IDENTICAL RELATIONS AND DECISION PROCEDURES FOR GROUPS

HERMANN HEINEKEN and PETER M. NEUMANN [1]

(Received 10 January 1966)

1. Introduction

Although varieties of groups can in theory be determined as well by the identical relations which the groups all satisfy as by some structural property inherited by subgroups, factor groups and cartesian products which the groups have in common, it seems in practice just as hard to answer questions about properties of a group from knowledge of identical relations as it is from, say, a presentation. Many of the important questions connected with Burnside's problems exemplify this difficulty: we still do not know if there is a bound on the derived length of finite groups of exponent 4, nor whether there is a bound on the nilpotency class of finite groups of exponent p ($p \geqq 5$, a fixed prime).

In this note we describe two procedures:

1. *to decide whether or not every finite group satisfying a given law* $w(x_1, \cdots, x_n) = 1$ *is nilpotent;*

2. *to decide whether or not every finite group satisfying the law* $w = 1$ *is soluble.*

These two questions have formed the starting point for a study of groups satisfying certain special laws (see papers by N. D. Gupta and H. Heineken [2], [3]) and this note arose from the observation that *ad hoc* methods described there could be greatly generalised. The restriction to just one law is unnecessary, our procedures will work for any finite number of laws. But such generalisation is, in the case of groups, equally unnecessary: as is well known, any finite number of laws $w_i = 1, i = 1, \cdots, N$ is equivalent to just one law obtained by forming the product $w_1 w_2 \cdots w_N$ with variables so chosen that no variable occurs in more than one of the factors.

In § 4 we describe four more significant problems, two of which we can show to be recursively soluble, the other two we *conjecture* to be recursively

[1] The authors would like to use this opportunity to express their gratitude to Monash University for such splendid hospitality during the third term, 1965.

insoluble. One of these, the question whether two finite sets of laws determine the same variety, is meaningful as it stands for varieties of any species of algebraic system, and we show that for algebras with two unary operators it is, in general, recursively undecidable.

NOTATION. We will write $\mathfrak{W}$ for the variety determined by w; that is, if G is a group then $G \in \mathfrak{W}$ if and only if $w(g_1, \cdots, g_n) = 1$ for all choices of $g_1, \cdots, g_n$ from G.

The length of w will be denoted by l; that is, if

$$w(x_1, \cdots, x_n) = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \cdots x_{i_N}^{\varepsilon_N} \qquad \varepsilon_j = \pm 1$$

and the expression on the right is a reduced word (no cancellations are possible) then $l = N$.

2. Nilpotence of finite groups in $\mathfrak{W}$

The variety $\mathfrak{W}$ will contain finite non-nilpotent groups if and only if it contains a finite non-nilpotent group all whose proper subgroups and proper factor groups are nilpotent. These minimal non-nilpotent groups are well-known (see, for example, L. Rédei [4; Satz 1], and [3; Lemma 2.5]). Such a group is metabelian, its derived group is an elementary abelian q-group for some prime q and is complemented by a cyclic group of prime order p. For convenience we describe the groups as matrix groups — they are subgroups of the group of the affine line over a finite field of characteristic q. Let p, q be distinct prime numbers, let m be the least positive integer such that $p \mid q^m - 1$, and put

$$g(\alpha, \theta) = \begin{pmatrix} \theta & 0 \\ \alpha & 1 \end{pmatrix}$$

where α, θ are elements of $GF(q^m)$, the field with q^m elements. Then

$$G(p, q) = \{g(\alpha, \theta) \mid \theta^p = 1\}$$

is a minimal non-nilpotent group and conversely, every minimal non-nilpotent group is isomorphic to $G(p, q)$ for some ordered pair of distinct primes p, q.

The first step of the procedure is this. Take matrices

$$X_i = \begin{pmatrix} t_i & 0 \\ a_i & 1 \end{pmatrix} \qquad i = 1, \cdots, n$$

where $a_1, \cdots, a_n, t_1, \cdots, t_n$ are commuting indeterminates (so that X_i is to be considered as a matrix over $Z[a_1, \cdots, a_n, t_1, \cdots, t_n]$, the polynomial ring in $2n$ indeterminates over the ring of integers). Put

https://doi.org/10.1017/S1446788700005073 Published online by Cambridge University Press

$$X_i^* = \begin{pmatrix} 1 & 0 \\ -a_i & t_i \end{pmatrix} \qquad i = 1, \cdots, n$$

and compute the matrix $w^*(X_1, \cdots, X_n)$ which is obtained from $w(x_1, \cdots, x_n)$ by replacing x_i by X_i, x_i^{-1} by X_i^* for all i. Then

$$w^*(X_1, \cdots, X_n) = \begin{pmatrix} T_1 & 0 \\ A & T_2 \end{pmatrix}$$

where T_1 and T_2 are monomials in $t_1, \cdots, t_n$; A is a polynomial in $a_1, \cdots, a_n, t_1, \cdots, t_n$; the degrees of T_1, T_2, A are at most l, and A is linear in the a_i. Actually, of course, T_1 is the product of the t_i arising from the positive powers of the x_i in w, T_2 is the product of the t_i arising from the negative powers of the x_i. Formally, therefore,

$$w(X_1, \cdots, X_n) = \begin{pmatrix} T_2^{-1} & 0 \\ 0 & T_2^{-1} \end{pmatrix} w^* = \begin{pmatrix} T_1 T_2^{-1} & 0 \\ A T_2^{-1} & 1 \end{pmatrix}.$$

Since A, T_1, T_2 have integer coefficients they can be interpreted as polynomials over any field, in particular over $GF(q^m)$, and since

$$g(\alpha, \theta)^{-1} = \begin{pmatrix} \theta^{-1} & 0 \\ 0 & \theta^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\alpha & \theta \end{pmatrix}$$

it follows that w is a law in $G(p, q)$ if and only if

$$A(\alpha_1, \cdots, \alpha_n, \theta_1, \cdots, \theta_n) = 0$$
$$T_1(\theta_1, \cdots, \theta_n) = T_2(\theta_1, \cdots, \theta_n)$$

for all choices of $\alpha_1, \cdots, \alpha_n, \theta_1, \cdots, \theta_n$ from $GF(q^m)$ with $\theta_1, \cdots, \theta_n$ being p^{th} roots of unity.

Calculate next the highest common factor [2] h of the absolute values of the coefficients appearing in A and $T_1 - T_2$. If $h \neq 1$ (which can happen only if T_1, T_2 are identical, and this in turn happens only when w lies in the commutator subgroup of the free group on $x_1, \cdots, x_n$) and $q \mid h$ (q prime), then $G(p, q) \in \mathfrak{W}$ for all primes p. This corresponds to the case where w is a product of q^{th} powers of commutators, so that $\mathfrak{A}_q\mathfrak{A} \subseteq \mathfrak{W}$, where $\mathfrak{A}_q\mathfrak{A}$ is the variety of all groups with a normal abelian subgroup of exponent q whose factor group is abelian. But if $h = 1$ then $G(p, q) \notin \mathfrak{W}$ whenever $p > l$. For, if $h = 1$, then $A(a_1, \cdots, a_n, t_1, \cdots, t_n)$ and $T_1(t_1, \cdots, t_n) - T_2(t_1, \cdots, t_n)$ are not both identically zero as polynomials over a field of characteristic q (for any q) and since there are at least p different values that each variable a_i, t_i may take in $GF(q^m)$ — the values of the t_i being

[2] The lattice of natural numbers ordered by divisibility is to be supplemented by adjunction of 0 as the maximum element.

restricted to p^{th} roots of unity — while the degrees in the a_i or t_i of these polynomials are at most $l < p$, at least one of them must take a non-zero value in $GF(q^m)$. Thus if $p > l$ then $G(p, q) \notin \mathfrak{W}$. There are now at most l remaining primes p for which we have not yet decided whether any of the groups $G(p, q)$ satisfy $w = 1$ identically. Each of these primes is to be considered separately.

Let p then be a prime number, $p \leqq l$. Define polynomials A_p, T_{1p}, T_{2p} by replacing any power $t_i^{m_i}$ by $t_i^{r_i}$ where

$$m_i \equiv r_i \pmod{p} \qquad 0 \leqq r_i < p$$

wherever possible in A, T_1 and T_2 respectively. Then clearly the degree in t_i of the resulting polynomials A_p, $T_{1p}-T_{2p}$ will be less than p for all relevant i — and A_p is of course still linear in the a_i. Moreover, if $\theta_1, \cdots, \theta_n$ are p^{th} roots of unity in $GF(q^m)$, then

$$A(\alpha_1, \cdots, \alpha_n, \theta_1, \cdots, \theta_n) = A_p(\alpha_1, \cdots, \alpha_n, \theta_1, \cdots, \theta_n)$$
$$T_1(\theta_1, \cdots, \theta_n) - T_2(\theta_1, \cdots, \theta_n) = T_{1p}(\theta_1, \cdots, \theta_n) - T_{2p}(\theta_1, \cdots, \theta_n)$$

for any elements $\alpha_1, \cdots, \alpha_n$ of $GF(q^m)$. Again we calculate h_p, the highest common factor of the absolute values of the coefficients of A_p and $T_{1p}-T_{2p}$. If $h_p \neq 1$ then $G(p, q) \in \mathfrak{W}$ whenever q divides h_p, if $h_p = 1$ then the same argument as before gives that $G(p, q) \notin \mathfrak{W}$ for any q.

Our prescription therefore is this:

Compute the (at most $l+1$) non-negative integers h, h_2, h_3, h_5, $\cdots$, h_{p_r} where 2, 3, 5, $\cdots$, p_r are the primes not bigger than l; if all these numbers are 1 then every finite group satisfying $w = 1$ identically is nilpotent; but if at least one of these numbers is not 1 then there are finite non-nilpotent groups satisfying $w = 1$ identically.

3. Solubility of finite groups in $\mathfrak{W}$

Our description of an algorithm to determine whether or not all the finite groups satisfying $w = 1$ are soluble depends on knowledge of the minimal non-soluble groups. These are, of course, the minimal simple groups, finite simple groups all whose proper subgroups are soluble. We will need the classification announced by J. G. Thompson [6]:

The minimal simple groups are among the groups[3] (*i*) $PSL(2, q)$; (*ii*) $PSL(3, 3)$; (*iii*) $Sz(2^p)$ (*Suzuki groups, Suzuki* [5]). It seems doubtful that so deep a result as this is really necessary for our purpose but we have not been able to prove the theorem any other way. The first part of our

[3] The groups $PSL(2, q)$ actually are minimal simple groups for (a) q prime, $q \geqq 5$, $q^2 \not\equiv 1 \pmod 5$; (b) $q = 2^p$ p prime; (c) $q = 3^p$ p any odd prime. The Suzuki groups are minimal for odd primes p.

https://doi.org/10.1017/S1446788700005073 Published online by Cambridge University Press

algorithm decides which of the projective special linear groups $PSL(2, q)$ satisfy $w = 1$, and the second part does the same for the Suzuki groups.

FIRST PART. We shall use the description of $PSL(2, q)$ as factor group of the group $\Sigma L(2, q)$ which consists of all 2×2 matrices over $GF(q)$ (q is now any prime power) whose determinants are squares in $GF(q)$ by the group of non-zero scalar matrices. So we begin with matrices

$$X_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \qquad i = 1, \cdots, n$$

in commuting indeterminates $a_1, \cdots, a_n, b_1, \cdots, b_n, c_1, \cdots, c_n, d_1, \cdots, d_n$, define

$$X_i^* = \begin{pmatrix} d_i & -b_i \\ -c_i & a_i \end{pmatrix} \qquad i = 1, \cdots, n,$$

and compute

$$w^*(X_1, \cdots, X_n) = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where, as before, w^* is the monomial obtained from $w(x_1, \cdots, x_n)$ by substituting X_i for x_i and X_i^* for x_i^{-1} wherever these occur. The entries A, B, C, D, are polynomials in the a_i, b_i, c_i, d_i with integer coefficients, of degree at most l. Let the highest common factor of the absolute values of the coefficients of B, C, $A-D$ be h. If $h \neq 1$ then $PSL(2, q)$ satisfies $w = 1$ identically whenever q is a power of a prime p which divides h, for in $GL(2, q)$ the inverse of the matrix X_i (whose entries now are interpreted as elements of $GF(q)$) is a scalar multiple of X_i^*, consequently $w(X_1, \cdots, X_n)$ will be a scalar multiple of $w^*(X_1, \cdots, X_n)$ and if the values of w^* are all scalar matrices then so are the values of w.

If $h = 1$ and $q > 2l+3$ then $PSL(2, q) \notin \mathfrak{W}$. For, if β, γ are arbitrary elements and δ is any non-zero element of $GF(q)$ then we still have available at least $\frac{1}{2}(q-1)$ values for α in $GF(q)$ for which $\alpha\delta-\beta\gamma$ is a non-zero square — namely, the elements $\delta^{-1}(\lambda^2+\beta\gamma)$ with $\lambda \neq 0$. This gives sets of at least $l+1$ independent values for each of the variables a_i, b_i, c_i, d_i $i = 1, \cdots, n$, for which the matrices X_i are in $\Sigma L(2, q)$. Since the polynomials B, C, $A-D$ have degree at most l, and since at least one of them is not identically zero as a polynomial over $GF(q)$, at least one of the values of the matrix $w^*(X_1, \cdots, X_n)$ is not scalar for $X_1, \cdots, X_n$ in $\Sigma L(2, q)$. It follows that w takes non-trivial values in $PSL(2, q)$ and so $PSL(2, q) \notin \mathfrak{W}$. The remaining fractional linear groups, of which there are at most $2l+4$, namely $PSL(3, 3)$ and $PSL(2, q)$ for $q \leqq 2l+3$, can then be checked one by one.

SECOND PART. We handle the Suzuki groups in a similar way, but with one significant difference. If $k \geqq 1$ and $q = 2^{2k+1}$ then $GF(q)$ has an auto-

https://doi.org/10.1017/S1446788700005073 Published online by Cambridge University Press

morphism θ given by

$$\alpha^\theta = \alpha^{2^{k+1}}$$

for all $\alpha \in GF(q)$. In the following we will handle θ as an ordinary exponent: θ is taken to exceed any integer so that the additive group generated by θ and 1 is ordered lexicographically, and a "polynomial of degree $r+s\theta$" then has the obvious meaning. With this convention we can describe the group $Sz(q)$. Let

$$h(\alpha, \beta) = \begin{pmatrix} 1 & & & \\ \alpha & 1 & & \\ \alpha^{1+\theta}+\beta & \alpha^\theta & 1 & \\ \alpha^{2+\theta}+\alpha\beta+\beta^\theta & \beta & \alpha & 1 \end{pmatrix},$$

$$k(\gamma) = \begin{pmatrix} \gamma^{1+\theta} & & & \\ & \gamma & & \\ & & \gamma^{-1} & \\ & & & \gamma^{-1-\theta} \end{pmatrix}, \qquad \tau = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix},$$

where $\alpha, \beta, \gamma \in GF(q)$, $\gamma \neq 0$, and entries in these matrices which have not been explicitly written down are all zero. Then (M. Suzuki [5]) every element of $Sz(q)$ is a product $h(\alpha, \beta)k(\gamma)$ or a product $h(\alpha, \beta)k(\gamma)\tau h(\delta, \varepsilon)$, and the expression of an element in one of these forms is unique. The inverse of a matrix $h(\alpha, \beta)$ is obtained by substituting $\alpha^{1+\theta}+\beta$ for β; since $\theta^2 = 2$ (that is, θ^2 is the automorphism of $GF(q)$ which maps any element to its square) this again gives a matrix whose entries are polynomials of degree at most $2+\theta$ in α and β. The inverse of $k(\gamma)$ is $k(\gamma^{-1})$ and τ is its own inverse. Notice that $k(\gamma)$ and its inverse are $\gamma^{-1-\theta}$ times matrices whose entries are polynomials of degree at most $2+2\theta$ in γ.

We now take matrices of the given form in commuting indeterminates a_i, b_i, c_i, d_i, e_i and compute the 2^n monomials obtained by substituting matrices $X_i = c_i^{1+\theta}h(a_i, b_i)k(c_i)$ or $X_i = c_i^{1+\theta}h(a_i, b_i)k(c_i)\tau h(d_i, e_i)$ for x_i in $w(x_1, \cdots, x_n)$ — again, in order to keep to matrices with polynomial entries, we substitute $c_i^{2+2\theta}X_i^{-1}$ for x_i^{-1} wherever it occurs. This gives 2^n 4×4 matrices each of which has polynomial entries with integer coefficients of degree at most $(6+4\theta)l$ in at most $5n$ variables. In each of these polynomials replace any even coefficient by 0, any odd coefficient by 1. If the resulting matrices are all scalar matrices (identically: off-diagonal entries are to be the zero polynomial, the diagonal entries one and the same polynomial) then all the Suzuki groups satisfy $w = 1$ identically. If, however, at least one of these matrices is not a scalar matrix then for all sufficiently large q — $q \geqq 128\, l^2$ will do — it will be the case that $Sz(q) \notin \mathfrak{W}$. For, if we fix k for the moment then we may replace θ in any exponent by 2^{k+1}. We can

https://doi.org/10.1017/S1446788700005073 Published online by Cambridge University Press

be sure that the resulting polynomials are still not all zero provided that we can distinguish monomials of degree $r_1+s_1 2^{k+1}$ from monomials of degree $r_2+s_2 2^{k+1}$. Since our polynomials all have degree at most $6l+4l\theta$ this will be so if

$$2^{k+1} > 6l.$$

If moreover

$$(6+4.2^{k+1})l < q = 2^{2k+1}$$

then the relevant non-zero polynomials will take some non-zero values over $GF(q)$. The latter inequality is certainly satisfied if

$$2^{2k+1} \geqq 8.2^{k+1}l,$$

that is, if

$$2^k \geqq 8l,$$

so that both inequalities are satisfied if $q \geqq 128l^2$. We are then left with at most $3+\log_2 l$ groups which again are to be checked one by one.

DIGRESSION. In both parts of this procedure we used (explicitly or implicitly) the highest common factor h of the absolute values of the coefficients of certain polynomials, polynomials which are determinable explicitly in terms of w. If h was divisible by p, or 2, then $PSL(2, q)$, $Sz(q)$, satisfied $w = 1$ identically whenever q was a power of p, or an odd power of 2 respectively. Actually, however, if w is a non-trivial word then h is automatically 1: any infinite set of the groups $PSL(2, q)$ or any infinite set of Suzuki groups generates the variety of all groups. As a matter of fact, any infinite set of the known finite non-abelian simple groups generates the variety of all groups; that is, only finitely many of the known non-abelian finite simple groups can satisfy a given non-trivial law. The classical groups and the other algebraic families can be handled as in § 2 or the first part of this section; the twisted versions are so "nearly algebraic" that they can be handled in the same way as we dealt with the Suzuki groups; the alternating groups and the remaining sporadic simple groups offer no difficulty. For all the families (other than the family of alternating groups) one must calculate that the relevant number h is 1. But the larger finite simple groups defined over a field $GF(p^k)$ always contain a subgroup $PSL(2, p^m)$ or $Sz(2^m)$ where m tends to infinity with k, so that it is sufficient to prove the statement for these latter groups.

4. Concluding remarks

It is sensible to ask of many of the problems arising in practice whether they admit an algorithmic solution. Here we survey briefly some of those we consider to be important.

https://doi.org/10.1017/S1446788700005073 Published online by Cambridge University Press

3. *Is it decidable whether every finite nilpotent group satisfying* $w = 1$ *identically has class at most* k?

4. *Is it decidable whether every finite soluble group satisfying* $w = 1$ *identically has derived length at most* k?

These two problems can be solved in essentially the same way as the word problem in residually finite groups: on the one hand enumerate all elements of the verbal closure of $w(x_1, \cdots, x_n)$ and [4] $[x_1, \cdots, x_{k+2}]$ in the free group on $x_1, \cdots, x_r$ $(r = \max(n, k+2))$, and on the other hand enumerate all finite groups, checking each one to decide whether it is nilpotent of class greater than k and satisfies $w = 1$ identically. Eventually this process must produce either the word $[x_1, \cdots, x_{k+1}]$ as a consequence of w and $[x_1, \cdots, x_{k+2}]$ or a finite nilpotent group satisfying $w = 1$ identically, but which is not of class k. A similar procedure works for the soluble case.

There is an important practical difference between the algorithms described in §§ 2, 3 and those described here. The former are primitive recursive procedures but the latter are, on the face of it, only recursive. In fact, we can predetermine an upper bound on the length of time taken for our first two algorithms in terms of the length of the word w, without actually going through with the computation.

Problem 5. *Is it decidable whether there is a bound on the class of (finite) nilpotent groups, or a bound on the derived length of (finite) soluble groups, satisfying* $w = 1$?

These are precisely the questions which seem most important at present in the study of Burnside's Problem (see § 1) and of groups satisfying an Engel identity $[x, y, \cdots, y] = 1$. It seems just possible, though hardly likely, that even for some one particular word w these questions may be undecidable [5] in, say, the Elementary Theory of Groups (and if this were the case we would immediately get a proof in the meta-theory that no bound exists for this particular word); but even if the questions are decidable for each word w individually, it is unlikely that there is a uniform procedure which will decide for every w.

Problem 6. *Is it decidable whether the varieties* $\mathfrak{W}_1$ *and* $\mathfrak{W}_2$ *determined by words* w_1, w_2 *are the same*?

This is an obvious generalisation of questions 3 and 4. The answer is affirmative if we know that $\mathfrak{W}_1$ and $\mathfrak{W}_2$ are generated by their finite groups, but in general we do not know.

[4] $[x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2$; $[x_1, \cdots, x_{i+1}] = [[x_1, \cdots, x_i], x_{i+1}]$.

[5] Undecidable in the sense that, although a bound must exist or not exist, if the latter happened to be the case there may nevertheless be no proof of this fact within the Elementary Theory of Groups. (The term Elementary Theory of Groups is used in the sense of E. Mendelson, Introduction to Mathematical Logic, van Nostrand, 1964, p. 58).

The last of these questions is, of course, relevant much more generally for varieties of algebras of any species (and is a special case of problems concerning the equivalence of two first-order theories) — and for most species there is no end of questions analogous to 1—5. But for algebras with, say, two unary operators Problem 6 is recursively undecidable. To see this, start from a finite set R of relations in two generators a, b which present a semigroup whose word problem is insoluble (see for example, M Davis [1], Theorem 4.6, page 98). Let $\mathfrak{W}$ be the variety of algebras with two unary operators α, β satisfying the one-variable laws

$$xr_1(\alpha, \beta) = xr_2(\alpha, \beta)$$

for all pairs r_1, r_2 for which the relation $r_1(a, b) = r_2(a, b)$ is in R. If $s_1(a, b)$, $s_2(a, b)$ are elements of the free semigroup generated by a, b, and $\mathfrak{W}_1$ is the subvariety of $\mathfrak{W}$ obtained by adding the one further law

$$xs_1(\alpha, \beta) = xs_2(\alpha, \beta),$$

then it is recursively undecidable whether or not $\mathfrak{W}_1 = \mathfrak{W}$.

References

[1] M. Davis, *Computability and unsolvability*, New York 1958.
[2] N. D. Gupta, 'Groups with Engel-like conditions' *Archiv Math.*, 17 (1966), 193—199.
[3] N. D. Gupta and H. Heineken, 'Groups with a two-variable commutator identity',
[4] L. Rédei, Über die einstufig nicht nilpotenten endlichen Gruppen', *Publ. Math. Debrecen* 4 (1956), 303—324.
[5] M. Suzuki, 'On a class of doubly transitive groups', *Ann. Math.* 75 (1962), 105—145.
[6] J. G. Thompson, 'The minimal simple groups', Lecture notes Chicago 1964.

Mathematisches Seminar der Universität
6 Frankfurt am Main
and
The Queen's College
Oxford