ON THE CLASSIFICATION OF SOME ONE-RELATOR GROUPS

by

STEPHEN A. MESKIN

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1968

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

May 14, 1968
date

G. Baumslag
Professor Gilbert Baumslag
Chairman of Examining Committee

May 14, 1968
date

Eldon Dyer
Professor Eldon Dyer
Executive Officer

Professor Louis Auslander

Professor Alex Heller

Professor F. William Lawvere

Supervisory Committee

The City University of New York

INTRODUCTION

One is often faced with the problem of deciding for a given set X of groups which groups in the set are isomorphic and which are not. A natural but often computationally difficult or impossible approach is to choose a test group T and then compute and compare the number of homomorphisms of G into T for each $G \in X$.

Giving the groups has been standardized to some extent by presenting the groups in terms of generators and defining relations. The computations become feasible although possibly still impractical if we restrict the groups in X to be finitely presented (finite number of generators and relations) and the test group T to be finite. Even under these restrictions, however, the method can be shown to fail [J. Dyer - unpublished]. It is possible, however, that it will work for groups with one relator which are residually finite (the intersection of all the normal subgroups of finite index is trivial). In this paper the above technique is used to try to classify

(1) $\{H(i,j) \mid \text{all integers } i \text{ and } j\}$

and

(2) $\{G(m_1,\ldots,m_t) \mid t > 0 \text{ , all integers } m_1,\ldots,m_t\}$,

where

$$H(i,j) = (a,b,c;\ a^{-1}[c^i,a][c^j,b])$$

and

$$G(m_1,\ldots,m_t) = (x_1,x_2,\ldots,x_t;\ x_1^{m_1}x_2^{m_2}\ldots x_t^{m_t}) \ .$$

The computations can be made more practical in three ways.

(1) Count only the epimorphisms.

(2) All the information available from abelian test groups can be obtained from the factor derived group. The Betti number and torsion coefficients form a complete set of invariants for the factor derived group. They can be computed by diagonalizing the relation matrix.

(3) Use the above techniques on the complete set of kernels of maps onto a well understood test group. Presentations for the kernels can be computed by using the method of Reidemeister and Schreier.

In Chapter 1, I define explicitly many of the terms mentioned here and state a few well known facts which are used in the sequel. Proofs are available in standard works, e.g. see [5].

In Chapter 2, I discuss the groups $H(i,j)$. The main result is a formula for the number of epimorphisms of a subgroup of index 2 onto each member of an infinite family of finite groups. The formula can be used to distinguish many of the groups, $H(i,j)$. In particular we have

Theorem A. The groups $H(i,j)$ are all distinct for (i,j) in the set $\{(1,1),(1,2),(1,3),(1,4),(1,7),(1,10),(2,2),(2,14),(2,15),(2,21),(3,2),(3,15),(5,10),(5,14)\}$.

In Chapter 3, I discuss the groups $G(m_1,\ldots,m_t)$. In this case somewhat better results are obtained.

Theorem B. The groups $G(m_1,\ldots,m_t)$ can be completely classified when $\gcd(m_1,\ldots,m_t) \neq 1$.

Theorem C. The groups $G(m_1,m_2,m_3)$ can be completely classified.

Most of the notation that is used is standard or it is introduced as it is needed. The few exceptions are listed below.

$\emptyset$ = the empty set.

$gp(X)$ = the subgroup of G generated by X, where X is a subset of the group G.

$gp_G(X)$ = the normal subgroup of G generated by X.

$x^y = y^{-1}xy$, where x and y are elements of a group.

$[x,y] = x^{-1}y^{-1}xy$.

$|X|$ = the cardinality of the set X.

$|a|$ = the absolute value of the number a.

ACKNOWLEDGMENTS

It is with great pleasure that I acknowledge my indebtedness to Professor Gilbert Baumslag. He has been a constant source of inspiration and ideas. He has taught me, advised me and worked untiringly in my behalf.

Because of her devotion, encouragement and many sacrifices my wife, Adrien, must share with me in full equality any credit accruing from my work.

I wish also to acknowledge the moral support of my family and friends and the faculty, staff and students of The City University of New York.

Finally, I wish to express my gratitude to the National Science Foundation and The City University of New York for their financial support throughout the past three years.

TABLE OF CONTENTS

CHAPTER 3. (continued)

CHAPTER 1 PRELIMINARIES

Section 1. Presentations and the method of Reidemeister and Schreier

If X is a set of generators, x, for a group G and R is a set of X-words (finite strings of x's and x^{-1}'s), $r(x)$, then we write $G = (X; R)$ and say that $(X; R)$ is a presentation for G if and only if the kernel K of the homomorphism μ of the free group F on an equally indexed set $Y = \{y_x | x \in X\}$ onto G which maps y_x to x is just $gp_F\{r(y_x) | r(x) \in R\}$. The elements of R are called relators.

We note first of all that if R is any set of X-words then $F/K = (X; R)$. Secondly if G_o is another group then a map θ of X into G_o extends to a homomorphism (epimorphism) of $G = (X; R)$ to G_o if and only if $r(x\theta) = 1$ for all $r(x) \in R$ (and $G_o = gp\{x\theta | x \in X\}$). Finally if $N = gp_G(R_o)$ then $G/N = (X; R \cup R_o)$.

Let H be a subgroup of G and η the natural isomorphism from F/K onto G induced by μ then $H\eta^{-1} = E/K$ where E is a subgroup of F. E is free (all subgroups of a free group are free), and the method of Schreier allows us to choose a free set of generators for E.

First we choose a system S of right coset representatives, s, for E in F such that

(i) $1 \in S$

(ii) if $s = y_1^{\epsilon_1} \ldots y_t^{\epsilon_t} \in S$ $(y_i \in Y,\ \epsilon_i = \pm 1)$ then

$$y_1^{\epsilon_1} \ldots y_j^{\epsilon_j} \in S \quad \text{for} \quad j = 1, \ldots, t-1 .$$

Such a system called a Schreier system always exists. Secondly we let σ be the map from F to S which sends each element of F to its coset representative in S. Finally E is freely generated by the set $Z(S,Y)$ of those elements $z(s,y) = sy(sy\sigma)^{-1}$, $s \in S$, $y \in Y$ which are not equal to 1.

By the Reidemeister rewriting process we may rewrite any word $e = e(y)$ in E as a word $e = \bar{e}(z)$ in the above generators of E. Indeed if $e(y) = y_1^{\epsilon_1} \ldots y_t^{\epsilon_t}$ then $\bar{e}(z) = z(s_1,y_1)^{\epsilon_1} \ldots z(s_t,y_t)^{\epsilon_t}$ where $s_j = (y_1^{\epsilon_1} \ldots y_{j-1}^{\epsilon_{j-1}})\sigma$ if $\epsilon_j = +1$ and $s_j = (y_1^{\epsilon_1} \ldots y_j^{\epsilon_j})\sigma$ if $\epsilon_j = -1$. Now $K = gp_F(R)$ is also $gp_E\{r(s) = srs^{-1} \mid r \in R, s \in S\}$. Using the Reidemeister rewriting process we set $R(S,Y) = \{\bar{r}(\bar{s})(z) \mid r \in R, s \in S\}$. Thus $E/K = (Z(S,Y); R(S,Y))$.

We can translate everything we have done for E to H by using μ. First of all H is generated by the set $W(S\mu,X)$ of elements $w(s\mu,x) = (z(s,y_x))\mu$. Secondly by the above discussion we see that for $R(S\mu,X) = \{\bar{r}(\overline{s\mu})(z\mu) \mid r \in R, s \in S\}$ where $H = (W(S\mu,X); R(S\mu,X))$. As a practical matter it is convenient to use μ to identify X-words with Y-words. Another way of putting it is that we discard G and look only at F/K.

Section 2. Betti numbers, torsion coefficients and the relation matrix

The factor derived group of G, $A(G) = G/G'$, where G' is the derived group of G. If G is finitely generated then so is $A(G)$ and hence there is a unique non-negative integer $\beta(G)$ and a unique possibly empty set of integers $\tau(G) = \{\tau_1(G),\ldots,\tau_n(G)\}$ all greater than 1, such that τ_i divides τ_{i+1} for $i \in \{1,\ldots,n-1\}$ with the property that $A(G)$ is isomorphic to a direct sum of β infinite cyclic groups and finite cyclic groups of order τ_i for each i. $\beta(G)$ is called the Betti number of $A(G)$ and $\tau(G)$ the set of torsion coefficients.

The Betti number and torsion coefficients of the factor derived group of a finitely presented group $G = (X; R)$ can be computed by diagonalizing its relation matrix. The relation matrix $M(G)$ has $|R|$ rows and $|X|$ columns; for convenience we may index them by R and X themselves. The entry at the r'th row and x'th column, $M(G)(r,x)$, is the exponent sum of x in r. By using elementary row and column operations any rectangular matrix and in particular a relation matrix can be put in diagonal form, that is with at most one non-zero entry in each row and column. Moreover these non-zero entries can all be chosen positive and so that when written down in increasing order $t_1,t_2,\ldots,t_s$ they have the property that t_i divides t_{i+1} for $i \in \{1,\ldots,s-1\}$. When this has been done for $M(G)$ the Betti number of $A(G)$, $\beta(G) = |X| - s$, and if $t_i = 1$ for $i \in \{1,\ldots,s-n\}$ but $t_{s-n+1} \neq 1$ then with $\tau_i(G) = t_{s-n+i}$ the set of torsion coefficients for $A(G)$ is $\tau(G) = \{\tau_1(G),\ldots,\tau_n(G)\}$.

We now list some elementary facts about elementary row and column operations which we will use frequently, often without explicit mention. First if a square matrix in diagonal form has exactly one non-zero entry in each row and column and each of these entries are equal then the action of any elementary row operation may be negated by an appropriately chosen elementary column operation. Secondly if a matrix in diagonal form has two non-zero entries a and b then by elementary row and column operations we may change a to $\underline{\gcd(a,b)}$, the positive greatest common divisor of a and b and b to $\underline{\operatorname{lcm}(a,b)}$ the positive least common multiple of a and b, leaving the balance of the matrix unchanged. Thirdly an entry a of a matrix in diagonal form may be changed to $|a|$. Finally if each non-zero entry of a matrix is the only non-zero entry in its column, then by elementary column operations the matrix may be transformed into a matrix in diagonal form with the gcd of the entries of each row placed in that row and some column, a distinct column for each distinct row. The gcd of a set of integers N may be defined inductively by

(1) $\gcd(\emptyset) = 0$;

(2) for any integer a $\gcd(a,0) = |a|$ and

(3) if $N = N_1 \cup N_2$ then $\gcd(N) = \gcd(\gcd N_1, \gcd N_2)$.

For uniformity of some formulae it is convenient to introduce the integer indexed sequence of non-negative $\underline{\text{extended torsion numbers}}$ $\overline{\tau}(G) = \{\overline{\tau}_i(G) \mid i \text{ an integer}\}$ which contains all the information given by $\beta(G)$ and $\tau(G) = \{\tau_1(G), \ldots, \tau_n(G)\}$ and has the added property that

$$A(G) \cong \bigoplus_{i=1}^{\infty} Z_{\overline{\tau}_i(G)}$$

where $Z_{\overline{\tau}_i(G)}$ is the cyclic group of exponent $\overline{\tau}_i(G)$. $\overline{\tau}(G)$ is defined by

$$\overline{\tau}_i(G) = \begin{cases} 0 & \text{for } i \leq \beta(G) \\ \tau_{\beta(G)+n+1-i}(G) & \text{for } \beta(G) < i \leq \beta(G) + n \\ 1 & \text{for } \beta(G) + n < i \ . \end{cases}$$

CHAPTER 2 THE GROUPS H(i,j)

Section 1. Some properties of the groups H(i,j)

(i) H(i,j) is the third term in an exact sequence

$$1 \to N \to H(i,j) \to Z \to 1$$

where N is free and Z is infinite cyclic;

(ii) the 2-generator subgroups of H(i,j) are free;

(iii) H(i,j) is residually nilpotent, i.e.

$$\bigcap_{c=1}^{\infty} \gamma_c H(i,j) = \{1\} ;$$

where $\gamma_c H(i,j)$ is the c'th term of the lower central series of H(i,j) ;

(iv) $H(i,j)/\gamma_c H(i,j)$ is free nilpotent of class c - 1 on two generators for c = 1,2,... ;

(v) $H(i,j)/H''(i,j)$ is free metabelian on two generators where $H''(i,j)$ is the second derived group of H(i,j) ;

(vi) $\Phi(H(i,j)) = \{1\}$ where $\Phi(H(i,j))$ is the intersection of all the maximal subgroups of H(i,j) ;

(vii) H(i,j) is not free unless i = 0 or j = 0 .

All the properties except (vi) are discussed and an indication of their proofs is given in [1]. (vi) is proven in [3]. All the properties except (vii) are shared by a free group on 2 generators and if i = 0 or j = 0 then H(i,j) is freely generated by b and c . Properties (iii) and (iv) imply that the groups are residually finite. Note also that if $(i',j') = (-i,-j)$ then $H(i',j') \cong H(i,j)$, whether the converse is true when the groups are not free is not known.

Thus we see that the groups are all very much alike, which makes distinguishing their isomorphism classes difficult. Because of properties (iv) and (v) we will not obtain any information about the isomorphism classes from test groups that are either nilpotent or metabelian.

Our course of action is to look at the subgroups of index two in $H(i,j)$ and show that we can restrict our investigation to one of these, $K_1(i,j)$, which often does not satisfy (v). For this subgroup metabelian test groups can distinguish isomorphism classes. We proceed to compute a general formula for the number of epimorphisms of $K_1(i,j)$ onto each number of a large class of finite metabelian groups. Applying the formula for some particular test groups we are able to determine a few classes of the groups $K_1(i,j)$ such that groups in distinct classes differ in the number of epimorphisms onto at least one of the test groups. Thus groups in distinct classes are not isomorphic and as we shall see this induces a similar classification of the groups $H(i,j)$.

Section 2. The subgroups of index 2 in $H(i,j)$

Since the relation matrix of $H(i,j)$ is

$$M(H(i,j)) = (-1,0,0)$$

(the columns are indexed by $a,b,$ and c in that order) we see that $A(H(i,j))$ is the free abelian group generated by $bH'(i,j)$ and $cH'(i,j)$. Thus there are exactly three subgroups of index 2 :

$$K_1(i,j) = gp(b^2,c,H'(i,j))$$

$$K_2(i,j) = gp(b,c^2,H'(i,j))$$

$$K_3(i,j) = gp(bc,c^2,H'(i,j)) .$$

At this point we can state

Theorem 2.1. $K_2(i,j) \cong K_3(i,j)$ for all i and j.

This is proven by using the method of Reidemeister and Schreier to find presentations for the groups. We postpone the computations until after a discussion of its immediate consequence.

Corollary 2.2. If $H(i,j) \cong H(i',j')$ then $K_n(i,j) \cong K_n(i',j')$ for $n = 1,2$ or 3.

Proof. By the hypothesis $K_n(i,j) \cong K_{n\pi}(i',j')$ where π is a permutation on $\{1,2,3\}$. If $1\pi = 1$ then $K_1(i,j) \cong K_1(i',j')$. Furthermore $2\pi \in \{2,3\}$ so $K_2(i,j) \cong K_{2\pi}(i',j') \cong K_2(i',j')$ by the theorem and similarly for $n = 3$. If $1\pi \in \{2,3\}$ and m is the element in $\{2,3\}$ not equal to 1π then $m\pi^{-1} \in \{2,3\}$ and $K_1(i,j) \cong K_{1\pi}(i',j') \cong K_m(i',j') \cong K_{m\pi^{-1}}(i,j) \cong K_2(i,j) \cong K_3(i,j)$. In a similar manner the $K_n(i',j')$ are all isomorphic to one another hence each subgroup of index two in $H(i,j)$ is isomorphic to all the

subgroups of index two in $H(i',j')$ proving the corollary in this case also.

Thus $K_1(i,j) \ncong K_1(i',j')$ implies that $H(i,j) \ncong H(i',j')$ and hence in the sequel when we distinguish non-isomorphic $K_1(i,j)$'s we are also distinguishing non-isomorphic $H(i,j)$'s . The reasons we choose $K_1(i,j)$ are first that we can write down its presentation uniformly for all i and j and secondly that $K_2(i,j)$ shares with $H(i,j)$ all properties of $H(i,j)$ listed in Section 1 (except that in (iv) and (v) two generators must be changed to read three generators) whereas $K_1(i,j)$ shares all the properties (similarly modified) with the important exception in some cases of (v).

The presentation of $K_1(i,j)$ is obtained in

Lemma 2.3. $K_1(i,j) = (u,v,w,x,y;\ x^{-1}[u^i,xu^{-j}v^j][w,v^{-j}]u^j, y^{-1}[v^i,yv^{-j}u^j])$.

Proof. Choose as a Schreier system $\{1,b\}$, then $K_1(i,j)$ is generated by a, bab^{-1}, b^2, c and bcb^{-1} . The relators when rewritten in terms of the generators are

$$a^{-1}[c^i,a]c^{-j}(b^2)^{-1}(bcb^{-1})^j b^2 \quad \text{and}$$

$$(bab^{-1})^{-1}[(bcb^{-1})^i, bab^{-1}](bcb^{-1})^{-j}c^j$$

corresponding to $a^{-1}[c^i,a][c^j,b]$ and $ba^{-1}[c^i,a][c^j,b]b^{-1}$ respectively. We get the required presentation by setting:

$$u = c\ ;$$

$$v = bcb^{-1}\ ;$$

$$w = b^2\ ;$$

$$x = a(bcb^{-1})^{-j}c^j \quad \text{and}$$

$$y = bab^{-1}c^{-j}(bcb^{-1})^j\ .$$

Theorem 2.1 is a consequence of the next four lemmas, each of which gives a presentation of $K_2(i,j)$ and $K_3(i,j)$ for various values of i and j modulo 2. In all cases we choose $\{1,c\}$ as a Schreier system for $K_n(i,j)$ in $H(i,j)$ and we see that

$$K_2(i,j) = gp(a,cac^{-1},b,cbc^{-1},c^2) \quad \text{and}$$

$$K_3(i,j) = gp(a,cac^{-1},cb,bc^{-1},c^2) .$$

Lemma 2.4. If $i = 2n$ and $j = 2m$ then

$K_2(i,j) \cong K_3(i,j) = (u,v,w,x,y;\ u^{-1}[w^n,u][w^m,x], v^{-1}[w^n,v][w^m,y])$.

Proof. The relators $a^{-1}[c^i,a][c^j,b]$ and $ca^{-1}[c^i,a][c^j,b]c^{-1}$ when rewritten in terms of the generators are

$$a^{-1}[(c^2)^n,a][(c^2)^m,b] \quad \text{and}$$

$$(cac^{-1})^{-1}[(c^2)^n,cac^{-1}][(c^2)^m,cbc^{-1}]$$

respectively for $K_2(i,j)$ and

$$a^{-1}[(c^2)^n,a][(c^2)^m,cb] \quad \text{and}$$

$$(cac^{-1})^{-1}[(c^2)^n,cac^{-1}][(c^2)^m,bc^{-1}]$$

respectively for $K_3(i,j)$. The result now follows by setting $u = a$, $v = cac^{-1}$, $w = c^2$, for K_2 $x = b$ and $y = cbc^{-1}$ and for K_3 $x = cb$ and $y = bc^{-1}$.

Lemma 2.5. If $i = 2n$ and $j = 2m + 1$ then

$K_2(i,j) \cong K_3(i,j) = (u,v,w,x,y;\ u^{-1}[w^n,u]w^{-m-1}y^{-1}w^{m+1}x,$

$v^{-1}[w^m,v]w^{-m}x^{-1}w^m y)$.

Proof. The rewritten relators are for K_2 and K_3 respectively:

$$a^{-1}[(c^2)^n,a](c^2)^{-m-1}(cbc^{-1})^{-1}(c^2)^{m+1}b \ ,$$

$$(cac^{-1})^{-1}[(c^2)^n,cac^{-1}](c^2)^{-m}b^{-1}(c^2)^m cbc^{-1} \quad \text{and}$$

$$a^{-1}[(c^2)^n,a](c^2)^{-m-1}(bc^{-1})^{-1}(c^2)^m cb \ ,$$

$$(cac^{-1})^{-1}[(c^2)^n,cac^{-1}](c^2)^{-m}(cb)^{-1}(c^2)^{m+1}bc^{-1} \ .$$

The required result follows by setting $u = a$, $v = cac^{-1}$, $w = c^2$, for K_2 $x = b$ and $y = cbc^{-1}$ and for K_3 $x = cb$ and $y = c^2bc^{-1}$.

Lemma 2.6. If $i = 2n + 1$ and $j = 2m$ then
$K_2(i,j) \cong K_3(i,j) = (u,v,w,x,y;\ u^{-1}w^{-n-1}v^{-1}w^{n+1}u[w^m,x],$
$v^{-1}w^{-n}u^{-1}w^n v[w^m,y])$.

Proof. The rewritten relators are for K_2 and K_3 respectively:

$$a^{-1}(c^2)^{-n-1}(cac^{-1})^{-1}(c^2)^{n+1}a[(c^2)^m,b] \ ,$$

$$(cac^{-1})^{-1}(c^2)^{-n}a^{-1}(c^2)^n cac^{-1}[(c^2)^m,cbc^{-1}] \quad \text{and}$$

$$a^{-1}(c^2)^{-n-1}(cac^{-1})^{-1}(c^2)^{n+1}a[(c^2)^m,cb] \ ,$$

$$(cac^{-1})^{-1}(c^2)^{-n}a^{-1}(c^2)^n cac^{-1}[(c^2)^m,bc^{-1}] \ .$$

The required result follows by setting $u = a$, $v = cac^{-1}$, $w = c^2$, for K_2 $x = b$ and $y = cbc^{-1}$ and for K_3 $x = cb$ and $y = bc^{-1}$.

Lemma 2.7. If $i = 2n + 1$ and $j = 2m + 1$ then
$K_2(i,j) \cong K_3(i,j) = (u,v,w,x,y;\ u^{-1}w^{-n-1}v^{-1}w^{n+1}uw^{-m-1}y^{-1}w^{m+1}x,$
$v^{-1}w^{-n}u^{-1}w^n vw^{-m}x^{-1}w^m y)$.

Proof. The rewritten relators are for K_2 and K_3 respectively:

$$a^{-1}(c^2)^{-n-1}(cac^{-1})^{-1}(c^2)^{n+1}a(c^2)^{-m-1}(cbc^{-1})^{-1}(c^2)^{m+1}b \ ,$$

$$(cac^{-1})^{-1}(c^2)^{-n}a^{-1}(c^2)^n cac^{-1}(c^2)^{-m}b^{-1}(c^2)^m cbc^{-1} \quad \text{and}$$

$$a^{-1}(c^2)^{n-1}(cac^{-1})^{-1}(c^2)^{n+1}a(c^2)^{-m-1}(bc^{-1})^{-1}(c^2)^m cb \ ,$$

$$(cac^{-1})^{-1}(c^2)^{-n}a^{-1}(c^2)^n cac^{-1}(c^2)^{-m}(cb)^{-1}(c^2)^{m+1}bc^{-1} \ .$$

The required results follow by setting $u = a$, $v = cac^{-1}$, $w = c^2$, for K_2 $x = b$ and $y = cbc^{-1}$ and for K_3 $x = cb$ and $y = c^2bc^{-1}$.

Section 3. The metabelian test groups

As test groups we use the non-abelian subgroups of the holomorph of a cyclic group of prime order q. Their derived groups are cyclic of order q, the factor derived groups are cyclic of order p where p divides $q - 1$ (p is not necessarily a prime). Hence the notation Z_qZ_p. Z_qZ_p has the presentation

$$(a,b;\ a^p, b^q, a^{-1}bab^{-\beta})$$

where $\beta^p = 1 \bmod q$, but $\beta^x \not\equiv 1 \bmod q$ for $x \in \{1,\ldots,p-1\}$. It follows that every element in Z_qZ_p can be written in the form a^sb^t where $s \in \{0,1,\ldots,p-1\}$ and $t \in \{0,1,\ldots,q-1\}$.

Note that the exponents of b may be thought of as lying in the field of q elements so it is meaningful to write the inverse of non-zero exponents, e.g. $b^{\beta^{-1}}$.

The following theorems concern some properties of the group Z_qZ_p which will be useful in the sequel.

Theorem 3.1. (i) $a^mb^n \cdot a^sb^t = a^{m+s}b^{n\beta^s+t}$;

(ii) $(a^sb^t)^n = a^{ns}b^{t(1-\beta^{ns})(1-\beta^s)^{-1}}$ for $s \not\equiv 0$;

(iii) $(a^sb^t)^{-1} = a^{-s}b^{-t\beta^{-s}}$;

(iv) $(a^sb^t)^{-1} \cdot a^mb^n \cdot a^sb^t = a^mb^{(1-\beta^m)t+n\beta^s}$;

(v) $[a^mb^n, a^sb^t] = b^{(1-\beta^m)t-(1-\beta^s)n}$.

Proof. (i) $a^mb^n \cdot a^sb^t = a^{m+s} \cdot (a^{-s}ba^s)^n \cdot b^t$ and $a^{-s}ba^s = a^{1-s}b^{\beta^s}a^{s-1} = (a^{1-s}ba^{s-1})^\beta$ and the result follows inductively.

(ii) By applying (i) repeatedly we have $(a^s b^t)^n = a^{ns} b^t(\beta^{s(n-1)} + \ldots + \beta^s + 1)$. Clearly $(1 - \beta^s)(1 + \beta^s + \ldots + \beta^{s(n-1)}) = 1 - \beta^{sn}$ proving the result.

(iii) This follows easily by applying (i) to compute $a^{-s} b^{-t\beta^{-s}} \cdot a^s b^t$.

(iv) Follows easily from (i) and (iii).

(v) Follows easily from (i) and (iv).

Corollary 3.2. For $s \neq 0$ the order of $a^s b^t$ is $p(\gcd(s,p))^{-1}$.

Proof. This follows easily from (ii) of Theorem 3.1.

Theorem 3.3. Aut $Z_q Z_p = \{\alpha_{\rho,\sigma} \mid a\alpha_{\rho,\sigma} = ab^\rho, b\alpha_{\rho,\sigma} = b^\sigma$, $\rho = 0,1,\ldots,q-1$ and $\sigma = 1,\ldots,q-1\}$.

Proof. It is clear that ab^ρ and b^σ generate $Z_q Z_p$. Furthermore by applying Theorem 3.1 and its corollary it is not difficult to see that ab^ρ and b^σ satisfy the necessary relators: $(ab^\rho)^p = 1$, $(b^\sigma)^q = 1$ and $(ab^\rho)^{-1} \cdot b^\sigma \cdot ab^\rho \cdot b^{-\beta\sigma} = b^{(1-\beta^0)\rho + \sigma\beta^1} \cdot b^{-\beta\sigma} = b^{\beta\sigma} \cdot b^{-\beta\sigma} = 1$. This shows that all the maps in question do extend to automorphisms in the natural way. It remains to show that these are the only maps.

Let $\alpha \in$ Aut $Z_q Z_p$ then it is clear that $b\alpha \in gp(b)$; let $b\alpha = b^\sigma$, $\sigma \neq 0$. Suppose $a\alpha = a^s b^\rho$ then we must have

$$\begin{aligned} 1 &= (a^{-1} bab^{-\beta})\alpha \\ &= [a^s b^\rho, b^{-\sigma}] b^{(1-\beta)\sigma} \\ &= b^{\sigma(\beta^s - \beta)} . \end{aligned}$$

This implies that $s = 1$ and concludes the proof of the theorem.

If θ is an epimorphism of a group G onto $Z_q Z_p$ then $\{\theta\alpha | \alpha \in \text{Aut } Z_q Z_p\}$ is a set of $q(q-1)$ distinct epimorphisms of G onto $Z_q Z_p$. Thus we may count all the epimorphisms of G onto $Z_q Z_p$ by counting one from each set and multiplying the result by $q(q-1)$.

Section 4. The main result and Theorem A

Our main result, Theorem 4.1, is just a formula for computing the number of epimorphisms of $K_1(i,j)$ onto $Z_q Z_p$. The proof is postponed until Section 5. We specialize this theorem in numerous corollaries until we obtain enough information to prove Theorem A of the introduction.

Theorem 4.1. The number of epimorphisms of $K_1(i,j)$ onto $Z_q Z_p$ is $q(q-1)$ times

$$(q+1)(3|S_1| + 3|S_2| + |S_3|) +$$

$$2q^2(|T_1(i,j)| + |T_2(i,j)|)\delta(j) +$$

$$q^2(|V_2(i,j) \cup V_2^{-1}(i,j)| + |V_3(i,j) \cup V_3^{-1}(i,j)|) +$$

$$q^3(|V_2(i,j) \cap V_2^{-1}(i,j)| + |V_3(i,j) \cap V_3^{-1}(i,j)|) ,$$

where:

$$S_n = \{(s_1,\ldots,s_n) \mid gp(a^{s_1},\ldots,a^{s_n}) = gp(a) \text{ and } s_k = 1,\ldots,p-1\} ;$$

$$T_n(i,j) = \{(s_1,\ldots,s_n) \in S_n \mid (1 - \beta^{s_1 i})\beta^{-s_1 j} = 1 \bmod q\} ;$$

$$U_n(i,j) = \{(s_1,\ldots,s_n) \in S_n \mid (1 - \beta^{s_1 i})\beta^{j(s_2 - s_1)} = 1 \bmod q\} ;$$

$$V_n(i,j) = T_n(i,j) \cap U_n(i,j) ;$$

$$X^{-1} = \{(s_2,s_1,\ldots,s_n) \mid (s_1,s_2,\ldots,s_n) \in X\} ;$$

$\delta(j) = 1$ if $j = 0 \bmod q$ and 0 otherwise.

Corollary 4.2. The number of epimorphisms of $K_1(i,j)$ onto $Z_q Z_2$ is $7(q^3 - q)$ unless $q = 3$, $i = 1 \bmod 2$ and $j = 3 \bmod 6$ when it is 384. (Note that $7(q^3 - q) = 168$ when $q = 3$).

Proof. We must first compute the parameters which enter into the formula given in Theorem 4.1.

$$S_1 = \{1\},\ S_2 = \{(1,1)\} \text{ and } S_3 = \{(1,1,1)\} .$$

$\beta = q - 1$ and $(1 - \beta^x)\ \beta^{-y} = 1 \bmod q$ iff $x = 1 \bmod 2$, $y = 1 \bmod 2$ and $(2 - q)(q - 1) = 1 \bmod q$. The last equation implies that $-2 = 1 \bmod q$ and indeed that $q = 3$.

Thus for $q \neq 3$ we have $T_n(i,j) = U_n(i,j) = V_n(i,j) = \emptyset$ for all n,i and j. The only contribution to the number of epimorphisms is from line 1 of the formula,

$$q(q - 1)(q + 1)\ \ (3\cdot 1 + 3\cdot 1 + 1) ,$$

proving the result in this case.

For $q = 3$ we have $T_n(i,j) = S_n$ for i and $j = 1 \bmod 2$, all n and $T_n(i,j) = \emptyset$ otherwise. In addition $U_n(i,j) = V_n(i,j) = \emptyset$ for all n,i and j. Thus in addition to the number of epimorphisms contributed by line 1, when $j = 0 \bmod 3$ we have from line 2,

$$3\cdot(3 - 1)\cdot 2\cdot 3^2\cdot(1 + 1)\cdot 1 = 216 .$$

This concludes the proof of the Corollary.

Corollary 4.3. The number of epimorphisms of $K_1(i,j)$ onto Z_5Z_4 is 20 times the sum of 336 and

200 for $i = 1 \bmod 4$ and $j = 2,5,6,14$ or $18 \bmod 20$
or $i = 2 \bmod 4$ and $j = 5$ or $15 \bmod 20$
or $i = 3 \bmod 4$ and $j = 2,6,14,15$ or $18 \bmod 20$

400 for $i = 1 \bmod 2$ and $j = 10 \bmod 20$

0 otherwise.

Proof. $S_1 = \{1,3\}$;

$S_2 = \{(1,z),(2,1),(2,3),(3,z) \mid z \in \{1,2,3\}\}$;

$S_3 = \{(x,y,z),(2,2,1),(2,2,3) \mid (x,y) \in S_2,\ z \in \{1,2,3\}\}$.

$\beta = 2$ and $(1 - \beta^x)\ \beta^{-y} = 1 \bmod 5$ iff

$(x,y) \in \{(1,2),(2,1),(3,3) \bmod 4\}$.

$T_n(i,j) = \{(s_1,\ldots,s_n) \in S_n \mid s_1 = 1\}$ for $(i,j) \in \{(1,2),(2,1),(3,3) \bmod 4\}$;

$= \{(s_1,\ldots,s_n) \in S_n \mid s_1 = 3\}$ for $(i,j) \in \{(1,1),(2,3),(3,2) \bmod 4\}$;

$= \emptyset$ otherwise.

$U_2(i,j)$ is given by the entries in the following table:

	0	1	2	3	= j mod 4
0	∅	∅	∅	∅	
1	∅	(1,3),(2,1)	(1,2)	(1,3),(2,3),(3,2)	
2	∅	(3,2)	∅	(1,2)	
3	∅	(1,2),(2,1),(3,1)	(3,2)	(2,3),(3,1)	

= i mod 4

$U_3(i,j)$ arises from $U_2(i,j)$ by replacing each entry (x,y) with three entries $(x,y,1),(x,y,2)$ and $(x,y,3)$.

$V_2(i,j) = \{(1,2)\}$ for $(i,j) = (1,2) \bmod 4$;

$= \{(3,2)\}$ for $(i,j) = (3,2) \bmod 4$;

$= \emptyset$ otherwise.

$V_3(i,j)$ arises from $V_2(i,j)$ just as $U_3(i,j)$ arose from $U_2(i,j)$.

The result follows by entering the above parameters in the formula given in Theorem 4.1.

Corollary 4.4. The number of epimorphisms of $K_1(i,j)$ onto Z_7Z_3 is 8,736 unless $i = 1 \bmod 3$ and $j = 7 \bmod 21$ or $i = 2 \bmod 3$ and $j = 14 \bmod 21$ when it is 21,084 .

Proof. $S_n = \{(s_1,\ldots,s_n) \mid s_i \in \{1,2\}\}$.

$\beta = 2$ and $(1 - \beta^x)\,\beta^{-y} = 1 \bmod 7$ iff x and $y = 2 \bmod 3$.

$T_n(i,j) = \{(s_1,\ldots,s_n) \in S_n \mid s_1 = 1\}$ for $(i,j) = (2,2) \bmod 3$;

$= \{(s_1,\ldots,s_n) \in S_n \mid s_1 = 2\}$ for $(i,j) = (1,1) \bmod 3$;

$= \emptyset$ otherwise.

$U_n(i,j) = \{(s_1,\ldots,s_n) \in S_n \mid s_1 = 1,\ s_2 = 2\}$ for $(i,j) = (2,1) \bmod 3$;

$= \{(s_1,\ldots,s_n) \in S_n \mid s_1 = 2,\ s_2 = 1\}$ for $(i,j) = (1,2) \bmod 3$;

$= \emptyset$ otherwise.

$V_n(i,j) = \emptyset$ all n,i and j .

The result follows by entering the above parameters in the formula given in Theorem 4.1.

Corollary 4.5. The number of epimorphisms of $K_1(i,j)$ onto Z_7Z_6 is 42 times the sum of 1,456 and 294 times

0 for i and j not mentioned below

1 for $i = 1$ or $4 \bmod 6$ and $j = 7 \bmod 42$

or $i = 2$ or $5 \bmod 6$ and $j = 35 \bmod 42$

2 for $i = 1$ or $3 \bmod 6$ and $j = 4,10,16,22,34$ or $40 \bmod 42$

or $i = 3$ or $5 \bmod 6$ and $j = 2,8,20,26,32$ or $38 \bmod 42$

3 for $i = 1 \bmod 6$ and $j = 28 \bmod 42$

or $i = 5 \bmod 6$ and $j = 14 \bmod 42$

4 for $i = 1 \bmod 6$ and $j = 35 \bmod 42$

or $i = 2 \bmod 6$ and $j = 2,3,8,9,15,20,26,27,32,33,38$ or $39 \bmod 42$

or $i = 3 \bmod 6$ and $j = 14$ or $28 \bmod 42$

or $i = 4 \bmod 6$ and $j = 3,4,9,10,15,16,22,27,33,34,39$ or $40 \bmod 42$

or $i = 5 \bmod 6$ and $j = 7 \bmod 42$

6 for $i = 2$ or $4 \bmod 6$ and $j = 21 \bmod 42$

7 for $i = 2 \bmod 6$ and $j = 14 \bmod 42$

or $i = 4 \bmod 6$ and $j = 28 \bmod 42$

(The classification of the groups given by this corollary includes that given by Corollary 4.4., see 1,3 and 7 above.)

Proof. $S_1 = \{1,5\}$;

$$S_2 = \{(x,z),(3,1),(3,2),(3,4),(3,5) \mid x \in S_1,\ z \in \{1,\ldots,5\}\} \cup (\{2,4\} \times \{1,3,5\}) ;$$

$$S_3 = \{(x,y,z),(3,3,1),(3,3,2),(3,3,4),(3,3,5) \mid (x,y) \in S_2,\ z \in \{1,\ldots,5\}\} \cup (\{2,4\} \times \{2,4\} \times \{1,3,5\}) ;$$

$\beta = 3$ and $(1 - \beta^x)\ \beta^{-y} = 1 \bmod 7$ iff $(x,y) \in \{(1,5),(2,3),(3,2),(4,4),(5,1) \bmod 6\}$.

$$T_1(i,j) = \{1,5\} \text{ for } (i,j) = (1,5) \text{ or } (5,1) \bmod 6$$
$$= \{1\} \text{ for } (i,j) = (2,3),(3,2) \text{ or } (4,4) \bmod 6$$
$$= \{5\} \text{ for } (i,j) = (2,2),(3,4) \text{ or } (4,3) \bmod 6$$
$$= \emptyset \text{ otherwise.}$$

$T_2(i,j)$ arises from $T_1(i,j)$ by replacing each element x with five elements (x,z), $z \in \{1,\ldots,5\}$, adding elements $(2,1),(2,3)$ and $(2,5)$ when $(i,j) \in \{(2,2),(5,2),(2,5),(5,5) \bmod 6\}$, and adding elements $(4,1),(4,3)$ and $(4,5)$ when

$(i,j) \in \{(1,1),(4,1),(1,4),(4,4) \bmod 6\}$. $T_3(i,j)$ arises from $T_2(i,j)$ by replacing each element (x,y) with five elements (x,y,z), $z \in \{1,\ldots,5\}$.

$U_2(i,j)$ is given by the entries in the following table:

	0	1	2	3	4	5
0	ø	ø	ø	ø	ø	ø
1	ø	(1,2),(2,5) (3,1),(5,4)	(3,2),(3,5),(4,5)	(2,1),(2,3),(2,5)	(3,1),(3,4),(4,3)	(2,5),(3,5)
2	ø	(1,4) (4,1),(5,1)	(2,3),(5,3)	(1,2),(1,4) (4,1),(4,3),(4,5)	(2,1),(5,1),(5,4)	(1,4) (4,1),(5,3)
3	ø	(1,5) (3,1),(5,3)	(1,3),(3,2) (3,5),(5,1),(5,4)	ø	(1,2),(1,5) (3,1),(3,4),(5,3)	(1,3) (3,5),(5,1)
4	ø	(1,3) (2,5),(5,2)	(1,2),(1,5),(4,5)	(2,1),(2,3) (2,5),(5,2),(5,4)	(1,3),(4,3)	(1,5) (2,5),(5,2)
5	ø	(3,1),(4,1)	(2,3),(3,2),(3,5)	(4,1),(4,3),(4,5)	(2,1),(3,1),(3,4)	(1,2),(3,5) (4,1),(5,4)

= j mod 6

= i mod 6

$U_3(i,j)$ arises from $U_2(i,j)$ by replacing each entry (x,y) with five entries (x,y,z), $z \in \{1,\ldots,5\}$, adding entries $(2,4,1)$, $(2,4,3)$ and $(2,4,5)$ when $(i,j) \in \{(2,1),(2,4),(5,1),(5,4) \bmod 6\}$ and entries $(4,2,1),(4,2,3)$ and $(4,2,5)$ when $(i,j) \in \{(1,2),(1,5),(4,2),(4,5) \bmod 6\}$.

$V_2(i,j)$ is given by the entries in the following table:

	0	1	2	3	4	5	$= j \bmod 6$
0	∅	∅	∅	∅	∅	∅	
1	∅	∅	∅	∅	(4,3)	∅	
2	∅	∅	(2,3),(5,3)	(1,2),(1,4)	∅	∅	
3	∅	∅	(1,3)	∅	(5,3)	∅	
4	∅	∅	∅	(5,2),(5,4)	(1,3),(4,3)	∅	
5	∅	∅	(2,3)	∅	∅	∅	

$= 1 \bmod 6$

$V_3(i,j)$ arises from $V_2(i,j)$ by replacing each entry (x,y) with five entries (x,y,z), $z \in \{1,\ldots,5\}$.

The result follows by entering the above parameters in the formula given in Theorem 4.1.

We are now in a position to prove Theorem A which we restate here for convenience. "The groups $H(i,j)$ are all distinct for (i,j) in the set $\{(1,1),(1,2),(1,3),(1,4),(1,7),(1,10),(2,2),(2,14),(2,15),(2,21),(3,2),(3,15),(5,10),(5,14)\}$."

Indeed by Corollary 4.5 if $H(i,j) \cong H(i',j')$ and (i,j) and (i',j') are both in the above set then either they are equal or they are both in one of the following sets:

$\{(1,1),(1,2),(1,3),(3,15),(5,10\}$,

$\{(1,4),(1,10),(3,2)\}$,

$\{(2,2),(2,15)\}$.

Applying Corollary 4.3 we divide all these sets up into singletons except $\{(1,1),(1,3)\}$ and $\{(1,2),(3,15)\}$. The result follows by applying Corollary 4.2.

Section 5. The proof of Theorem 4.1

It is convenient to consider various cases separately. Let η be the natural map of $Z_q Z_p$ onto Z_p. If θ is an epimorphism of $K_1(i,j)$ onto $Z_q Z_p$ then $\theta\eta$ is an epimorphism of $K_1(i,j)$ onto Z_p. We will have one subcase for each epimorphism onto Z_p. In order to do this we need the very easy to prove

Lemma 5.1. The number of epimorphisms of $K_1(i,j)$ onto Z_p is $3|S_1| + 3|S_2| + |S_3|$ for all i,j.

Proof. Modulo $K_1'(i,j)$, $K_1(i,j)$ is free abelian on three generators, $uK_1'(i,j)$, $vK_1'(i,j)$ and $wK_1'(i,j)$. Clearly there are $3|S_1|$ maps when two of the generators map trivially, $3|S_2|$ maps when only one of the generators maps trivially and $|S_3|$ when none of them map trivially, proving the lemma.

We now give formal labels to the various cases. It is convenient to assume that $Z_p = gp(a)$ in $Z_q Z_p$.

Definition 5.2. If θ is an epimorphism of $K_1(i,j)$ onto $Z_q Z_p$ then θ belongs to case:

I(s) iff $u\theta\eta = v\theta\eta = 1$, $w\theta\eta = a^s$, $s \in S_1$;

II(s) iff $u\theta\eta = a^s$, $v\theta\eta = w\theta\eta = 1$, $s \in S_1$;

III(s) iff $u\theta\eta = 1$, $v\theta\eta = a^s$, $w\theta\eta = 1$, $s \in S_1$;

IV(s,t) iff $u\theta\eta = 1$, $v\theta\eta = a^s$, $w\theta\eta = a^t$, $(s,t) \in S_2$;

V(s,t) iff $u\theta\eta = a^s$, $v\theta\eta = 1$, $w\theta\eta = a^t$, $(s,t) \in S_2$;

VI(s,t) iff $u\theta\eta = a^s$, $v\theta\eta = a^t$, $w\theta\eta = 1$, $(s,t) \in S_2$;

VII(s,t,r) iff $u\theta\eta = a^s$, $v\theta\eta = a^t$, $w\theta\eta = a^r$, $(s,t,r) \in S_3$.

For each θ belonging to a given case there is a unique ordered set of five integers between 0 and $q-1$, $(k_1,\ldots,k_5)$ such that:

$$u\theta = u\theta\eta b^{k_1},\ v\theta = v\theta\eta b^{k_2},\ w\theta = w\theta\eta b^{k_3},$$

$$x\theta = b^{k_4},\ y\theta = b^{k_5}.$$

It is our task to count the number of such sets in each case.

For each case there is a unique map, φ, of $\{u,v,w\}$ onto Z_p such that θ is covered by that case iff $\theta\eta$ restricted to $\{u,v,w\}$ equals φ.

Lemma 5.3. Given an arbitrary set $(k_1,\ldots,k_5)$ there will exist an epimorphism θ of $K_1(i,j)$ onto Z_qZ_p satisfying:

$$u\theta = u\varphi b^{k_1},\ v\theta = v\varphi b^{k_2},\ w\theta = w\varphi b^{k_3},\ x\theta = b^{k_4},\ y\theta = b^{k_5} \tag{1}$$

if and only if at least one of the k_i's is not 0 and they satisfy the following two equations:

$$\begin{aligned} b^{k_4} &= [(u\varphi b^{k_1})^i, b^{k_4}(u\varphi b^{k_1})^{-j}(v\varphi b^{k_2})^j][w\varphi b^{k_3}, (v\varphi b^{k_2})^{-j}](u\varphi b^{k_1})^j, \\ b^{k_5} &= [(v\varphi b^{k_2})^i, b^{k_5}(v\varphi b^{k_2})^{-j}(u\varphi b^{k_1})^j] \end{aligned} \tag{2}$$

Proof. We must show that the map θ of $\{u,v,w,x,y\}$ into Z_qZ_p defined by the equations (1) extends to an epimorphism of $K_1(i,j)$ onto Z_qZ_p. Indeed since $\{u,v,w,x,y\}$ generates $K_1(i,j)$, the condition that one of the k_i's not be zero is necessary and sufficient to imply that the images of $\{u,v,w,x,y\}$ generates Z_qZ_p. Equations (2) are just the condition that the images satisfy the relators of $K_1(i,j)$ (see Lemma 2.3).

We now turn to the process of selecting from each set $\{\theta\alpha \mid \alpha \in \text{Aut } Z_q Z_p\}$ of homomorphisms of $K_1(i,j)$ onto $Z_q Z_p$ a unique one. First of all one of $\{u\theta, v\theta, w\theta\}$ must be of the form $a^s b^k$ with $s \neq 0$. By applying an automorphism $\alpha_{\rho,\sigma}$ where $\rho = -\sigma k(1 - \beta)(1 - \beta^s)^{-1} \bmod q$, we may choose $k = 0$. Among the images of the remainder of the generators of $K_1(i,j)$ there must be one of the form $a^t b^k$ with $k \neq 0$. This time we want to apply only automorphisms $\alpha_{\rho,\sigma}$ which leave a^s fixed. That is, we require that $\rho = 0$. By applying $\alpha_{0,k-1}$ we may choose $k = 1$. Now the only automorphism which leaves both a^s and $a^t b$ fixed is $\alpha_{0,1}$ -- the identity automorphism.

It follows that we can select the required unique homomorphism by the following process. The process depends only on the case we are in.

(1) Select $z \in \{u,v,w\}$ such that $z\varphi \neq 1$.

(2) Consider only $(k_1,\ldots,k_5)$'s such that $k_\ell = 0$ where $\ell = 1,2,3$ according as $z = u,v,w$.

(3) Consider only $(k_1,\ldots,k_5)$'s such that $k_\ell = 1$ where ℓ is the least m for which $k_m \neq 0$.

Our analysis of each case, X, is further divided up into $q + 2$ subcases, $X_A, X_B, X_0, \ldots, X_{q-1}$, according to the possible values of k_1, k_2 and k_3. For subcase X_A we allow only $k_1 = k_2 = k_3 = 0$. For subcase X_B we have $k_1 = k_2 = 0$ and $k_3 = 1$ except for $I(s)_B$ where $k_1 = k_3 = 0$ and $k_2 = 1$. For subcase X_k we have $k_3 = k$ except for $I(s)_k$ where $k_3 = 0$. Furthermore $k_1 = 0$ except for $I(s)_k$, $III(s)_k$ and $IV(s,t)_k$ where $k_1 = 1$. Finally, for $I(s)_k$, $k_2 = k$, for $III(s)_k$ and $IV(s,t)_k$ we have $k_2 = 0$ otherwise $k_2 = 1$.

It is important to notice that the subcases are, except for A , set up to insure that $(k_1,\ldots,k_5)$ satisfies the selection criteria. For subcase A , the criteria becomes: either $k_4 = 1$ or $k_4 = 0$ and $k_5 = 1$.

The proof of Theorem 4.1 is an easy consequence of the next seven lemmas. Each lemma takes care of a different set of cases.

Lemma 5.4. The number of solutions for cases I(s), $s \in S_1$ is $(q + 1)|S_1|$.

Proof. Equations (2) become

$$b^{k_4} = [a^s, b^{-jk_2}]b^{jk_1} \quad \text{and}$$

$$b^{k_5} = 1 .$$

Thus for each s and each subcase there is a unique solution for k_4 and k_5 . In particular for subcase A we have $k_4 = k_5 = 0$ which does not satisfy the criteria. Hence for each $s \in S_1$ and each subcase except A there is one solution, proving the lemma.

Lemma 5.5. The number of solutions for cases II(s), $s \in S_1$ is $(q + 1)|S_1| + q^2|T_1(i,j)|\,\delta(j)$.

Proof. Equations (2) become

$$b^{k_4} = [a^{is}, b^{k_4}a^{-js}b^{jk_2}] = [a^{is}, b^{jk_2}][a^{is}, b^{k_4}]^{a^{-js}}$$

$$b^{k_5} = [b^{ik_2}, b^{k_5 - jk_2}a^{js}] = [b^{ik_2}, a^{js}]$$

Thus for each s and each subcase there is a unique solution for k_5 . In particular for subcase A we have $k_5 = 0$.

From the first equation we have

$$b^{k_4} = b^{(1-\beta^{is})(jk_2 + k_4\beta^{-js})} .$$

Equivalently $k_4(1 - (1 - \beta^{is})\beta^{-js}) = (1 - \beta^{is})jk_2 \bmod q$. Now $s \in T_1(i,j)$ iff $1 - (1 - \beta^{is})\beta^{-js} = 0 \bmod q$ and this in turn implies that $(1 - \beta^{is}) \not\equiv 0 \bmod q$. We now analyze each subcase separately.

Subcase A. $(k_2 = 0)$ We must have $k_4 = 1$. If $s \in T_1(i,j)$ the equation becomes $0 = 0$ so that we have 1 solution. If $s \notin T_1(i,j)$ we have no solutions. In all we have $|T_1(i,j)|$ solutions.

Subcase B. $(k_2 = 0)$ If $s \in T_1(i,j)$ any k_4 in $\{0,1,\ldots,q-1\}$ is a solution. If $s \notin T_1(i,j)$ only $k_4 = 0$ will do. In all we have $|S_1| + (q-1)|T_1(i,j)|$ solutions.

Subcases k. $(k_2 = 1)$ If $s \in T_1(i,j)$ there are q solutions for each of the q k's when $j = 0 \bmod q$, otherwise there are no solutions. If $s \notin T_1(i,j)$ then for each of the q k's there is a unique solution. In all we have $q(|S_1| - |T_1(i,j)|) + q^2|T_1(i,j)|\delta(j)$ solutions.

The lemma follows by adding up the number of solutions in each of the three subcases.

Lemma 5.6. The number of solutions for cases III(s), $s \in S_1$ is $(q+1)|S_1| + q^2|T_1(i,j)|\delta(j)$.

Proof. Equations (2) become

$$b^{k_4} = [b^{ik_1}, b^{k_4 - jk_1}a^{js}][b^{k_3}, a^{-js}] = [b^{ik_1}, a^{js}][b^{k_3}, a^{-js}]$$

$$b^{k_5} = [a^{is}, b^{k_5}a^{-js}b^{jk_1}] = [a^{is}, b^{jk_1}][a^{is}, b^{k_5}]^{a^{-js}} .$$

Thus for each s and each subcase there is a unique solution for k_4 . In particular for subcase A we have $k_4 = 0$. Note that k_1 has the same value in each subcase that k_2 had in Lemma 5.5. It follows that the second equation arises from the first equation in Lemma 5.5 by

changing k_2 and k_4 to k_1 and k_5. The proof of the lemma then follows exactly as that of Lemma 5.5.

Lemma 5.7. The number of solutions for cases IV(s,t), $(s,t) \in S_2$ is $(q+1)|S_2| + q^2|T_2(i,j)|\,\delta(j)$.

Proof. Equations (2) become

$$b^{k_4} = [b^{ik_1}, b^{k_4 - jk_1} a^{js}][a^t b^{k_3}, a^{-js}] = [b^{ik_1}, a^{js}][a^t b^{k_3}, a^{-js}]$$

$$b^{k_5} = [a^{is}, b^{k_5} a^{-js} b^{jk_1}] = [a^{is}, b^{jk_1}][a^{is}, b^{k_5}]^{a^{-js}} .$$

The equations parallel almost exactly those of Lemma 5.6. S_2 and $T_2(i,j)$ are the appropriate analogues of S_1 and $T_1(i,j)$ and the proof follows exactly as those of Lemmas 5.5 and 5.6.

Lemma 5.8. The number of solutions for cases V(s,t), $(s,t) \in S_2$ is $(q+1)|S_2| + q^2|T_2(i,j)|\,\delta(j)$.

Proof. Equations (2) become

$$b^{k_4} = [a^{is}, b^{k_4} a^{-js} b^{jk_2}][a^t b^{k_3}, b^{-jk_2}]^{a^{js}}$$

$$= [a^{is}, b^{jk_2}][a^{is}, b^{k_4}]^{a^{-js}}[a^t, b^{-jk_2}]^{a^{js}}$$

$$b^{k_5} = [b^{ik_2}, b^{k_5 - jk_2} a^{js}] = [b^{ik_2}, a^{js}] .$$

From the first equation we have

$$b^{k_4} = b^{(1-\beta^{is})(jk_2 + k_4\beta^{-js}) + (1-\beta^t)(-jk_2)\beta^{js}}$$

Equivalently $k_4(1 - (1 - \beta^{is})\beta^{-js}) = [(1 - \beta^{is}) - (1 - \beta^t)\beta^{js}]jk_2 \bmod q$. Now $1 - (1 - \beta^{is})\beta^{-js} = 0 \bmod q$ implies that $(1 - \beta^{si}) - (1 - \beta^t)\beta^{js} = \beta^{t+js} \neq 0 \bmod q$. Therefore the proof follows exactly as those of Lemmas 5.5, 5.6 and 5.7.

Lemma 5.9. The number of solutions for cases VI(s,t), $(s,t) \in S_2$ is $(q+1)|S_2| + q^2|V_2(i,j) \cup V_2(i,j)| + q^3|V_2(i,j) \cap V_2^{-1}(i,j)|$.

Proof. We analyze the subcases separately.

Subcase A $(k_1 = k_2 = k_3 = 0)$ Equations (2) become

$$b^{k_4} = [a^{is}, b^{k_4} a^{-js+jt}] = [a^{is}, b^{k_4}]^{aj(t-s)}$$

$$b^{k_5} = [a^{it}, b^{k_5} a^{-jt+js}] = [a^{it}, b^{k_5}]^{aj(s-t)}$$

These equations yield

$$b^{k_4} = b^{(1-\beta^{is})k_4 \beta^{j(t-s)}} \quad \text{and} \quad b^{k_5} = b^{(1-\beta^{it})k_5 \beta^{j(s-t)}}$$

Equivalently $k_4(1 - (1 - \beta^{is})\beta^{j(t-s)}) = 0 \bmod q$ and $k_5(1 - (1 - \beta^{it})\beta^{j(s-t)}) = 0 \bmod q$. We need simultaneous solutions to these equations satisfying the further condition that either $k_4 = 1$ or $k_4 = 0$ and $k_5 = 1$. Note that $(s,t) \in U_2(i,j)$ iff $1 - (1 - \beta^{it})\beta^{j(s-t)} = 0 \bmod q$. Hence if $(s,t) \notin U_2(i,j) \cup U_2(i,j)$ there are no solutions, if $(s,t) \in U_2(i,j) \backslash U_2^{-1}(i,j)$ there is only one solution $k_4 = 1$, $k_5 = 0$, if $(s,t) \in U_2^{-1}(i,j) \backslash U_2(i,j)$ there is only one solution $k_4 = 0$, $k_5 = 1$ and if $(s,t) \in U_2(i,j) \cap U_2^{-1}(i,j)$ there are $q+1$ solutions, $k_4 = 1$, $k_5 = 0,1,\ldots,q-1$ or $k_4 = 0$, $k_5 = 1$. In all there are $|U_2(i,j) \cup U_2^{-1}(i,j)| + q|U_2(i,j) \cap U_2^{-1}(i,j)|$ solutions.

Subcase B $(k_1 = k_2 = 0, k_3 = 1)$. Equations (2) become

$$b^{k_4} = [a^{is}, b^{k_4} a^{-js+jt}][b, a^{-jt}]^{ajt} = [a^{is}, b^{k_4}]^{aj(t-s)}[b, a^{-jt}]^{ajs}$$

$$b^{k_5} = [a^{is}, b^{k_5} a^{-jt+js}] = [a^{it}, b^{k_5}]^{aj(s-t)}$$

The second equation is exactly the same as in subcase A.

From the first equation we get

$$b^{k_4} = b^{(1-\beta^{is})k_4\beta j(t-s)-(1-\beta^{-jt})\beta js} .$$

Equivalently $k_4(1 - (1 - \beta^{is})\beta^{j(t-s)}) = - (1 - \beta^{-jt})\beta^{js} \bmod q$. We must solve this equation and $k_5(1 - (1 - \beta^{it})\beta^{j(s-t)}) = 0 \bmod q$ simultaneously.

Note that $(s,t) \in V_2(i,j) = T_2(i,j) \cap U_2(i,j)$ iff $(1 - (1 - \beta^{is})\beta^{j(t-s)}) = 0 \bmod q$ and $(1 - (1 - \beta^{is})\beta^{-js}) = 0 \bmod q$ which is equivalent to $(1 - (1 - \beta^{is})\beta^{j(t-s)}) = 0 \bmod q$ and $- (1 - \beta^{-jt})\beta^{js} = 0 \bmod q$. Hence if $(s,t) \notin U_2(i,j) \cup U_2^{-1}(i,j)$ there is only one solution, $k_4 = - (1 - \beta^{-jt})\beta^{js}(1 - (1 - \beta^{is})\beta^{j(t-s)})^{-1}$ $(= \mu)$, $k_5 = 0$. If $(s,t) \in U_2(i,j)\backslash V_2(i,j)$ there are no solutions. If $(s,t) \in V_2(i,j)\backslash U_2^{-1}(i,j)$ there are q solutions, $k_4 = 0,1,\ldots,q - 1$, $k_5 = 0$. If $(s,t) \in U_2^{-1}(i,j)\backslash U_2(i,j)$ there are q solutions $k_4 = \mu$, $k_5 = 0,1,\ldots,q - 1$. If $(s,t) \in V_2(i,j) \cap U_2^{-1}(i,j)$ there are q^2 solutions, $k_4 = 0,1,\ldots,q - 1$, $k_5 = 0,1,\ldots,q - 1$. In all there are

$$(|S_2| - |U_2(i,j) \cup U_2^{-1}(i,j)|) + q|V_2(i,j) \backslash U_2^{-1}(i,j)|$$
$$+ q|U_2^{-1}(i,j)\backslash U_2(i,j)| + q^2|V_2(i,j) \cap U_2^{-1}(i,j)| .$$

Subcases k. ($k_1 = 0$, $k_2 = 1$, $k_3 = k$) Equations (2) become

$$b^{k_4} = [a^{is},(a^tb)^j][a^{is},b^{k_4}]^{a^{-js}(a^tb)^j}[b^k,(a^tb)^{-j}]^{ajs}$$

$$b^{k_5} = [(a^tb)^i,a^{js}][(a^tb)^i,b^{k_5}]^{(a^tb)^{-j}ajs} .$$

The corresponding simultaneous equations are

$$k_4(1 - (1 - \beta^{is})\beta^{j(t-s)}) = (1 - \beta^{jt})[(1 - \beta^{is})(1 - \beta^t)^{-1} + k\beta^{j(s-t)}] \bmod q$$

$$k_5(1 - (1 - \beta^{it})\beta^{j(s-t)}) = (1 - \beta^{js})[(1 - \beta^{it})(1 - \beta^t)^{-1}] \bmod q$$

If $(s,t) \notin U_2(i,j) \cup U_2^{-1}(i,j)$ there is one solution for each subcase k, k_4 and k_5 are uniquely determined.

If $(s,t) \in (U_2(i,j)\backslash V_2(i,j)\backslash U_2^{-1}(i,j)$ there are no solutions unless $k = -(1 - \beta^{it})(1 - \beta^{t})^{-1}\beta^{j(t-s)}$, when there are q solutions, $k_4 = 0,1,\ldots,q-1$ and k_5 is uniquely determined. If $(s,t) \in (U_2(i,j)\backslash V_2(i,j)) \cap V_2^{-1}(i,j)$ there are no solutions unless k is as above when there are q^2 solutions, $k_4 = 0,1,\ldots,q-1$, $k_5 = 0,1,\ldots,q-1$. If $(s,t) \in U_2^{-1}(i,j)\backslash V_2^{-1}(i,j)$ there are no solutions. If $(s,t) \in V_2(i,j)\backslash U_2^{-1}(i,j)$ there are q solutions for each k, $k_4 = 0,1,\ldots,q-1$ and k_5 is uniquely determined. If $(s,t) \in V_2^{-1}(i,j)\backslash U_2^{-1}(i,j)$ there are q solutions for each k, k_4 is uniquely determined, $k_5 = 0,1,\ldots,q-1$. Finally if $(s,t) \in V_2(i,j) \cap V_2^{-1}(i,j)$ there are q^2 solutions for each k, $k_4 = 0,1,\ldots,q-1$, $k_5 = 0,1,\ldots,q-1$. In all there are $q(|S_2| - |U_2(i,j) \cup U_2^{-1}(i,j)|) + q|(U_2(i,j)\backslash V_2(i,j))\backslash U_2^{-1}(i,j)| + q^2(|V_2(i,j) \cup V_2^{-1}(i,j)| - |V_2(i,j) \cap U_2^{-1}(i,j)|) + q^3|V_2(i,j) \cap V_2^{-1}(i,j)|$.

The lemma follows by adding up the number of solutions in each of the three subcases.

Lemma 5.10. The number of solutions for cases VII(s,t,r), $(s,t,r) \in S_3$ is $(q+1)|S_3| + q^2|V_3(i,j) \cup V_3^{-1}(i,j)| + q^3|V_3(i,j) \cap V_3^{-1}(i,j)|$.

Proof. This lemma has the same relationship to Lemma 5.9 as Lemma 5.7 and 5.8 have to Lemmas 5.5 and 5.6. Indeed the simultaneous equations of Lemma 5.9 remain unchanged for subcase A and B whereas for subcases k only the entry $(1 - \beta^{is})$ on the right hand side of the equation for k_4 changes to $(1 - \beta^{si}) - (1 - \beta^{r})\beta^{-jt}$ which does not affect the analysis. Therefore the proof follows exactly as that of Lemma 5.9.

CHAPTER 3 THE GROUPS $G(m_1,\ldots,m_t)$

Section 1. Some properties of the groups $G(m_1,\ldots,m_t)$

We recall that $G(m_1,\ldots,m_t) = (x_1,\ldots,x_t;\ x_1^{m_1}\ldots x_t^{m_t})$.

(i) the 2-generator subgroups of $G(m_1,\ldots,m_t)$ are free when $\gcd(m_1,\ldots,m_t) = 1$ and $t \geq 3$;

(ii) $G(m_1,\ldots,m_t)$ is residually nilpotent when $\gcd(m_1,\ldots,m_t) = 1$ and $t \geq 3$;

(iii) $G(m_1,\ldots,m_t)/\gamma_c G(m_1,\ldots,m_t)$ is free nilpotent of class $c - 1$ on $t - 1$ generators for $c = 1,2,\ldots$ when $\gcd(m_1,\ldots,m_t) = 1$ and $t \geq 3$;

(iv) $G(m_1,\ldots,m_t)$ is residually finite;

(v) $\Phi(G(m_1,\ldots,m_t)) = \{1\}$ unless $t = 1$ and m_1 is divisible by a square;

(vi) $G(m_1,\ldots,m_t)$ is not free unless $m_i = 0$ for all i or $m_i = 1$ for at least one i .

Properties (i) - (iv) are due to G. Baumslag (see [2], [3] and [4]), while property (v) follows from [6]. Property (vi) is quite clear. For if $m_i \neq 0$ for at least one i then by looking at the factor derived group we see that if $G(m_1,\ldots,m_t)$ is free then it is free on $t - 1$ generators. On the other hand if $m_i \neq 1$ for all i , then by adding the relations $x_i^{m_i} = 1$ we see that $G(m_1,\ldots,m_t)$ has a t-generator homomorphic image. Thus under the combined circumstances $G(m_1,\ldots,m_t)$ is not free. Conversely if $m_i = 0$ for all i then $G(m_1,\ldots,m_t)$ is free on t generators and if $m_i = 1$ for at least one i then it is free on $t - 1$ generators.

Note that if $(m_1',\ldots,m_t')$ arises from $(m_1,\ldots,m_t)$ by a permutation or change of sign of some or all the m_i's then $G(m_1',\ldots,m_t') \cong G(m_1,\ldots,m_t)$. Whether the converse is true when the groups are not free is not completely known. My work may be considered as a partial proof of the validity of the converse.

In Section 2 we introduce some notation and obtain very easily a partial classification of the groups by looking at their factor derived groups. In Section 3 we state without proof all the results we need which are obtained by looking at the kernels of the maps onto a cyclic group of prime order. With just Section 3 (indeed by Theorem 3.1 alone) we are able to deal with the case that $\gcd(m_1,\ldots,m_t) \neq 1$ (see Theorem B). The goal of the balance of the chapter is the case that $t = 3$ (see Theorem C).

In Section 4 we state again without proof the results we need which are obtained by looking at the kernels of the maps onto a cyclic group of order pq, p and q distinct primes. Sections 5 through 9 deal with the complicated computations needed to prove two theorems of Section 3 and two theorems of Section 4. In particular the lemma proved in Section 7 contains the essential part of the proofs of the theorems in Sections 6 and 9. Sections 10 and 11 deal with the proofs of the remaining theorems of Sections 3 and 4 respectively.

Section 2. The factor derived groups and some notation

We view G as a map from t-tuples of integers to groups. We want to know when two of the tuples map under G onto isomorphic groups. Since we know already that permutations of the t-tuples map onto isomorphic groups, it is convenient to let G be a map into isomorphism classes of groups whose domain consists of sets of permutations of t-tuples. We can also assume that integers are non-negative.

To this end we need some definitions.

Definition 2.1. M = the set of formal polynomials in one indeterminate x with positive integer coefficients and non-negative exponents.

Any such polynomial can be written uniquely (up to the order of its terms) with only unit coefficients.

Definition 2.2. Let $m = x^{m_1} + x^{m_2} + \ldots + x^{m_t} \in M$ then $(m)G$ = the isomorphism class of $G(m_1,\ldots,m_t)$.

Aside from being a notational convenience, we will see that by giving these polynomials an ordering and a multiplicative structure that is a bit unusual we can greatly simplify the proofs of Theorems 3.4 and 3.5.

Definition 2.3. We give maps defined on $(M)G$, the image of M under G , a bar, e.g. $\overline{A}$. The composition of G and $\overline{A}$ we denote by A . We say that m is A-equivalent to m' if and only if $(m)A = (m')A$. The identity map on $(M)G$ is called $\overline{G}$.

We may view our goal then as trying to determine G-equivalence classes. Clearly if $\overline{A}$ is any map defined on some union of G-equivalence classes then the A-equivalence classes will themselves be unions of G-equivalence classes.

By looking at the factor derived groups it is easy to prove

Theorem 2.4. M is the disjoint union of the sets listed below which are themselves unions of G-equivalence classes.

For $g = 2,3,\ldots$ and $t = 1,2,\ldots$

$$A_{t,g} = \{x^{m_1} + \ldots + x^{m_t} \in M \mid g = \gcd(m_1,\ldots,m_t)\} ;$$

For $t = 1,2,\ldots$

$$A_{t,0} = \{tx^0\} \cup \{x^1 + x^{m_2} + \ldots + x^{m_{t+1}} \in M\} ;$$

For $t = 2,3,\ldots$

$$A_{t,1} = \{x^{m_1} + \ldots + x^{m_t} \in M \setminus A_{t-1,0} \mid 1 = \gcd(m_1,\ldots,m_t)\} ;$$

And finally $A_{1,1} = \{x^1\}$.

Proof. It is clear that for $m \in A_{t,g}$

$$\begin{aligned} \bar{\tau}_n(G(m_1,\ldots)) &= 0 \quad \text{for} \quad n < t ; \\ &= g \quad \text{for} \quad n = t ; \\ &= 1 \quad \text{for} \quad n > t . \end{aligned}$$

The extended torsion numbers depend only on isomorphism class so we have the map

$$\bar{A} : mG \to \{\bar{\tau}_n(G(m_1,\ldots)) \mid n = 0, \pm 1,\ldots\} .$$

The A-equivalence classes are $A_{t,g}$ with $g \neq 0,1$, $A_{t,0} \cup A_{t+1,1}$ and $A_{1,1}$.

It remains to split up the sets $A_{t,0} \cup A_{t+1,1}$. But under the map G the elements of $A_{t,0}$ map to the isomorphism class of the free group of rank t , whereas the elements of $A_{t+1,1}$ map to isomorphism classes of groups which are not free. This concludes the proof of the theorem.

Corollary 2.5. $A_{t,g}$ is a G-equivalence class when $g = 0$ or $t = 1$.

Section 3. Kernels of prime index and Theorem B

The primes in question will be called p and we will take the elements of Z_p to be $\{0,1,\ldots,p-1\}$. The proofs of the theorems are complicated and are consequently postponed.

All the results in this section follow from the next two theorems.

Theorem 3.1. If ψ is a homomorphism of $G(m_1,\ldots,m_t)$ onto Z_p and $(x_i^{m_i})\,\psi = 0$ for all i then

$$\overline{\tau}_{(t-2)p+2}\ (\text{kernel } \psi) = \gcd(m_i \mid x_i\psi = 0)$$

Theorem 3.2. If ψ is a homomorphism of $G(m_1,\ldots,m_t)$ onto Z_p and $(x_i^{m_i})\,\psi \neq 0$ for at least one i then

$$\overline{\tau}_{(t-2)p+2}\ (\text{kernel } \psi) = \gcd(m_1,\ldots,m_t)\ .$$

Now the homomorphisms of $G(m_1,\ldots,m_t)$ into Z_p are either onto or trivial. For the epimorphisms we put $\lambda(\psi) = \overline{\tau}_{(t-2)p+2}\ (\text{kernel } \psi)$. For the trivial map we put $\lambda(\psi) = g$. We are now in a position to make the important

Definition 3.3. $\overline{f}_p(mG) = \Sigma_x^{\lambda(\psi)}$

the sum being taken over all homomorphisms of an element of mG into Z_p. Remember that $f_p = G\overline{f}_p$.

We are now able to use induction to prove

Theorem 3.4. The f_p-equivalence classes on $A_{t,g}$ where p divides g and $g \neq 0$ are all singletons.

Theorem B follows immediately for when $\gcd(m_1,\ldots,m_t) > 1$ there is a prime p which divides $\gcd(m_1,\ldots,m_t)$.

By using all the maps f_p simultaneously we can prove

Theorem 3.5. The G-equivalence classes on

$$B_t = \{m \in A_{t,1} \mid \gcd(m_j \mid j \neq i) \neq 1 \text{ for each } i\}$$

are all singletons.

Since $A_{2,1} = B_2$ we have immediately

Corollary 3.6. The G-equivalence classes on $A_{2,1}$ are all singletons.

Theorem 3.5 is a first step in determining what we may call f-classes, that is the intersections of the f_p-equivalence classes for all primes p. On $A_{3,1}$ the f-classes divide up nicely according to the number of gcd's of pairs of $\{m_1,m_2,m_3\}$ which are not one: 3 in B_3, 2 in C, 1 in D and none in E. Indeed if we let a,b,α and β be non-negative integers and put

$$C = \{C\binom{\alpha\ \beta}{a\ b} \mid \gcd(a\alpha, b\beta) = 1,\ \alpha \neq 1,\ \beta \neq 1\}$$

where $C\binom{\alpha\ \beta}{a\ b} = \{m \in A_{3,1} \mid m_i = a\alpha,\ m_j = b\beta,$

$$\gcd(m_i,m_k) = \alpha,\ \gcd(m_j,m_k) = \beta,\ i \neq j \neq k \neq i\}.$$

$$D = \{D\binom{\alpha}{a} \mid \gcd(a,\alpha) = 1,\ a \neq 1,\ \alpha \neq 1\}$$

where $D\binom{\alpha}{a} = \{m \in A_{3,1} \mid m_i = a,\ \gcd(m_j,m_k) = \alpha$

$$\gcd(m_i,m_j) = \gcd(m_i,m_k) = 1,\ i \neq j \neq k \neq i\}.$$

and $$E = \{m \in A_{3,1} \mid \gcd(m_1,m_2) = \gcd(m_1,m_3) = \gcd(m_2,m_3) = 1\}.$$

Then we can prove

Theorem 3.7. The f-classes on $A_{3,1}$ are just the elements of B_3,C,D, and $\{E\}$.

This classification greatly simplifies the proof of Theorem C which we discuss in Section 4.

Section 4. Kernels of index pq and Theorem C

Here p and q are distinct primes. Let the elements of Z_{pq} be $\{0,1,\ldots,pq-1\}$. As in Section 3 proofs are postponed. Corresponding to Theorem 3.1 we have

Theorem 4.1. If ψ is a homomorphism of $G(m_1,\ldots,m_t)$ onto Z_{pq} and $(x_i^{m_i})\psi = 0$ for all i then

$$\overline{\tau}_{(t-2)pq+2}(\text{kernel } \psi) = \gcd(m_i \mid x_i\psi = 0) .$$

It is the information that we obtain from Theorem 4.1 that allows us to finish off the proof of Theorem C (i.e. all the G-equivalence classes on $A_{3,1}$ are singletons). Indeed suppose we can choose p and q so that p divides m_1 and q divides m_2 for some $m \in A_{3,1}$. Then the map which sends x_1 to q, x_2 to p and x_3 to 0 extends to a homomorphism, ψ, which falls within the scope of Theorem 4.1. We conclude then that $\overline{\tau}_{pq+2}(\text{kernel } \psi) = m_3$. If we can somehow distinguish this homomorphism from all the others, then we will have shown that for any m', G-equivalent to m, $m_i' = m_3$ for some i.

We must first make sure that for any m' which is G-equivalent to m there are i and j, $i \neq j$ in $\{1,2,3\}$ so that p divides m_i' and q divides m_j'. This is easy for $m \in C\binom{\alpha\ \beta}{a\ b}$ or $D\binom{\alpha}{a}$. Indeed we let p divide α and q divide β in the first case and p divide a and q divide α in the second case. For $m \in E$ we need the next two lemmas. The first is trivial and its proof is omitted. The second uses some results obtained in the proof of Theorem 4.1.

Lemma 4.2. If for some i $\gcd(m_i,s) = 1$ then $G(m_1,\ldots,m_t)/gp(g^s \mid g \in G(m_1,\ldots,m_t))$ can be generated by $t-1$ elements.

Lemma 4.3. If p_i divides m_i for each i and $s = p_1p_2p_3$ then $G(m_1,m_2,m_3)/gp(g^s(g \in G(m_1,m_2,m_3))$ needs 3 generators.

Theorem 4.1 does not deal with all homomorphisms onto Z_{pq}. Although we do not have the required information for all homomorphisms we can prove

Theorem 4.4. If ψ is a homomorphism of $G(m_1,m_2,m_3)$ onto Z_{pq} of the type described after Theorem 4.1 which does not fall within the scope of Theorem 4.1 then $\overline{\tau}_{pq+2}$ (kernel ψ) is either $\gcd(m_i \mid x_i^p\psi = 0)$ or 1 depending on whether $x_i^{m_ip}\psi = 0$ for all i or not.

We are now in a position to finish off the proof of Theorem C (see Theorem 3.7) by proving

Theorem 4.5. The G-equivalence classes on $C\binom{\alpha\ \beta}{a\ b}$, $D\binom{\alpha}{a}$ and E are all singletons.

Section 5. The proof of Theorem 3.1

We begin by restating Theorem 3.1.

"If ψ is a homomorphism of $G(m_1,\ldots,m_t)$ onto Z_p and $(x_i^{m_i})\psi = 0$ for all i then

$$\overline{\tau}_{(t-2)p+2}\ (\text{kernel } \psi) = \gcd(m_i \mid x_i\psi = 0)\ ."$$

We may assume without loss of generality that $x_t\psi = 1$ and that there is a u in $\{0,1,\ldots,t-1\}$ such that $x_i\psi = 0$ iff $i \leq u$. It follows that p divides m_i for $i > u$.

The first step is to use Reidemeister-Schreier to find a presentation for kernel ψ. We may take $S = \{x_t^n \mid n = 0,1,\ldots,p-1\}$ as our Schreier system. The map σ from $G(m_1,\ldots,m_t)$ to S is $x\sigma = x_t^{x\psi}$. The $(t-1)p+1$ generators for kernel ψ are

$$x_{i,n+1} = x_t^n x_i x_t^{\theta n \theta n_i} \quad \text{for } i \neq t,\ n = 0,1,\ldots,p-1$$

$$x_{t,p} = x_t^p\ ,$$

where $n_i = x_i\psi$ and we use the notation $\oplus$ and θ to indicate the operations in Z_p, or alternatively that the resulting number is to be reduced mod p to lie in $\{0,1,\ldots,p-1\}$. Notice that the subscript $n+1$ ranges between 1 and p. This is for notational convenience. It will be necessary at times to write these subscripts as sums and in that case we use $\oplus$ and θ to indicate that numbers are to be reduced mod p but this time they must lie in $\{1,\ldots,p\}$.

It is not difficult to show that the p relators for kernel ψ are r_n, $n = 1,\ldots,p$ where:

$$r_n = \overline{x_t^{n-1}x_1^{m_1}\cdots x_t^{m_t}x_t^{1-n}} = r_n(1)\cdots r_n(t) \quad \text{and}$$

$$r_n(i) = x_{i,n}^{m_i} \quad \text{for} \quad i \leq u \ ;$$

$$= (x_{i,n}x_{i,n\oplus n_i}\cdots x_{i,n\oplus(p-1)n_i})^{m_i p^{-1}} \quad \text{for} \quad u < i < t \ ;$$

$$= x_{t,p}^{m_t p^{-1}} \quad \text{for} \quad i = t \ .$$

The entry $r_{n,(i-1)p+j}$ at the n'th row ($n = 1,\ldots,p$) and $(i-1)p + j$'th column ($i = 1,\ldots,t$, $j = 1,\ldots,p$ unless $i = t$ when $j = 1$ only) of the relation matrix of kernel Ψ is:

m_i when $i \leq u$ and $j = n$

0 when $i \leq u$ and $j \neq n$

$m_i p^{-1}$ when $i > u$.

The next step is to diagonalize the relation matrix. Note that $i \leq u$ the submatrices consisting of the $(i-1)p + j$'th columns, $j = 1,\ldots,p$ are in diagonal form whose possible non-zero entries are all equal. For the balance of the matrix the rows are all equal. We diagonalize the matrix in three steps:

(1) Subtract the first row from each of the others.

(2) Restore the submatrices to diagonal form which originally were in diagonal form.

(3) Put the gcd of the entries in the n'th row in the n'th row and n'th column; make all the remaining entries 0 .

The resulting matrix is 0 except for $p-1$ entries equal to $\gcd(m_1,\ldots,m_u)$ and one entry equal to $\gcd(m_1,\ldots,m_u,m_{u+1}p^{-1},\ldots,m_t p^{-1})$. Thus we have

$$\overline{\tau}_n \text{ (kernel } \psi) = 0 \quad \text{for} \quad n \leq (t-2)p + 1$$

$$= \gcd(m_1, \ldots, m_u) \quad \text{for} \quad (t-2)p + 1 < n \leq (t-1)p$$

$$= \gcd(m_1, \ldots, m_t p^{-1}) \quad \text{for} \quad n = (t-1)p + 1$$

$$= 1 \quad \text{for} \quad n > (t-1)p + 1$$

This concludes the proof of Theorem 3.1. It is easier then and can serve as a guide to the proofs of Theorems 3.2, 4.1 and 4.4.

Section 6. The proof of Theorem 3.2

"If ψ is a homomorphism of $G(m_1,\ldots,m_t)$ onto Z_p and $(x_i^{m_i})\psi \neq 0$ for at least one i then

$$\overline{\tau}_{(t-2)p+2}(\text{kernel } \psi) = \gcd(m_1,\ldots,m_t) .\text{"}$$

We may assume without loss of generality that $x_t\psi = 1$ and that there are u and v in $\{0,1,\ldots,t-1\}$ such that

$$x_i\psi = 0 \text{ iff } i \leq u \text{ and}$$

$$x_i^{m_i}\psi = 0 \text{ iff } i \leq v .$$

It follows that $u \leq v \leq t-2$, that p divides m_i for $u < i \leq v$ and that p does not divide m_i for $v < i \leq t$. It is of no consequence whether or not p divides m_i when $i \leq u$.

We take $S = \{x_t^n \mid n = 0,1,\ldots,p-1\}$ as our Schreier system. The resulting $(t-1)p+1$ generators for kernel ψ are

$$x_{i,n+1} = x_t^n x_i x_t^{-n} \quad \text{for } i \leq u$$

$$x_{i,n+1} = x_t^n x_i x_t^{\theta n \theta n_i} \quad \text{for } u < i < t,\ n_i = x_i\psi \text{ and}$$

$$x_{t,p} = x_t^p$$

The p relators for kernel ψ are r_n, $n = 1,\ldots,p$ where

$$r_n = \overline{x_t^{n-1}x_1^{m_1}\ldots x_t^{m_t}x_t^{1-n}} = r_n(1)\ldots r_n(t) \text{ and}$$

$$r_n(i) = x_{i,n}^{m_i} \quad \text{for } i \leq u ;$$

$$= (x_{i,n}x_{i,n\oplus n_i}\ldots x_{i,n\theta n_i})^{m_i p^{-1}} \quad \text{for } u < i \leq v ;$$

$$= (x_{i,n\oplus k_i}x_{i,n\oplus k_i\oplus n_i}\ldots x_{i,n\oplus k_i\theta n_i})^{[m_i p^{-1}]}$$

$$x_{i,n\oplus k_i}x_{i,n\oplus k_i\oplus n_i}\ldots x_{i,n\oplus k_i\oplus(\{m_i p^{-1}\}-1)n_i}$$

for $u < i < t$ (our notation here is $k_i = m_1 + \ldots + m_{i-1}$ and $[m_i p^{-1}]$ and $\{m_i p^{-1}\}$ are integers satisfying

$$m_i = [m_i p^{-1}]p + \{m_i p^{-1}\} \text{ with } \{m_i p^{-1}\} \in \{1,\ldots,p-1\}) ;$$

$$= x_{t,p}^{[m_t p^{-1}]+1} \quad \text{for } i = t \text{ and } n = 1,2,\ldots,\{m_t p^{-1}\} ;$$

$$= x_{t,p}^{[m_t p^{-1}]} \quad \text{for } i = t \text{ and } n = \{m_t p^{-1}\} + 1,\ldots,p .$$

The entry $r_{n,(i-1)p+j}$ at the n'th row $(n = 1,\ldots,p)$ and $(i-1)p + j$'th column $(i = 1,\ldots,t,\ j = 1,\ldots,p$ unless $i = t$ when $j = 1$ only) of the relation matrix of kernel Ψ is:

m_i when $i \leq u$ and $j = n$;

0 when $i \leq u$ and $j \neq n$;

$m_i p^{-1}$ when $u < i \leq v$;

$[m_i p^{-1}] + 1$ when $u < i < t$ and $j = n \oplus k_i \oplus (s-1)n_i$,
or $i = t$, $j = 1$ and $n = s$, with
$s = 1,\ldots,\{m_i p^{-1}\}$;

$[m_i p^{-1}]$ same as above except with $s = \{m_i p^{-1}\} + 1,\ldots,p$.

It is important to note that for all i and j the sum of the entries in the $(i-1)p + j$'th column is m_i . Indeed the theorem follows from this fact and

Lemma 6.1. By using only elementary column operations and permutations of the rows, the square submatrix consisting of the columns $(t-2)p + 1$, $(t-2)p + 2,\ldots,(t-1)p$ can be transformed into a matrix such that the entry at the n'th row and k'th column is:

$$\begin{array}{ll} 1 & \text{when } k = n \neq p \ ; \\ 0 & \text{when } k \neq n \neq p \ ; \\ -1 & \text{when } k \neq n = p \ ; \\ m_{t-1} & \text{when } k = n = p \ . \end{array}$$

We postpone the proof of Lemma $\bar{6}.1$ until we have finished proving the theorem. Since in Lemma 6.1 we used only permutations of the rows, it is still true that the sum of the entries of the transformed matrix in the $(i - 1)p + j$'th column is m_i for $i \neq t - 1$.

The next step in diagonalizing the matrix is to subtract $r_{n,(i-1)p+j}$ times the $(t - 2)p + n$'th column from the $(i - 1)p + j$'th column for all $i \neq t - 1$, j and $n \neq p$. The effect of this step is to replace for $i \neq t - 1$ the $r_{n,(i-1)p+j}$'th entry with 0 if $n \neq p$ and m_i if $n = p$. The only non-zero entry remaining in the n'th row for $n \neq p$ is 1 in the $(t - 2) + n$'th column. The entry in the p'th row below this 1 is -1 . The other entries in the p'th row are $m_1,\ldots,m_t$. We replace the -1's with 0 by adding the 1'st through $p - 1$'st rows to the last. Finally we put the gcd of the elements in the last row (that is $\gcd(m_1,\ldots,m_t)$) into the first column and make all the remaining entries in the last row 0 .

The resulting matrix is in diagonal form. It is 0 except for $p - 1$ entries equal to 1 and one entry equal to $\gcd(m_1,\ldots,m_t)$. Thus we have:

$$\begin{aligned} \bar{\tau}_n \text{ (kernel } \psi) &= 0 && \text{for } n \leq (t - 2)p + 1 \\ &= \gcd(m_1,\ldots,m_t) && \text{for } n = (t - 2)p + 2 \\ &= 1 && \text{for } n > (t - 2)p + 2 \ . \end{aligned}$$

This concludes the proof of the theorem.

Section 7. The proof of Lemma 6.1

We restate the lemma slightly more generally. This form makes it useful in Section 9 as well as Section 6.

Let a,b,c,d and p be fixed integers $0 < d < p$ such that $\gcd(c,p) = \gcd(d,p) = 1$. Let the entry at the n'th row and k'th column of a $p \times p$ square matrix be:

$$a + 1 \quad \text{iff} \quad k = n + b + sc \bmod p,\ s = 0,1,\ldots,d - 1$$

$$a \quad \text{iff} \quad k = n + b + sc \bmod p,\ s = d,\ldots,p - 1 .$$

(We do not assume that p is prime.) Then by permuting the rows and using elementary column operations we can transform it into a matrix such that the entry at the n'th row and k'th column is:

$$\begin{array}{ll} 1 & \text{when } k = n \neq p ; \\ 0 & \text{when } k \neq n \neq p ; \\ -1 & \text{when } k \neq n = p ; \\ ap + d & \text{when } k = n = p . \end{array}$$

Proof. (1) Permute the rows by the permutation which maps the $nc \bmod p$'th row to the n'th row.

(2) Permute the columns by the permutation which maps $(k + d - 1)c + b \bmod p$'th column to the k'th column.

In the resulting matrix the entry at the n'th row and k'th column is:

$$a + 1 \quad \text{iff} \quad n = k \oplus s \quad s = 0,\ldots,d - 1 ;$$

$$a \quad \text{iff} \quad n = k \oplus s \quad s = d,\ldots,p - 1 .$$

(3) Subtract the $k + 1$'st column from the k'th column, $k = 1,\ldots,p - 1$, starting with $k = 1$.

In the resulting matrix the entry at the n'th row and k'th column is zero except that it is:

$$1 \quad \text{for} \quad n = k \mp p \ ;$$

$$-1 \quad \text{for} \quad n = k + d \bmod p, \ k \mp p \ ;$$

$$\text{unchanged for} \quad k = p \ .$$

(4) Permute the rows and columns by the permutation which maps the $\ell d \bmod p$'th row or column to ℓ'th row or column respectively. In particular the p'th column remains fixed.

(5) Add the $k + 1$'st column to the k'th column for $k = 1,\ldots,p - 2$, starting $k = p - 2$.

The resulting matrix is just what we want except for the p'th column which is just a permutation of one of the original columns. The sum of the entries in the p'th column is $ap + d$. We finish the proof of the lemma by using the first $p - 1$ columns to sum the p'th column to the last row. That is we replace each entry in the p'th column with zero except the entry in the p'th row which becomes $ap + d$. This concludes the proof of Lemma 6.1.

Section 8. The proof of Theorem 4.1

"If ψ is a homomorphism of $G(m_1,\ldots,m_t)$ onto Z_{pq} and $(x_i^{m_i})\psi = 0$ for all i then

$$\overline{\tau}_{(t-2)pq+2}(\text{kernel } \psi) = \gcd(m_i \mid x_i\psi = 0) \text{ ."}$$

We divide the proof up into two parts which differ in the way we choose our Schreier system. In either case we may assume $p > q$.

Case I. There exists an x_i such that $x_i\psi$ generates Z_{pq} (or equivalently $x_i\psi$ is divisible by neither p nor q).

We may assume without loss of generality that $x_t\psi = 1$ and that there are u,v and w in $\{0,1,\ldots,t-1\}$ such that:

$$x_i\psi = 0 \text{ iff } i \le u ;$$

$$x_i^p\psi = 0 \text{ iff } i \le v ;$$

$$x_i^q\psi = 0 \text{ iff } i \le u \text{ or } v < i \le w .$$

It follows that $u \le v \le w$, p divides m_i while q but not p divides $n_i = x_i\psi$ for $u < i \le v$, q divides m_i while p but not q divides n_i for $u < i \le w$ and pq divides m_i while neither p nor q divides n_i for $w < i \le t$.

We take $S = \{x_t^n \mid n = 0,1,\ldots,pq-1\}$ as our Schreier system. The resulting $(t-1)pq+1$ generators for kernel ψ are

$$x_{i,n+1} = x_t^n x_i x_t^{-n} \quad \text{for } i \le u$$

$$x_{i,n+1} = x_t^n x_i x_t^{\theta n \theta n_i} \quad \text{for } u < i < t \text{ and}$$

$$x_{t,pq} = x_t^{pq} .$$

The pq relators for kernel Ψ are r_n, $n = 1,\ldots,pq$, where:

$$r_n = \overline{x_t^{n-1}x_1^{m_1}\ldots x_t^{m_t}x_t^{1-n}} = r_n(1)\ldots r_n(t) \quad \text{and}$$

$$r_n(i) = x_{i,n}^{m_i} \quad \text{for} \quad i \leq u$$

$$= (x_{i,n}x_{i,n\oplus n_i}\ldots x_{i,n\oplus(p-1)n_i})^{m_i p^{-1}}$$

$$\text{for} \quad u < i \leq v$$

$$= (x_{i,n}x_{i,n\oplus n_i}\ldots x_{i,n\oplus(q-1)n_i})^{m_i q^{-1}}$$

$$\text{for} \quad v < i \leq w$$

$$= (x_{i,n}x_{i,n\oplus n_i}\ldots x_{i,n\theta n_i})^{m_i p^{-1}q^{-1}}$$

$$\text{for} \quad w < i < t$$

$$= x_{t,pq}^{m_t p^{-1}q^{-1}} \quad \text{for} \quad i = t .$$

The relation matrix for kernel Ψ is zero except that the entry at the n'th row, $n = 1,\ldots,pq$, and k'th column, $k = 1,\ldots,(t-1)pq + 1$, is:

m_i for $k = (i-1)pq + n$ $i \leq u$;

$m_i p^{-1}$ for $k = (i-1)pq + jq + h$, $n = \ell q + h$,
$u < i \leq v$, $j,\ell = 0,1,\ldots,p-1$ and $h = 1,\ldots,q$;

$m_i q^{-1}$ for $k = (i-1)pq + jp + h$, $n = \ell p + h$,
$v < i \leq w$, $j,\ell = 0,1,\ldots,q-1$ and $h = 1,\ldots,p$;

$m_i p^{-1}q^{-1}$ for $k > wpq$ and all n .

We proceed to diagonalize the matrix.

(1) Subtract the $(i-1)pq + h$'th columns from the equal $(i-1)pq + jq + h$'th columns, $u < i \leq v$, $j = 1,\ldots,p-1$ and $h = 1,\ldots,q$.

(2) Subtract the $(i - 1)pq + h$'th columns from the equal $(i - 1)pq + jp + h$'th columns, $v < i \leq w$, $j = 1,\ldots,q - 1$ and $h = 1,\ldots,p$.

(3) Subtract the $(i - 1)pq + 1$'st columns from the equal $(i - 1)pq + j$'th columns, $w < i < t$, $j = 2,\ldots,pq$.

(4) Subtract the first row from each of the other rows.

(5) Add the $(i - 1)pq + j$'th columns to the $(i - 1)pq + 1$'st column for all i and $j = 2,\ldots,pq$.

The resulting matrix is 0 except that the entry at the n'th row and k'th column is:

m_i for $k = (i - 1)pq + n$ $i \leq u$;

$m_i p^{-1}$ for $k = (i - 1)pq + h$, $n = \ell q + h$,
$u < i \leq v$ $(\ell,h) \in \{0,1,\ldots,p-1\} \times \{2,\ldots,q\} \cup (0,1)$;

$m_i q^{-1}$ for $k = (i - 1)pq + h$, $n = \ell q + h$
$v < i \leq w$, $(\ell,h) \in \{0,1,\ldots,q-1\} \times \{2,\ldots,p\} \cup (0,1)$;

$m_i p^{-1} q^{-1}$ for $k = (i - 1)pq + 1$, $n = 1$, $i > w$.

In order to continue we must define two maps on the set $\{1,\ldots,p - 1\}$, α and β . Indeed for all $\ell \in \{0,\ldots,p - 1\}$ there exist unique integers $\alpha_\ell \in \{1,\ldots,p\}$ and $\beta_\ell \in \{0,\ldots,q - 1\}$ so that

$$\ell q + 1 = \beta_\ell p + \alpha_\ell .$$

It is important to note that $\alpha_\ell = \alpha_{\ell'}$ implies $\ell = \ell'$ and that $\alpha_0 = 1$. Thus as ℓ runs through $\{1,\ldots,p - 1\}$, α_ℓ runs through $\{2,\ldots,p\}$. We continue the diagonalization process.

(6) Subtract the $\ell q + 1$'st rows from the $\beta p + \alpha_\ell$'th rows $\beta \neq \beta_\ell$, $\ell = 2,\ldots,q$.

(7) Subtract the h'th rows from the now equal $\ell q + h$'th rows $\ell = 1,\ldots,p - 1$ and $h = 2,\ldots,q$.

(8) Restore the square submatrices consisting of the $(i - 1)pq + j$'th columns $j = 1,\ldots,pq$ for $i \leq u$ to diagonal form. (They were in diagonal form with equal "non-zero" entries to begin with).

The resulting matrix is zero except that the entry at the n'th row and k'th column is:

m_i for $k = (i - 1)pq + n$ $i \leq u$, all n ;

$m_i p^{-1}$ for $k = (i - 1)pq + n$, $u < i \leq v$, $n = 1,\ldots,q$;

$m_i q^{-1}$ for $k = (i - 1)pq + \alpha_\ell$, $n = \ell q + 1$, $v < i \leq w$, $\ell = 0,\ldots,p - 1$;

$m_i p^{-1} q^{-1}$ for $k = (i - 1)pq + 1$, $n = 1$, $w < i \leq t$.

Hence we are in a position to complete the process.

(9) Put the gcd of the entries in the n'th rows into the n'th columns; make all the remaining entries 0 .

The resulting matrix is zero except that the entry at the n'th row and column is:

$g_1 = \gcd(m_i \mid i \leq u)$ for $n \neq 1,\ldots,q,1 + q,1 + 2q,\ldots,1 + (p - 1)q$;

$g_2 = \gcd(g_1, \{m_i p^{-1} \mid u < i \leq v\})$ for $n = 2,\ldots,q$;

$g_3 = \gcd(g_1, \{m_i q^{-1} \mid v < i \leq w\})$ for $n = 1 + q,\ldots,1 + (p - 1)q$;

$g_4 = \gcd(g_2, g_3, \{m_i p^{-1} q^{-1} \mid w < i \leq t\})$ for $n = 1$.

Thus we have

$$\bar{\tau}_n(\text{kernel } \psi) = \begin{cases} 0 & \text{for } n \le (t-2)pq + 1 \\ g_1 & \text{for } (t-2)pq + 1 < n \le (t-1)pq - p - q + 2 \\ \operatorname{lcm}(g_2, g_3) & \text{for } (t-1)pq - p - q + 2 < n \le (t-1)pq - p + 1 \\ g_3 & \text{for } (t-1)pq - p + 1 < n \le (t-1)pq - q + 1 \\ \gcd(g_2, g_3) & \text{for } (t-1)pq - q + 1 < n \le (t-1)pq \\ g_4 & \text{for } n = (t-1)pq + 1 \\ 1 & \text{for } n > (t-1)pq + 1 \end{cases}$$

This concludes the proof of the theorem in the first case.

Case II. For all x_i, $x_i\psi$ does not generate Z_{pq} (or equivalently $x_i\psi$ is divisible by either p or q).

We may assume without loss of generality that $x_t\psi = p$ and that there are u and s in $\{0,1,\ldots,t-1\}$ such that:

$$x_i\psi = 0 \text{ iff } i \le u ;$$

$$x_i^p\psi = 0 \text{ iff } i \le s ;$$

$$x_s\psi = q \quad \text{and}$$

$$x_i^q\psi = 0 \text{ iff } i \le u \text{ or } i > s .$$

It follows that $u < s$, p divides m_i while q but not p divides $n_i = x_i\psi$ for $u < i \le s$, and q divides m_i while p but not q divides n_i for $i > s$.

We take $S = \{x_s^m x_t^n \mid m = 0,1,\ldots,p-1,\ n = 0,1,\ldots,q-1\}$ as our Schreier system. The resulting $(t-1)pq + 1$ generators for kernel ψ are:

$$x_{i,m,n} = x_s^m x_t^n x_i x_t^{-n} x_s^{-m} \quad \text{for } i \le u, \text{ all } m \text{ and } n ;$$

$$= x_s^m x_t^n x_i x_t^{-n} x_s^{\theta m \theta (n_i q^{-1})} \quad \text{for } u < i < s, \text{ all } m \text{ and } n ;$$

$$= x_s^m x_t^n x_i x_t^{\theta n \theta (n_i p^{-1})} x_s^{-m} \quad \text{for } s < i < t, \text{ all } m \text{ and } n ;$$

$$= x_s^p \quad \text{for } i = s, m = p - 1, n = 0 ;$$

$$= x_s^m x_t^n x_s x_t^{-n} x_s^{\theta m \theta 1} \quad \text{for } i = s, \text{ all } m, n \neq 0 ;$$

$$= x_s^m x_t^q x_s^{-m} \quad \text{for } i = t, \text{ all } m, n = q - 1 .$$

The pq relators for kernel Ψ are $r_{m,n}$ $m = 0,1,\ldots,p-1$, $n = 0,1,\ldots,q-1$, where

$$r_{m,n} = \overline{x_s^m x_t^n x_1^{m_1} x_2^{m_2} \ldots x_t^{m_t} x_t^{-n} x_s^{-m}} = r_{m,n}(1) \ldots r_{m,n}(t) \quad \text{and}$$

$$r_{m,n}(i) = x_{i,m,n}^{m_i} \quad \text{for } i \le u, \text{ all } m \text{ and } n ;$$

$$= (x_{i,m,n} x_{i,m\oplus(n_i q^{-1}),n} \cdots x_{i,m\theta(n_i q^{-1}),n})^{m_i p^{-1}}$$

$$\text{for } u < i < s, \text{ all } m \text{ and } n ;$$

$$= x_{s,p-1,0}^{m_s p^{-1}} \quad \text{for } i = s, \text{ all } m, n = 0 ;$$

$$= (x_{s,m,n} x_{s,m\oplus 1,n} \cdots x_{s,m\theta 1,n})^{m_s p^{-1}} \quad \text{for } i = s, \text{ all } m, n \neq 0 ;$$

$$= (x_{i,m,n} x_{i,m,n\oplus(n_i p^{-1})} \cdots x_{i,m,n\theta(n_i p^{-1})})^{m_i q^{-1}}$$

$$\text{for } s < i < t, \text{ all } m \text{ and } n ;$$

$$= x_{t,m,q-1}^{m_t q^{-1}} \quad \text{for } i = t, \text{ all } m \text{ and } n .$$

The relation matrix for kernel Ψ is zero except that the entry at the $np + m + 1$'st row and $(i-1)pq + \bar{n}p + \bar{m} + 1$'st column $m,\bar{m} = 0,1,\ldots,p-1$ $n,\bar{n} = 0,1,\ldots,q-1$, $i = 1,\ldots,t$, is:

m_i for $i \leq u$, $m = \bar{m}$, $n = \bar{n}$;

$m_i p^{-1}$ for $u < i < s$, all m and $\bar{m}$, $n = \bar{n}$;

$m_{i+1} q^{-1}$ for $s \leq i < t - 1$, $m = \bar{m}$, all n and $\bar{n}$;

$m_s p^{-1}$ for $i = t - 1$, $m = \bar{m}$, all n and $\bar{n} = 0$;

$m_s p^{-1}$ for $i = t - 1$, all m and $\bar{m}$, $n = \bar{n} \neq 0$ or

for $i = t$, all m, $\bar{m} = n = \bar{n} = 0$.

We proceed to diagonalize the matrix.

(1) Subtract the $(i - 1)pq + \bar{n}p + 1$'st columns from the equal $(i - 1)pq + \bar{n}p + \bar{m} + 1$'st columns, for $u < i < s$, $\bar{m} \neq 0$ and all $\bar{n}$ or for $i = t - 1$, $\bar{m} \neq 0$, $\bar{n} \neq 0$.

(2) Subtract the $(i - 1)pq + \bar{m} + 1$'st columns from the equal $(i - 1)pq + \bar{n}p + \bar{m} + 1$ columns, for $s \leq i < t - 1$, all $\bar{m}$, $\bar{n} \neq 0$.

(3) Subtract the $np + 1$'st rows from the $np + m + 1$'st rows. Then add the $(i - 1)pq + \bar{n}p + \bar{m} + 1$'st columns to the $(i - 1)pq + \bar{n}p + 1$'st columns. For all i, m and $\bar{m} \neq 0$, all n and $\bar{n}$.

(4) Subtract $m + 1$'st rows from the $np + m + 1$'st rows. Then add the $(i - 1)pq + \bar{n}p + \bar{m} + 1$'st columns to the $(i - 1)pq + \bar{m} + 1$'st columns for $i \neq t - 1$. Add the $(t - 2)pq + \bar{n}p + 1$'st columns to the $(t - 1)pq + 1$'st column. For all m and $\bar{m}$, n and $\bar{n} \neq 0$.

The resulting matrix is zero except that the entry at the $np + m + 1$'st row and $(i - 1)pq + \bar{n}p + \bar{m} + 1$'st column is:

m_i for $i \leq u$, $m = \bar{m}$, $n = \bar{n}$;

$m_i p^{-1}$ for $u < i < s$, $m = \bar{m} = 0$, $n = \bar{n}$;

$m_{i+1} q^{-1}$ for $s \leq i \leq t - 1$, $m = \bar{m}$, $n = \bar{n} = 0$;

$m_s p^{-1}$ for $i = t - 1$, $m = \bar{m} = 0$, $n = \bar{n} \neq 0$ or

for $i = t$, $m = \bar{m} = n = \bar{n} = 0$.

We are now at a point in the proof very similar to where we were in the first case after step 8. Indeed if in this case I had written $mq + n$ rather than $np + m$ we would have exactly the same matrix. In any case continuing by the same process as in the first case we get exactly the same final answer for $\bar{\tau}_n$ (kernel ψ) except that $g_4 = \gcd(g_2, g_3)$. This concludes the proof of the theorem.

Section 9. The proof of Theorem 4.4

We will see in the proof of Theorem 4.5 that all the homomorphisms in question are covered by the two cases listed below. In order to keep the number of cases down to two and avoid repetition it is convenient to suppose that ψ is a homomorphism defined on $G(m_1,\ldots,m_t)$ for arbitrary t. The results we want are:

$$\overline{\tau}_{(t-2)pq+2}\ (\text{kernel } \psi) = \gcd(m_i \mid x_i^p\psi = 0) \quad \text{for Case 1 and}$$

$$\overline{\tau}_{(t-2)pq+2}\ (\text{kernel } \psi) = \gcd(m_1,\ldots,m_t) \quad \text{for Case 2.}$$

Case 1. There are exactly two i's such that $x^{m_i}\psi \neq 0$, $x^{m_i}\psi = 0$ implies $x_i^p\psi = 0$, $x_i^q\psi = 0$ implies $x_i\psi = 0$ and $x_i^{m_i p}\psi = 0$ for all i.

We may assume without loss of generality that $x_t\psi = 1$ and that there are u,v and w in $\{0,1,\ldots,t-1\}$ such that:

$$x_i\psi = 0 \quad \text{iff} \quad i \leq u\ ;$$

$$x_i^{m_i}\psi = 0 \quad \text{iff} \quad i \leq v\ ;$$

$$x_i^p\psi = 0 \quad \text{iff} \quad i \leq w\ .$$

It follows that $u \leq v \leq w$, $v = t-2$, p divides m_i for $u < i \leq v$, p does not divide m_i for $v < i \leq w$, q but not p divides $n_i = x_i\psi$ for $u < i \leq w$ and q but not p divides m_i while neither p nor q divides n_i for $w < i \leq t$.

We take $S = \{x_t^n \mid n = 0,1,\ldots,pq-1\}$ as our Schreier system. The resulting $(t-1)pq+1$ generators for kernel ψ are:

$$x_{i,n+1} = x_t^n x_i x_t^{-n} \quad \text{for} \quad i \leq u\ ;$$

$$x_{i,n+1} = x_t^n x_i x_t^{\theta n \theta n_i} \quad \text{for} \quad u < i < t \quad \text{and;}$$

$$x_{t,pq} = x_t^{pq}\ .$$

The pq relators for kernel ψ are r_n, $n = 1,\ldots,pq$, where:

$$r_n = \overline{x_t^{n-1}x_1^{m_1}\ldots x_t^{m_t}x_t^{1-n}} = r_n(1)\ldots r_n(t) \quad \text{and}$$

$$r_n(i) = x_{i,n}^{m_i} \quad \text{for } i \le u ;$$

$$= (x_{i,n}x_{i,n\oplus n_i}\ldots x_{i,n\oplus(p-1)n_i})^{m_ip^{-1}} \quad \text{for } u < i \le u ;$$

$$= (x_{i,n\oplus k_i}\ldots x_{i,n\oplus k_i\oplus(p-1)n_i})^{[m_ip^{-1}]}$$

$$x_{i,n\oplus k_i}\ldots x_{i,n\oplus k_i\oplus(\{m_ip^{-1}\}-1)n_i} \quad \text{for } v < i \le w ;$$

(for notation see the proof of Theorem 3.2)

$$= (x_{i,n\oplus k_i}\ldots x_{i,n\oplus k_i\theta n_i})^{[m_ip^{-1}q^{-1}]}$$

$$x_{i,n\oplus k_i}\ldots x_{i,n\oplus k_i\oplus(\{m_ip^{-1}q^{-1}\}-1)n_i} \quad \text{for } w < i < t ;$$

$$= x_{t,pq}^{[m_tp^{-1}q^{-1}]+1} \quad \text{for } i = t \text{ and } n \le \{m_tp^{-1}q^{-1}\} ;$$

$$= x_{t,pq}^{[m_tp^{-1}q^{-1}]} \quad \text{for } i = t \text{ and } n > \{m_tp^{-1}q^{-1}\} .$$

The relation matrix for kernel ψ is zero except that the entry at the n'th row, $n = 1,\ldots,pq$, and $(i-1)pq + k$'th column, $k = 1,\ldots,pq$ except when $i = t$ where $k = 1$, is:

m_i for $i \le u$ and $k = n$;

m_ip^{-1} for $u < i \le v$ and $k = n \bmod q$;

$[m_ip^{-1}] + 1$ for $v < i \le w$, $k = n \oplus k_i \oplus sn_i$ and $s = 0,1,\ldots,\{m_ip^{-1}\} - 1$;

$[m_ip^{-1}]$ same as above except that $s = \{m_ip^{-1}\},\ldots,p$;

$[m_ip^{-1}q^{-1}] + 1$ for $w < i < t$, $k = n \oplus k_i \oplus sn_i$ or for $i = t$, $k = 1$, $n = s \oplus 1$ and $s = 0,1,\ldots,\{m_ip^{-1}q^{-1}\} - 1$;

$[m_ip^{-1}q^{-1}]$ same as above except that $s = \{m_ip^{-1}q^{-1}\},\ldots,pq$.

The first step in the diagonalization process is to eliminate the k_i's by permuting the columns by the permutation which maps the $(i-1)pq + k$'th column to the $(i-1)pq + (k \ominus k_i)$'th column.

The succeeding steps divide up into two subcases according to the value of w. Assume first of all that $w = t-2 = v$. Then $\gcd(n_{t-1}, pq) = 1$ and hence $xn_{t-1} \bmod pq$ runs through all the values $1,\ldots,pq$ as x does. Thus the following steps are meaningful.

(1) Permute the rows by the permutation which maps the $nn_{t-1} \bmod pq$'th row to the n'th row.

(2) Permute the columns by the permutation which maps the $(t-2)pq + (k + \{m_{t-1}p^{-1}q^{-1}\}-1)n_{t-1}$'th column to the $(t-2)pq + k$'th column, where the second term is taken mod pq in both instances.

(3) Permute the columns by the permutation which maps the $(i-1)pq + kn_{t-1}$'th column to the $(i-1)pq + k$'th column, for $i < t-1$ where the second term is taken mod pq in both instances.

In the resulting matrix the entry at the n'th row and $(i-1)pq + k$'th row is zero except that it is:

m_i for $i \le u$ and $k = n$;

$m_i p^{-1}$ for $u < i < t-1$ and $k = n \bmod q$;

$[m_{t-1}p^{-1}q^{-1}] + 1$ for $i = t-1$, $n = k \oplus s$ and $s = 0,\ldots,\{m_{t-1}p^{-1}q^{-1}\}-1$;

$[m_{t-1}p^{-1}q^{-1}]$ for $i = t-1$, $n = k \oplus s$ and $s = \{m_{t-1}p^{-1}q^{-1}\},\ldots,pq-1$;

$[m_t p^{-1}q^{-1}] + 1$ for $i = t$, $k = 1$ and $nn_{t-1} = 1,\ldots,\{m_t p^{-1}q^{-1}\}$

$[m_t p^{-1}q^{-1}]$ for $i = t$, $k = 1$ and $nn_{t-1} = \{m_t p^{-1}q^{-1}\} + 1,\ldots,pq$

(4) Subtract the $(t-2)pq + k + 1$'st column from the $(t-2)pq + k$'th column, $k = 1,\ldots,pq-1$.

In the resulting matrix the entry at the p'th row and $(t - 2)pq + k$'th column for $k \neq pq$ is zero except that when $n = k$ it is 1 and when $n = k \oplus \{m_{t-1}p^{-1}q^{-1}\}$ it is -1. The remaining columns are unchanged.

Since q but not p divides m_{t-1} the same is true for $\{m_{t-1}p^{-1}q^{-1}\} = m_{t-1} - [m_{t-1}p^{-1}q^{-1}]pq$. Hence as x runs through $1,\ldots,p$ and y runs through $0,1,\ldots,q - 1$, $x\{m_{t-1}p^{-1}q^{-1}\} \oplus y$ runs through $1,\ldots,pq$ and equals pq when $x = p$ and $y = 0$. Thus the following steps are meaningful.

(5) Permute the rows by the permutation which maps the $\ell\{m_{t-1}p^{-1}q^{-1}\} \oplus m$'th row $\ell = 1,\ldots,p$, $m = 0,\ldots,q - 1$ to the $(q - 1 - m)p + \ell$'th row.

(6) Permute the columns by the permutation which maps the $(i - 1)pq + (h\{m_{t-1}p^{-1}q^{-1}\} \oplus j)$'th column $h = 1,\ldots,p$, $j = 0,\ldots,q - 1$ to the $(i - 1)pq + (q - 1 - j)p + h$'th column for $i \neq t$. In particular the $(t - 1)pq$'th column remains fixed.

(7) Add the $(t - 2)pq + jp + \bar{h}$'th columns to the $(t - 2)pq + jp + h$'th column for each $\bar{h}$, $h < \bar{h} < p$, where $j = 0,1,\ldots,q - 1$ and $h = 1,\ldots,p - 2$.

(8) Add the $(t - 2)pq + jp + 1$'st column to the $(t - 2)pq + (j + 1)p$'th column, where $j = 0,1,\ldots,q - 2$.

In the resulting matrix the entry at the n'th row and $(i - 1)pq + k$'th column is zero except that it is:

m_i for $i \leq u$ and $k = n$;

$m_i p^{-1}$ for $u < i < t - 1$, $n = mp + \ell$, $k = jp + h$

$m = j = 0,\ldots,q - 1$ and $\ell, h = 1,\ldots, p$;

1 for $i = t - 1$ and $k = n \mp pq$;

-1 for $i = t - 1$, $n = p, 2p, \ldots, pq$,
and $k = n - p + 1, \ldots, n - 1$;

$[m_{t-1}p^{-1}q^{-1}] + 1$ for $i = t - 1$, $k = pq$, $n = mp + \ell$, $m = 0, \ldots, q - 1$
and ℓ takes on $\{m_{t-1}p^{-1}q^{-1}\}q^{-1}$ distinct values
in $\{1, \ldots, p\}$;

$[m_{t-1}p^{-1}q^{-1}]$ for $i = t - 1$, $k = pq$, $n = mp + \ell$, $m = 0, \ldots, q - 1$
and ℓ takes on the other values in $\{1, \ldots, p\}$;

$[m_{t}p^{-1}q^{-1}] + 1$ for $i = t$, $k = 1$, $n = mp + \ell$, $m = 0, \ldots, q - 1$
and ℓ takes on $\{m_{t}p^{-1}q^{-1}\}q^{-1}$ distinct values
in $\{1, \ldots, p\}$;

$[m_{t}p^{-1}q^{-1}]$ for $i = t$, $k = 1$, $n = mp + \ell$, $m = 0, \ldots, q - 1$
and ℓ takes on the other values in $\{1, \ldots, p\}$.

We can now view the rows as consisting of q sets with p rows each. We are in a position similar to the position we were in in the proof of Theorem 3.2 after the application of Lemma 6.1. Proceeding then in a similar manner it is not difficult to show that:

$$\begin{aligned}
\overline{\tau}_n \text{ (kernel } \psi) &= 0 \quad \text{for} \quad n \leq (t - 2)pq + 1 \ ; \\
&= \gcd(m_1, \ldots, m_{t-2}) \\
&\qquad \text{for} \quad n = (t - 2)pq + 2, \ldots, (t - 2)pq + q \ ; \\
&= \gcd(m_1, \ldots, m_{t-2}, m_{t-1}q^{-1}, m_t q^{-1}) \\
&\qquad \text{for} \quad n = (t - 2)pq \not\equiv q + 1 \ ; \\
&= 1 \quad \text{for} \quad n > (t - 2)pq + 1 \ .
\end{aligned}$$

This completes the discussion of the first subcase. We assume now that $w = t - 1$. Note that q divides n_{t-1}.

(1) Permute the rows by the permutation which maps the $\ell q + m$'th row, $\ell = 0,1,\ldots,p - 1$, $m = 1,\ldots,q$, to the $(m - 1)p + \ell + 1$'st row.

(2) Permute the columns by the permutation which maps the $jq + h$'th columns, $j = 0,1,\ldots,p - 1$, $h = 1,\ldots,q$, to the $(h - 1)p + j + 1$'st column.

In the resulting matrix the entry at the $mp + \ell$'th row, $m = 0,\ldots,q - 1$, $\ell = 1,\ldots,p$ and $(i - 1)pq + hp + j$'th column, $h = 0,\ldots,q$, $j = 1,\ldots,p$ is zero except that it is:

m_i for $i \leq u$, $m = h$ and $\ell = j$;

$m_i p^{-1}$ for $u < i < t - 1$ and $m = h$;

$[m_{t-1}p^{-1}] + 1$ for $i = t - 1$, $m = h$, $j = \ell + sn_{t-1}q^{-1} \bmod p$ and $s = 0,\ldots,\{m_i p^{-1}\} - 1$;

$[m_{t-1}p^{-1}]$ same as above except that $s = \{m_i p^{-1}\},\ldots,p - 1$;

$[m_t p^{-1} q^{-1}] + 1$ for $i = t$, $h = 0$, $j = 1$, $m = 0,\ldots,q - 1$ and ℓ takes on $\{m_t p^{-1} q^{-1}\}q^{-1}$ values in $\{1,\ldots,p\}$;

$[m_t p^{-1} q^{-1}]$ same as above except that ℓ takes on the other values in $\{1,\ldots,p\}$.

Again we view the rows as consisting of q sets with p rows each. We are in a position similar to the position we were in in the proof of Theorem 3.2 just before the application of Lemma 6.1. Proceeding then in a similar manner it is not difficult to show that:

$\overline{\tau}_n$ (kernel ψ) = 0 for $n \leq (t-2)pq + 1$;

= $\gcd(m_1,\ldots,\overline{m}_{t-1})$ for $n = (t-2)pq + 2,\ldots,(t-2)pq + q$;

= $\gcd(m_1,\ldots,m_{t-1}m_t q^{-1})$ for $n = (t-2)pq + q + 1$;

= 1 for $n > (t-2)pq + 1$.

This concludes the discussion of case 1.

Case 2. There is an i such that:

(1) neither p nor q divide m_i ;

(2) neither p nor q divide $x_i\psi$;

(3) $gp(x_j\psi \mid j \neq i) = Z_{pq}$.

The discussion of this case follows almost exactly the lines of the proof of Theorem 3.2. It is only necessary to prove something slightly more general than the statement of Lemma 6.1 in the proof of Theorem 3.2, which we have done in Section 7. It is not difficult to show that:

$\overline{\tau}_n$ (kernel ψ) = 0 for $n \leq (t-2)pq + 1$

= $\gcd(m_1,\ldots,m_t)$ for $n = (t-2)pq + 2$

= 1 for $n > (t-2)pq + 2$.

This concludes the proof of Theorem 4.4.

Section 10. The proofs of Theorems 3.4, 3.5 and 3.7

Before we actually prove the theorems it is necessary to discuss in detail the map f_p. In our discussion we derive two formulas for f_p and show that with a slight modification f_p maps the natural additive structure of M into a multiplicative structure for M. The computations involved in the proofs of the lemmas do not bear directly on the proofs of the theorems and are consequently postponed.

The first formula is a direct application of Theorems 3.1 and 3.2.

Lemma 10.1. If $m = x^{m_1} + \ldots + x^{m_t} \in M$ then

$$(m)f_p = \sum_J n(J)x^{g(J)} \quad \text{where:}$$

the sum is taken over all subsets J of $\{1,\ldots,t\}$;

$$a(J) = |\{j \in J \mid p \text{ does not divide } m_j\}|;$$

$$g(J) = \gcd(m_i \mid i \notin J) \quad \text{if} \quad a(J) = 0;$$

$$= \gcd(m_1,\ldots,m_t) \quad \text{if} \quad a(J) \neq 0;$$

$$n(J) = (p-1)^{|J|-a(J)}((p-1)^{a(J)} + (-1)^{a(J)}(p-1))p^{-1}.$$

Indeed if ψ is a homomorphism of $G(m_1,\ldots,m_t)$ into Z_p and $J = \{i \mid x_i\psi \neq 0\}$ then $g(J) = \lambda(\psi)$. It is only required to show that the number of homomorphisms, ψ, such that $J = \{i \mid x_i\psi \neq 0\}$ is $n(J)$.

We now modify the map f_p slightly.

Definition 10.2. Henceforth the map f_p will be taken to mean the map defined by the formula given in Lemma 10.1 except that $g(J) = 1$ if $a(J) \neq 0$.

Note that f_p remains unchanged when p divides $\gcd(m_1,\ldots,m_t)$ or when $\gcd(m_1,\ldots,m_t) = 1$. Since these are the only times that f_p

is applied there can be no real confusion. We can now state the second and more explicit formula for f_p .

Lemma 10.3. Let $m = x^{m_1} + \ldots + x^{m_t} \in M$, $H = \{i \mid p \text{ divides } m_i\}$ and $K = \{i \mid p \text{ does not divide } m_i\}$ then

$$(m)f_p = \delta(K)(p^{t-1} - p^{|H|})x^1 + \sum_{J \subseteq H} (p-1)^{|H|-|J|} x^{\gcd(m_i \mid i \in J \cup K)}$$

where $\delta(K) = 0$ if $K = \emptyset$ and $\delta(K) = 1$ if $K \neq \emptyset$.

In order to facilitate the proof of Lemma 10.3 we define inductively a multiplication on M .

Definition 10.4. $(x^{m_1} + \ldots + x^{m_t}) \cdot x^{m_0} = x^{\gcd(m_1, m_0)} + \ldots + x^{\gcd(m_t, m_0)}$ and for $m, \bar{m} \in M$, $m \cdot (\bar{m} + x^{m_0}) = m \cdot \bar{m} + m \cdot x^{m_0}$.

It follows that M is a commutative monoid under multiplication (the identity is x^0) and that multiplication distributes over addition. This can be proved directly. Alternately we can embed M in an integral semigroup ring. The semigroup consists of the non-negative integers where the product of h and k is $\gcd(h,k)$.

The multiplication is useful because of

Lemma 10.5. If $m \in M$ and p divides m_0 then

$$(m + x^{m_0})f_p = (m)f_p \cdot (x^{m_0})f_p .$$

We need only one more concept before we can proceed with the proofs of the theorems.

Definition 10.6. If h and k are non-negative integers then $h <_o k$ iff $h \neq 0$ and either $h < k$ or $k = 0$. $h \leq_o k$ iff $h = k$ or $h <_o k$.

It follows that for any pair of non-negative integers h and k, $\gcd(h,k) \leq_o h$.

The proof of Theorem 3.4.

"The f_p-equivalence classes on $A_{t,g}$ where p divides g and $g \neq 0$ are all singletons."

Indeed suppose $m = x^{m_1} + \ldots + x^{m_t}$ and $\bar{m} = x^{\bar{m}_1} + \ldots + x^{\bar{m}_t}$ belong to $A_{t,g}$ where the exponents are in increasing order, $m_1 \leq_o m_2 \leq_o \ldots$. Suppose further that $m \neq \bar{m}$. The theorem will follow if we can show $(m)f_p \neq (\bar{m})f_p$. Fix i to be the least index for which $m_j = \bar{m}_j$ for all $j > i$. Hence $m_i \neq \bar{m}_i$.

From Lemma 10.3 we have:

$$(x^{m_0})f_p = x^{m_0} + (p-1)x^0 \quad \text{if } p \text{ divides } m_0 ;$$

$$(x^{n_1} + \ldots + x^{n_s})f_p = (\Sigma\, x^{\ell_j}) + (p-1)^s x^0 \quad \text{where}$$

$\ell_j \leq_o \max(n_1, \ldots, n_s)$ if p divides $\gcd(n_1, \ldots, n_s)$.

Consequently

$$(m)f_p = (x^{m_1} + \ldots + x^{m_{i-1}})f_p \cdot (x^{m_i})f_p \cdot (x^{m_{i+1}} + \ldots + x^{m_t})f_p ;$$

$$= (\Sigma\, x^{h_j} + (p-1)^{i-1}x^0) \cdot (x^{m_i} + (p-1)x^0) \cdot (\Sigma^{k_j} + (p-1)^{t-i}x^0)$$

where $h_j \leq_o m_{i-1} \leq_o m_i$ for all j ;

$$= (\Sigma\, x^{h_j}) \cdot (x^{m_i} + \ldots + x^{m_t})f_p + (p-1)^{(i-1)}x^{m_i} \cdot \Sigma\, x^{k_j} +$$

$$(p-1)^{t-1}x^{m_i} + (p-1)^i(x^{m_{i+1}} + \ldots + x^{m_t})f_p$$

$$= \Sigma\, x^{r_j} + (p-1)^{t-1}x^{m_i} + (p-1)^i(x^{m_{i+1}} + \ldots + x^{m_t})f_p$$

where $r_j \leq_o m_i$ for all j .

The theorem follows now by comparing this with the corresponding expression for $(\bar{m})f_p$.

Before proceeding to the proof of Theorem 3,5 we draw a corollary from Lemma 10.3.

Corollary 10.7. If $m \in A_{t,1}$ and p divides $m_2,\ldots,m_t$ then

$$(m)f_p = (p-1)^{t-1}x^{m_1} + (p-1)^{t-2}x^{m_1}.(x^{m_2} + \ldots + x^{m_t}) +$$
$$(p-1)^{t-3}x^{m_1}.(x^{m_2}.x^{m_3} + \ldots + x^{m_2}.x^{m_t} + \ldots + x^{m_{t-1}}.x^{m_t}) +$$
$$\ldots + (p-1)x^{m_1}(x^{m_2}.\ \ldots\ .x^{m_{t-1}} + \ldots + x^{m_3}.\ \ldots\ .\ x^{m_t}) + x^1 .$$

The proof of Theorem 3.5.

"The G-equivalence classes on $B_t = \{m \in A_{t,1} \mid \gcd(m_j \mid j \neq i) \neq 1$ for each $i\}$ are all singletons."

First we note that $m_i \neq m_j$ for all $i \neq j$ in $\{1,\ldots,t\}$. Secondly if p divides less than $t-1$ of the m_i's then by Lemma 10.3 the coefficient of x^1, $\delta(K)(p^{t-1} - p^{|H|}) + 1$, is greater than or equal to p. On the other hand if p divides exactly $t-1$ of the m_i's then by Corollary 10.7 the coefficient of x^1 is exactly 1. Hence $(m)f_p = (p-1)^{t-1}x^{m_i} + \Sigma x^{\ell_j} + x^1$ where $1 <_o \ell_j \leq_o m_i$ for each j iff p divides $\gcd(m_j \mid j \neq i)$. As p runs over all primes, t distinct integers will appear as the greatest exponent in $(m)f_p$ when the coefficient of x^1 is 1. This distinguishes the whole set from the other elements of $A_{t,1}$ and the integers themselves distinguish the elements from one another, concluding the proof of the theorem.

The proof of Theorem 3.7.

"The f-classes on $A_{3,1}$ are the elements of B_3,C,D and $\{E\}$."

There are three possible forms for $(m)f_p$ when $m \in A_{3,1}$:

(i) $(p-1)^2x^{m_i} + (p-1)(x^{\gcd(m_i,m_j)} + x^{\gcd(m_i,m_k)}) + x^1$ if p divides m_j and m_k, $i \neq j \neq k \neq i$;

(ii) $(p-1)x^{\gcd(m_j,m_k)} + (p^2 - p + 1)x^1$ if p divides m_i but not m_j or m_k, $i \neq j \neq k \neq i$;

(iii) p^2x^1 if p divides neither m_1, m_2 nor m_3.

Clearly form (i) can never look like form (iii) but form (ii) can if $\gcd(m_j, m_k) = 1$. It follows that $(m)f_p = p^2x^1$ for all p iff $m \in E$. Hence E is an f-class. Form (i) can look like form (ii) but only if $\gcd(m_i, m_j) = \gcd(m_i, m_k) = 1$ in form (i) and $p = 2$.

The coefficient of x^1 can be p only in form (i) when one but not both of $\gcd(m_i, m_j)$ and $\gcd(m_i, m_k)$ are 1. Of course p divides $\gcd(m_j, m_k)$ so that it is not 1. It follows that all the elements $m \in A_{3,1}$ with two gcd is not equal to 1 are in a different f-class than the remainder of $A_{3,1}$. Furthermore $m \in C\binom{\alpha\ \beta}{a\ b}$ iff

$$(m)f_p = (p-1)^2x^{a\alpha} + (p-1)^\alpha + px^1 \text{ if } p \text{ divides } \beta;$$

$$= (p-1)^2x^{b\beta} + (p-1)^\beta + px^1 \text{ if } p \text{ divides } \alpha;$$

$$= (p-1)x^\alpha + (p^2 - p + 1)x^1 \text{ if } p \text{ divides } b \text{ but not } \beta;$$

$$= (p-1)x^\beta + (p^2 - p + 1)x^1 \text{ if } p \text{ divides } a \text{ but not } \alpha;$$

$$= p^2x^1 \text{ otherwise.}$$

Proving that the elements of C are f-classes.

Finally $m \in D\binom{\alpha}{a}$ iff

$$(m)f_p = (p-1)^2x^a + (2p-1)x^1 \text{ if } p \text{ divides } \alpha;$$

$$= (p-1)x^\alpha + (p^2 - p + 1)x^1 \text{ if } p \text{ divides } a;$$

$$= p^2x^1 \text{ otherwise.}$$

The only confusion that can arise is between $D\binom{\alpha}{a}$ and $D\binom{a}{\alpha}$. But $\gcd(a,\alpha) = 1$ so that 2 can divide only one of α and a. By choosing a prime which divides the odd one they are easily distinguished. This completes the proof of the theorem.

The proof of Lemma 10.1.

We are only required to show that the number of homomorphisms, ψ, of $G(m_1,\ldots,m_t)$ into Z_p for which $J = \{i \mid x_i\psi \neq 0\}$ is $n(J)$ which equals

$$(p - 1)^{|J| - a(J)}((p - 1)^{a(J)} + (-1)^{a(J)}(p - 1))p^{-1},$$

where $a(J) = |\{j \in J \mid p \text{ does not divide } m_j\}|$.

If $j \in J$ and $m_j = 0 \bmod p$ then $x_j\psi$ can take on any of the $p - 1$ values $\{1,\ldots,p - 1\}$. Whereas for $j \in J$ and $m_j \neq 0 \bmod p$ we must have the equation $\Sigma m_j(x_j\psi) = 0 \bmod p$. Hence $n(J)$ equals $(p - 1)^{|J| - a(J)}$ times $\mu(a)$, the number of zero sums mod p which can arise from $a = a(J)$ given non-zero mod p integers with non-zero mod p coefficients unless $a = 0$ when $\mu(a) = 1$. We want to show then that for all a

$$\mu(a) = ((p - 1)^a + (-1)^a(p - 1))p^{-1}.$$

This is certainly true for $a = 0$. We proceed inductively and assume $a > 0$. The total number of zero sums for a non-zero mod p integers is clearly p^{a-1}. Using our induction assumption and the fact that the number of these zero sums with exactly j non-zero mod p coefficients is $\binom{a}{j}\mu(j)$ for $j = 0,1,\ldots,a - 1$ we have

$$\mu(a) = p^{a-1} - \sum_{j=i}^{a-1} \binom{a}{j}\mu(j) \ ;$$

$$= p^{-1}(p^a - \sum_{j=0}^{a-1} \binom{a}{j}(p-1)^j - \sum_{j=0}^{a-1} \binom{a}{j}(-1)^j(p-1)) \ ;$$

$$= p^{-1}((p-1)^a + (-1)^a(p-1)) \ .$$

This concludes the proof of the lemma.

The proof of Lemma 10.5.

$$(m)f_p \cdot (x^{m_0})f_p = (\sum_J n(J)x^{g(J)}) \cdot (x^{m_0} + (p-1)x^0) \ ;$$

$$= \sum_J n(J)x^{\gcd(g(J),m_0)} + \sum_J (p-1)n(J)x^{g(J)} \ ;$$

where the sums are taken over all subsets, J, of $\{1,\ldots,t\}$. There is a one to one correspondence between the subsets of $\{1,\ldots,t\}$ and pairs of subsets of $\{0,1,\ldots,t\}$ which assigns to each subset, J, of $\{1,\ldots,t\}$ the pair $(J, J \cup \{0\})$. It is clear that $a(J) = a(J \cup \{0\})$ and that $(p-1)n(J) = n(J \cup \{0\})$. Furthermore if we let $\gamma(\ )$ be the function with respect to $\{0,1,\ldots,t\}$ corresponding to $g(\ )$ then $\gamma(J) = \gcd(g(J),m_0)$ and $\gamma(J \cup \{0\}) = g(J)$. Therefore

$$\sum_J n(J)x^{\gcd(g(J),m_0)} = \sum_J n(J)x^{\gamma(J)} \quad \text{and}$$

$$\sum_J (p-1)n(J)x^{g(J)} = \sum_{J \cup \{0\}} n(J \cup \{0\})x^{\gamma(J \cup \{0\})} \ .$$

Their sum then is just $(m + x^{m_0})f_p$, proving the lemma.

The proof of Lemma 10.3.

The proof is by induction on $|H|$.

If $|H| = 0$ then $H = \emptyset$ and $K = \{1,\ldots,t\} \neq \emptyset$.

We want to show that

$$(m)f_p = (p^{t-1} - 1)x^1 + x^{\gcd(m_1,\ldots,m_t)} \ .$$

This follows directly from Lemma 10.1. Indeed let J be a subset of $\{1,\ldots,t\}$ then $a(J) = 0$ iff $J = \emptyset$, $g(\emptyset) = \gcd(m_1,\ldots,m_t)$ and $n(\emptyset) = 1$. If $J \neq \emptyset$ then $a(J) = |J|$, $g(J) = 1$ and $n(J) = ((p-1)^{|J|} + (-1)^{|J|}(p-1))p^{-1}$. Thus

$$\begin{aligned}\sum_{J\neq\emptyset} n(J)x^{g(J)} &= \sum_{j=1}^{t}\binom{t}{j}((p-1)^j + (-1)^j(p-1))p^{-1}x^1 \\ &= (p^t - 1 - (p-1))p^{-1}x^1 \\ &= (p^{t-1} - 1)x^1 .\end{aligned}$$

This proves the result when $|H| = 0$.

If $|H| \neq 0$ then $m = \bar{m} + x^{mt}$ where p divides m_t and $\bar{m} \in M$ unless $t = 1$. If $t = 1$ then $m = x^{mt}$ and $(m)f_p = n(\emptyset)x^{g(\emptyset)} + n(1)x^{g(1)}$ where $a(\emptyset) = 0$, $g(\emptyset) = m_1$, $n(\emptyset) = 1$ and $a(1) = 0$, $g(1) = 0$, $n(1) = (p-1)$. Thus $(m)f_p = x^{m1} + (p-1)x^0$, which is just what is required. If $t \neq 1$ then $|\bar{H}| = |H| - 1$ where $\bar{H}$ corresponds to H with respect to $\bar{m}$ and we can assume that the lemma holds for $\bar{m}$. Note that K is the same for both m and $\bar{m}$.

$$\begin{aligned}(m)f_p &= (\bar{m})f_p(x^{mt})f_p \\ &= (\delta(K)(p^{t-2} - p^{|\bar{H}|})x^1 + \sum_{J\subseteq\bar{H}}(p-1)^{|\bar{H}|-|J|}x^{\gcd(m_i\,|\,i\in J\cup K)}) \cdot \\ &\quad (x^{mt} + (p-1)x^0)\end{aligned}$$

Now $x^1(x^{mt} + (p-1)x^0) = px^1$ so that

$$\delta(K)(p^{t-2} - p^{|\bar{H}|})x^1\cdot(x^{mt} + (p-1)x^0) = \delta(K)(p^{t-1} - p^{|H|}) .$$

Furthermore

$$\left(\sum_{J\subseteq\overline{H}} (p-1)^{|\overline{H}|-|J|}\, x^{\gcd(m_i \mid i\in J\cup K)}\right).x^{m_t} =$$
$$\sum_{J\subseteq\overline{H}} (p-1)^{|H|-|J\cup\{t\}|}\, x^{\gcd(m_i \mid i\in J\cup K\cup\{t\})}$$

and

$$\left(\sum_{J\subseteq\overline{H}} (p-1)^{|\overline{H}|-|J|}\, x^{\gcd(m_i \mid i\in J\cup K)}\right).(p-1)x^{0} =$$
$$\sum_{J\subseteq\overline{H}} (p-1)^{|H|-|J|}\, x^{\gcd(m_i \mid i\in J\cup K)}\ .$$

The lemma follows by putting together the above equations.

Section 11. The proofs of Lemma 4.3 and Theorem 4.5

The proof of Lemma 4.3.

"If p_i divides m_i for each i and $s = p_1p_2p_3$ then $G(m_1,m_2,m_3)/gp(g^s \mid g \in G(m_1,m_2,m_3))$ needs 3 generators."

Assume first of all that there are distinct primes p and q so that p divides p_1 and q divides p_2. Let ψ be the homomorphism of $G(m_1,\ldots,m_t)$ onto Z_{pq} which maps x_1 to q, x_2 to p and x_3 to 0. By the proof of Theorem 4.1 we see that $N/N' = Z_0^{pq+1} \oplus Z_{m_3}^{(p-1)(q-1)} \oplus \ldots$, where N = kernel ψ. Let $K = gp(\{g^{p3} \mid g \in N\},N')$ then K is characteristic in N and thus normal in $G(m_1,m_2,m_3)$. N/K is a direct sum of more than $pq + 1$ cycles of order p_3 and has index pq in $G(m_1,m_2,m_3)/K$. If $G(m_1,m_2,m_3)/K$ needed only two generators then by the Schreier index theorem N/K would need no more than $pq + 1$ generators. Hence $G(m_1,m_2,m_3)/K$ needs three generators. Since $g^s \in K$ for each $g \in G(m_1,m_2,m_3)$ we see that $G(m_1,m_2,m_3)/K$ is a homomorphic image of $G(m_1,m_2,m_3)/gp(g^s \mid g \in G(m_1,m_2,m_3))$, proving the lemma in this case. If $p_1 = p_2 = p_3 = p$ a prime then we prove the lemma in a similar way substituting Theorem 3.1 for Theorem 4.1.

The proof of Theorem 4.5.

"The G-equivalence classes on $C\binom{\alpha\ \beta}{a\ b}$, $D\binom{\alpha}{a}$ and E are all singletons."

We will deal with $C\binom{\alpha\ \beta}{a\ b}$, $D\binom{\alpha}{a}$ and E separately. For all cases though, the number of homomorphisms of $G(m_1,m_2,m_3)$ onto Z_{pq} is $(p^2 - 1)(q^2 - 1)$. If ψ is a homomorphism then $\lambda(\psi)$ will be an abbreviation for $\overline{\tau}_{pq+2}$ (kernel ψ).

The class $C\binom{\alpha\ \beta}{a\ b}$. Let $m \in C\binom{\alpha\ \beta}{a\ b}$. We may assume without loss of generality that $\gcd(m_1,m_2) = \alpha$, $\gcd(m_1,m_3) = \beta$, $m_2 = a\alpha$ and $m_3 = b\beta$. Choose distinct primes p and q so that p divides α and q divides β. Then by Theorem 4.1 we see that $\lambda(\psi)$ is:

0 if $x_1\psi \neq 0$, $x_2\psi = q,\ldots,(p-1)q$, $x_3\psi = p,\ldots,(q-1)p$;

m_1 if $x_1\psi = 0$, $x_2\psi = q,\ldots,(p-1)q$, $x_3\psi = p,\ldots,(q-1)p$;

$a\alpha$ if $x_1\psi \neq 0 \bmod p$, $x_2\psi = 0$, $x_3\psi = p,\ldots,(q-1)p$;

$b\beta$ if $x_1\psi \neq 0 \bmod q$, $x_2\psi = q,\ldots,(p-1)q$, $x_3\psi = 0$;

1 if $x_1\psi \neq 0 \bmod p$ and $\bmod q$, $x_2\psi = 0$, $x_3\psi = 0$.

The total number of maps listed above is $(p^2-1)(q^2-1)$: $(pq-1)(p-1)(q-1)$ for 0, $(p-1)(q-1)$ for m_1, $(pq-q)(q-1)$ for $a\alpha$, $(pq-p)(p-1)$ for $b\beta$ and $(p-1)(q-1)$ for 1. Therefore we have listed all of them. Clearly m is distinguished from all the other elements of $C\binom{\alpha\ \beta}{a\ b}$ by the second line, proving the theorem in this case.

The class $D\binom{\alpha}{a}$. Let $m \in D\binom{\alpha}{a}$. We may assume without loss of generality that $m_1 = a$ and $\gcd(m_2,m_3) = \alpha$. Choose distinct primes p and q so that p divides a and q divides α. By Theorem 4.1 we see that $\lambda(\psi)$ is:

0 if $x_1\psi = q,\ldots,(p-1)q$, $x_2\psi = p,\ldots,(q-1)p$, $x_3\psi = p,\ldots,(q-1)p$,

m_2 if $x_1\psi = q,\ldots,(p-1)q$, $x_2\psi = 0$, $x_3\psi = p,\ldots,(q-1)p$,

m_3 if $x_1\psi = q,\ldots,(p-1)q$, $x_2\psi = p,\ldots,(q-1)p$, $x_3\psi = 0$.

By Theorem 4.4 (Case 1), $\lambda(\psi)$ is:

1 if $x_1\psi = 0 \bmod q$, $x_2\psi \not\equiv 0 \bmod p$ and q, $x_3\psi = q,\ldots,(p-1)q$;

or if $x_1\psi = 0 \bmod q$, $x_2\psi = q,\ldots,(p-1)q$, $x_3\psi \not\equiv 0 \bmod p$ and q ;

a if $x_1\psi = 0 \bmod q$, $x_2\psi$ and $x_3\psi \not\equiv 0 \bmod p$ and q ;

where in all cases we must have $m_2(x_2\psi) + m_3(x_3\psi) = 0 \bmod p$.

The total number of maps listed above is $(p^2-1)(q^2-1)$: $(p-1)(q-1)^2$ for 0, $(p-1)(q-1)$ for m_2, $(p-1)(q-1)$ for m_3, $2p(p-1)(q-1)$ for 1 and $p(p-1)(q-1)^2$ for a . Therefore we have listed all of them. Cleraly m is distinguished from all the other elements of $D\binom{\alpha}{a}$ by the second and third line, proving the theorem in this case.

The class E . Let $m \in E$. Let p,q and r be distinct primes which divide m_1, m_2 and m_3 respectively. By Lemmas 4.2 and 4.3 if $\bar{m}$ is G-equivalent to m then p,q and r also divide $\bar{m}_1, \bar{m}_2$ and $\bar{m}_3$, in some order, respectively. First we look at the maps onto Z_{pq} and show that the $\bar{m}_i$ which is divisible by r must equal m_3 . The exact same process works for maps onto Z_{pr} and Z_{qr} proving that $\bar{m}_1, \bar{m}_2$ and $\bar{m}_3$ must be m_1, m_2 and m_3 in some order, which is just what is required.

For all maps ψ onto Z_{pq} $x_3\psi$ is uniquely determined, once $x_1\psi$ and $x_2\psi$ have been chosen, by the equations $m_1(x_1\psi) + m_3(x_3\psi) = 0 \bmod q$ and $m_2(x_2\psi) + m_3(x_3\psi) = 0 \bmod p$.

By Theorem 4.1 $\lambda(\psi)$ is

m_3 if $x_1\psi = q,\ldots,(p-1)q$, $x_2\psi = p,\ldots,(q-1)p$, $x_3\psi = 0$.

By Theorem 4.4 (Case 1) $\lambda(\psi)$ is

1 if $x_1\psi = 0 \bmod q$, $x_2\psi \neq 0 \bmod p$ and q, $x_3\psi = q,\ldots,(p-1)q$.

By Theorem 4.4 (Case 1), the roles of p and q interchanged) $\lambda(\psi)$ is

1 if $x_1\psi \neq 0 \bmod p$ and q, $x_2\psi = 0 \bmod p$, $x_3\psi = p,\ldots,(q-1)p$.

By Theorem 4.4 (Case 2) $\lambda(\psi)$ is

1 if $x_1\psi \neq 0 \bmod q$, $x_2\psi \neq 0 \bmod p$, $x_3\psi \neq 0 \bmod p$ and q .

The total number of maps listed above is $(p^2-1)(q^2-1)$: $(p-1)(q-1)$ for m_1 and $p(p-1)(q-1) + q(p-1)(q-1) + (pq-p)(pq-q)$ for 1 . Therefore we have listed all of them. The required result follows from the first line.

BIBLIOGRAPHY

[1] Baumslag, G., Some groups that are just about free, Bull. Amer. Math. Soc. 73, (1967) pp. 621-622.

[2] Baumslag, G., Groups with the same lower central sequence as a relatively free group. I: The groups, Trans. Amer. Math. Soc. 129, (1967) pp. 308-321.

[3] Baumslag, G., Groups with the same lower central sequence as a relatively free group. II: Properties, Trans. Amer. Math. Soc. (to appear).

[4] Baumslag, G., On the residual finiteness of generalized free products of nilpotent groups, Trans. Amer. Math. Soc. 106, (1963) pp. 193-209.

[5] Whittemore, A., The Frattini subgroup, Dissertation, The City University of New York, (1967).

[6] Magnus, W., Karrass, A., and Solitar, D., Combinatorial group theory, Interscience Publishers, New York, (1966).

AUTOBIOGRAPHICAL STATEMENT

Stephen A. Meskin was born June 15, 1940 in New York City. He attended East Meadow High School on Long Island graduating in 1958 and then Rensselaer Polytechnic Institute at Troy, New York, graduating cum laude in 1962. He did a year of graduate work at New York University and spent two years at New York Life Insurance Company before beginning his doctoral studies at The City University of New York in September, 1965. He received an M.A. from Queens College in 1967. He is a member of Pi Mu Epsilon, the Mathematical Association of America, the American Mathematical Society and formerly an Associate of the Society of Actuaries.

In 1962 he married the former Adrien J. Bien. They have a son, Aaron, born in 1966.