THE LAWS OF FINITE POINTED GROUPS

ROGER M. BRYANT

1. *Introduction*

The well-known theorem of Oates and Powell **[8]** states that every finite group has a finite basis for its laws. (That is, there is a finite set of laws of which every law is a consequence.) Here we shall examine the analogous statement for finite pointed groups, where a *pointed group* is a pair (G, g) consisting of a group G together with a distinguished element g of G.

By a law of a pointed group (G, g) we shall mean a word w of the free group on the countable set $\{y, x_1, x_2, \ldots\}$ such that w always becomes equal to the identity element of G when g is substituted for y and arbitrary elements of G are substituted for $x_1, x_2, \ldots$. (For example, $[y, x_1]$ is a law of (G, g) if g is central in G.) Included among the laws of (G, g) are the laws of the group G, or, more precisely, those words in $x_1, x_2, \ldots$ which are laws of G. It would seem plausible that a simple modification of the proof of the Oates–Powell theorem would yield that every finite pointed group has a finite basis for its laws. But, rather surprisingly, this is not so. It will be shown in this paper that there is a finite pointed group (P, p) whose set of laws has no finite basis.

A pointed group may be regarded as a group with an extra nullary operation; so it is an algebra in the sense of universal algebra. Thus our investigation may be viewed in the wider context of the finite basis question for the identities of finite algebras. It was at one time conjectured that there is a finite basis for the identities of every finite algebra belonging to a variety in which the congruence lattice of every algebra is modular. (See **[9]** for a discussion of this conjecture and its motivation.) But examples of Polin **[11]** and Oates Macdonald and Vaughan-Lee **[10]** show the conjecture to be false. The pointed group (P, p) constructed below provides a further counterexample: for note that the congruences of a pointed group are the same as the congruences of its underlying group; these correspond to the normal subgroups of the group and so form a modular lattice.

Detailed information concerning varieties of groups may be found in **[7]**. The more general concepts relating to universal algebra and varieties of algebras are described in **[3]**. It is useful to note the form that some of these concepts take for pointed groups. As indicated above, the factor algebras of a pointed group (G, g) are the pointed groups $(G/N, gN)$ where N is a normal subgroup of G. The subalgebras of (G, g) are the (H, g) where H is a subgroup of G containing g. The Cartesian product of a family $((G_\lambda, g_\lambda) : \lambda \in \Lambda)$ is (G, g) where G is the Cartesian product of $(G_\lambda : \lambda \in \Lambda)$ and g is the element of G with value g_λ at λ for all $\lambda \in \Lambda$. A generating set for a pointed group (G, g) is a subset S of G such that $S \cup \{g\}$ generates G. If (G, g) can be generated by a set with n or fewer elements we shall say that (G, g) is an n-generator pointed group. A variety of pointed groups is the class of all pointed groups in which the elements of some given set of words are all laws. Equivalently it is a class closed under the operations of taking factor algebras, subalgebras and

Received 16 June 1981.

Cartesian products. We shall write var (G, g) for the variety generated by (G, g); that is, the intersection of all varieties containing (G, g).

In the finite pointed group (P, p) constructed below there are normal subgroups K and N of P with $K < N$ such that K has exponent 4 and class 2, N/K is an elementary abelian 3-group and P/N is an elementary abelian 2-group. One cannot hope for an example with substantially simpler structure. This is because the laws of a pointed group (G, g) have a finite basis if G is either nilpotent or metabelian, as can be proved by modification of the proofs of the corresponding results for groups due to Lyndon [**6**] and Cohen [**2**]. Details of the necessary modifications were given by Khan [**5**]. It is also likely that the similar but much more complicated proof of Bryant and Newman [**1**] for groups whose commutator subgroups are nilpotent of class 2 can be modified to apply to pointed groups.

One further fact worthy of note is that every finite pointed group (G, g) belongs to the variety generated by a finite pointed group (G^*, g^*) with a finite basis for its laws: if $G = \{g_1, \ldots, g_n\}$ it is sufficient to take (G^*, g^*) as the product $(G, g_1) \times \ldots \times (G, g_n)$ whose laws are finitely based by the Oates–Powell theorem. Hence, by what we shall prove, there exists a finite pointed group (P^*, p^*) with a finite basis for its laws such that the variety generated by (P^*, p^*) contains a finite pointed group (P, p) with no finite basis for its laws.

2. *The example*

For each positive integer n let v_n denote the word $y^{x_1} y^{x_2} \ldots y^{x_n}$ and w_n the word $[y^3, (y^3)^{v_n}]$. We shall show that there is a finite pointed group (P, p) which has all the w_n as laws and such that there are pointed groups (Q_n, q_n), one for each n, such that (Q_n, q_n) does not have w_{2^n} as a law but every $(n-1)$-generator subalgebra of (Q_n, q_n) belongs to var (P, p). Hence, for every n, every law of (P, p) which contains fewer than n of the variables $x_1, x_2, \ldots$ is a law of (Q_n, q_n), but not every law of (P, p) is a law of (Q_n, q_n). It follows that there is no finite basis for the laws of (P, p).

We shall begin by constructing the pointed groups (Q_n, q_n): but first a comment on notation. There will be several instances of a group G acting (on the right) as a group of automorphisms of another group H. When this holds HG will denote the corresponding semidirect product. If $g \in G$ and $h \in H$, we shall write h^g for the image of h under the action of g, whether or not the semidirect product HG is mentioned explicitly.

Let n be a positive integer. Let A be an elementary abelian group of order 2^n and let W be the wreath product $\langle \beta \rangle \operatorname{wr} A$, where $\langle \beta \rangle$ is a cyclic group of order 3. Let B be the base group of W. Thus B is an elementary abelian 3-group with basis $\{\beta^a : a \in A\}$ and W is a semidirect product, $W = BA$.

The number of maximal subgroups of A is $2^n - 1$. Let $r = 2^{n-1} - 1$ and let the maximal subgroups of A be $M_0, M_1, \ldots, M_{2r}$. For each i,

$$[B, M_i] = \langle (\beta^a)^{-1} \beta^{a\mu} : a \in A, \mu \in M_i \rangle,$$

so $B/[B, M_i]$ has order 9. Note that $[B, M_i]M_i$ is a normal subgroup of W. Let $W_i = W/[B, M_i]M_i$ and let $\phi_i : W \to W_i$ be the natural homomorphism. Let $\beta_i = \beta\phi_i$, $\beta_i' = \beta^a\phi_i$ and $\xi_i = a\phi_i$ where a is any element of $A \setminus M_i$. Then $W_i = \langle \beta_i, \beta_i' \rangle \langle \xi_i \rangle$ and W_i is isomorphic to $\langle \beta_i \rangle \operatorname{wr} \langle \xi_i \rangle$, a group of order 18.

Let Z_i and Z_i' be groups isomorphic to the quaternion group of order 8. Then W_i can be given an action on $Z_i \times Z_i'$ such that $Z_i^{\xi_i} = Z_i'$ and such that Z_i and Z_i' are invariant under β_i and β_i' with β_i acting non-trivially on Z_i but trivially on Z_i' and β_i' acting trivially on Z_i but non-trivially on Z_i'. (To see this consider the group $(Z_i\langle\beta_i\rangle)\,\mathrm{wr}\,\langle\xi_i\rangle$ with β_i acting non-trivially on Z_i.) Let $\langle\zeta_i\rangle$ and $\langle\zeta_i'\rangle$ be the centres (of order 2) of Z_i and Z_i', respectively, and let C_i denote the group $(Z_i \times Z_i')/\langle\zeta_i\zeta_i'\rangle$. Thus C_i is a group of order 32. Let γ_i denote the image in C_i of some element of order 4 of Z_i' and let $\delta_i = \gamma_i^2$. Thus $\langle\delta_i\rangle$ has order 2 and is both the centre and commutator subgroup of C_i. Since W_i fixes $\zeta_i\zeta_i'$, W_i acts on C_i. Note that $\gamma_i^{\beta_i} = \gamma_i$ and $[\gamma_i, \gamma_i^{\beta_i'}] = \delta_i$.

Let C be the direct product of the groups C_i $(0 \leqslant i \leqslant 2r)$. Then W can be given an action on C such that W acts on each C_i via the homomorphism ϕ_i. Let D be the subgroup of C generated by all the elements $\delta_i\delta_j$ $(0 \leqslant i < j \leqslant 2r)$. Each δ_i is fixed under the action of W, so W acts on C/D. Let γ be the element $\gamma_0\gamma_1 \dots \gamma_{2r}$ of C. Let Q_n be the semidirect product $(C/D)W$ and let q_n be the element $(\gamma^{-1}D)\beta$ of Q_n. Thus we have defined a pointed group (Q_n, q_n).

We shall now show that w_{2^n} is not a law of (Q_n, q_n). Let the elements of A be $\alpha_1, \dots, \alpha_{2^n}$. Let ρ and σ be the elements of CW defined by

$$\rho = (\gamma^{-1}\beta)^{\alpha_1} \dots (\gamma^{-1}\beta)^{\alpha_{2^n}}, \quad \sigma = [(\gamma^{-1}\beta)^3, ((\gamma^{-1}\beta)^3)^\rho].$$

Thus σ is a value of w_{2^n} in $(CW, \gamma^{-1}\beta)$. It is sufficient to show that $\sigma \notin D$. First note that $(\gamma^{-1}\beta)^3 = \gamma$ since $\gamma^\beta = \gamma$. Also, C is nilpotent of class 2. Hence $\sigma = [\gamma, \gamma^\tau]$ where

$$\tau = \beta^{\alpha_1} \dots \beta^{\alpha_{2^n}}.$$

Since $\sigma \in C$ we can write $\sigma = \sigma_0\sigma_1 \dots \sigma_{2r}$ where $\sigma_i \in C_i$ $(0 \leqslant i \leqslant 2r)$. We have $\sigma_i = [\gamma_i, \gamma_i^{\tau\phi_i}]$. But

$$\tau\phi_i = (\beta^{\alpha_1} \dots \beta^{\alpha_{2^n}})\phi_i = (\beta_i\beta_i')^{2^{n-1}},$$

which is equal to $\beta_i\beta_i'$ or $(\beta_i\beta_i')^{-1}$, and $[\gamma_i, \gamma_i^{\beta_i\beta_i'}] = \delta_i$. Hence $\sigma_i = \delta_i$. But $\delta_0\delta_1 \dots \delta_{2r} \notin D$. Hence $\sigma \notin D$ as required.

Now we shall prove that the intersection of the normal subgroups $[B, M_i]M_i$ of W is trivial. Since the M_i have trivial intersection it is sufficient to prove that the $[B, M_i]$ have trivial intersection. Suppose otherwise, and regard B as a right A-module in the usual way. Then there is an irreducible submodule I which is contained in $[B, M_i]$ for all i. The kernel of I contains some maximal subgroup M_i of A and we have $I \subseteq [B, M_i] \cap C_B(M_i)$. But $B = [B, M_i] \times C_B(M_i)$, by Theorem 5.2.3 of [4], and so we have a contradiction. Thus the intersection of the $[B, M_i]M_i$ is trivial.

Let (R, q_n) be any $(n-1)$-generator subalgebra of (Q_n, q_n). Recall that $Q_n = (C/D)BA$ and let χ be the projection homomorphism from Q_n onto A. Then $(R\chi, q_n\chi)$ is an $(n-1)$-generator algebra. Since $q_n\chi = 1$ it follows that $R\chi$ can be generated by $n-1$ or fewer elements. Thus, for some maximal subgroup M of A, (R, q_n) is a subalgebra of $((C/D)BM, q_n)$.

Let S be any maximal subgroup of A which is not equal to M. Then, since $A/S \cap M$ is elementary abelian of order 4, there is one and only one maximal subgroup T of A such that $S \neq T$ and $S \cap M = T \cap M$. This gives a pairing of the maximal subgroups of A not equal to M. So let us assume that the maximal subgroups of A are numbered $M_0, M_1, \ldots, M_{2r}$ in such a way that $M_0 = M$ and $M_{2i-1} \cap M = M_{2i} \cap M$ for $i = 1, 2, \ldots, r$.

Let E be the subgroup of C generated by the elements $\delta_{2i-1}\delta_{2i}$ $(1 \leqslant i \leqslant r)$. Thus $((C/D)BM, q_n)$ is a factor algebra of $((C/E)BM, (\gamma^{-1}E)\beta)$. Let $N_0 = [B, M_0]M_0$ and, for $i = 1, \ldots, r$, let

$$N_i = [B, M_{2i-1}]M_{2i-1} \cap [B, M_{2i}]M_{2i}.$$

Let $F_0 = C_0$ and, for $i = 1, \ldots, r$, let $F_i = (C_{2i-1} \times C_{2i})/E_i$ where $E_i = \langle \delta_{2i-1}\delta_{2i} \rangle$. Note that $E = E_1 \times \ldots \times E_r$ and we can regard C/E as $F_0 \times F_1 \times \ldots \times F_r$. For $i = 0, 1, \ldots, r$, let

$$K_i = (F_0 \times F_1 \times \ldots \times F_{i-1} \times F_{i+1} \times \ldots \times F_r)N_i.$$

Then each K_i is a normal subgroup of $(C/E)BM$ of index at most $2^{10} \times 3^4$. Since $N_0 \cap N_1 \cap \ldots \cap N_r = 1$ we have $K_0 \cap K_1 \cap \ldots \cap K_r = 1$. For $i = 0, 1, \ldots, r$, let Ω_i be the factor algebra of $((C/E)BM, (\gamma^{-1}E)\beta)$ corresponding to K_i. Then $((C/E)BM, (\gamma^{-1}E)\beta)$ is isomorphic to a subalgebra of $\Omega_0 \times \Omega_1 \times \ldots \times \Omega_r$.

The number of elements in Ω_i is at most $2^{10} \times 3^4$, a number independent of n, M and i. There are, up to isomorphism, only finitely many pointed groups with a given finite number of elements. Let (P, p) be the product of one representative of each isomorphism class of all the pointed groups Ω_i for all choices of n, M and i. (It can be shown that, with slightly more care in the construction, only two isomorphism classes are required.) Thus (P, p) is a finite pointed group and, for all n, every $(n-1)$-generator subalgebra of (Q_n, q_n) belongs to var (P, p).

It remains only to show that, for all m, w_m is a law of (P, p). To do this it is sufficient to show that w_m is a law of Ω_i for all choices of n, M and i. Thus, in the notation used above, it is sufficient to show that w_m is a law of $((C/E)BM, (\gamma^{-1}E)\beta)$.

Let $\kappa_1, \ldots, \kappa_m$ be any elements of CBM and let

$$g = (\gamma^{-1}\beta)^{\kappa_1} \ldots (\gamma^{-1}\beta)^{\kappa_m}, \quad h = [(\gamma^{-1}\beta)^3, ((\gamma^{-1}\beta)^3)^g].$$

It is sufficient to show that $h \in E$. For $j = 1, \ldots, m$, let $\kappa_j = \lambda_j\mu_j$ where $\lambda_j \in CB$ and $\mu_j \in M$. Then a simple calculation shows that $h = [\gamma, \gamma^b]$ where $b = \beta^{\mu_1} \ldots \beta^{\mu_m}$. Since $h \in C$ we can write $h = h_0h_1 \ldots h_{2r}$ where $h_i \in C_i$ $(0 \leqslant i \leqslant 2r)$. Then $h_i = [\gamma_i, \gamma_i^{b\phi_i}]$, so $h_i = \delta_i$ or $h_i = 1$. It is enough to show that $h_0 = 1$ and, for $i = 1, \ldots, r$, $h_{2i-1} = 1$ if and only if $h_{2i} = 1$.

Since $M\phi_0 = 1$ we have $\beta^{\mu_j}\phi_0 = \beta_0$ for all j. Thus

$$h_0 = [\gamma_0, \gamma_0^{\beta_0^m}] = 1.$$

Now suppose $1 \leqslant i \leqslant r$. Then

$$b\phi_{2i-1} = (\beta^{\mu_1} \ldots \beta^{\mu_m})\phi_{2i-1} = (\beta_{2i-1})^k(\beta'_{2i-1})^{m-k}$$

where k is the number of values of j for which $\mu_j \in M_{2i-1}$. Since $\mu_1, \ldots, \mu_m \in M$ and $M_{2i-1} \cap M = M_{2i} \cap M$ we have

$$b\phi_{2i} = (\beta^{\mu_1} \ldots \beta^{\mu_m})\phi_{2i} = (\beta_{2i})^k(\beta'_{2i})^{m-k}.$$

It follows that $[\gamma_{2i-1}, \gamma_{2i-1}^{b\phi_{2i-1}}] = 1$ if and only if $[\gamma_{2i}, \gamma_{2i}^{b\phi_{2i}}] = 1$, as required.

References

1. R. M. BRYANT and M. F. NEWMAN, 'Some finitely based varieties of groups', *Proc. London Math. Soc.* (3), 28 (1974), 237–252.
2. D. E. COHEN, 'On the laws of a metabelian variety', *J. Algebra* 5 (1967), 267–273.
3. P. M. COHN, *Universal algebra* (Harper and Row, New York, 1965).
4. D. GORENSTEIN, *Finite groups* (Harper and Row, New York, 1968).
5. Z. A. KHAN, 'A generalisation of laws in groups', M.Sc. Thesis, University of Manchester Institute of Science and Technology, 1976.
6. R. C. LYNDON, 'Two notes on nilpotent groups', *Proc. Amer. Math. Soc.* 3 (1952), 579–583.
7. H. NEUMANN, *Varieties of groups* (Springer-Verlag, Berlin, 1967).
8. S. OATES and M. B. POWELL, 'Identical relations in finite groups', *J. Algebra* 1 (1964), 11–39.
9. S. OATES MACDONALD, 'Various varieties', *J. Austral. Math. Soc.* 16 (1973), 363–367.
10. S. OATES MACDONALD and M. R. VAUGHAN-LEE, 'Varieties that make one Cross', *J. Austral. Math. Soc.* 26 (1978), 368–382.
11. S. V. POLIN, 'The identities of finite algebras', *Sib. Math. J.* 17 (1976), 1356–1366.

Department of Mathematics,
University of Manchester Institute of Science and Technology,
Manchester M60 1QD.