lambda(G)$ and $\Lambda(G)$ into $P(G)$ respectively as follows:

(12) $$\mu(u, v)\eta_1 = \mu\big(\alpha(u), \alpha(v)\big)$$
$$\mu(u, v)\eta_2 = \mu\big(\beta(u), \beta(v)\big).$$

By (8), (9), (10) both η_1 and η_2 are well defined mappings, and by (11), η_1 and η_2 are inverses of one another. A product in $P(G)$ has the form $\mu(u, v)\mu(u', v') = \mu(uu', vu')$ with $u' = 0$ or $(-2)^t$. Then by (9) and (10) η_1 is a homomorphism. Hence $P(G) \cong \Lambda(G)$.

Conversely, let $P(G) \cong \Lambda(G)$. If $m = 1$, there is nothing to prove. Let $m > 1$ and let T denote the subset of N with elements of the form $2j$.

Let η be an isomorphism of $P(G)$ onto $\Lambda(G)$. Since $\mu(0, 0)$ is the zero element of $P(G)$ and $\Lambda(G)$, $\mu(0, 0)\eta = \mu(0, 0)$. Further, since $m > 1$, $P(G)\mu(u, v) = \mu(0, 0)$ is satisfied precisely when $u = 0$. Thus $\mu(0, v)\eta = \mu\big(0, \theta(v)\big)$ for some permutation θ of T. Suppose $\mu(-2, 0)\eta = \mu(c, e)$; then $c = 2^l$ for some l. Since $\big(\mu(0, v)\mu^t(-2, 0)\big)\eta = \mu\big(0, \theta(v)\big)\mu^t(c, e) = \mu\big(0, c^t\theta(v)\big)$; we have,

(13) $$\mu\big(0, (-2)^t v\big)\eta = \mu\big(0, c^t\theta(v)\big).$$

In particular, since θ is $1-1$, for all $t = 1, 2, \cdots$,

$$\big((-2)^t - 1\big)x = 0 \quad \text{and} \quad (c^t - 1)x = 0$$

have the same number of solutions $x \in T$. Now $\mu(-2, 0)$ and $\mu(c, e)$ both generate cyclic sub-semigroups of $P(G)$ and $\Lambda(G)$ respectively and by the isomorphism condition it is easy to see that c and 2 are powers of one another, so that

$$\big((-2)^t - 1\big)x = 0 \quad \text{and} \quad (2^t - 1)x = 0$$

have the same number of solutions $x \in T$. Let $d_1 = \big((-2)^t - 1, n\big)$ and $d_2 = (2^t - 1, n)$. Then the number of solutions are ϵd_1 and ϵd_2

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

respectively where $\varepsilon = \frac{1}{2}$ or 1 according as n is even or odd. Thus $d_1 = d_2$ and we get in particular

$$(2^t-1, n) = (2^t+1, n) = (2^{2t}-1, n) = 1, \tag{14}$$

for all positive odd integers t.

Now let $1 \neq p$ be a prime divisor of m. If $\text{ind}_p 2 \not\equiv 0 \pmod 4$, there is an odd or twice-an-odd integer s such that $p|2^s-1$ and so $p|(2^s-1, n)$ which is contrary to (14). Hence $\text{ind}_p 2 \equiv 0 \pmod 4$. This completes the proof of the theorem.

Remark. If $r = 0$ or 1, then it can be independently proved that $P(G) \subset \Lambda(G)$ if and only if the least positive integer s, satisfying $2^s \equiv -1 \pmod m$, is odd and $\Lambda(G) \subset P(G)$ if and only if $\text{ind}_m 2$ is odd. Further, the proper inclusion of commutation semigroups does not hold if $r > 1$.

PART II

Commutation semigroups of nilpotent groups

Let G be a nilpotent group. For $l \geqq 1$, let $P_l = P_l(G)$ $(\Lambda_l = \Lambda_l(G))$ denote the set of all elements of $P(G)$ $(\Lambda(G))$ which can be expressed as a product of l single elements of $P(G)$ $(\Lambda(G))$. Thus if G is nilpotent of class n, then $P_n = \Lambda_n = \{0\}$.

Let G be nilpotent of class at most 4. Since $\rho(a) = \rho(b)$ and $\lambda(a^{-1}) = \lambda(b^{-1})$ are both equivalent to $ab^{-1} \in Z(G)$, the center of G, there is a unique one-to-one mapping of P_1 onto Λ_1 which maps $\rho(a)$ to $\lambda(a^{-1})$. Thus we have,

$$|P_1| = |\Lambda_1|. \tag{1}$$

Further since $[g, a, b] = [b, [a, g]]^{[g,a]} = [b, [a, g]]$ for all $g \in G$, we have $\rho(a)\rho(b) = \lambda(a)\lambda(b)$ which gives

$$P_2 = \Lambda_2. \tag{2}$$

Also $[g, a, b, c] = [c^{-1}, [b^{-1}, [a^{-1}, g]]]$ for all $g \in G$ implies that $\rho(a)\rho(b)\rho(c) = \lambda(a^{-1})\lambda(b^{-1})\lambda(c^{-1})$ which gives

$$P_3 = \Lambda_3. \tag{3}$$

If $\rho(a) = \rho(b)\rho(c)$, then

$$\begin{aligned}[g, b, c] = [g, a] &= [a^{-1}, g][a^{-1}, g, a] \\ &= [a^{-1}, g][a^{-1}, g, b, c] = [a^{-1}, g][g, a, b, c] = [a^{-1}, g],\end{aligned}$$

so that $\rho(a) = \lambda(a^{-1}) = \rho(b)\rho(c)$ which gives by (2) that

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

$$P_1 \cap P_2 = \Lambda_1 \cap \Lambda_2. \tag{4}$$

If $\rho(a) = \rho(b)\rho(c)\rho(d)$, then $[g, b, c, d] = [g, a] = [a^{-1}, g][a^{-1}, g, a] = [a^{-1}, g]$, so that $\rho(a) = \lambda(a^{-1}) = \rho(b)\rho(c)\rho(d) = \lambda(b^{-1})\lambda(c^{-1})\lambda(d^{-1})$ which gives by (3) that

$$P_1 \cap P_3 = \Lambda_1 \cap \Lambda_3. \tag{5}$$

Also from (2) and (3) we get

$$P_2 \cap P_3 = \Lambda_2 \cap \Lambda_3. \tag{6}$$

Thus it follows from (1)—(6), that

$$|P| = |\Lambda|. \tag{7}$$

In particular if G is nilpotent of class 2 then $\rho(a) = \lambda(a^{-1})$ and so $P = \Lambda$. If G is nilpotent of class 3, then $\rho(a)\rho(b) = \rho(a^{-1})\rho(b^{-1}) = \lambda(a^{-1})\lambda(b^{-1}) = \lambda(a)\lambda(b)$ and it follows from above that

(i) $\rho(a) = \rho(b)$ if and only if $\lambda(a^{-1}) = \lambda(b^{-1})$
(ii) $\rho(a) = \rho(b)\rho(c)$ if and only if $\lambda(a^{-1}) = \lambda(b^{-1})\lambda(c^{-1})$
(iii) $\rho(a)\rho(b) = \rho(c)\rho(d)$ if and only if $\lambda(a^{-1})\lambda(b^{-1}) = \lambda(c^{-1})\lambda(d^{-1})$.

Thus there exists an isomorphism of P onto Λ mapping $\rho(a)$ to $\lambda(a^{-1})$ for all $a \in G$. Thus we have proved the following theorem:

THEOREM 2. *Let G be a nilpotent group. Then* (i) $P(G) = \Lambda(G)$ *if G has class* 2; (ii) $P(G) \cong \Lambda(G)$ *if G has class* 3 *and* (iii) $|P(G)| = |\Lambda(G)|$ *if G has class* 4.

Next we prove the following theorem:

THEOREM 3. *If G is a nilpotent group of class* 5, *then $P(G)$ and $\Lambda(G)$ are not in general isomorphic.*

PROOF. To prove this theorem we construct a group G of class precisely 5 and later we shall show that $P \ncong \Lambda$.

First construct,

$$A = \text{gp}\{x_1, x_2, x_3, x_4\}, \tag{8}$$

as an elementary abelian group of order 5^4. We then extend A by adjoining an element a with relations,

$$a^5 = 1,\ x_1^a = x_1x_2,\ x_2^a = x_2x_3,\ x_3^a = x_3x_4,\ x_4^a = x_4. \tag{9}$$

It can be checked that a induces an automorphism of order 5 in A, so that $B = \text{gp}\{A, a\}$ is of order 5^5 and is a splitting extension of A by gp $\{a\}$. In the same way we extend B by adjoining an element b with relations,

$$b^5 = 1,\ x_1^b = x_1x_3,\ x_2^b = x_2x_4,\ x_3^b = x_3,\ x_4^b = x_4,\ a^b = a. \tag{10}$$

As before $C = \text{gp}\{B, b\}$ is of order 5^6 and is a splitting extension of B by gp $\{b\}$. Finally we extend C by adjoining an element c, with relations,

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

$$(11)\quad c^5 = 1,\ x_1^c = x_1,\ x_2^c = x_2,\ x_3^c = x_3,\ x_4^c = x_4,\ a^c = ax_1^{-1},\ b^c = bx_2^{-1}.$$

It can be checked that $G = \text{gp}\{C, c\}$ is of order 5^7 and is a splitting extension of C by gp $\{c\}$.

G is a metabelian group and can be regarded as generated by the elements a, b and c with the following commutator relations:

$$(12)\quad \begin{aligned} &[c, a] = x_1, && [c, b] = x_2, && [a, b] = 1, \\ &[c, a, a] = x_2, && [c, a, b] = x_3, && [c, a, c] = 1, \\ &[c, b, a] = x_3, && [c, b, b] = x_4, && [c, b, c] = 1, \\ &[c, a, a, a] = x_3, && [c, a, a, a, a] = x_4, && [c, a, b, b] = 1. \end{aligned}$$

Any element $g \in G$ can be written as:

$$(13)\quad g = a^u b^v c^w z \text{ where } u, v, w = 0, 1, 2, 3, 4$$

and

$$z = x_1^i x_2^j x_3^k x_4^l \text{ where } i, j, k, l = 0, 1, 2, 3, 4.$$

In what follows we shall prove that $P(G) \cong \Lambda(G)$.

From relations (12), it can be verified that in $P(G)$, $\rho(a)\rho(a) = \rho(b)$. We prove the following,

LEMMA 1. *In* $P(G)$,

$$\rho(ac^i x_1^j x_2^k)\rho(a) = \rho(bx_1^i x_2^j x_3^k),$$

where $i, j, k = 0, 1, 2, 3, 4$.

PROOF. Let $g \in G$. Then we have

$$\begin{aligned} &g\rho(ac^i x_1^j x_2^k)\rho(a) \\ &= [g, ac^i x_1^j x_2^k, a] \\ &= [a^u b^v c^w z, ac^i x_1^j x_2^k, a] && \text{by (13)} \\ &= [a^u b^v c^w z, c^i x_1^j x_2^k, a][a^u b^v c^w z, a, a] && \text{by (11)} \\ &= [a^u b^v, c^i x_1^j x_2^k, a][c^w z, b] && \text{by (10) and (11)} \\ &= [a^u b^v, c^i, a][a^u b^v, x_1^j, a][a^u b^v, x_2^k, a][c^w z, b] \\ &= [c^i, a^u b^v, a]^{-1}[x_1^j, a^u b^v, a]^{-1}[x_2^k, a^u b^v, a]^{-1}[c^w z, b] \\ &= [c^i, a, a^u b^u]^{-1}[x_1^j, a, a^u b^v]^{-1}[x_2^k, a, a^u b^v]^{-1}[c^w z, b] && \text{by 2.7} \\ &= [[c, a]^i, a^u b^v]^{-1}[[x_1, a]^j, a^u b^v]^{-1}[[x_2, a]^k, a^u b^v]^{-1}[c^w z, b] \\ &= [x_1^i, a^u b^v]^{-1}[x_2^j, a^u b^v]^{-1}[x_3^k, a^u b^v]^{-1}[c^w z, b] && \text{by (12)} \\ &= [x_1^i x_2^j x_3^k, a^u b^v]^{-1}[c^w z, b] \\ &= [a^u b^v c^w z, x_1^i x_2^j x_3^k][a^u b^v c^w z, b] && \text{by (10) and (11)} \\ &= [a^u b^v c^w z, bx_1^i x_2^j x_3^k] \\ &= g\rho(bx_1^i x_2^j x_3^k). \end{aligned}$$

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

The proofs of the following lemmas are omitted since they are long and computational:

LEMMA 2. $\rho(ab^2c^r x_1^s x_2^t)\rho(a^2) = \rho(b^2 x_1^i x_2^j x_3^k)$

where $i, j, k = 0, 1, 2, 3, 4$; and $r = 3i \pmod 5$, $s = (3j-4i) \pmod 5$, $t = (3k-4j+2i) \pmod 5$.

LEMMA 3. $\rho(a^2bc^r x_1^s x_2^t)\rho(a^4) = \rho(b^3 x_1^i x_2^j x_3^k)$

where $i, j, k = 0, 1, 2, 3, 4$; and $r = 4i \pmod 5$, $s = (4j-i) \pmod 5$, $t = (4k-j) \pmod 5$.

LEMMA 4. $\rho(a^2b^3c^r x_1^s x_2^t)\rho(a^2) = \rho(b^4 x_1^i x_2^j x_3^k)$

where $i, j, k = 0, 1, 2, 3, 4$; and r, s, t are as in Lemma 2.

We now prove the following,

LEMMA 5. *In $\Lambda(G)$, $\lambda(b^2)$ does not belong to Λ_2.*

PROOF. Let $h_1 = a^i b^j c^k z_1$ and $h_2 = a^l b^m c^n z_2$ where $i, j, k, l, m, n = 0, 1, 2, 3, 4$ and $z_1, z_2 \in G'$. Suppose that $\lambda(b^2) = \lambda(h_1)\lambda(h_2)$, then $[b^2, g] = [h_2, [h_1, g]]$ for all $g \in G$, i.e. $[g, b^2]^{-1} = [g, h_1, h_2]$ since G' is abelian. In particular we have in turn

$$[c, h_1, h_2] = [c, b^2]^{-1};$$
$$[c, a^i b^j c^k z_1, a^l b^m c^n z_2] = [c, b^2]^{-1};$$
$$[c, a^i b^j, a^l b^m] = [c, b]^{-2}[c, b, b]^{-1} \quad \text{by (11);}$$
$$[c, b^j, a^l b^m][c, a^i, a^l b^m][c, a^i, b^j, a^l b^m] = [c, b]^{-2}[c, b, b]^{-1};$$
$$[c, b^j, b^m][c, b^j, a^l][c, a^i, b^m][c, a^i, a^l][c, a^i, a^l, b^m][c, a^i, b^j, a^l] = [c, b]^{-2}[c, b, b]^{-1}.$$

Collecting the powers of $[c, a, a]$, $[c, a, a, a]$ and $[c, a, a, a, a]$ from the above equation, we get

(14) $il+2 \equiv 0 \pmod 5$

(15) $2im+2jl+il(i+l-2) \equiv 0 \pmod 5$

(16) $$\frac{il(l-1)(l-2)}{6} + \frac{li(i-1)(i-2)}{6} + \frac{i(i-1)}{2} \cdot \frac{l(l-1)}{2} + ijl+ilm+jm + \frac{mi(i-1)}{2} + \frac{jl(l-1)}{2} + 1 \equiv 0 \pmod 5.$$

From (14) we have, either $il = 3$ or $il = 8$.

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press

When $il = 3$, let $i = 1$ and $l = 3$. Then from (15) we have, $m+3j+3 \equiv 0 \pmod 5$; which gives $m \equiv -(3j+3) \pmod 5$. Also from (16) we have, $mj+j+3m+2 \equiv 0 \pmod 5$; so that $3j^2+j+7 \equiv 0 \pmod 5$. But this is not solvable for any integral value of j (we arrive at similar conclusion by choosing $i = 3$ and $l = 1$).

When $il = 8$, let $i = 2$ and $l = 4$. Then from (15) we have, $m+2j+3 \equiv 0 \pmod 5$; which gives $m \equiv -(2j+3) \pmod 5$. Also from (16) we have, $mj+4m+4j \equiv 0 \pmod 5$; so that $j^2+j+1 \equiv 0 \pmod 5$. But this is again not solvable for any integral value of j (we arrive at similar conclusion by choosing $i = 4$ and $l = 2$). This completes the proof of lemma 5.

LEMMA 6. *In $\Lambda(G)$, $\lambda(b^2)$ is prime.*

PROOF. By lemma 5, it is sufficient to show that $\lambda(b^2)$ does not belong to Λ_3, Λ_4 or Λ_5.

But, for $i = 3, 4, 5$, $\lambda(b^2) \in \Lambda_i$ gives in turn $\lambda(b^2)\lambda(a)\lambda(a) = 0$; $\rho(b^2)\rho(a)\rho(a) = 0$; $[c, b^2, a, a] = 1$; $[c, b, a, a] = 1$, which gives the required contradiction.

We can now complete the proof of Theorem 3. Let $\bar{P}$ denote the set of all prime elements $\alpha \in P(G)$ such that $\alpha^2 \neq 0$, $\alpha^3 = 0$, $\alpha P_3(G) = 0$; and let $\bar{\Lambda}$ be the corresponding set of all prime elements $\beta \in \Lambda(G)$ such that $\beta^2 \neq 0$, $\beta^3 = 0$, $\beta\Lambda_3(G) = 0$.

If $\alpha = \rho(a^i b^j c^k z) \in \bar{P}$, then $\alpha P_3 = 0$ implies in particular that $[c, a^i b^j c^k z, a, a, a] = 1$ and $[a, a^i b^j c^k z, a, a, a] = 1$ which give respectively $[c, a, a, a, a]^i = 1$ and $[c, a, a, a, a]^k = 1$ so that we have $i \equiv 0 \pmod 5$ and $k \equiv 0 \pmod 5$. Thus $\alpha = \rho(b^j z)$ which by lemmas 1, 2, 3 and 4 implies that α is not prime. Hence $\bar{P} = \emptyset$, the empty set.

On the other hand, by lemma 6, $\lambda(b^2)$ is prime and $\lambda^2(b^2) \neq 0$, $\lambda^3(b^2) = 0$, $\lambda(b^2)\Lambda_3(G) = 0$ so that $\bar{\Lambda} \neq \emptyset$. Since under any isomorphism of P onto Λ, $\bar{P}$ maps onto $\bar{\Lambda}$, we have that $P(G) \ncong \Lambda(G)$. This completes the proof.

Finally for $n > 5$ we prove the following theorem,

THEOREM 4. *For each integer n greater than 5, there exists a nilpotent group $\mathfrak{G}$ of class n such that $P(\mathfrak{G}) \ncong \Lambda(\mathfrak{G})$.*

PROOF. Let G be the group as constructed in theorem 3, and let H be the dihedral group of order 2^{n+1}, given as,

$$H = \text{gp}\{d, e | d^{2^n} = 1 = e^2,\ ede = d^{-1}\}.$$

Let $\mathfrak{G} = G \times H$ be the direct product of G and H, then we proceed to show that $\mathfrak{G}$ is the required group.

Since H is of class $n (> 5)$, it follows that $\mathfrak{G}$ is of class n. Every element

of $\mathfrak{G}$ can be uniquely written as $a^i b^j c^k z e^\varepsilon d^l$ where $i, j, k = 0, 1, 2, 3, 4$; $\varepsilon = 0, 1$; $l = 1, 2, \cdots, 2^n$ and $z \in G'$.

Let $\bar{P}(\mathfrak{G})$ denote the set of all prime elements $\alpha \in P(\mathfrak{G})$ such that $\alpha^2 \neq 0$, $\alpha^3 = 0$, $\alpha P_3(\mathfrak{G}) = 0$; and let $\bar{\Lambda}(\mathfrak{G})$ be the corresponding set of all prime elements $\beta \in \Lambda(\mathfrak{G})$ such that $\beta^2 \neq 0$, $\beta^3 = 0$, $\beta \Lambda_3(\mathfrak{G}) = 0$.

If $\alpha = \rho(a^i b^j c^k z e^\varepsilon d^l) \in \bar{P}(\mathfrak{G})$, by using $\alpha P_3(\mathfrak{G}) = 0$ we get, as in theorem 3, that $i = 0$, $k = 0$; so that $\alpha = \rho(b^j z e^\varepsilon d^l)$. If $\varepsilon = 1$, then $\alpha^3 = 0$ gives in particular $1 = [d, b^j z e d^l, b^j z e d^l, b^j z e d^l] = [d, e, e, e] = d^{-2^3}$ which is a contradiction (since $n > 5$). Thus $\varepsilon = 0$. Further $\alpha P_3(\mathfrak{G}) = 0$ gives in particular $1 = [e, b^j z d^l, e, e, e] = [e, d, e, e, e]^l = [d, e, e, e, e]^{-l} = d^{-2^4 l}$, which gives that $l = 0$ or $l = \pm 2^{n-4}$. Thus $\alpha = \rho(b^j z)$ or $\alpha = \rho(b^j z d^{\pm 2^{n-4}})$. But by lemmas 1, 2, 3 and 4, $\alpha \neq \rho(b^j z)$; therefore $\alpha = \rho(b^j z d^{\pm 2^{n-4}})$. Further, since $\rho(d^{\pm 2^{n-4}}) = \rho(d^{\mp 2^{n-5}})\rho(e)$, if $\rho(b^j z) = \rho(g_1)\rho(g_2)$ then it can be easily seen that $\rho(b^j z d^{\pm 2^{n-4}}) = \rho(g_1 d^{\mp 2^{n-5}})\rho(g_2 e)$ and hence $P(\mathfrak{G}) = \emptyset$.

On the other hand, from theorem 3, we have $\lambda(b^2) \in \bar{\Lambda}(G)$ and hence $\lambda(b^2) \in \bar{\Lambda}(\mathfrak{G})$ so that $\bar{\Lambda}(\mathfrak{G}) \neq \emptyset$. Thus by the argument used in the theorem 3, $P(\mathfrak{G}) \ncong \Lambda(\mathfrak{G})$.

Department of Mathematics
Institute of Advanced Studies
The Australian National University
Canberra

https://doi.org/10.1017/S1446788700003980 Published online by Cambridge University Press