ILLINOIS JOURNAL OF MATHEMATICS
Volume 39, Number 3, Fall 1995

FREE GROUPS AND UNIFICATION IN $\mathfrak{A}_m\mathfrak{A}_2$

MICHAEL H. ALBERT AND DAVID PATRICK

1. Introduction

In [3], the order of the free r-generated group in the variety generated by a dihedral group D of order $2^{d+1}e$ (where e is odd) is determined to be $2^{r+s}e^{r'}$ where

$$\begin{aligned} r' &= 2^r(r-1)+1 \\ s &= \sum_{t=2}^{d}(d+1-t)(t-1)\binom{r+1}{t} \end{aligned}$$

(there is a typographical error in the definition of r' in [3]).

The proof of this result depends on a structure theorem for the variety generated by D;

$$\operatorname{var} D = \begin{cases} \mathfrak{A}_e\mathfrak{A}_2 & \text{when } d < 2, \\ \mathfrak{A}_e\mathfrak{A}_2 \vee (\mathfrak{A}_{2^{d-1}}\mathfrak{A}_2 \wedge \mathfrak{N}_d) & \text{when } d \geq 2. \end{cases}$$

Here the notation is as in [7]; in particular $\mathfrak{A}_n$ is the variety of abelian groups of exponent dividing n, $\mathfrak{N}_c$ is the variety of nilpotent groups of class c, and if $\mathfrak{A}$ and $\mathfrak{B}$ are varieties, then $\mathfrak{A}\mathfrak{B}$ is the variety of all groups which are an extension of a group in $\mathfrak{A}$ by one in $\mathfrak{B}$.

In the case $d \geq 2$ the calculation of the order then depends on the results in [4] which give a normal form description for elements of the free groups in the varieties $\mathfrak{A}_{p^\alpha}\mathfrak{A}_p$ (where p is a prime).

In this paper we will restrict our attention to the first case, $d < 2$. As a matter of personal preference we use m rather than e for the odd part, and so our goals are to describe the free groups of the variety

$$\mathfrak{A}_m\mathfrak{A}_2$$

where m is odd, and to determine the *unification type* of this variety, which in this context amounts to describing a single most general solution to any system of equations

$$\Sigma = \{t_1(x) = 1, t_2(x) = 1, \dots, t_n(x) = 1\}$$

Received March 9, 1993
1991 Mathematics Subject Classification. Primary 2.E10.

in a finite sequence of variables

$$x = x_1, x_2, \ldots, x_k.$$

When giving a presentation or description of a free group, it has been traditional (as in [4]) to do so by means of some sort of "normal form" description of the elements in terms of the free generators. However, such a description may or may not lead to a clear understanding of the free group as a whole, for example in terms which permit one to understand the structure of the lattice of normal subgroups (and hence presumably the structure of all k-generated groups in the variety). We give a description which is heavily weighted towards these kinds of questions and not incidentally towards a description which allows us to determine solutions to equations.

The next section is devoted to this description, and the following section addresses the question of solving equations in these groups.

2. Presentation of the free groups

Let G_k be the k-generated free group in the variety $\mathfrak{A}_m\mathfrak{A}_2$. Then G_k contains a normal subgroup A which is a direct sum of $2^k(k-1)+1$ copies of Z_m, and the group G_k/A which is isomorphic to Z_2^k acts on A by conjugation. In fact as the projection $G_k \to G_k/A$ splits, we may identify G_k/A with some subgroup U of G_k. We write A additively, and U multiplicatively. Let

$$u = u_1, u_2, \ldots, u_k$$

be a sequence of generators for U. There exists for each sequence

$$\varepsilon = \varepsilon_1\, \varepsilon_2, \ldots, \varepsilon_k \in \{1, -1\}^k$$

a subgroup $A_\varepsilon \leq A$ such that

$$a_\varepsilon^{u_j} = a_\varepsilon^{\varepsilon_j}$$

for all $a_\varepsilon \in A_\varepsilon$. We say that the *signature* of a_ε with respect to u is ε and write $\varepsilon = \operatorname{sig}(a_\varepsilon, u)$. Furthermore

$$A = \bigoplus_{\varepsilon} A_\varepsilon.$$

For $J \subseteq \{1, 2, \ldots, k\}$ we define

$$u_J = \prod_{j \in J} u_j, \quad \varepsilon_J = \prod_{j \in J} \varepsilon_j.$$

Then for $a \in A$, we have

$$a = \sum_{\varepsilon} a_{\varepsilon}$$

where

$$a_{\varepsilon} = \frac{1}{2^k} \sum_{u_J \in U} \varepsilon_J a^{u_J}.$$

Finally we can say that if $\varepsilon = 1$ is the sequence of all 1's (so that $A_{\varepsilon} = Z(G)$) then A_1 is isomorphic to Z_m^k while for any other signature, $A_{\varepsilon} \cong Z_m^{k-1}$ (this is where the representation theory comes into its own, but again the result can be proven in an elementary way by considering automorphisms of G_k which permute the A_{ε}).

All this can be obtained from integral representation theory [1], [2] or more easily by direct arguments akin to elementary linear algebra, involving the "diagonalization" of the actions of the u_i on A by conjugation, and then a consideration of the permutations of the A_{ε} induced by various automorphisms of U.

For the record, we can write down an explicit set of free generators for G_k. If ε contains a -1 let $N(\varepsilon)$ denote the position of the first occurrence of -1 in ε and let $N(1) = 0$. Choose generators

$$a_{\varepsilon, j}, 1 \leq j \leq k, j \neq N(\varepsilon)$$

for A_{ε} and for $1 \leq i \leq k$ define

$$x_i = \left(\sum \{a_{\varepsilon, i}: N(\varepsilon) \neq i\}\right) u_i.$$

Then it can be verified that these k elements generate G_k and hence form a set of free generators for G_k.

3. Unification in dihedral varieties

Let Σ be a system of equations of the form:

$$t(x) = 1$$

where t is a term in the language of groups, and

$$x = x_1, x_2, \ldots, x_k.$$

Notice in particular that these equations do not contain any parameters. We consider the set of solutions to Σ in the group G_{ω}, the countably generated free group of var D_m. Henceforth we will denote this group simply by G. A solution to Σ is really just a homomorphism $\alpha\colon F_k \to G$ such that $t \in \ker \alpha$ for each equation $t(x) = 1$ in Σ. Here F_k is the absolutely free group on k generators. However, all such maps factor through G_k, so we usually consider solutions to be homomorphisms from G_k to G. With this in mind it is natural to make the following definition:

DEFINITION 1. *When α and β are solutions to Σ we say that α generalizes β if for some endomorphism θ of G, $\theta\alpha = \beta$.*

When α generalizes β we write $\alpha \leq \beta$. Of course $\leq$ is not a partial order, but it is reflexive and transitive. We say that α is a most general solution to Σ if $\alpha \leq \beta$ for *every* solution β.

We will show that every system of equations Σ has a most general solution for G. In the general context of varieties of groups this is somewhat unusual behavior. The corresponding result is true (and we shall make use of it) for any abelian variety, but it fails in any non-abelian nilpotent variety, and also in the variety of all groups. In the first case there are equations for which every solution has a proper generalization. In the latter case there are equations such as

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

which have an infinite family of solutions, none of which has a proper generalization, and all of which are incomparable with respect to $\leq$.

In the case of an abelian variety $\mathfrak{A}_m$, for the sake of illustration, consider the equation

$$2x + 3y = 0.$$

If m is odd, we get at most general solution

$$y = a, \qquad x = (-3a)/2.$$

If m is not a multiple of 3 we get a most general solution

$$x = b, \qquad y = (-2b)/3.$$

If m is a multiple of 6 then the most general solution is

$$x = (m/2)a + 3b, \qquad y = (m/3)c - 2b.$$

Finally, in $\mathfrak{A}$ itself, the most general solution is

$$x = 3a, \qquad y = -2a.$$

In each case, in order for the solution to be most general, the parameters a, b, c are to be generators of the countably generated free group in the variety. Of course there are also other most general solutions such as

$$x = 3a - 6c \qquad y = -2a + 4c$$

which involve one (or more) redundant parameters. However, all such solutions are equivalent to one another and so any one of them can deservedly be called "most general." The solutions which we construct for systems of equations in the varieties generated by dihedral groups will almost certainly contain such redundant parameters.

We need a little preparatory work before we can construct most general solutions in G. The main idea is to take a general solution in the Sylow 2-subgroup of G and to modify it to take into account the remainder of G.

Fix a Sylow 2-subgroup U of G. Note that U is a countably generated elementary abelian 2-group, and this is the countably generated free group in the variety of elementary abelian 2-groups. Let $A = [G, G]$ be the subgroup of G consisting of all elements of order dividing m, so A is isomorphic to a direct sum of countably many copies of Z_m. Again we write A additively. The arguments of the preceding section are easily modified to obtain:

PROPOSITION 2. *Let b be any sequence of k elements in U. For any $a \in A$ there exists a unique set of elements*

$$\left\{a_\varepsilon \colon \varepsilon \in \{-1, 1\}^k\right\} \subseteq A$$

such that

$$a = \sum_\varepsilon a_\varepsilon \quad \textit{and} \quad \operatorname{sig}(a_\varepsilon, b) = \varepsilon.$$

In fact

$$a_\varepsilon = \frac{1}{2^k} \sum_{J \subseteq \{1,2,\dots,k\}} \varepsilon_J a^{b_J}$$

where

$$b_J = \prod_{j \in J} b_j \qquad \varepsilon_J = \prod_{j \in J} \varepsilon j.$$

What we really have here is

$$A = \bigoplus_\varepsilon A_\varepsilon(b)$$

where

$$A_\varepsilon(b) = \{a \in A \colon \mathrm{sig}(a, b) = \varepsilon\}.$$

However, we will also have cause to use the exact formula for a_ε below.

Let a system of equations Σ be given. We first construct a solution α and then verify that it is a most general solution. Considering Σ as a set of equations in U take a most general solution

$$x_i = w_i(u)$$

where u is some chosen finite subset of a free generating set for U. The solution α which we construct will have

$$a(x_i) = a_i w_i(u)$$

where $a_i \in A$. By the above proposition each a_i can be uniquely decomposed into elements $a_{\varepsilon, i}$ of signature ε with respect to the sequence

$$w_1(u), w_2(u), \dots, w_k(u).$$

Now we view the $a_{\varepsilon, i}$ as indeterminates and formally compute each term

$$\alpha t(x) = t(a_1 w_1(u), a_2 w_2, \dots, a_k w_k(u)).$$

paying attention to the relations

$$a_{\varepsilon, i}^{w_j(u)} = a_{\varepsilon, i}^{\varepsilon_j}.$$

We find that in order to have a solution to Σ, it is necessary and sufficient that the $a_{\varepsilon, i}$ satisfy certain equations of the form

$$(1) \qquad \sum_i \lambda_{\varepsilon, i} a_{\varepsilon, i} = 0$$

(one of these arises from each t and each ε). These are equations in A_ε, an abelian group of exponent m, and so they have a most general solution

$$(2) \qquad a_{\varepsilon, i} = w_{\varepsilon, i}(v_\varepsilon)$$

However, we require that v_ε be of signature ε with respect to the sequence

$$w_1(u), w_2(u), \dots, w_k(u).$$

It is not immediately clear how to enforce this condition and allow v_ε to be sufficiently "general." We require the following lemma:

LEMMA 3. *Let w be a sequence of elements of U, and let H be any finitely generated subgroup of G containing w. For each ε there exists an element v_ε in A such that the signature of v_ε with respect to w is ε, and for any endomorphism θ of G and any element a of signature ε with respect to $\theta(w)$ there exists an endomorphism θ' which agrees with θ on H and such that $\theta(v_\varepsilon) = a$.*

Proof. Let x be some generator of G which does not occur in w. Define

$$v_\varepsilon = \frac{1}{2^k}\sum_J \varepsilon_J (x^2)^{w_J}.$$

Then v_ε has signature ε with respect to w. Furthermore, for any endomorphism θ, if the signature of a with respect to $\theta(w)$ is ε then

$$a = \frac{1}{2^k}\sum_J \varepsilon_J a^{\theta(w_J)}$$

So we can choose θ' such that $\theta'(x^2) = a$ (possible since m is odd) and then $\theta'(v_\varepsilon) = a$ as required. □

Obviously by applying this lemma repeatedly, and extending H each time by our new element v_ε we can meet the requirements of the lemma for any collection of a's of the same or different signatures with respect to $\theta(w)$ simultaneously.

Apply this idea to choose sufficiently many elements v_ε to satisfy the need for parameters in (2) and all meeting the conditions of the lemma with respect to

$$w_1(u), w_2(u), \ldots, w_k(u),$$

Then define the solution α to Σ to be

$$a(x_i) = \left(\sum_\varepsilon w_{\varepsilon,i}(v_\varepsilon)\right) w_i(u).$$

This is a most general solution to Σ. For suppose that β is any solution. Let $\pi\colon G \to U$ be a retraction with kernel A. We can find $\nu\colon U \to U$ such that

$$\nu\pi\alpha = \pi\beta$$

and we can choose $\theta\colon G \to G$ such that

$$\nu\pi = \pi\theta$$

So for each i,

$$\beta(x_i) = a_i\theta(w_i(u))$$

for some $a_i \in A$. As usual we decompose a_i into $a_{\varepsilon,i}$ with respect to $\theta(w_i(u))$, and note that formally the $a_{\varepsilon,i}$ must satisfy the equations (1). So there exist

$$b_\varepsilon \in A_\varepsilon(w_1(u), \dots, w_k(u))$$

such that

$$a_{\varepsilon,i} = w_{\varepsilon,i}(b_\varepsilon)$$

but now the fact that the v_ε were constructed using the lemma, allows us to choose θ' which agrees with θ on $w_i(u)$ for each i and sends v_ε to b_ε for each ε. All in all we get

$$\theta'\alpha = \beta$$

as required.

This proves:

THEOREM 4. *Every equation over G has a most general solution.*

In fact the absence of parameters from G in the equations is not important. Namely the argument goes through as before, except that the equation (1) will not be homogeneous. However, if they have no solution then the original system has no solution either. If they do have a solution, then they have a most general solution obtained from a particular solution and the homogeneous solution above (where the subgroup H of the lemma is chosen to include all the elements of G in the particular solution).

In many cases there is a much simpler way to construct a most general solution. Suppose that N is the normal subgroup of G_k generated by the elements $t(x)$ which are the left hand sides of the equations in Σ. Think of G_k as a subgroup of G in the natural way. Then if the projection π: $G_k \to G_k/N$ splits via a map γ: $G_k/N \to G_k$ we define a solution

$$\alpha = \gamma\pi.$$

Now if β is any solution, β factors through G_k/N, say $\beta = \nu\pi$. We need θ: $G \to G$ such that $\theta\gamma\pi = \alpha$. But it suffices to find such a (θ: $G_k \to G$ (since the rest of the generators could be sent to 1). For this we simply take

$$\theta = \nu\pi.$$

Then

$$\theta\alpha = \nu\pi\gamma\pi = \nu\pi = \beta$$

as required.

In particular if m is square free, then all projections $G_k \to G_k/N$ split [8] and the work above is unnecessary. But if m is not square free, then we are not so lucky and the work above seems to be necessary!

4. Conclusion

The problem of solving equations, with or without parameters, in the absolutely free group has a lengthy history. Various results around this area are discussed in the last few sections of the first chapter of [6]. John Lawrence [5] introduced us to the problem restricted to other varieties of groups. In these notes he has a number of results which indicate that "most" varieties generated by a finite group will have equations for which there are no most general solutions. The fact that a case which remained open from his work was "non-square free exponent and abelian Sylow subgroups" led us to our consideration of the dihedral groups.

It is not hard (but of doubtful utility) to generalize the results we have to the case of varieties $\mathfrak{A}_m\mathfrak{A}_n$ where $n|(q-1)$ for every prime divisor q of m (in this case Z_m contains a non-trivial nth root of unity and the "diagonalization" can still be carried out). For the general case $\mathfrak{A}_m\mathfrak{A}_n$ when m and n are relatively prime, it seems that the main result (existence of most general solutions) is still correct. However, the direct sum decomposition which figures so prominently in the argument is no longer so easily described, and such technical obstructions have prevented us from actually describing the solutions in this case.

The authors would like to thank an anonymous referee of an earlier work who pointed out that the machinery of integral representation theory may be used to give explicit presentations of groups such as G_k above.

References

1. Karl W. Gruenberg, *Cohomological Topics in Group Theory*, Springer Lecture Notes 143, Springer Verlag, New York, 1970.
2. ______, *Relation modules of finite groups*, Regional conference series in mathematics, vol. 25, Amer. Math Soc., Providence RI, 1975.
3. L.G. Kovács, *Free groups in a dihedral variety*, Proc. Royal Irish Acad. **89A** (1989), 115–117.
4. L.G. Kovács and M.F. Newman, *On non-Cross varieties of groups*, J. Austral. Math. Soc. **12** (1971), 129–144.
5. J. Lawrence, *Notes on unification in groups*, private communication, 1990.
6. Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer Verlag, New York, 1977.
7. H. Neumann, *Varieties of groups*, Springer Verlag, New York, 1967.
8. Peter Neumann, *Splitting groups and projectives in varieties of groups*, Quart. J. Math. Oxford (2) **18** (1967), pp. 325–332.

Carnegie Mellon University
Pittsburgh, Pennsylvania