A PRESENTATION OF THE FREE GROUP ON FINITELY MANY GENERATORS IN THE VARIETY GENERATED BY D_m

by

Michael H. Albert

Department of Mathematics
Carnegie Mellone University
Pittsburgh, PA U.S.A.

and

David Patrick

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

Research Report No. 91–139

November, 1991

A PRESENTATION OF THE FREE GROUP ON FINITELY MANY GENERATORS IN THE VARIETY GENERATED BY D_m

MICHAEL H. ALBERT AND DAVID PATRICK

November 21, 1991

ABSTRACT. When m is an odd number the variety generated by the dihedral group of order $2m$ is $\mathfrak{A}_m\mathfrak{A}_2$. The free group on k generators in this variety is a semi-direct product of Z_m^r by Z_2^k where $r = 2^k(k-1)+1$. We give a natural presentation of this group in terms of "eigenvectors" of the action of Z_2^k on Z_m^r, and characterize the free generators in terms of this presentation.

1. INTRODUCTION

In [2], the order of the free k-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 $r' = 2^r(r-1)+1$ and:

$$s = \sum_{t=2}^{d}(d+1-t)(t-1)\binom{r+1}{t}$$

(there is a typographical error in the definition of r' in [2].)

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 [6].

In the case $d \geq 2$ the calculation of the order then depends on the results in [3] 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 goal is to

1991 *Mathematics Subject Classification.* Primary 20E10.
Key words and phrases. varieties of groups, free groups.

describe the free groups of the variety:

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

where m is odd.

When giving a presentation or description of a free group, it has been traditional (as in [3]) 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. The reasons for desiring such a description are described further in the final section.

The third section of this paper contains the structure theorem and its proof. However, in this bare form the result is somewhat post hoc. So we have included in the second section some results and investigations which led us to the final description.

Throughout the paper Z denotes the additive group of the integers, and Z_n the additive group of the integers modulo n.

2. The ideas

Fix an odd positive integer $m > 1$, and a positive integer k and for convenience let:

$$r = 2^k(k-1)+1$$

for the rest of this section. Let F_k denote the absolutely free group on k generators, U the characteristic (verbal) subgroup of F_k generated by the squares, and V the characteristic subgroup of U generated by the commutators and all elements of the form u^m. Then the k-generated free group of $\operatorname{var} D_m$ (which is $\mathfrak{A}_m\mathfrak{A}_2$) is just:

$$G_k = F_k/V.$$

Let U' be the commutator subgroup of U. The action of F_k on U by conjugation induces an action of F_k/U on U/U'. Since $U/U' \cong Z^n$ we can interpret this action as multiplication by some matrices in $M_r(Z)$. Furthermore $F_k/U \cong Z_2^k$, so the generators of F_k/U give rise to a sequence of matrices $A_1, A_2, \ldots, A_k \in M_r(Z)$ which satisfy:

$$A_1^2 = A_2^2 = \cdots = A_k^2 = 1 \quad \text{and} \quad A_iA_j = A_jA_i \quad \text{for } 1 \le i < j \le k.$$

We will show that the matrices $A_1, A_2, \ldots, A_k$ can be simultaneously diagonalized over the ring $Z[1/2]$ of dyadic rationals (those rationals whose denominator in lowest terms is a power of 2.) This is a consequence of the following more general result which must be known, but which we have not been able to find in the literature:

Proposition 1. *Let R be a principal ideal ring, and suppose that $A \in M_s(R)$ is such that the distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ of A all lie in R. Suppose also that:*

$$(A - \lambda_1 I)(A - \lambda_2 I)\cdots(A - \lambda_n I) = 0,$$

and

$$\lambda_i - \lambda_j \text{ is a unit of } R \text{ for } 1 \le i < j \le n.$$

Then A is diagonalizable over R.

Proof. It suffices to show that R^s has a basis (as R-module) which consists of eigenvectors of A. This will be true provided that R^s is the direct sum of the eigenspaces $V_{\lambda_1}, V_{\lambda_2}, \ldots, V_{\lambda_n}$ of A. Here:

$$V_{\lambda_i} = \{v \in R^s : Av = \lambda_i v\}$$

By considering A as an element of $M_s(F)$ where F is the quotient field of R we see that

$$V_{\lambda_i} \cap \bigoplus_{j \neq i} V_{\lambda_j} = \{0\}.$$

Thus it remains to show that each v in R^s is a sum of elements of V_{λ_i}. But the system of equations:

$$\begin{array}{ccccccccc}
v_1 & + & v_2 & + & \ldots & + & v_n & = & v \\
\lambda_1 v_1 & + & \lambda_2 v_2 & + & \ldots & + & \lambda_n v_n & = & Av \\
 & & & & \vdots & & & & \\
\lambda_1^{n-1} v_1 & + & \lambda_2^{n-1} v_2 & + & \ldots & + & \lambda_n^{n-1} v_n & = & A^{n-1} v
\end{array}$$

or briefly:

$$V^T(\lambda_1, \lambda_2, \ldots, \lambda_n)\mathbf{v} = \mathbf{v},$$

(where V is a VanDerMonde matrix) has a solution with $v_1, v_2, \ldots, v_n \in R^s$ since:

$$\det V = \prod_{1 \le i < j \le n} (\lambda_i - \lambda_j)$$

is a unit in R so $V^{-1} \in M_s(R)$. But then

$$v_i \in V_{\lambda_i}$$

since this is true when we solve the same system of equations in $M_s(F)$, or we can establish this directly by using the first two equations to show that:

$$\left(\prod_{i \neq i}(A - \lambda_i I)\right) v = \sum_{t=1} \left(\prod_{i \neq i}(\lambda_t - \lambda_i)\right) v_t = \left(\prod_{i \neq i}(\lambda_j - \lambda_i)\right) v_j.$$

Hence:

$$((A - \lambda_i I))\, v_i = \frac{1}{\prod_{j \neq i}(\lambda_i - \lambda_j)} \left((A - \lambda_i I)\prod_{j \neq i}(A - \lambda_j I)\right) v = 0.$$

●

Note that the same result holds when R is any integral domain which has the property that all finitely generated projective R modules are free. This includes all commutative local rings (see [1] p. 413) and, by the Quillen-Suslin theorem ([4] p. 490, [7]) also all polynomial rings over fields.

How does the result apply to our problem? By standard results from linear algebra, it is a corollary to the above that any finite set of commuting matrices satisfying the conditions of the proposition are simultaneously diagonalizable over R. Since each of the matrices in $A\backslash, A_2, \ldots, Ak$ (thought of as a matrix over $Z[l/2]$) satisfies:

$$(A - I)(A + I) = 0,$$

and since 2 = 1 — (—1) is a unit of Z[1/2], $A\backslash, A_2, \ldots, Ak$ are simultaneously diagonalizable over $Z[l/2]$.

The quotient map from U/U^1 to U/V is just reduction modulo m. Since m is odd, 2 is a unit in Z_m so the diagonalizing matrix and its inverse reduce naturally to matrices in $M_r(Z_m)$ (since we only divide by powers of 2.) Hence, for each sequence e = (ci, $6_2, \ldots$, $€k$) from {1, —1} there is a subgroup $V_€$ of U/V where:

$$v \text{ G } K \ \wedge => A\{V = 6\{V \text{ for } 1 \leq i \leq \&,$$

and

$$U/V = \bigoplus_{\epsilon} V_\epsilon.$$

Since $Gk = Fk/V$ contains U/V we may think of the groups V_e as subgroups of Gk- Moreover, the 2-Sylow subgroup of Gk is isomorphic to Fk/U, and has trivial intersection with U, *so* Gk is isomorphic to the semidirect product of U/V by Fk/U. So we henceforth identify Gk with this semidirect product.

Let 1 = (1,1,... , 1). Now we ask: what are the dimensions of the subgroups $V_€$?

Proposition 2. *The dimension ojV\ is k, and if e ^ 1 then the dimension of* $V_€$ *isk-* 1.

Proof. Recall that $Gk = Fk/V$, and consider the automorphism of Gk which fixes the free generators #,• for $i \wedge j$ and sends Xj to $XjXk$ for some $k \wedge j$. This map induces a permutation of the subgroups $V_€$ of Gk as follows:

$$V_€ \text{ H+ } V_€> \text{ where } e\backslash = 6\text{- for } i \wedge j,\ e'j = €j€_k.$$

In particular we can use such an automorphism to change e to any e' which differs from 6 only in the sign of a single element, provided that both 6 and e' contain at least one —1. But by a sequence of such transformations we can transform any e containing a —1 into any c' which also contains a —1. So dimK = dimK' for all such e and e'. Let ddimF_c for any e =^ 1.

The subgroup:

$$H = \bigoplus_{\epsilon \neq 1} V_\epsilon$$

of *Gk* is normal, and

$$G_k/H \cong Z_2^k \oplus A_1.$$

But *Gk/H* is fc-generated, hence:

$$\dim{}^\wedge i \leq k.$$

Finally note that:

$$2^{fc}(Jk - 1) + 1 = \dim Ax + \wedge_{\epsilon \neq 1} \dim V_\epsilon = \dim A_x + (2^* - 1)d.$$

When $k > 1$ the only solution in positive integers to this equation which has $\dim A\backslash \leq k$ is given by:

$$\dim A_i = fc, \ \dim V^\wedge = k - 1, \ (\text{for } \epsilon \wedge 1).$$

When $k = 1$ we know that dimAi = 1 and dim>l_i = 0 so this case also works. •

This gives us a complete understanding of the structure of G&, and all that remains is to find an explicit set of generators, which is the purpose of the next section.

3. JUST THE FACTS

Let m be an odd positive integer, and let fcbea positive integer. We now construct the free fc-generated group in $2t_m 2l2$«

If G $\simeq$ Z£ then we say that a sequence of elements fli,52? • • • *i9j* form a *basis* for G if G is the direct sum of the cyclic subgroups generated by the elements #; for $1 \leq i \leq h$
Let:

$$\epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_k).$$

denote an arbitrary sequence of length k from {—1,1}. For each such *e* other than 1 = (1,1,... ,1) let N_ϵ be the position of the first occurrence of —1 in e, and let

For each *e* other than 1 define an abelian group $V_e \simeq Z^{\wedge\sim x}$ with basis $v_e j$ for $1 \leq j \leq fc, 3 \wedge N_\epsilon$. Define $A_x \simeq Z^k_m$ with basis v_{hj} for $1 \leq j \leq k$. Then define:

$$A = \bigoplus_\epsilon V_\epsilon.$$

Let $U \simeq Z\backslash$ have basis *Uj* for $1 \leq j \leq$ fc. Finally define G to be a semidirect product of *A* with *U* given by the relations:

$$u_i v_{\epsilon,j} u_i = v_{\epsilon,j}^{\epsilon_i}.$$

Notice that for each $x = v_x u_x$ G G with u_x G U and v_x G A there exist unique elements v_x^+ and v_x^- in A such that:

$$\begin{aligned} u_x v_x^+ u_x &= v_x^+ \\ u_x v_x^- u_x &= (\mathrm{vj})^{"1}, \end{aligned}$$

and that

$$v_x^+ = x^{m+1} \quad v^- u = x^m.$$

Theorem 3. G *is the k-generated free group in the variety* $2\mathrm{t}_m 2\mathrm{l}_2$.

Proof We see that the order of G is:

$$m^{(2^k-1)(k-1)+k}2^k = m^{2^k(k-1)+1}2^k.$$

By the results in paragraph 21 of [6] the order of G is the same as the order of the fc-generated free group in $2\mathrm{l}_m 2\mathrm{l}_2$- Furthermore, from the construction it is clear that G belongs to this variety. So to show that it is the /^-generated free group it suffices to prove that G is ^-generated.

For $1 \leq i \leq k$ define x_t- G G as follows:

$$x_i = \left(\prod \{a_{\epsilon,i} : N_\epsilon \neq i\}\right) u_i.$$

Then:

$$\begin{aligned} u_{x_i} &= u_i \\ v_{x_i}^+ &= \prod \{v_{\epsilon,i} : N_\epsilon \neq i, \epsilon_i = 1\} \\ v_{x_i}^- &= \prod \{v_{\epsilon,i} : N_\epsilon \neq i, \epsilon_i = -1\} \end{aligned}$$

Notice that $v_{\epsilon i}$, occurs as a factor in $v^-_{x_i}$ if and only if e,- = —1 and €j = —1 for some $j < i$*

We claim that xi, x 2,... , x_k generate G. Let H denote the subgroup of G generated by 2'a, z 2,... ,%k

To see that H = G we will first show that iz(G if for each i. First note that

$$u_x = x^{TM}_1 \text{ G } \#.$$

For a:2 note that:

$$v_{x_2}^- u_2 = x? \quad £H.$$

Then:

$$u_1 v_{x_2}^- u_2 u_1 = \{v_{x_2}^-)^{-l} u_2 \text{ G iT},$$

(since for the $t/_{Cj2}$ in vj2 we must have e_x = —1.) Thus $(v_x^- J^2$ and hence vj2 are in H so tz2 is also in H.

We can complete this argument inductively. For if $u_1, u_2, \ldots, u_{i-1} \in H$ then:

$$v_{x_i}^- u_i = x_i^m \in H$$

But each $v_{\epsilon,i}$ which occurs in $v_{x_i}^-$ satisfies $\epsilon_j = -1$ for some $j < i$. Then successive conjugation by $u_1, u_2, \ldots, u_{i-1}$ allows the removal of all such factors as above. Hence $u_i \in H$.

It remains to show that for any j and ϵ (with $N_\epsilon \neq j$), that $v_{\epsilon,j} \in H$. To do this note that since u_j and $v_{x_j}^+$ are in H so is $v_{x_j}^-$. So we need only show how to strip the remaining factors (other than $v_{\epsilon,j}$) of one of these products away. But conjugation by u_i allows us to strip away all the factors corresponding to sequences ϵ' with $\epsilon_i' \neq \epsilon_i$. If we do this successively for all i we are left only with the factor $v_{\epsilon,j}$ which we wanted.

□

4. Discussion

The reader may well wonder why we desire such a detailed understanding of the free groups in var D_m. One reason is to make it possible to address the *unification problem* in these varieties which is the problem of finding general "parametric" solutions to systems of equations. For (a trivial) example, the equation $x^3 = 1$ in var D_9 has most general solution $x = y^6$ since in any free group in this variety all the elements of order three are sixth powers. However, in some cases such general solutions do not exist. For example in absolutely free groups the equation $xy = yx$ has an infinite family of most general solutions, $x = u^n$, $y = u^m$. In other varieties (non-abelian p-groups or nilpotent groups) it can be shown that there exist equations or systems of equations which have no most general solution. John Lawrence has made extensive progress on the question of determining when systems of equations must have most general solutions in finitely generated varieties of groups ([5]), to the extent that one of the few open questions remaining concerns varieties generated by non-abelian groups of non-square-free exponent, all of whose Sylow subgroups are abelian. Of course when m is odd and not square free, then var D_m is just such a variety. In a subsequent paper we hope to be able to illustrate how our detailed understanding of the free groups in these varieties enables us to solve the unification problem.

The arguments in section 2 also lead to presentations of free groups in other varieties such as $\mathfrak{A}_7\mathfrak{A}_3$ and generally $\mathfrak{A}_{p^k}A_q$ where p and q are primes and $q|p-1$.

Extensive use was made of the symbolic algebra programs *Maple* and *Mathematica* to assemble (via a constructive version of the Nielsen-Schreier theorem) examples of k-generated free groups in var D_m for small k and m which were instrumental in suggesting the form of the final structure theorem, and the results of section 2.

References

1. N. Jacobson, *Basic Algebra II*, W.H. Freeman, New York, 1980.
2. L.G. Kovács, "Free groups in a dihedral variety", *Proc. Royal Irish Acad.*, **89A** (1989), 115–117.
3. L.G. Kovács and M.F. Newman, "On non-Cross varieties of groups", *J. Austral. Math. Soc.* **12** (1971), 129–144.
4. S Lang, *Algebra*, Second Edition, Addison-Wesley, Redwood City, CA, 1984.
5. J. Lawrence, Notes on unification in groups, private communication (1990).
6. H. Neumann, *Varieties of groups*, Springer Verlag, Berlin, HeidelBerg, New York, 1967.
7. D. Quillen, "Projective modules over polynomial rings", *Invent. Math.*, **36** (1971), 167–171.

(M. Albert) Department of Mathematics, Carnegie Mellon University, Pittsburgh PA 15213

E-mail address, M. Albert: ma1q@hillgrove.math.cmu.edu