Can. J. Math. Vol. **46** (6), 1994 pp. 1135–1149

UNIFICATION IN VARIETIES OF GROUPS: NILPOTENT VARIETIES

MICHAEL H. ALBERT AND JOHN LAWRENCE

ABSTRACT. In this paper we show that any system of equations over a free nilpotent group of class c is either *unitary* or *nullary*. In fact, such a system either has a most general solution (akin to the most general solution of a system of linear dipohantine equations), or every solution has a proper generalization. In principle we provide an algorithm for determining whether or not a most general solution exists, and exhibiting it if it does.

1. **Introduction.**

The process of solving equations is central to much of algebra. In a general setting, there are two questions to answer when presented with an equation: "Does a solution exist?", and "If so, what is the most general form of a solution?". In this paper we address these questions in the context of nilpotent groups. Before we begin, a discussion of the exact meaning of the second question is in order.

We work in a variety V (of groups—though the following remarks can be applied in a more general context.) A system Σ of equations in the variables $\mathbf{x} = x_1, x_2, \ldots, x_n$ is a finite set of elements of the form:

$$t(\mathbf{x}) = 1$$

where t is a term in the language of groups, and 1 denotes the identity element. A *solution* of Σ in a group $G \in V$ is a sequence of elements $\mathbf{a} = a_1, a_2, \ldots, a_n$ from G such that $t(\mathbf{a}) = 1_G$ for each element of Σ. Another way to put this is that if $F_V(\mathbf{x})$ is the relatively free group in V with generators $\mathbf{x}$, then a solution of Σ is a homomorphism τ from $F_V(\mathbf{x})$ to G whose kernel contains each of the terms t which appear on the left hand side of the equations in Σ. The group in which we search for solutions will be the countably generated relatively free group of V-–which we will generally denote F. Although formally solutions are homomorphisms, we will often make an informal statement of the type "$\mathbf{x} = \mathbf{a}$ is a solution" by which we mean "the homomorphism α which sends x_i to a_i for each i is a solution". Although it is not critical, we assume that each of the variables in $\mathbf{x}$ actually appears in some equation in Σ (if this is not the case, any extra variables are "free" and play no role in the search for most general solutions.)

Notice that the equations we consider do not contain any parameters from the group in which we will be solving them. In particular the sequence all of whose elements are the identity will always be a solution to any system of equations, so the existence of a

Received by the editors March 2, 1993.

AMS subject classification: Primary: 20F18; secondary: 20E10, 68Q40.

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

solution is never in doubt. See the remarks at the end of this section for a brief discussion of what is known if parameters are allowed.

Given two solutions τ_1 and τ_2 of Σ we say that τ_1 is *at least as general as* τ_2, and write $\tau_1 \leq \tau_2$ if there is an endomorphism $\alpha\colon F_\omega \longrightarrow F_\omega$ such that $\alpha\tau_1 = \tau_2$. Clearly $\leq$ is a transitive and reflexive relation; however it need not be anti-symmetric. There is a naturally associated equivalence relation $\sim$ defined by:

$$\sigma \sim \tau \Longleftrightarrow \sigma \leq \tau \quad \text{and} \quad \tau \leq \sigma$$

and a partial order on the equivalence classes of this relation which is induced by $\leq$.

This definition of generalization is one which has been arrived at in the study of resolution methods of theorem proving, and term rewriting systems (where "solving equations" goes by the name of "unification".) It corresponds to the natural understanding of generalization as the following simple example illustrates:

Consider the single equation

$$2x + 3y + 6z = 0$$

in the variety of abelain groups. One solution is given by:

$$x = 0, \quad y = 2a, \quad z = -a$$

for any generator a of the free abelian group. Another solution is given by:

$$x = 3b, \quad y = -2b + 2c, \quad z = -c,$$

for generators b and c. It is clear that the second solution is more general than the first, and this is witnessed by any endomorphism which maps b to 0 and c to a. In fact the second solution is a *most general solution* to the equation: it is at least as general as any solution to the equation (for any other solution $x = s$, $y = t$, $z = u$, an endomorphism which sends c to $-u$ and b to $-t-2u$ establishes this.) In fact, any system of equations in the variety of abelian groups has such a most general solution—which amounts to a general solution of the same system viewed as homogeneous linear diophantine equations. Simple Gaussian elimination (avoiding fractions) can be used to find such solutions but may lead to a "blow up" in the size of coefficients at intermediate points in the calculation. This problem can be avoided and polynomial time algorithms for solving such systems are known; see for example [3] and [2].

The generalization relation need not always behave so nicely. For example consider the equation:

$$xyx^{-1}y^{-1} = 1$$

in the variety of all groups. It is known that all solutions to this equation in a free group are of the form:

$$x = t^n, \quad y = t^m$$

for some t and integers n and m. Any solution is generalized by one in which t is a generator and n and m are relatively prime. Among these more general solutions none

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

has any strict generalization, but any two such solutions which differ in the exponents (by anything other than a sign change) are incomparable. Therefore, this single equation has an infinite set of most general solutions.

In the variety of all groups it can be shown using the Nielsen-Schreier theorem, and the fact that free groups of finite rank are Hopfian, that any system of equations has a set of most general solutions. The argument is quite straightforward. Given a solution α, we call the rank of the image of α (as a free group), the rank of α. We can certainly find $\beta \leq \alpha$ such that β has the same rank as α and the image of β is a free factor of F (just by considering α as a map onto its range, and taking an isomorphism from the range of α to a free factor of F.) Call a solution whose range is a free factor of F, "good". If $\beta_1 \leq \beta_2$ and both β_1 and β_2 are good solutions then the rank of β_1 must be greater than or equal to the rank of β_2. Also, if the ranks are equal the two solutions are equivalent. Since the rank of a solution is at most the number of variables in the set of equations, this shows that among the good solutions there is a set of most general solutions, and every solution is generalized by one of these.

Let us make our terminology a little more precise. A *most general solution* σ of Σ is one which has no proper generalization (*i.e.* if $\tau \leq \sigma$ then $\sigma \leq \tau$). We say that Σ is *unitary* if there is a single most general solution which generalizes every solution (this solution need not be unique); *finitary* if there are finitely many most general solutions, such that every solution is generalized by at least one of them; *infinitary* if there is an infinite family of most general solutions of this type; and *nullary* if none of the preceding cases occurs, which means that there is at least one solution which is not generalized by any most general solution. In terms of the partial order obtained from $\leq$ above, Σ is unitary if the order has a smallest element, finitary (infinitary) if the set of minimal elements is finite (infinite) and every element lies above a minimal element, and nullary if there is some element which does does not lie above a minimal element.

We will see that for each $c > 1$ every system of equations in the variety of all nilpotent groups of class c is either unitary of nullary. In fact, if a system is nullary, then we will prove that every solution has a strict generalization. The proof will implicitly specify an algorithm which either finds the most general solution to a system of equations, or establishes that no such solution exists. The algorithm can be made polynomial, and in fact quite practical, at least for small values of c (we give some examples for the case $c = 2$.)

If systems of equations which contain parameters from the free nilpotent group are allowed, then the situation is much more complex. First of all of course there is no longer a guarantee that any solution will exist. In [8] it is shown that the unification problem in the free nilpotent group of class $c \geq 9$ is undecidable. Subsequently [7] and [1] lowered this to $c \geq 5$, and very recently, [9] to $c \geq 3$. It seems likely that for $c = 2$ the unification problem is decidable. However, it must be stressed that in all these results, the presence of parameters in the equations is critical.

We hope that this paper will be accessible to a wide audience, and so we have attempted to make it as self-contained as possible. In particular Section 2.1 contains a

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

great deal of basic material. There is no doubt that an acquaintance with the material on nilpotent groups which can be found in [6] would be of more than a little value. The results and definitions which we require from this reference are collected at the beginning of the next section.

2. **Results.**

2.1 *Preliminaries.* The language of groups contains symbols for multiplication, inverse, and the identity element (which we denote 1). To this language we add the commutator bracket:

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

and the "left-normed commutators of weight $c+1$" defined inductively by:

$$[x_1, x_2, \ldots, x_{c+1}] = \big[[x_1, x_2, \ldots, x_c], x_{c+1}\big].$$

A group G is said to be *nilpotent of class c* ($c \geq 1$) if for all $g_1, g_2, \ldots, g_{c+1} \in G$,

$$[g_1, g_2, \ldots, g_{c+1}] = 1.$$

So the groups which are nilpotent of class 1 are just abelian groups.

For any c, the nilpotent groups of class c form a *variety of groups* denoted $\mathcal{N}_c$, *i.e.* a class of groups closed under the formation of subgroups, quotient groups, and Cartesian products. In $\mathcal{N}_c$ (more generally in any variety), there exists, for every set X, a free group $F(X)$ generated by X, with the following universal mapping property:

> for every $G \in \mathcal{N}_c$ and every function $f: X \longrightarrow G$ there is a group homomorphism $f: F(X) \longrightarrow G$ which extends f.

Given a free group F in a variety, any subset X of F which generates F and has the above universal mapping property is referred to as a free generating set of F.

When we speak of "the" free group in a variety we will mean a countably generated free group on an unspecified generating set (from which we will occasionally pull elements.)

The center of a free group of $\mathcal{N}_c$ is the group generated by all commutators of weight c. This group is free abelian, and if the generating set is linearly ordered, has a basis consisting of all the basic weight c commutators. It is not absolutely essential to know what a basic commutator is, but the curious reader should consult [6] p. 79. By "general nonsense" the quotient of a free group of $\mathcal{N}_c$ by its commutator subgroup is also a free abelian group, generated by the images of the generators of the original group.

The following specializes Theorem 42.31 of [6] to the situation at hand.

PROPOSITION 1. *Let A be a subset of a free group F in $\mathcal{N}_c$. If the image of A under the natural homomorphism from F to F/F' is independent and generates a direct factor of F/F' then A can be extended to a free generating set of F.*

Finally we need the following fact, related to results of J. Lawrence in [4] whose proof we defer until Section 2.4.

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

LEMMA 2. *Let F be the free group in $\mathcal{N}_c$, let r be a positive integer, and let p be a prime which is not a divisor of r. Then for all positive integers k there exists a positive integer $\phi(k)$ such that, for any $M > \phi(k)$, and any subset $\{u_{ij} : 1 \leq i \leq M, 1 \leq j \leq c\}$ of cM distinct elements of a free generating set the equation:*

$$z^p \prod_{j=1}^{k} [x_j, y_j] = \Big(\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}] \Big)^r$$

has no solution in F.

2.2 *Unification in nilpotent class c groups.* Let Σ be any finite set of group equations. First consider a most general solution ν to this system in the variety of abelian groups which uses the smallest possible number of free parameters

$$\mathbf{z} = z_1, z_2, \ldots, z_k.$$

In particular k is the dimension (over $\mathbf{Q}$) of the null space of the matrix associated to Σ, and we will call this the *dimension* of Σ. Moreover, there are terms $t_1, t_2, \ldots, t_k$ such that if

$$\mathbf{b} = b_1, b_2, \ldots, b_n$$

is any solution to Σ in a torsion free abelian group then:

$$b_i = w_i\big(t_1(\mathbf{b}), t_2(\mathbf{b}), \ldots, t_k(\mathbf{b})\big).$$

So we may write:

$$\nu(x_i) = w_i(\mathbf{z})$$
$$t_j\big(\nu(\mathbf{x})\big) = z_j.$$

For illustrative purposes, consider the example in the introduction (variable names changed for consistency):

$$2x_1 + 3x_2 + 6x_3 = 0.$$

Here we may take:

$$\nu(x_1) = 3z_1, \quad \nu(x_2) = -2z_1 + 2z_2, \quad \nu(x_3) = -z_2$$

and

$$t_1(x_1, x_2, x_3) = x_1 + x_2 + 2x_3, \quad t_2(x_1, x_2, x_3) = -x_3.$$

Fix Σ, the w_i and the t_j for the remainder of this section. Now consider Σ in the variety $\mathcal{N}_c$. Suppose that α is a solution to Σ in $\mathcal{N}_c$. We will let α_{ab} be the corresponding solution in the variety of abelian groups, obtained by factoring the composition of α with the projection from F to F/F' through F_n/F_n'.

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

PROPOSITION 3. *If Σ has a solution α in $\mathcal{N}_c$ such that α_{ab} is a most general solution in the variety of abelian groups, then α generalizes every solution in $\mathcal{N}_c$.*

PROOF. The proof is by induction on the nilpotency class c. The result is of course trivial in the case that $c = 1$. So assume that $c > 1$ and that the result holds for all smaller nilpotency classes.

We suppose that α_{ab} is the solution ν discussed above. The image of α modulo F' is a free abelian group of rank k which is a direct summand of F/F'. Now using Theorem 42.35 of [6] it follows that the elements:

$$t_1\big(\alpha(\mathbf{x})\big), t_2\big(\alpha(\mathbf{x})\big), \ldots, t_k\big(\alpha(\mathbf{x})\big)$$

can be identified with a subset of the free generating set of F.

Let β be any other solution of Σ in $\mathcal{N}_c$. We must show that $\alpha \leq \beta$. Let $\bar{\alpha}$ and $\bar{\beta}$ be the corresponding solutions in $\mathcal{N}_{c-1}$ *i.e.*:

$$\bar{\alpha}\colon F_n/Z(F_n) \longrightarrow F/Z(F)$$

is such that $\bar{\alpha}\pi = \pi\alpha$, where π represents the projection from a group G to $G/Z(G)$.

By the inductive hypothesis there exists $\bar{\theta}\colon F/Z(F) \longrightarrow F/Z(F)$ such that

$$\bar{\theta}\bar{\alpha} = \bar{\beta}.$$

Choose any $\theta\colon F \longrightarrow F$ such that the corresponding map is $\bar{\theta}$. It need not be the case that $\theta\alpha = \beta$. However,

$$\beta(x_i) = \theta\alpha(x_i)C_i$$

where $C_i \in Z(F)$ for $1 \leq i \leq n$. Since both $\theta\alpha$ and β are solutions of Σ, and the C_i are central, an easy computation establishes that τ where

$$\tau(x_i) = C_i \quad 1 \leq i \leq n$$

is also a solution of Σ, and since α_{ab} is a most general solution for abelian groups, we may choose $\psi\colon F \longrightarrow F$ whose range is contained in $Z(F)$ such that:

$$\psi\alpha(x_i) = C_i.$$

But now we define the homomorphism γ from F to F on the generators z by:

$$\gamma(z) = \theta(z)\psi(z)$$

then

$$\gamma\big(w(\mathbf{z})\big) = \theta\big(w(\mathbf{z})\big)\psi\big(w(\mathbf{z})\big)$$

for any term w (since the range of ψ is contained in the center of F), and hence:

$$\gamma\alpha = \beta.$$

So α is indeed a most general solution. ■

What happens in the case where Σ does not have a solution α such that α_{ab} is as general as possible?

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

PROPOSITION 4. *Let α be a solution of Σ in $\mathcal{N}_c$ $(c > 1)$ such that α_{ab} is not a most general general abelian solution. Then α has a proper generalization.*

PROOF. Let

$$a_i = \alpha(x_i).$$

From the most general abelian solution to Σ we see that:

$$a_i = w_i(\mathbf{b})C_i$$

$b_j = t_j(\mathbf{a})$ and $C_i \in F'$. However, it cannot be the case that $\mathbf{b}$ freely generates a direct summand of F/F' since α_{ab} is not most general abelian. So without loss of generality, there exists an integer $r > 0$, a prime p not dividing r, integers $\lambda_2, \lambda_3, \ldots, \lambda_k$, and $C \in F'$ such that:

$$b_1^r = b_2^{\lambda_2} b_3^{\lambda_3} \cdots b_k^{\lambda_k} D^p C.$$

Here we use the fact that if a sequence $\mathbf{d}$ in a free abelian group does not generate a direct summand then there must be a prime p and some integer combination of $\mathbf{d}$ whose coefficients are not all multiples of p but whose value is a multiple of p.

But now we consider a new sequence of elements:

$$c_1 = b_1 \prod_{s=0}^{m} [y_{cs+1}, y_{cs+2}, \ldots, y_{cs+c-1}]$$
$$c_j = b_j \quad (2 \leq j \leq k)$$

where the $\mathbf{y}$ are free generators which do not occur in any of $\mathbf{b}$, nor in D nor C. Then

$$a_i' = w_i(\mathbf{c})C_i \quad \text{for } 1 \leq i \leq n$$

is still a solution to Σ, with corresponding homomorphism α'. Moreover:

$$c_j = t_j(\mathbf{a}').$$

This solution α' is at least as general as α since we may obtain α from it by mapping all the y-generators to 1. However, any homomorphism τ which sent a_i to a_i' for $1 \leq i \leq n$ would send b_j to c_j for $1 \leq j \leq k$ since $c_j = t_j(\mathbf{a}')$ and $b_j = t_j(\mathbf{a})$. In particular we would have:

$$c_1^r = c_2^{\lambda_2} c_3^{\lambda_3} \cdots c_k^{\lambda_k} \tau(D)^p \tau(C).$$

Hence:

$$\prod_{s=0}^{m} [y_{cs+1}, y_{cs+2}, \ldots, y_{cs+c-1}]^r = C^{-1} D^{-p} \tau(D)^p \tau(C).$$

This last equation can be rewritten as:

$$\prod_{s=0}^{m} [y_{cs+1}, y_{cs+2}, \ldots, y_{cs+c-1}]^r = Z^p \prod_{i=1}^{t} [X_i, Y_i]$$

where

$$Z, X_1, X_2, \ldots, X_t, Y_1, Y_2, \ldots, Y_t.$$

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

are certain elements of F, and most importantly, t is independent of m. In fact we can manage with

$$t = p + 1 + 2 \text{ (number of commutators in } C).$$

But by Lemma 2 if m is chosen sufficiently large, no such elements exist, and hence α' is strictly more general than α. ■

These two propositions give:

THEOREM 5. *Let Σ be a set of equation over $\mathcal{N}_c$. If there is a solution to Σ in $\mathcal{N}_c$ which induces a most general abelian solution to Σ (via the quotient by F') then Σ is unitary. Otherwise Σ is nullary, and in fact every solution has a proper generalization.*

2.3 *Examples.* We consider here a few examples which we hope will help to clear up the details in the proofs above. As a first example consider the equation:

$$[x, y] = 1 \tag{1}$$

in $\mathcal{N}_2$. As usual F denotes the countably generated free group in this variety. The "abelianized" version of this equation is:

$$0x + 0y = 0$$

and accordingly has dimension 2. We take the terms

$$t_1(x_1, x_2) = x_1 \quad t_2(x_1, x_2) = x_2$$
$$w_1(x_1, x_2) = x_1 \quad w_2(x_1, x_2) = x_2.$$

However it is impossible for any solution to equation (1) in $\mathcal{N}_2$ to generate a free group of rank 2, so according to the theorem above every solution to this equation must have a proper generalization. Generically a solution α will look like:

$$\alpha(x) = a^k C_1 \quad \alpha(y) = a^l C_2$$

for some element $a \in F$ integers k and l, and elements C_1 and C_2 of F'. Clearly we may assume that the greatest common divisor of k and l is 1, and that $k \neq 0$. In the notation of the proof, we have $b_1 = a^k C_1$, $b_2 = a^l C_2$ and so:

$$b_1^l = b_2^k C$$

where

$$C = C_2^k C_1^{-l}.$$

Then we define a new solution

$$\alpha'(x) = a^k \Big(\prod_{s=0}^{M} [z_{2s}, z_{2s+1}] \Big) C_1 \quad \alpha'(y) = a^l C_2$$

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

which will be strictly more general than α provided that M is chosen sufficiently large (and the z's are generators of F not occuring in a, C_1 or C_2.) For if $\tau\alpha = \alpha'$ then:

$$\tau(b_1^l) = \tau(b_2^k)\tau(C)$$
$$\left(a^k \prod_{s=0}^{M}[z_{2s}, z_{2s+1}]C_1\right)^l = (a^l C_2)^k \tau(C)$$
$$\prod_{s=0}^{M}[z_{2s}, z_{2s+1}]^l = C^{-1}\tau(C).$$

But the right hand side of the last equation is the product of a number of commutators which is independent of M, and this equation cannot be satisfied for M sufficiently large.

Now for an example where p actually plays a role, consider the equation:

$$x^2y^2z^{-2} = 1$$

again in $\mathcal{N}_2$. The abelian version has dimension two, and we can take:

$$w_1(b_1, b_2) = b_1, \quad w_2(b_1, b_2) = b_2, \quad w_3(b_1, b_2) = b_1b_2$$

and

$$t_1(x_1, x_2, x_3) = x_1, \quad t_2(x_1, x_2, x_3) = x_2.$$

Now suppose we have a solution a_1, a_2, a_3. With $b_1 = a_1$, $b_2 = a_2$ we see that:

$$a_3 = b_1b_2C_3$$

for some $C_3 \in F'$. Substituting in the given equation we get:

$$b_1^2b_2^2(b_1b_2)^{-2}C_3^2 = 1$$

which simplifies to:

$$[b_1, b_2]^{-3}C_3^2 = 1.$$

Again this implies that b_1 and b_2 cannot freely generate a direct summand of F/F' and without loss of generality:

$$b_1^k = b_2^l D^2 C$$

for some odd integer k, $D \in F$ and $C \in F'$.

Now define a new solution:

$$\alpha'(x) = b_1 \prod_{s=0}^{M}[z_{2s}, z_{2s+1}]$$
$$\alpha'(y) = b_2$$
$$\alpha'(z) = b_1b_2C_3 \prod_{s=0}^{M}[z_{2s}, z_{2s+1}].$$

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

Again it is clear that $\alpha' \leq \alpha$, and if $\tau\alpha = \alpha'$ then:

$$\begin{aligned}\tau(b_1^k) &= \tau(b_2^l)\tau(D^2C)\\ b_1^k\Big(\prod_{s=0}^{M}[z_{2s}, z_{2s+1}]\Big)^k &= b_2^l\tau(D^2C)\\ \Big(\prod_{s=0}^{M}[z_{2s}, z_{2s+1}]\Big)^k &= C^{-1}D^{-2}\tau(D^2C).\end{aligned}$$

The right hand side is the product of a perfect square and a number of commutators which is independent of M and the exponent k on the left hand side is odd, so for M sufficiently large, this equation has no solution and hence α' is strictly more general than α.

Finally consider the equation

$$x^2y^3z^{-5} = 1.$$

A most general abelian solution is:

$$\begin{aligned}x &= a^3b\\ y &= a^{-2}b\\ z &= b.\end{aligned}$$

When we compute $x^2y^3z^{-5}$ formally in $\mathcal{N}_2$ taking a and b as generators we get:

$$x^2y^3z^{-5} = (a^3b)^3(a^{-2}b)^2b^{-5} = [b,a]^{-15}$$

so we can form a solution in $\mathcal{N}_2$ by taking:

$$x = a^3b \quad y = a^{-2}b \quad z = b[b,a]^3.$$

By the theorem above, since the abelianization of this solution is a most general abelian solution, this is a most general solution in $\mathcal{N}_2$.

2.4 *An important technical lemma.* This section is devoted to the proof of Lemma 2 which we restate here for convenience:

LEMMA. *For all positive integers k, non-zero integers r and primes p which do not divide r, there is a positive integer $\phi(k)$ such that, for any $M > \phi(k)$, the equation:*

$$z^p\prod_{j=1}^{k}[x_j, y_j] = \Big(\prod_{i=1}^{M}[u_{i1}, u_{i2}, \ldots, u_{ic}]\Big)^r$$

has no solution in any free group in $\mathcal{N}_c$ in which $\{u_{il} : 1 \leq i \leq M, 1 \leq l \leq c\}$ is a subset of cM elements of a free generating set.

PROOF. The proof is similar to the argument in [4]. We first construct a finite group H_c which is a nilpotent class c p-group, generated by a sequence $a_1, a_2, \ldots, a_c$, such that $[a_1, a_2, \ldots, a_c]$ is not a p-th power. Then we exhibit a homomorphism from the free group

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

in $\mathcal{N}_c$ to H_c which sends the left hand side of the equation above to $[a_1, a_2, \ldots, a_c]$, while sending each of the commutators on the right to 1.

Consider the $\mathbb{Z}_{p^2}$-algebra generated by $x_1, x_2, \ldots, x_c$ with the following relations:

1. Any monomial containing more than one occurrence of any variable is 0,
2. $x_i x_j = x_j x_i$ for all $i, j \in \{2, 3, \ldots, c\}$.

Observe that in this algebra, if M is a sum of monomials of degree at least one then:

$$M^{c+1} = 0$$

since any monomial in M^{c+1} contains a repeated variable.

Let G_c be the group of units of this algebra of the form $1 + M$ where M is a sum of monomials of degree at least 1. The group G_c is a p-group since for any such monomial M, if n is such that

$$p^2 \text{ is a divisor of } \binom{p^n}{1}, \binom{p^n}{2}, \ldots, \binom{p^n}{c}$$

then:

$$(1 + M)^{p^n} = 1 + \sum_{j=1}^{c} \binom{p^n}{j} M^j = 1.$$

If M and N are such sums which in addition are homogeneous (of degree 0 or 1) in each variable, then $(1 - M)^{-1} = 1 + M$ and $(1 - N)^{-1} = 1 + N$ and furthermore:

$$[1 - M, 1 - N] = 1 + MN - NM. \tag{2}$$

Note that $MN - NM$ is also homogeneous in each variable.

Let:

$$a_i = 1 - x_i \quad \text{so} \quad a_i^{-1} = 1 + x_i$$

and let H_c be the multiplicative subgroup of G_c by $a_1, a_2, \ldots, a_c$. For each $u \in H_c$, ua_1u^{-1} contains x_1 in each of its non-constant monomials, and hence commutes with $a_1 = 1 + x_1$. Therefore the normal closure A_1 of $\{a_1\}$ in H_c is abelian. Certainly the subgroup generated by $a_2, a_3, \ldots, a_c$ is also abelian since x_i and x_j commute for $i, j > 1$.

It is clear that:

$$[a_1, a_2, \ldots, a_c] \neq 1$$

since from (2) it will equal

$$1 + \sum_{X \subseteq \{2,3,\ldots,n\}} (-1)^{|X|} \Big(\prod_{j \in X} a_j\Big) a_1 \Big(\prod_{k \notin X} a_k\Big).$$

On the other hand, any commutator of $a_1, a_2, \ldots, a_c$ of weight greater than c contains a repeated symbol, hence is equal to 1. Thus H_c is nilpotent of class c. It remains to show that $[a_1, a_2, \ldots, a_c]$ is not a p-th power.

Suppose otherwise, namely that for some M which is sum of monomials all of degree at least 1:

$$(1 + M)^p = [a_1, a_2, \ldots, a_c].$$

We first claim that M contains a monomial of degree less than c whose coefficient is not a multiple of p. Otherwise, $M = pN + Y$ where N is a sum of monomials of degree at least one, and Y is sum of monomials of degree c, and:

$$(pN+Y)^2 = p^2N^2 + pNY + pYN + Y^2 = 0.$$

Hence:

$$(1+pN+Y)^p = 1+p(pN+Y) = 1+pY.$$

But none of the coefficients of $[a_1, a_2, \ldots, a_c]$ are multiples of p so this is not possible.

So choose a monomial m from M of smallest degree whose coefficient is not a multiple of p. Thus:

$$M = pA + m + B$$

for some A which is a sum of monomials of degree at least one, and B which is a sum of monomials not including m whose degree is at least as great as the degree of m. Then:

$$\begin{aligned}(1+pA+m+B)^p &= 1+p(pA+m+B) + \text{ terms of higher degree than } m\\ &= 1+p(m+B) + \text{ terms of higher degree than } m,\end{aligned}$$

and this cannot equal $[a_1, a_2, \ldots, a_c]$ since it contains a monomial of degree less than c.

Let $\mathbb{A}$ be the c-generated relatively free group in the variety generated by H_c (and fix generators $b_1, b_2, \ldots, b_c$ of $\mathbb{A}$). Since H_c is finite, so is $\mathbb{A}$ (in general the relatively free group on finitely many generators in the variety generated by a finite group are finite, but in this case we may also note that $\mathbb{A}$ is a finitely generated nilpotent group of finite exponent.) Let $N = |\mathbb{A}|$. Since H_c is generated by c elements, it is a homomorphic image of $\mathbb{A}$.

Returning finally to our equation:

$$z^p \prod_{j=1}^{k} [x_j, y_j] = \Big(\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}]\Big)^r.$$

Suppose that $M > N^{2k+1}$. If we have a solution to this equation in the free group of $\mathcal{N}_c$:

$$D^p \prod_{j=1}^{k} [p_j, q_j] = \Big(\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}]\Big)^r,$$

then we may assume that $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_k$ are contained in the subgroup generated by

$$\{u_{il} : 1 \leq i \leq M, 1 \leq l \leq c\}.$$

This subgroup is of course also free on this set of generators. Consider the homomorphisms from this group to $\mathbb{A}$ determined as follows:

$$\theta_i(u_{sj}) := \begin{cases} b_j & \text{if } s = i \\ 1 & \text{if } s \neq i. \end{cases}$$

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

Now define a map $\psi\colon \{1,2,\ldots,M\} \longrightarrow \mathbb{A}^{2k}$ by:

$$\psi(i) = \big(\theta_i(p_1), \theta_i(p_2), \ldots, \theta_i(p_k), \theta_i(q_1), \theta_i(q_2), \ldots, \theta_i(q_k)\big) \quad \text{for } 1 \leq i \leq M.$$

Since $M > N^{2k+1}$ and $N = |\mathbb{A}|$ there exist N distinct elements i of $\{1,2,\ldots,M\}$ for which the values $\psi(i)$ are all the same. Since the maps θ_i can be permuted by permuting our generating set, we may for convenience assume that:

$$\psi(1) = \psi(2) = \cdots = \psi(N).$$

Since $\mathbb{A}$ is free in the variety generated by H_c and $b_1, b_2, \ldots, b_c$ is a sequence of free generators for $\mathbb{A}$, for any c-tuple $\bar{x}$, and for each $1 \leq j \leq k$:

$$p_j(\bar{1}, \ldots, \bar{1}, \bar{x}, \bar{1}, \ldots, \bar{1}, \ldots) = p_j(\bar{1}, \ldots, \bar{1}, \bar{1}, \bar{1}, \ldots, \bar{x}, \ldots)$$
$$q_j(\bar{1}, \ldots, \bar{1}, \bar{x}, \bar{1}, \ldots, \bar{1}, \ldots) = q_j(\bar{1}, \ldots, \bar{1}, \bar{1}, \bar{1}, \ldots, \bar{x}, \ldots)$$

(where $\bar{1}$ denotes a c-tuple of 1's) provided that both occurrences of $\bar{x}$ are in the first N blocks.

Now consider the homomorphism γ from the free group in $\mathcal{N}_c$ to H_c defined by:

$$u_{il} \longmapsto \begin{cases} a_l & \text{for } 1 \leq i \leq N, 2 \leq l \leq c \\ a_1 & \text{for } i = 1, l = 1 \\ 1 & \text{otherwise.} \end{cases}$$

Let $\bar{a} = a_1, a_2, \ldots, a_c$, and $\hat{a} = 1, a_2, \ldots, a_c$. Then for $1 \leq j \leq k$:

$$p_j(\overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N}, \bar{1}, \ldots, \bar{1}) = p_j(\hat{a}, \bar{1}, \ldots, \bar{1}, \bar{1}, \ldots, \bar{1})^N = 1.$$

The first equality follows from the relations above, and the fact that the subgroup of H_c generated by $a_2, \ldots, a_n$ is abelian. The second comes from the fact that $N = |\mathbb{A}|$ and H_c is a homomorphic image of $\mathbb{A}$. The same calculation yields:

$$q_j(\overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N}, \bar{1}, \ldots, \bar{1}) = 1.$$

Hence, for $1 \leq j \leq k$,

$$\gamma(p_j) = p_j(\bar{a}, \overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N-1}, \bar{1}, \ldots, \bar{1}) \in A_1$$
$$\gamma(q_j) = q_j(\bar{a}, \overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N-1}, \bar{1}, \ldots, \bar{1}) \in A_1$$

since $\bar{a} \cong \hat{a} \pmod{A_1}$. But since A_1 is abelian, this implies that:

$$\gamma\Big(D^p \prod_{j=1}^{k} [p_j, q_j]\Big) = \gamma(D)^p$$

while

$$\gamma\Big(\Big(\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}]\Big)^r\Big) = [a_1, a_2, \ldots, a_c]^r$$

which is not a p-th power by the above (recall that p is not a divisor of r.) This contradiction concludes the proof. ∎

3. **Conclusion.** We have seen that there is a close connection between solving systems of equations without parameters in nilpotent groups and doing so in abelian groups. Similar methods can be used to show that some systems of equations in other varieties of groups (particularly those which are generated by a finite group) are also nullary. In fact, the proof in this paper applies to any variety of groups which is nilpotent, contains the groups H_c used in the technical lemma for each prime p, and such that each free group is residually a finite p-group for each p. A particular variety of this type is the intersection of the variety of metabelian groups and $\mathcal{N}_c$. In fact, the authors have shown that any nilpotent non-abelian variety has a nullary system of equations. However, a complete classification of systems of equations in an arbitrary variety of groups would seem to be very difficult.

QUESTION 1. Can systems of equations in solvable groups, in particular in metabelian groups, be classified as above?

QUESTION 2. Can the unification type of the variety generated by a finite group G be determined?

The second author has proven that systems of equations over the absolutely free group are either infinitary or unitary, with the latter occuring only when there exists a solution in the free group whose rank (*i.e.* the rank of the free group generated by the solution) equals the rank of the corresponding abelian system. In particular this implies the well known result that if in the free group F:

$$a^2b^2 = c^2,$$

then a, b, and c commute. For if not, they would generate a free group of rank 2 which would induce by the natural quotient map a most general solution to this system in $\mathcal{N}_2$, and we have seen that no such solution exists. In a similar way many of the results in Chapter 1 Section 6 of [5] can be proven. The authors hope to explore these ideas in a future paper.

The authors would like to thank J. K. Truss for pointing us towards the literature concerning unification for sets of equations with parameters in nilpotent groups.

REFERENCES

1. E. K. Burke, *The undecidability of the unification problem for nilpotent groups of class* ≥ 5, J. London Math. Soc., to appear.

2. T. J. Chou and G. E. Collins, *Algorithms for the solution of systems of linear diophantine equations*, SIAM J. Comput. **11**(1982), 687–708.

3. Costas S. Iliopoulos, *Worst-case complexity bounds on algorithms for computing the canonical structure of infinite abelian groups and solving systems of linear diophantine equations*, SIAM J. Comput. **18**(1989), 658–669.

4. J. Lawrence, *The definability of the commutator subgroup in a variety generated by a finite group*, Canad. Math. Bull. **28**(1985), 505–507.

5. Roger C. Lyndon and Paul E. Schupp, *Combinatorial Group Theory*, Springer Verlag, Berlin, Heidelberg, New York, 1977.

6. H. Neumann, *Varieties of groups*, Springer Verlag, Berlin, Heidelberg, New York, 1967.

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press

7. N. N. Repin, *Some simply presented groups for which an algorithm recognizing solvability of equations is impossible (Russian)*, Voprosy Kibernet. (Moscow) **134**(1988), 167–175.

8. V. A. Roman'kov, *Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings*, Algebra and Logic **16**(1977), 310–320.

9. J. K. Truss, *Equation solving in free nilpotent groups of class* 2 *and* 3, University of Leeds preprint series **24**, 1992.

Department of Mathematics
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213
U.S.A.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
N2L 3G1

https://doi.org/10.4153/CJM-1994-064-8 Published online by Cambridge University Press