1997

Presentations of direct products of metacyclic groups

Jared Everett Derksen

PRESENTATIONS OF DIRECT PRODUCTS OF METACYCLIC GROUPS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Jared Everett Derksen

June 1997

PRESENTATIONS OF DIRECT PRODUCTS OF METACYCLIC GROUPS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by Jared Everett Derksen

June 1997

Approved by:

[redacted]

Paul Vicknair, Department Chair

6-10-97

Date

[redacted]

Peter Williams, Chair, Mathematics

[redacted]

Zahid Hasan

[redacted]

Teri Hallett, Graduate Coordinator

ABSTRACT

It has been proven that metacyclic groups, groups which have a cyclic subgroup whose factor group is also cyclic, can be presented efficiently. However, when the direct product of these groups is taken, the (d)efficiency is unknown. This paper examines work that has been done on this problem and contributes to part of the solution. It will be shown that under certain conditions, the direct product of two Z-metacyclic groups can be presented efficiently.

ACKNOWLEDGMENTS

The author wishes to thank Dr. Peter Williams for first demonstrating to the author the beauty of finite group theory and for spending many hours assisting with the completion of this project. Without Dr. Williams' effort, this project would not have been possible.

DEDICATION

To Mr. Dennis Stanton, who first kindled
my love for mathematics and to my wife
Jennifer, who gave me the confidence to
do more than I thought I was capable
of doing.

TABLE OF CONTENTS

CHAPTER 1

BACKGROUND MATERIAL

In this paper, our primary concern is the efficient presentation of the direct product of metacyclic groups. Let us begin with a discussion of free groups and group presentations.

Let X be a set and X' a set in one to one correspondence with X, so that if x is in X, then x^{-1} is in X'. Let A be the union of X with X', which we will denote as $A = \{a_1, a_2, a_3...\}$. A **word** will be defined to be a string of elements of A placed in juxtaposition. The **empty word** is defined to be a word of length zero and will be denoted by the symbol 1. Exponents of any integer power may be placed on the elements of A and as usual we define:

$$a^0 = 1,$$
$$a^{-j} = (a^{-1})^j.$$

Within a word, exponents may added as per standard multiplicative notation: $a_2^3 \cdot a_2^{-7} = a_2^{-4}$. If the exponent on any a_i becomes zero, that element is replaced by 1. By adding exponents of like terms and replacing a_i^0 with 1, for all i, we create a **reduced word.**

The set of all reduced words formed by A will be indicated by $F[A]$. In order to make $F[A]$ a group, we will define a multiplication on our words in a natural manner:

for any two words, w and z in $F[A]$, we will define $w \cdot z$ to be the reduced word created by the juxtaposition of the two words. Clearly, 1 acts as the identity in this multiplication, and the inverse of a will be a^{-1}.

DEFINITION: A **free group**, $F[A]$, generated by the set A is the group consisting of the reduced words of A and using the multiplication described above.

DEFINITION: If $F[A]$ is free group, the **rank of the free group** is equal to the cardinality of the set X.

DEFINITION: Let S be a subset of a group G. The **normal closure** of S, $\overline{S}$, is the intersection of all normal subgroups of G that contain S.

For a more complete discussion of free groups, see [3], [4], [6], and [7].

Since it has been proven that every group is an epimorphic image of some free group [5], we offer this definition:

Definition: Let G be an epimorphic image of a free group $F[X]$ and let N be a normal subgroup of F so that $F/N \cong G$. Furthermore, let $R \subseteq F$ be such that $\overline{R} = N$. Then we say

that $\langle X|R \rangle$ is a **presentation** of G. The elements of R are called relators.

If $|X|$ and $|R|$ are finite, then we say that $\langle X|R \rangle$ is a finite presentation. For the purposes of this paper, we will be dealing exclusively with finite presentations. For any finite presentation of a finite group, it can be proved that $|R| \geq |X|$. We can then make the following definitions:

DEFINITION: The **deficiency of a finite presentation** is $|R| - |X|$, which is clearly greater than or equal to zero.

DEFINITION: The **deficiency of a group**, G, is the minimum deficiency over all finite presentations of G.

But how do we know the deficiency of a group? What if there is a presentation with a lower deficiency than the presentations that have been examined? How do we know when the minimum deficiency has been attained?

Associated with each finite group, G, is a unique finite abelian group known as the Schur multiplicator of G and denoted as $M(G)$. A lower bound for the deficiency of G is given by the minimal number of generators of $M(G)$.

DEFINITION: For a finite group $G = \langle X|R \rangle$, where F = F[X], R $\subset$ F and $\overline{R}$ is the normal closure of R in F, then the **Schur multiplicator**, $M(G)$, is defined to be

$$M(G) = \frac{F' \cap \overline{R}}{[F, \overline{R}]}.$$

In 1907, J. Schur proved that M(G) is independent of the finite presentation of G, that is, it is an invariant of G. Also, Schur proved that M(G) is generated by at most def G elements [5]. Now we use the Schur group to define efficiency:

DEFINITION: A presentation of a group is **efficient** if the deficiency of the group is equal to the rank of the Schur multiplicator.

The deficiency of G may or may not be equal to this rank. This is where many interesting questions begin to arise. If an efficient presentation for a group can be found, then we know that the minimal number of relations has been attained. However, if an efficient presentation is not known, then how are we to know if the deficiency has been attained? Perhaps it is impossible to find an efficient presentation--indeed, this has been proved for certain groups. However, there are many groups whose efficiency remains unsolved. One class of groups that has not been

closely examined is the direct product of efficiently presented groups. Will this necessarily be efficient? We will look at this problem in Chapter 2.

METACYCLIC GROUPS

DEFINITION: A group G is **metacyclic** if it has a normal cyclic subgroup N, such that G/N is also cyclic.

If G is finite, then we can consider $N \cong C_m = \langle x \rangle$, and $G / N = C_n \cong \langle Ny \rangle$, where x, y are elements of G, m and n are natural numbers, and C_k is the cyclic group of order k. Zassenhaus, among others, has proved that all finite metacyclic groups have the following presentation:

$$G(m, n, r, s) = \left\langle x, y \middle| x^m = 1, yxy^{-1} = x^r, y^n = x^s \right\rangle,$$

where m, n, r, and s are natural numbers, $r, s \leq m$ and $r^n \equiv 1 (\mathrm{mod}\ m)$ and $rs \equiv s (\mathrm{mod}\ m)$ [5].

It has been proved by Beyl and Wamsley that all metacyclic groups can be presented efficiently [1]. The Schur multiplicator of a metacyclic group has rank either one or zero. In the case where the rank is one, the presentation above is already efficient. If not, then Beyl gives the following efficient presentation:

$$\left\langle x, y \middle| y^n = x^{m/(m,r-1)}, \left[y, x^v\right] = x^{(m,r-1)} \right\rangle,$$

where $(m, r-1) \equiv v(r-1) (\mathrm{mod}\ m)$ and $(m, v) = 1$.

Thus, the metacyclic groups are efficient [1].

Another useful presentation of metacyclic groups has been given by Beyl [1]. This presentation indicates the rank of the Schur multiplicator, which we will indicate by λ. The variable s is removed in this presentation and the variables m, n, and r remain the same:

$$G(m,n,r,\lambda) = \left\langle x,y \middle| x^m = 1, yxy^{-1} = x^r, y^n = x^{\frac{m\lambda}{(m,r-1)}} \right\rangle.$$

Since λ is useful to our ends, we will use $G(m, n, r, \lambda)$ instead of $G(m, n, r, s)$, unless otherwise indicated. An example of a metacyclic group is:

$$G(8, 2, 5, 1) = \left\langle a,b \middle| a^8 = 1, bab^{-1} = a^5, a^2 = b^2 \right\rangle.$$

One example of a class of metacyclic groups are the dihedral groups. All dihedral groups are metacyclic and it has been proven that the direct product of dihedral groups is efficient [2].

Metacyclic groups have been classified into various categories [8]. In a metacyclic group, G/N is cyclic for some normal cyclic subgroup N. Because G/N is cyclic, G' is contained in N. Thus, for all finite metacyclic groups G' is cyclic, although G/G' need not by cyclic as the above example illustrates ($G/G' \cong C_4 \times C_2$).

DEFINITION: A metacyclic group G is **Z-metacyclic** if G/G' is cyclic.

DEFINITION: If all the Sylow subgroups of a Z-metacyclic group are cyclic, then G is called **ZS-metacyclic.**

Zassenhaus [8] has shown that a Z-metacyclic group can always be presented as:

$$Z(m,\ n,\ r) = \left\langle x, y \middle| x^m = y^n = 1,\ yxy^{-1} = x^r \right\rangle$$

with the same conditions on m, n, and r as above and with the added condition that $(m,\ r-1) = 1$. A presentation of ZS-metacyclic groups is similar, except that we add the restriction that $(m,\ n) = 1$.

Let's look at some specific examples of these groups. To begin, here is a presentation of a Z-metacyclic group which is not ZS-metacyclic:

$$Z(9,12,5) = \left\langle x, y \middle| x^9 = y^{12} = 1,\ yxy^{-1} = x^5 \right\rangle.$$

We know that this group is not ZS-metacyclic because of the subgroup generated by x and y^4. This subgroup is normal and has order 27, thus it is the unique Sylow 3-subgroup. Since x and y^4 do not commute, this Sylow subgroup cannot be cyclic. A computer program called ce (coset enumeration) was used to verify the order and normality of this subgroup. The program uses coset enumeration to find, among other things, the order of a group when given its presentation, whether or not a subgroup is normal, and the order of a subgroup within a group.

Here is a ZS-metacyclic group:

$$Z(5,8,2) = \left\langle x, y \middle| x^5 = y^8 = 1,\ yxy^{-1} = x^2 \right\rangle.$$

In working with metacyclic groups, an interesting dilemma arises. What is the relationship between the parameters in $G(m, n, r, \lambda)$ and $Z(m, n, r)$? If G is a Z-metacyclic or ZS-metacyclic group, is the m, n, and r the same value for both? In fact, as one begins to examine different groups and their presentations, one quickly stumbles across groups that are Z-metacyclic or ZS-metacyclic, but their presentations do not initially have the appropriate conditions. For example, the metacyclic group $G(10, 4, 3, 1)$ is ZS-metacyclic, even though $(10, (3 - 1)) \neq 1$ and $(10, 4) \neq 1$. We will see that $G(10, 4, 3, 1)$ is isomorphic to $Z(5, 8, 3)$.

The first observation we make regarding Z-metacyclic groups, is that their Schur multiplier is always trivial. Thus if a group is presented in the $G(m, n, r, \lambda)$ form and is Z-metacyclic, λ must equal 1. Let us simplify our notation then by letting $G(m, n, r)$ refer to a group with λ equal to 1. Now if $G(m, n, r)$ is isomorphic to some $Z(m', n', r')$, what is the relationship between the six parameters involved?

We stated earlier that Zassenhaus [8] proved that for Z-metacyclic groups, $(m, r-1) = 1$. We prove that now.

LEMMA 1: In a Z-metacyclic group presented as

$$Z = \left\langle x, y \middle| x^m = 1, y^n = 1, yxy^{-1} = x^r \right\rangle$$

then $(m, r-1) = 1$.

PROOF: We know that $r^n \equiv 1 (\text{mod } m)$. Since every commutator is a power of $yxy^{-1}x^{-1}$ and $yxy^{-1} = x^r$, then $yxy^{-1}x^{-1} = x^{r-1}$. Then x^{r-1} generates G, which forces $(m, r-1) = 1$. QED

Now a useful result about Z-metacyclic groups that do not have the proper (Zassenhaus) presentation initially .

LEMMA 2: If G is a Z-metacyclic group, and $(m, r - 1) = f$ where f does not equal 1, and G is presented as

$$G = \left\langle a, b \middle| a^m = 1, b^n = a^{m/f}, bab^{-1} = a^r \right\rangle,$$

then $(f, m/f) = 1$.

PROOF: Zassenhaus has proven that all Z-metacyclic groups can be presented so that $(m, r - 1) = 1$ [8]. So we know that there is a sequence of Tietze transformations (see appendix) that will take us from the above presentation to the Zassenhaus form. Now suppose that $(f, m/f) \neq 1$. Because $bab^{-1} = a^r$, then $bab^{-1}a^{-1} = a^{r-1}$. This implies that a^{r-1} is an element of G'. Since the order of a^{r-1} and G' is m/f, then a^{r-1} is a generator of G'. Now let x and y be the generating elements of the Zassenhaus presentation and

without loss of generality, let $x = a^{r-1}$. Now y must be some product of the generators of G, say $y = a^j b^i$. We know from the Zassenhaus presentation that $yxy^{-1} = x^{r^i}$, for some integer i. However, $r^i - 1$ is not coprime to m/f for any i. Thus no such y exists. But it has been proven that it must, so $(f, m/f) = 1$. QED

Now returning to $G(m, n, r)$ and $Z(m', n', r')$, we know that the order of G is mn and the order of Z is $m'n'$. Let $f = (m, r-1)$. Because we want $(m', r') = 1$, a logical choice for m' would be m/f. And since mn must equal $m'n'$, n' must equal nf. Consider then the two groups:

$$G = \left\langle a, b \middle| a^m = 1, bab^{-1} = a^r, b^n = a^{m/f} \right\rangle$$

$$Z = \left\langle x, y \middle| x^{m/f} = 1, y^{nf} = 1, yxy^{-1} = x^{r'} \right\rangle$$

We wish to show that G is isomorphic to Z by using Tietze transformations. Let $y = b$ and $x = a^f$. This implies that $y^{nf} = 1$ and $x^{m/f} = 1$, as desired.

Since $(f, m/f) = 1$, there exists natural numbers k and j such that $kf + j(m/f) = 1$, which implies that $kf = 1 - j(m/f)$. We will use this relation to solve for a in terms of x and y.

$$
\begin{aligned}
x &= a^t \\
x^k &= a^{kf} \\
x^k &= a^{-j\left(m/f\right)+1} \\
x^k &= b^{-nj}a \\
x^k &= y^{-nj}a \\
a &= y^{nj}x^k
\end{aligned}
$$

This also implies that $\left[x^k, y^{nj}\right] = 1$. Now we substitute into the original presentation to derive a new presentation in terms of x and y. We obtain:

$$
Z = \left\langle x, y \middle| \left(x^k y^{nj}\right)^m = 1, yx^k y^{nj} y^{-1} = \left(x^k y^{nj}\right)^r, \right.
$$
$$
\left. y^n = \left(x^k y^{nj}\right)^{m/f}, x = \left(x^k y^{nj}\right)^f, y = y, y^{nf} = x^{m/f} = 1 \right\rangle.
$$

The relation $y = y$ is clearly unnecessary. Because $f|m$ and $\left[x^k, y^{nj}\right] = 1$, the relation $\left(x^k y^{nj}\right)^m = 1$ is also unneeded. Then we have:

$$
Z = \left\langle x, y \middle| yx^k y^{nj} y^{-1} = \left(x^k y^{nj}\right)^r, y^n = \left(x^k y^{nj}\right)^{m/f}, \right.
$$
$$
\left. x = \left(x^k y^{nj}\right)^f, y^{nf} = x^{m/f} = 1 \right\rangle.
$$

Since $(m, r-1) = f$, we let $lf = r - 1$, so $r = lf + 1$. Then,

$$
\begin{aligned}
yx^k y^{nj} y^{-1} &= \left(x^k y^{nj}\right)^{lf+1} \\
yx^k y^{nj} y^{-1} &= x^{klf+k} y^{njlf+nj} \\
yx^k y^{-1} &= x^{klf+k} \\
yxy^{-1} &= x^{lf+1} \\
yxy^{-1} &= x^r.
\end{aligned}
$$

So we see that the value of r' in the new presentation is the same value as r in the original presentation:

$$Z = \left\langle x, y \,\middle|\, yxy^{-1} = x^r, y^n = \left(x^k y^{nj}\right)^{m/f}, \right.$$
$$\left. x = \left(x^k y^{nj}\right)^f, y^{nf} = x^{m/f} = 1 \right\rangle.$$

We can eliminate the relation $y^n = \left(x^k y^{nj}\right)^{m/f}$ as follows:

$$\begin{aligned} & \left(x^k y^{nj}\right)^{m/f} \\ &= x^{mk/f} y^{mnj/f} \\ &= y^{nmj/f} \\ &= y^{n(1-kf)} \\ &= y^n. \end{aligned}$$

We can change the relation $x = \left(x^k y^{nj}\right)^f$ to the relation $1 = x^{fk-1} y^{fnj}$ and then we see that

$$\begin{aligned} & x^{fk-1} y^{fnj} \\ &= x^{kf-1} \\ &= x^{j(m/f)} \\ &= 1. \end{aligned}$$

Therefore our presentation has been simplified and is in the Zassenhaus form:

$$Z = \left\langle x, y \,\middle|\, yxy^{-1} = x^r, y^{nf} = x^{m/f} = 1 \right\rangle.$$

So if $G(m, n, r)$ is Z-metacyclic, it is isomorphic to $Z(m/f, nf, r)$. Going back to our example, we now have $G(10, 4, 3, 1) \cong ZS(5, 8, 2)$.

CHAPTER 2

METACYCLIC GROUPS AND DIRECT PRODUCTS

We now turn to the direct product, which is defined as follows:

DEFINITION: The **direct product** of two groups, say G and H, is defined to be $G \times H = \langle (g,h) | g \in G, h \in H \rangle$ where we define the product of elements in a natural manner: $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

It is easily proved that $G \times H$ is a group.

The primary question of interest for us is, can the direct product of two efficient groups be presented efficiently? Could the direct product of two inefficient groups have an efficient presentation? What about the direct product of two metacyclic groups, can it be efficiently presented or not?

The latter question has not been completely answered to date. P.D. Williams has provided a partial answer and this paper addresses another case. P.D. Williams has proven that the direct product of a ZS-metacyclic group by itself has an efficient presentation. He proved that $ZS(m, n, r) \times ZS(m, n, r)$ can be presented as:

$$ZS \times ZS = \langle a, b \| [a^m, b^m] = 1, ab^{tn}a^{-1} = b^{(t+1)n}, ba^{tn}b^{-1} = a^{(t+1)n} \rangle,$$

where t is such that $um + t(r - 1) = 1$.

This paper will prove, in Chapter 3, that under certain conditions, the direct product of two Z-metacyclic groups can be presented efficiently.

It is worth noting that the direct product of two metacyclic groups may itself be metacyclic and therefore is necessarily efficient by the work of Beyl and Wamsley. We now give a condition for the direct product of two Z-metacyclic groups to be metacyclic.

THEOREM 1: If $G = Z(m, n, r)$ and $H = Z(p, q, s)$ are two Z-metacyclic groups, with $(n, q) = (m, p) = 1$, then $G \times H$ is metacyclic.

PROOF: We know that G and H may be presented as:

$$G = \langle a, b | a^m = b^n = 1, bab^{-1} = a^r \rangle$$
$$H = \langle c, d | c^p = d^q = 1, dcd^{-1} = c^s \rangle.$$

Let $x = bd$ and $y = ac$. Then there exist integers α, β, γ, δ such that $\alpha n + \beta q = 1$ and $\gamma m + \delta p = 1$. Now we find c in terms of y:

$$y^{\gamma m} = a^{\gamma m}c^{\gamma m} = c^{1-\delta p} = c.$$

Using similar arguments, we have $y^{\delta p} = a$, $x^{\alpha n} = d$, and $x^{\beta q} = a$. Now note that the normal subgroup $N = \langle a, c \rangle$ is cyclic, since N also equals $\langle y \rangle$.

Now N is normal in $G \times H$ also. For, $bab^{-1} \in N$ (it is equal to a^r), $bcb^{-1} \in N$ ($[b, c] = 1$). $dad^{-1} \in N$, and $dcd^{-1} \in N$. Thus, for all generators of $G \times H$, say g, $gyg^{-1} \in N$. Now we can look at a presentation of $G \times H/N = K$:

$$K = \langle a, b, c, d | a^m = b^n = c^p = d^q = [a,c] = [b,c] = 1,$$
$$[a,d] = [b,d] = 1, bab^{-1} = a^r, dcd^{-1} = c^s, a = c = 1 \rangle$$
$$= \langle b, d | b^n = d^q = [b,d] = 1 \rangle$$
$$\cong \langle x | x^{nq} = 1 \rangle.$$

Therefore, N is a cyclic and a normal subgroup in $G \times H$ whose factor group is also cyclic, implying that $G \times H$ is metacyclic. QED

An example of this theorem can be seen with the group the groups $G = G(7, 3, 2)$ and $H = G(11, 2, 10)$. The direct product of these groups is isomorphic to:

$$G \times H \cong \langle a, b | a^{77} = 1, b^6 = 1, bab^{-1} = a^{10} \rangle$$

Thus this direct product results in a ZS-metacyclic group.

In Chapter 3, it will be proved that $G \times H$, two Z-metacyclic groups, can be presented efficiently if $(m, q) = (n, p) = 1$ and $(n, q) \neq 1$. It will be shown that

$$G \times H = \left\langle x,\ y \middle| yx^{tq}y^{-1} = x^{(t+1)q},\right.$$
$$\left. xy^{um}x^{-1} = y^{n(u+1)}, \left[y^p, x^m\right] = 1\right\rangle \qquad (1)$$

with groups G and H as above and for certain integers t and u. Moreover, we shall show that this group is not metacyclic. Given this presentation and these conditions, the group $G = G(11, 10, 6) \times H = G(33, 2, 32)$ is an example of a group that can be presented efficiently using (1). This result was also verified using ce. For the full 10 relation presentation of $G \times H$, ce verified that the order of the group is equal to 7260 = $mnpq$, as required. When reduced to the 3 relation presentation as in (1), ce has more difficulty finding the order of G. However, ce's work is drastically reduced if we use x or y as subgroup generators. Using x as a subgroup generator on the 3 relation presentation, we obtained an order of 330 = pn, as expected. Similarly, the order of the subgroup generated by y was 22 = mq.

Let's examine the Schur multiplicator associated with $G \times H$ in order to see that (1) is an efficient presentation. Using the Schur-Künneth formula

$$M(G \times H) = M(G) \times M(H) \times (G \otimes H).$$

For metacyclic groups we then have

$$M(G \times H) = C_\lambda \times C_{\lambda'} \times ((G / G') \otimes (H / H')).$$

And since the Schur multiplicator is trivial for Z-metacyclic groups, this reduces to

$$M(G \times H) = (G / G') \otimes (H / H')$$
$$= C_n \otimes C_q$$
$$= C_{(n,q)}.$$

Thus, if $(n, q) = 1$, the Schur multiplicator of $G \times H$ is trivial. If not, then the Schur multiplicator has rank one and the presentation (1) is efficient.

At times, the direct product results in a presentation that is automatically efficient. For example, if G and H are not Z-metacyclic, the Schur multiplicator is

$$M(G \times H) = C_\lambda \times C_{\lambda'} \times ((G / G') \otimes (H / H'))$$
$$= C_\lambda \times C_{\lambda'} \times ((C_k \times C_{jk}) \otimes (C_l \times C_{il})).$$

The rank of the Schur multiplicator will then depend upon how many of these values are relatively prime. If they have no common divisors, the rank will be six. If the Schur mutiplicator of G or H is trivial, the rank will decrease.

Take for example $G(16, 4, 5) \times G(32, 25, 4)$. The Schur mutiplicator for both groups is trivial and the factor by the derived groups are $C_4 \times C_4$ and $C_4 \times C_8$, respectively. Thus, the rank of the Schur multiplicator is four. However, since these groups have a trivial Schur multiplicator individually, we can use Beyl's two relation, two generator efficient presentation when taking the cross product [1]. The standard presentation of the direct product will be a

four generator, eight relation presentation (see appendix) which is then efficient.

Also, when forming a direct product, it is often the case that some of the relations are trivial (as we will see in Chapter three). Thus if some of the values in the Schur multiplicator are relatively prime, the presentation will reduce to an efficient one quite easily. The reader will see, however, that the presentation in Chapter three requires a great deal of effort to be reduced because the rank of the Schur multiplicator is only one.

CHAPTER 3

EFFICIENT PRESENTATION OF A DIRECT PRODUCT

We now present our main result regarding the direct product of two Z-metacyclic groups. We begin with a theorem that will prove useful to our ends.

THEOREM 1: Let $F_{m,\,p,\,n,\,q}$, a group, be defined by:

$$F_{m,\,p,\,n,\,q} = \langle w, z \| [w^m, z^p] = 1,$$
$$wz^{un}w^{-1} = z^{n(u+1)},\ zw^{tq}z^{-1} = w^{q(t+1)} \rangle,$$

under the conditions that:

1) $(m,\ q) = (p,\ n) = 1,\ m,\ q,\ p,\ n > 1.$
2) There exists integers positive r and s such that $(m, r-1) = 1$, $(p, s-1) = 1$, and such that $s^q \equiv 1 (\mathrm{mod}\ p)$, and $r^n \equiv 1 (\mathrm{mod}\ m)$.
3) t and u are integers such that $t(r-1) \equiv 1 (\mathrm{mod}\ m)$ and $u(s-1) \equiv 1 (\mathrm{mod}\ p)$.

Then $z^{np} = 1$ and $w^{mq} = 1$.

We will use a series of lemmas to prove this result.

LEMMA 1: For each natural number k the relation $w^k z^{u^k n} w^{-k} = z^{(u+1)^k n}$ holds in F.

PROOF: The statement holds for $k = 1$. Assume true for some $k \geq 1$, then

$$w^k z^{u^k n} w^{-k} = z^{(u+1)^k n}$$

$$w^{k+1} z^{u^{k+1} n} w^{-k-1} = w z^{(u+1)^k n u} w^{-1} = z^{(u+1)^k n(u+1)} = z^{n(u+1)^{k+1}} \quad \text{QED}$$

LEMMA 2: If $\varphi = (u+1)^m - u^m$, then $|z|$ divides $np\varphi$.

PROOF: From Lemma 1, we know that

$$w^m z^{u^m n} w^{-m} = z^{(u+1)^m n}.$$

If we raise both sides to the pth power,

$$w^m z^{u^m np} w^{-m} = z^{(u+1)^m np}.$$

Given that $\left[w^m, z^p\right] = 1$,

$$z^{u^m np} = z^{(u+1)^m np}$$

$$\Rightarrow \quad z^{(u+1)^m np - u^m np} = 1$$

$$\Rightarrow \quad z^{np((u+1)^m - u^m)} = 1 \qquad \text{QED}$$

LEMMA 3: In F, the following relations hold:

$$w^m z^u w^{-m} = z^{u + \varphi \delta n (s-1)^{m-1}}$$

$$w^m z w^{-m} = z^{1 + \varphi \delta n (s-1)^m},$$

where δ is an integer such that $\gamma p + \delta n = 1$.

PROOF: Lemma 1 implies that

$$w^m z^{u^m n} w^{-m} = z^{(u+1)^m n}.$$

Raising to the power δ,

$$w^m z^{u^m n \delta} w^{-m} = z^{(u+1)^m n \delta}$$

$$\Rightarrow \quad w^m z^{u^m - u^m \gamma p} w^{-m} = z^{(u+1)^m n\delta}$$

$$\Rightarrow \quad w^m z^{u^m} w^{-m} = z^{(u+1)^m n\delta + u^m \gamma p}$$

since $\left[z^p, w^m\right] = 1$.

Now by definition,

$$\varphi = (u + 1)^m - u^m$$

$$\Rightarrow \quad \varphi + u^m = (u + 1)^m,$$

Examining the exponent on z:

$$(u + 1)^m n\delta + u^m \gamma p$$

$$= (\varphi + u^m) n\delta + u^m \gamma p$$

$$= \varphi n\delta + u^m (n\delta + \gamma p)$$

$$= \varphi n\delta + u^m$$

$$\Rightarrow \quad w^m z^{u^m} w^{-m} = z^{\varphi n\delta + u^m}.$$

Now, using induction, we'll prove that

$w^m z^{u^{m-i}} w^{-m} = z^{u^{m-i} + \varphi n\delta (s-1)^i}$, for i a non-negative integer.

When $i = 0$, this clearly holds from the previous statement. Then assuming true for $i \geq 0$, and raising both sides to the $(s - 1)$ power, we have:

$$w^m z^{u^{m-i}(s-1)} w^{-m} = z^{u^{m-i}(s-1) + \varphi n\delta (s-1)^{i+1}}$$

$$w^m z^{u^{m-(i+1)} u (s-1)} w^{-m} = z^{u^{m-i}(s-1) + \varphi n\delta (s-1)^{i+1}}$$

$$w^m z^{u^{m-(i+1)}(1-\theta p)} w^{-m} = z^{u^{m-i}(s-1) + \varphi n\delta (s-1)^{i+1}}$$

$$w^m z^{u^{m-(i+1)}} w^{-m} = z^{u^{m-i}(s-1) + \varphi n\delta (s-1)^{i+1} + \theta p u^{m-(i+1)}}$$

$$w^m z^{u^{m-(i+1)}} w^{-m} = z^{u^{m-(i+1)}(1-\theta p) + \varphi n\delta (s-1)^{i+1} + \theta p u^{m-(i+1)}}$$

$$w^m z^{u^{m-(i+1)}} w^{-m} = z^{u^{m-(i+1)} + \varphi n\delta (s-1)^{i+1}}$$

If $i = m$ or $m - 1$ the lemma is proved. QED

LEMMA 4: In F, $zw^{mq}z^{-1} = z^{(1+\varphi\delta n(s-1)^m)^q - 1}w^{mq}$.

PROOF: From lemma 3 we have that

$$w^m z w^{-m} = z^{1+\varphi\delta n(s-1)^m}$$

Conjugating by powers of w^m, we have

$$w^{mi} z w^{-mi} = z^{(1+\varphi\delta n(s-1)^m)^i}$$

In particular, if $i = q$, then

$$w^{mq} z w^{-mq} = z^{(1+\varphi\delta n(s-1)^m)^q}$$

$$\Rightarrow \quad z^{-1}w^{mq}z = z^{(1+\varphi\delta n(s-1)^m)^q - 1}w^{mq} \qquad \text{QED}$$

LEMMA 5: $(p, \varphi) = 1$.

PROOF: Recall that $\varphi = (u+1)^m - u^m$. Suppose that $(p, \varphi) \neq 1$. Then there exists a prime, say k, such that $k|\varphi$ and $k|p$. We define θ such that $\theta p + u(s-1) = 1$. Then,

$$\theta k p' + u(s-1) = 1, \text{ where } p = kp'.$$

$$\Rightarrow (u, k) = 1, \ (k, s-1) = 1.$$

$$\text{Since } k|\varphi, \Rightarrow \varphi \equiv 0 (\bmod k).$$

Also, $u(s-1) \equiv 1 (\bmod k)$, or $us \equiv 1 + u (\bmod k)$. Now $\varphi = (u+1)^m - u^m \equiv (us)^m - u^m (\bmod k)$, $\Rightarrow u^m(s^m - 1) \equiv 0 (\bmod k)$. Since k is prime, this implies that $u^m \equiv 0 (\bmod k)$ or $s^m - 1 \equiv 0 (\bmod k)$. Since the former is clearly false because $(u, k) = 1$, then the latter is true. However, this is impossible

$$\text{since, } s^q \equiv 1 (\text{mod } k)$$

$$\text{and, } s^m \equiv 1 (\text{mod } k)$$

$$\Rightarrow \quad s^{(m,q)} \equiv 1 (\text{mod } k)$$

$$\Rightarrow \quad s \equiv 1 (\text{mod } k)$$

$\Rightarrow$ $k \mid s - 1$, which is a contradiction.

Therefore, $(p, \varphi) = 1$. QED

LEMMA 6: In F, $zw^{mq}z^{-1} = w^{mq}$.

PROOF: Because $(p, \varphi) = 1$, then $(p, n\varphi) = 1$, because $(p, n) = 1$. Now from Lemma 4 we have that $zw^{mq}z^{-1} = z^{(1+\varphi\delta n(s-1)^m)^q - 1}w^{mq}$. Let $h = (1 + \varphi\delta n(s - 1)^m)^q - 1$. If we can show that h is congruent to 0 (mod $pn\varphi$), the proof will be complete. Clearly, $h \equiv 0 (\text{mod } \varphi n)$, so we will show that $h \equiv 0 (\text{mod } p)$ and the result will follow. Note that $\delta n \equiv 1 (\text{mod } p)$. Now,

$$h \equiv (1 + \varphi(s - 1)^m)^q - 1 (\text{mod } p)$$

$$\equiv (1 + [(u + 1)^m - u^m](s - 1)^m)^q - 1 (\text{mod } p)$$

$$\equiv (1 + [(u + 1)(s - 1)]^m - [u(s - 1)]^m)^q - 1 (\text{mod } p).$$

But since $u(s - 1) \equiv 1 (\text{mod } p)$, we reduce to

$$h \equiv s^{mq} - 1 (\text{mod } p)$$

$$\equiv 1 - 1 \equiv 0 (\text{mod } p).$$ QED

Our main result, that in F, $w^{mq} = 1$ and $z^{np} = 1$, is now easily proved:

PROOF OF THEOREM 1: From Lemma 6, $zw^{mqt}z^{-1} = w^{mqt}$. However, using our original relation we know that $zw^{mtq}z^{-1} = w^{mq(t+1)}$. Therefore, $w^{mq} = 1$. Proving that $z^{np} = 1$ can be done in a similar fashion, using the appropriate corresponding variables. QED

Now consider the groups

$$G = \langle a, b \mid a^m = 1,\ b^n = 1,\ bab^{-1} = a^r \rangle$$
$$\text{and } H = \langle c, d \mid c^p = 1,\ d^q = 1,\ dcd^{-1} = c^s \rangle,$$

with the conditions necessary for these groups to be Z-metacyclic, namely that $r^n \equiv 1 (\text{mod } m)$, $(m, r-1) = 1$, $s^q \equiv 1 (\text{mod } p)$, and that $(p, s-1) = 1$. We will require the additional condition that $(m, q) = 1$ and $(n, p) = 1$. Now we form the direct product of these two groups:

$$G \times H = \langle a, b, c, d \mid a^m = 1,\ c^p = 1,\ b^n = 1,\ d^q = 1,$$
$$bab^{-1} = a^r,\ dcd^{-1} = c^s,\ [a,c] = [a,d] = [b,c] = [b,d] = 1 \rangle.$$

Now we define $x = ad$ and $y = bc$. Because $(m, q) = 1$, there exists integers a and b such that $\alpha m + \beta q = 1$. Similarly, there exist γ and δ such that $\gamma p + \delta n = 1$. Therefore,

$$x^{\beta q} = a^{\beta q} d^{\beta q}$$
$$x^{\beta q} = a^{\beta q}$$
$$x^{\beta q} = a^{1-\alpha m}$$
$$x^{\beta q} = a.$$

Using similar arguments we arrive with the results: $x^{\alpha m} = d$, $y^{\gamma p} = b$, $y^{\delta n} = c$.

Thus, reducing $G \times H$ to a presentation on two generators we have,

$$G \times H = \langle x, y | x^{\beta qm} = y^{\gamma pn} = y^{\delta pn} = x^{\alpha qm} = 1,\ y^{\gamma p} x^{\beta q} y^{-\gamma p} = x^{\beta rq},$$
$$x^{\alpha m} y^{\delta n} x^{-\alpha m} = y^{\delta ns},\ x = x^{\beta q} x^{\alpha m},\ y = y^{\gamma p} y^{\delta n},$$
$$[x^{\beta q}, y^{\delta n}] = [x^{\beta q}, x^{\alpha m}] = [y^{\gamma p}, y^{\delta n}] = [y^{\gamma p}, x^{\alpha m}] = 1 \rangle .$$

The relations $\left[x^{\beta q}, x^{\alpha m}\right] = \left[y^{\gamma p}, y^{\delta n}\right] = 1$, $x = x^{\beta q} x^{\alpha m}$, and $y = y^{\gamma p} y^{\delta n}$ are clearly trivial. Since $(\alpha, \beta) = 1$, then

$$x^{\beta qm} = x^{\alpha qm} = 1$$
$$\Rightarrow x^{mq} = 1.$$

Similarly, $y^{np} = 1$. Thus our presentation is reduced to

$$G \times H = \langle x, y | x^{mq} = y^{np} = 1,\ y^{\gamma p} x^{\beta q} y^{-\gamma p} = x^{\beta rq},$$
$$x^{\alpha m} y^{\delta n} x^{-\alpha m} = y^{\delta ns},\ \left[x^{\beta q}, y^{\delta n}\right] = \left[y^{\gamma p}, x^{\alpha m}\right] = 1 \rangle \quad .$$

Now we will simplify some of these relations.

$$x^{\alpha m} y^{\delta n} x^{-\alpha m} = y^{\delta ns}$$
$$\Rightarrow x^{1-\beta q} y^{\delta n} x^{\beta q - 1} = y^{\delta ns}.$$

And as $\left[x^{\beta q}, y^{\delta n}\right] = 1$, then $xy^{\delta n} x^{-1} = y^{\delta ns}$.

Similarly, $yx^{\beta q} y^{-1} = x^{\beta rq}$.

Also, $\left[x^{\beta q}, y^{\delta n}\right] = 1$ which implies that $\left[x^{\beta q}, y^{\delta n^2}\right] = 1$, so $\left[x^{\beta q}, y^{n(1-\gamma p)}\right] = 1$, resulting in $\left[x^{\beta q}, y^{n}\right] = 1$.

Similarly, $\left[x^{q}, y^{n}\right] = 1$ and $\left[y^{p}, x^{m}\right] = 1$.

So now our presentation looks like this:

$$G \times H = \left\langle x, y \middle| x^{mq} = y^{np} = 1,\ yx^{\beta q}y^{-1} = x^{\beta rq},\right.$$
$$\left. xy^{\delta n}x^{-1} = y^{\delta ns},\ \left[x^q, y^n\right] = \left[y^p, x^m\right] = 1\right\rangle.$$

We now eliminate the relation $\left[y^n, x^q\right] = 1$:

$$yx^{\beta q}y^{-1} = x^{\beta rq}$$
$$y^n x^{\beta q} y^{-n} = x^{\beta r^n q}$$
$$y^n x^{\beta q} y^{-n} x^{-\beta q} = x^{\beta(r^n - 1)q}$$
$$\text{As } r^n - 1 \equiv 0 (\text{mod } m)$$
$$\beta q \equiv 0 (\text{mod } q)$$
$$(r^n - 1)\beta q \equiv 0 (\text{mod } mq),$$
$$\Rightarrow \left[y^n, x^{\beta q}\right] = 1$$

And so $\left[y^n, x^q\right] = 1$, using previous arguments.

Thus we have reduced the presentation to

$$G \times H = \left\langle x, y \middle| x^{mq} = y^{np} = 1,\ yx^{\beta q}y^{-1} = x^{\beta rq},\right.$$
$$\left. xy^{\delta n}x^{-1} = y^{\delta ns},\ \left[y^p, x^m\right] = 1\right\rangle.$$

We remove the last of the δ's and β's as follows:

$$yx^{\beta q}y^{-1} = x^{\beta rq}$$
$$\Leftrightarrow yx^{1-\alpha m}y^{-1} = x^{r - r\alpha m}$$
$$\Leftrightarrow yx^{q-\alpha qm}y^{-1} = x^{rq - r\alpha qm}$$
$$\Leftrightarrow yx^q y^{-1} = x^{rq}.$$

Similarly, $xy^{\delta n}x^{-1} = y^{\delta ns} \Leftrightarrow xy^n x^{-1} = y^{sn}$.

So,

$$G \times H = \left\langle x, y \middle| x^{mq} = y^{np} = 1,\ yx^q y^{-1} = x^{rq},\right.$$
$$\left. xy^n x^{-1} = y^{ns},\ \left[y^p, x^m\right] = 1\right\rangle.$$

Now consider the fact that $(m, r-1) = 1$ and $(p, s-1)=1$. This implies that we can find integers so that $\phi m + t(r-1) = 1$ and $\theta p + u(s-1) = 1$. Then we can make the following argument:

$$xy^n x^{-1} = y^{ns}$$

$$xy^{un}x^{-1} = y^{uns} = y^{n(-\theta p+u+1)} = y^{nu+u} = y^{n(u+1)}.$$

Similarly, we have that $yx^{tq}y^{-1} = x^{(t+1)q}$.

Then,

$$G \times H = \langle x, y | x^{mq} = y^{np} = 1,\ yx^{tq}y^{-1} = x^{(t+1)q},$$
$$xy^{un}x^{-1} = y^{n(u+1)},\ [y^p, x^m] = 1\rangle.$$

But now we can apply the Theorem 1 presented at the beginning, which results in the following presentation:

$$G \times H = \langle x, y | yx^{tq}y^{-1} = x^{(t+1)q},$$
$$xy^{un}x^{-1} = y^{n(u+1)},\ [y^p, x^m] = 1\rangle.$$

We know that if $(n, q) \neq 1$, that the Schur multiplier has rank one. Thus when this condition holds, the above presentation is efficient.

Clearly, this paper has left open many more avenues to be explored. Most immediately, what if (n, q) does equal 1? Can a two generator, two relation presentation be found? Other problems for further investigation include:

1) To find an efficient presentation for the direct product of a Z-metacyclic group by itself. For example, can $Z(9, 12, 5) \times Z(9, 12, 5)$ be presented efficiently?

2) To find an efficient presentation for the direct product of a metacyclic group by itself. For example, can $G(8, 2, 5, 1) \times G(8, 2, 5, 1)$ be presented efficiently?

3) To find an efficient presentation for three, four or more of these groups taken in direct products together (i.e., $G \times H \times F$).

4) When the Schur multiplicator is trivial, finding an efficient presentation is even more difficult in all of these cases. For example, $Z(11, 5, 3) \times Z(22, 2, 21)$ has a trivial Schur multiplicator and thus requires an equal number of generators and relations to be presented efficiently.

A very preliminary exploration into case number 1 has been started by the author and P.D. Williams. Using a computer program, we tried to reduce a specific direct product and had a difficult time. It appears that this case is quite difficult.

APPENDIX

A FEW USEFUL METHODS

LEMMA 1: If x and y are elements of a group, G, and the relation $yxy^{-1} = x^r$ holds in G for r a positive integer, then $y^k x^j y^{-k} = x^{jr^k}$, for j an integer and k a positive integer.

PROOF: We will begin by using induction on k. If $k = 1$, then the statement is clearly true. Now assume that true for some positive integer k:

$$y^k x y^{-k} = x^{r^k}.$$

Then rasing both sides to the power r, we have

$$\left(y^k x y^{-k}\right)^r = \left(x^{r^k}\right)^r$$

$$y^k x y^{-k} y^k x y^{-k} \ldots y^k x y^{-k} = x^{r^{k+1}} \qquad \text{(r times)}$$

$$y^k x^r y^{-k} = x^{r^{k+1}}$$

$$y^k \left(y x y^{-1}\right) y^{-k} = x^{r^{k+1}}$$

$$y^{k+1} x y^{-k-1} = x^{r^{k+1}}.$$

Now if we raise both sides to the jth power, the y's cancel again and we have

$$y^k x^j y^{-k} = x^{jr^k}. \qquad \text{QED}$$

LEMMA 2: If G is a group with x an element of G and $x^m = 1$ and $x^n = 1$ for n and m, positive integers, then $x^{(m,n)} = 1$.

PROOF: Let $(n, m) = d$. Then we know there exist integers α and β such that $\alpha n + \beta m = d$. Then

$$x^d = x^{\alpha n + \beta m} = x^{\alpha n} x^{\beta m} = 1. \qquad \text{QED}$$

TIETZE TRANSFORMATIONS

If you have a group, $G = \langle X|R \rangle$ and Y is a set of generators of G, then $G = \langle Y|R(X(Y)), Y = Y(X(Y)) \rangle$. This has the following meaning. Rewrite every relation in R by replacing the elements of X with the corresponding word in Y. Then, add more relations which are obtained by equating each element of Y to its equivalent in terms of X. This assumes, of course, that we can find a way of writing each element of Y in terms of X and vice versa.

PRESENTATIONS OF DIRECT PRODUCTS

For two groups, $G = \langle X|R \rangle$ and $H = \langle Y|S \rangle$, then

$$G \times H = \langle X, Y|R, S, [x_i, y_j] \rangle,$$

where $x_i \in X$ and $y_j \in Y$. The commutator relations must be added because the variables in a direct product always commute.

BIBLIOGRAPHY

[1] Beyl, F.R., *The Schur Multiplicator of Metacyclic Groups*, Proceeds of the American Mathematical Society, vol 40, (2), October, 1973.

[2] Campbell, C.M., Robertson, E.F., and Williams, P.D., *On the Efficiency of Some Direct Powers of Groups*, Groups-Canberra 1989, Lecture Notes in Mathematics v 1456, 106-113, Springer-Verlag, 1990.

[3] Durbin, J.R., Modern Algebra, John Wiley & Sons, Inc., New York, 1992.

[4] Fraleigh, J.B., A First Course in Abstract Algebra, Addison-Wesley Publishing Company, Reading, Massachusetts, 1982.

[5] Johnson, D.L., Presentations of Groups, Cambridge University Press, Cambridge, 1990.

[6] Lang, Serg, Algebra, Addison-Wesley Publishing Company, Inc., Redwood City, CA, 1984.

[7] Rotman, J.J., An Introduction to the Theory of Groups, Allyn and Bacon, Inc., Boston, 1984.

[8] Zassenhaus, H., Theory of Groups, Chelsea, New York, 1958.