Formal Dept

Free Generators and the Free Differential Calculus

A Dissertation presented

by

Ira Miles Topping

to

The Graduate School

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Mathematics

State University of New York

at

Stony Brook

June, 1973

STATE UNIVERSITY OF NEW YORK

AT STONY BROOK

THE GRADUATE SCHOOL

Ira Miles Topping

We, the dissertation committee for the above candidate for the Doctor of Philosophy degree, hereby recommend acceptance of the dissertation.

James Simons, Chairman

Elvira R. Strasser, Advisor

Shing-Tung Yau

Irving Gerst

The dissertation is accepted by the Graduate School.

Herbert Weisinger, Dean

May 14, 1973

Abstract of the Dissertation

Free Generators and the Free Differential Calculus

by

Ira Miles Topping

Doctor of Philosophy

in

Mathematics

State University of New York at Stony Brook

1973

Let X be the free group on two generators, x and y. The object of this paper is to give a characterization of the free generators of X. The basis of this work will be the free differential calculus, developed by R. H. Fox. The setting is the integral group ring, ZX, of X.

A derivation in the group ring is a mapping $D: ZX \to ZX$ such that for any two elements p and q in ZX,

$$D(p + q) = D(p) + D(q)$$

$$D(pq) = D(p)q^* + pD(q)$$

where q^* is the image of q under what is called the augmentation homomorphism of ZX onto X; it maps the element $\sum n_i g_i$ of ZX onto its coefficient sum.

The derivations in ZX form a right ZX-module which is generated by the derivations D_x and D_y, called, respectively, the partial derivative with respect to x

and the partial derivative with respect to y. D_x and D_y are defined by

$$D_x(x) = 1, \; D_x(y) = 0$$
$$D_y(x) = 0, \; D_y(y) = 1.$$

For any element p of ZX, the partial derivatives of p will be denoted by p_x and p_y.

There is a formula, due to Fox, which states that for an arbitrary element p of ZX,

$$p - p^* = p_x(x - 1) + p_y(y - 1).$$

Thus, from the partial derivatives of an element, one can recover that element.

An element u of X will be said to have relatively prime partial derivatives if there exist elements p and q of ZX such that $u_x p + u_y q = 1$. It is shown that if u is a free generator of X, then u has relatively prime partial derivatives.

As a first step in establishing the converse of this theorem, it is shown that if an element u of X has relatively prime partial derivatives, then, modulo the first commutator subgroup, u is a free generator. It is then proven that, in fact, u must be a free generator modulo the second commutator subgroup; that is, u must be the product of a free generator with an element of the second commutator subgroup.

Obstacles to extending these results to free groups on more than two generators are also discussed.

Dedication

To the liberation of all peoples.

Table of Contents

Introduction

Let X be the free group on two generators, x and y. The object of this paper is to give a characterization of the free generators of X. The basis of this work will be the free differential calculus, developed by R. H. Fox in [6]. The setting is the integral group ring, ZX, of X.

A derivation in the group ring is a mapping $D: ZX \to ZX$ such that for any two elements p and q in ZX,

$$D(p + q) = D(p) + D(q)$$

$$D(pq) = D(p)q^* + pD(q)$$

where q^* is the image of q under what is called the augmentation homomorphism of ZX onto X; it maps the element $\sum n_i g_i$ of ZX onto its coefficient sum.

The derivations in ZX form a right ZX-module which is generated by the derivations D_x and D_y, called, respectively, the partial derivative with respect to x and the partial derivative with respect to y. D_x and D_y are defined by

$$D_x(x) = 1, \; D_x(y) = 0$$

$$D_y(x) = 0, \; D_y(y) = 1.$$

For any element p of ZX, the partial derivatives of p will be denoted by p_x and p_y.

The kernel of the augmentation homomorphism is called the augmentation ideal of ZX, and is freely generated by $x - 1$ and $y - 1$. For any element p of the augmentation ideal, the fundamental formula, presented in Section I, tells us that

$$p = p_x(x - 1) + p_y(y - 1).$$

Thus, from the partial derivatives of an element, one can recover that element.

An element u of X will be said to have relatively prime partial derivatives if there exist elements p and q of ZX such that $u_x p + u_y q = 1$. In Section I we prove that if u is a free generator of X, then u has relatively prime partial derivatives. The other results of Section I are taken from Fox's paper [6]. To lay the groundwork for the generalization of the results in the following pages to free groups on more than two generators, it is not assumed that X has only two generators until Section II. In that Section, it is proven that if an element u of X has relatively prime partial derivatives, then, modulo the first commutator subgroup, u is a free generator. In Section III it is proven that if u has relatively prime partial derivatives, then, in fact, u is a free generator modulo the second commutator subgroup. Thus, if u is a free generator, then u has relatively prime partial derivatives, and conversely, if u has relatively prime partial derivatives, then u must be the product of a free generator with an element of the second commutator subgroup. In Section III, the obstacles to extending these results to free groups on more than two generators is also discussed.

Throughout this paper, the notation $\{a_i\}$ is used to mean a collection of objects of the form a_i, where i varies over some indexing set.

A major contribution of R. H. Fox to topology and group theory has been the Free Differential Calculus - it developed from his investigations of the Alexander polynomial of a knot. In the bibliography are listed some of the works in which it has been used.

I Derivations in a Group Ring

Let G be a multiplicative group. The group ring (more specifically, the integral group ring) of G, denoted by ZG, is composed of elements of the form $\sum_g n_g g$, where the n_g, belonging to the ring of integers Z, are almost all zero, and the summation is taken over all group elements, g. Addition and multiplication in ZG are defined by

$$\sum_g n_g g + \sum_g m_g g = \sum_g (n_g + m_g) g$$
$$\left(\sum_g n_g g\right)\left(\sum_g m_g g\right) = \sum_g \left(\sum_h n_{gh} m_{h^{-1}}\right) g.$$

Alternatively, an element of ZG is of the form $\sum_{i=1}^{r} n_i g_i$. One defines addition in the purely formal way of juxtaposing terms, where $ng + mh = (n + m)g$ if and only if $g = h$, and one defines multiplication by

$$\left(\sum_{i=1}^{r} n_i g_i\right)\left(\sum_{j=1}^{s} m_j h_j\right) = \sum_{i=1}^{r}\left(\sum_{j=1}^{s} n_i m_j g_i h_j\right).$$

The group element g is identified with the group ring element 1g, and the integer n is identified with the group ring element $n1_G$, where 1_G is the group identity. In this way, both Z and G are considered as subsets of ZG.

Given a homomorphism of groups $f:G \to H$, one defines the induced ring homomorphism $f:ZG \to ZH$ by $f(\sum_i n_i g_i) = \sum_i n_i f(g_i)$. Let N be a normal subgroup of G and let $f:G \to G/N$ be the natural homomorphism. Then the ring homomorphism $f: ZG \to Z(G/N)$ has a two-sided ideal, $\mathfrak{N}$, as its kernel, and we say that $\mathfrak{N}$ corresponds to N. Clearly N and $\mathfrak{N}$ have no elements in common. Conversely, given a two-sided ideal $\mathfrak{M}$ in ZG, one considers the natural ring homomorphism $F: ZG \to ZG/\mathfrak{M}$. Looking at the restriction of F to G, one gets a normal subgroup M of G, consisting of those elements of G which are mapped to 1 by F, and we say that M is determined by $\mathfrak{M}$.

Theorem 1.

The ideal $\mathfrak{N}$ that corresponds to the normal subgroup N also determines N, and is the smallest ideal which determines N.

Proof.

Let $f: G \to G/N$ be the natural homomorphism. Then $\mathfrak{N}$ is just the kernel of the extension of f to ZG, so the normal subgroup determined by $\mathfrak{N}$ is just the group-kernel of the restriction to G of the extension of f, which is the kernel of the homomorphism we started with, which is N.

Now suppose another ideal $\mathfrak{A}$ also determines N, and let $F: ZG \to ZG/\mathfrak{A}$, so F restricted to G also has group-kernel N. Suppose $\hat{a} = \Sigma a_i g_i$ is any element of the ideal $\mathfrak{N}$. Then

$$0 = f(\hat{a}) = f(\Sigma a_i g_i) = \Sigma a_i f(g_i)$$

is a linear combination of cosets of N, say $\sum_j A_j f(g_j)$, where A_j is the sum of those n_i such that $f(g_i) = f(g_j)$. Now $0 = \sum_j A_j f(g_j)$ implies that each A_j is zero, since distinct cosets of N are linearly independent in $Z(G/N)$. To show that $\hat{a}$ must also belong to the ideal $\mathfrak{a}$, we calculate

$$F(\hat{a}) = F(\sum_i n_i g_i) = \sum_i n_i F(g_i).$$

Now $F(g_i) = F(g_j)$ if and only if $f(g_i) = f(g_j)$, since F restricted to G and f restricted to G have the same kernel. Thus $F(\hat{a}) = \sum_j B_j F(g_j)$, where B_j is the sum of those n_i such that $F(g_i) = F(g_j)$, and so $B_j = A_j = 0$ for each j. Therefore, $F(\hat{a}) = 0$, and so $\hat{a}$ belongs to $\mathfrak{a}$.

The following theorem shows how elements of the ideal corresponding to a given normal subgroup are related to the elements of that subgroup.

Theorem 2.

If the normal subgroup H of G is generated by $\{h_t\}$, then the ideal $\mathfrak{H}$ corresponding to H is generated by $\{h_t - 1\}$.

Proof.

Let f be the homomorphism with group-kernel H and ring-kernel $\mathfrak{H}$, and let $\sum n_i g_i$ be any element of $\mathfrak{H}$, so $0 = f(\sum n_i g_i) = \sum n_i f(g_i)$. For each j such that $f(g_j) = f(g_1)$, we have $\sum_j n_j = 0$, so

$$\sum_j n_j g_j = \sum_j n_j (g_j g_1^{-1} - 1) g_1 + \sum_j n_j g_1 = \sum_j n_j (g_j g_1^{-1} - 1) g_1.$$

Since $f(g_j g_1^{-1}) = 1$, we know that $g_j g_1^{-1}$ is an element of H, so $\sum_j n_j g_j$ is a linear combination of elements of the form $h - 1$, where h is in H. To show that $\sum_j n_j g_j$ is then a linear combination of the $h_t - 1$, it need only be shown that $h - 1$ is. But since h is a product of conjugates of the h_t and the h_t^{-1}, this follows immediately from the identities

$$\text{i)}\quad h^{-1} - 1 = -h^{-1}(h - 1)$$

$$\text{ii)}\quad hk - 1 = h(k - 1) + (h - 1)$$

$$\text{iii)}\quad ghg^{-1} - 1 = g(h - 1)g^{-1},$$

thusly: since h is in H, we have $h = \prod_{i=1}^{s} b_i h_{t_i}^{\varepsilon_i} b_i^{-1}$, where b_i is in G and ε_i is ± 1, so by identity (ii) we have

$$h - 1 = \sum_{i=1}^{s} (b_1 h_{t_1}^{\varepsilon_1} b_1^{-1} \cdots b_{i-1} h_{t_{i-1}}^{\varepsilon_{i-1}} b_{i-1}^{-1})(b_i h_{t_i}^{\varepsilon_i} b_i^{-1} - 1).$$

Thus $h - 1$ is a combination of terms, each a multiple of $(b_i h_{t_i}^{\varepsilon_i} b_i^{-1} - 1)$, which equals $b_i(h_{t_i}^{\varepsilon_i} - 1)b_i^{-1}$, which, by identity (i), is a multiple of $(h_{t_i} - 1)$.

Throughout this paper, we will designate by τ the trivial homomorphism, $\tau : G \to 1$, whose group-kernel is G itself. The induced homomorphism maps ZG onto Z by $\tau(\sum n_i g_i) = \sum n_i$; thus, an element of ZG is mapped onto its coefficient sum. The notation a^* will also be used to denote the coefficient sum of the element a in ZG. The ring-kernel of τ, denoted by $\mathfrak{A}$, is called the fundamental ideal, or the augmentation ideal, of ZG, and consists of all elements whose coefficient sum is zero. From Theorem 2, we see that $\mathcal{A}$ is generated by $\{g_t - 1\}$, where $\{g_t\}$ generates G.

Definition 1.

A derivation in the group ring ZG is a map $D: ZG \to ZG$ such that for any two elements a and b in ZG, we have

(8.1) $$D(a + b) = D(a) + D(b)$$

(8.2) $$D(ab) = D(a)b^* + aD(b).$$

Some basic and easy facts are the following:

(8.3) $D(gh) = D(g) + gD(b)$ where g and h belong to G

(8.4) $D(n) = 0$ where n is an integer

(8.5) $D(\Sigma n_i g_i) = \Sigma n_i D(g_i)$

(8.6) $D(a_1 \cdots a_s) = \sum_{i=1}^{s} a_1 \cdots a_{i-1} D(a_i) a_{i+1}^* \cdots a_s^*$, where the a_i belong to ZG

(8.7) $D(g^{-1}) = -g^{-1}D(g)$

The set of derivations in ZG forms a right ZG-module, where addition is defined by $(D_1 + D_2)(a) = D_1(a) + D_2(a)$, and right multiplication by an element b of ZG is defined by $(Db)(a) = D(a)b$. It is trivial to verify that what we have defined are still derivations.

We now turn to derivations in the group ring of a free group. Although the main results of this paper are valid only for the free group on two generators, this section will deal with arbitrary free groups (a denumerable set of generators is assumed only for the sake of ease of notation, for otherwise subscripts would have a way of getting out of hand).

Let X be the free group on the generators $x_1, x_2, \ldots$ An element of X is an equivalence class of words formed from the x_i and the x_i^{-1}, where two words are called equivalent if one may be obtained from the other by a finite number of insertions or deletions of symbols of the form $x_j x_j^{-1}$ or $x_j^{-1} x_j$. Each equivalence class of words may be represented by a unique "reduced word" $\prod_{i=1}^{n} x_{j_i}^{\varepsilon_i}$, meaning that $\varepsilon_i = \pm 1$, and if $j_k = j_{k+1}$ then $\varepsilon_k + \varepsilon_{k+1}$ does not equal zero. Without any harm, an element of the free group is often taken to be its reduced representative.

The fundamental ideal of X will be denoted by $\mathfrak{X}$. From Theorem 2, we see that $\mathfrak{X}$ is generated by $\{x_i - 1\}$. After the following theorem, in which we will distinguish certain derivations in ZX, namely, the partial derivatives with respect to a generator x_i, we will show that the $x_i - 1$ actually form a basis for $\mathfrak{X}$.

Theorem 3.

To each free generator x_j of X there corresponds a derivation $D_j : a \to (\partial a/\partial x_j)$, called the derivative with respect to x_j, such that

(10.1) $(\partial x_k/\partial x_j) = \delta_{j,k}$ (the Kroneker delta).

Furthermore, given elements $b_1, b_2, \ldots$ in ZX, there exists a unique derivation D mapping x_i into b_i for each i; it is given by the formula

(10.2) $$D(a) = \sum(\partial a/\partial x_j)b_j.$$

Proof.

For every natural number j and for every element u of X, define

$$\langle j,u\rangle = \begin{cases} 1 & \text{if } x_j \text{ is an initial segment of } u \\ 0 & \text{otherwise} \end{cases}$$

and extend this definition linearly to ZX:

$$\langle j, \sum n_u u\rangle = \sum n_u \langle j,u\rangle.$$

Now, for every natural number j, for every element w of X, and for every element a of ZX, define

$$\langle j,w,a\rangle = \langle j,w^{-1}a\rangle - \langle j,w^{-1}\rangle a^*.$$

If $a = \sum n_u u$, we have

$$\begin{aligned}\langle j,w,a\rangle &= \langle j,w,\sum n_u u\rangle \\ &= \langle j,\sum n_u w^{-1}u\rangle - \langle j,w^{-1}\rangle \sum n_u \\ &= \sum n_u \langle j,w^{-1}u\rangle - \sum n_u \langle j,w^{-1}\rangle \\ &= \sum n_u (\langle j,w^{-1}u\rangle - \langle j,w^{-1}\rangle) \\ &= \sum n_u \langle j,w,u\rangle.\end{aligned}$$

If w is not an initial segment of u, then $\langle j,w^{-1}u\rangle - \langle j,w^{-1}\rangle$ will equal zero, for in this case, x_k is an initial segment of $w^{-1}u$ if and only if it is an initial segment of w^{-1}. Since w is not an initial segment of u for all but a finite number of w in X, we see that, given a natural number j and an element a of ZX, $\langle j,w,a\rangle$ will equal zero for almost all w in X. We now define the derivative of a with respect to x_j to be the finite sum

$$(\partial a/\partial x_j) = \sum_w \langle j,w,a\rangle w.$$

By the linearity of the definition of $\langle j,w,a\rangle$, it is clear that (8.1) is satisfied, so to show that $(\partial a/\partial x_j)$ is a derivation, we need only prove (8.3), which, together with (8.1), will establish (8.2). Let u and v be any two elements of X. Then

$$\begin{aligned}(\partial uv/\partial x_j) &= \sum_w \langle j,w,uv\rangle w\\ &= \sum_w (\langle j,w^{-1}uv\rangle - \langle j,w^{-1}\rangle)w\\ &= \sum_w (\langle j,w^{-1}u\rangle - \langle j,w^{-1}\rangle)w + \sum_w (\langle j,w^{-1}uv\rangle - \langle j,w^{-1}u\rangle)w.\end{aligned}$$

In the last sum, let $t = u^{-1}w$, whence $w^{-1}u = t^{-1}$, and as w ranges through X, so does t, and so we get

$$\begin{aligned}(\partial uv/\partial x_j) &= (\partial u/\partial x_j) + \sum_t (\langle j,t^{-1}v\rangle - \langle j,t^{-1}\rangle)ut\\ &= (\partial u/\partial x_j) + u\sum_t (\langle j,t^{-1}v\rangle - \langle j,t^{-1}\rangle)t\\ &= (\partial u/\partial x_j) + u(\partial v/\partial x_j).\end{aligned}$$

Therefore, $(\partial a/\partial x_j)$ is a derivation.

To prove (10.1), we use the fact that the only initial segments of x_k are 1 and x_k itself, so

$$\begin{aligned}(\partial x_k/\partial x_j) &= \sum_w \langle j,w,x_k\rangle w\\ &= \langle j,1,x_k\rangle + \langle j,x_k,x_k\rangle x_k\\ &= \langle j,x_k\rangle - \langle j,1\rangle + (\langle j,1\rangle - \langle j,x_k^{-1}\rangle)x_k\end{aligned}$$

$$(\partial x_k/\partial x_j) = \delta_{j,k} - 0 + (0 - 0)x_k$$
$$= \delta_{j,k}.$$

To prove (10.2), we notice that $\sum_j(\partial a/\partial x_j)b_j$ is a finite sum, since $(\partial a/\partial x_j)$ is zero for almost all j. Since each $(\partial a/\partial x_j)$ is a derivation, and the set of all derivations in ZX is a right ZX-module, the map given by (10.2) is a derivation, and obviously sends each x_k into b_k. To show D is unique, suppose D' is another derivation mapping x_k into b_k for each k. Then $D' - D$ is a derivation mapping x_k into 0, hence mapping x_k^{-1} into $-x_k^{-1}(0) = 0$, by (8.7), hence mapping every element of ZX into 0, and so $D' = D$.

To show, now, that the $x_i - 1$ form a basis for $\mathfrak{X}$, suppose $0 = \sum_i b_i(x_i - 1)$. Differentiating both sides with respect to x_k, we get

$$\begin{aligned} 0 &= \sum_i D_k[b_i(x_i - 1)] \\ &= \sum_i[D_k(b_i)(x_i - 1)^* + b_i D_k(x_i - 1)] \\ &= b_k D_k(x_k - 1) \\ &= b_k. \end{aligned}$$

Since each b_i must be zero, the $x_i - 1$ are independent.

The fundamental formula states, that for any element a of ZX,

$$a - a^* = \sum_j(\partial a/\partial x_j)(x_j - 1).$$

This formula is derived from Theorem 3 and the fact that the mapping $D: a \to a - a^*$ is a derivation: that D

satisfies (8.1) is trivial, and to show D satisfies (8.2), one notices that $D(ab) = ab - (ab)^* = ab - a^*b^* = ab - ab^* + ab^* - a^*b^* = a(b - b^*) + (a - a^*)b^* = aD(b) + D(a)b^*$. The fundamental formula suggests that the partial derivatives of an element have some importance.

There is a way to write down $(\partial u/\partial x_j)$ immediately for any element u of X. First, if $u = x_k^p$ is a power of a generator, we use the fundamental formula and the fact that $(\partial x_k/\partial x_j)$ is zero if $j \neq k$ to get $x_k^p - 1 = (\partial x_k^p/\partial x_k)(x_k - 1)$, so

$$(\partial x_k^p/\partial x\ ) = \frac{x_k^p - 1}{x_k - 1} = \begin{cases} 1 + x_k + \cdots + x_k^{p-1} & \text{if } p \geq 1 \\ 0 & \text{if } p = 0 \\ -x_k^p - x_k^{p-1} - \cdots - x_k^{-1} & \text{if } p \leq -1 \end{cases}.$$

Now that the derivative of a power of a generator, with respect to that generator, can immediately be written down, we use (8.6), after writing u in the form $u = u_0 x_j^{p_1} u_1 x_j^{p_2} \cdots u_{s-1} x_j^{p_s} u_s$, where each u_i does not involve x_j (so $(\partial u_i/\partial x_j) = 0$), to get

$$(\partial u/\partial x_j) = \sum_{i=1}^{s} u_0 x_j^{p_1} \cdots u_{i-1} (\partial x_j^{p_i}/\partial x_j).$$

For example, if $u = x_1^3 x_2^7 x_1^{-5} x_2^{13}$, one calculates

$$(\partial u/\partial x_1) = 1 + x_1 + x_1^2 - x_1^3 x_2^7 (x_1^{-1} + x_1^{-2} + x_1^{-3} + x_1^{-4} + x_1^{-5}).$$

The next theorem is called the Chain Rule Theorem.

Theorem 4.

If f is a homomorphism from a free group Y to a free group X, then for any a in ZY,

$$\partial f(a)/\partial x_j = \sum_k f(\partial a/\partial y_k)\partial f(y_k)/\partial x_j,$$

where the $\{y_k\}$ freely generate Y.

Proof.

It suffices to prove the theorem for $a = v$, an element of Y. For the sake of neatness and clarity of notation, we make the assumption that $v = y_1^{n_1}\cdots y_t^{n_t}$, where y_i may equal y_j even though $i \neq j$. Let $w_i = f(y_i)$, so $f(v) = w_1^{n_1}\cdots w_t^{n_t}$. Then, taking x_j to be x_1,

$$\partial f(v)/\partial x_1 = \sum_1^t w_1^{n_1}\cdots w_{i-1}^{n_{i-1}}(\partial w_i^{n_i}/\partial x_1).$$

We must show the above expression equals

$\sum_1^t f(\partial v/\partial y_k)\partial w_k/\partial x_1$.

Now, $f(\partial v/\partial y_k) = f\left(y_1^{n_1}\cdots y_{k-1}^{n_{k-1}}(\partial y_k^{n_k}/\partial y_k)\right)$

$$= w_1^{n_1}\cdots w_{k-1}^{n_{k-1}} f(\partial y_k^{n_k}/\partial y_k), \text{ so}$$

$\sum_1^t f(\partial v/\partial y_k)\partial f(y_k)/\partial x_1 = \sum_1^t w_1^{n_1}\cdots w_{k-1}^{n_{k-1}} f(\partial y_k^{n_k}/\partial y_k)\partial f(y_k)/\partial x_1.$

Assuming $n_k > 0$ (the same proof works for $n_k < 0$), we have $f(\partial y_k^{n_k}/\partial y_k)\partial f(y_k)/\partial x_1 =$

$$= f\left(1 + y_k + \cdots + y_k^{n_k - 1}\right)\partial f(y_k)/\partial x_1$$

$$= \left(1 + w_k + \cdots + w_k^{n_k - 1}\right)\partial w_k/\partial x_1$$

$$= \partial w_k^{n_k}/\partial x_1,$$

so $\partial f(v)/\partial x_1 = \sum_1^t f(\partial v/\partial y_k)\partial f(y_k)/\partial x_1$. This completes the proof.

Definition 2.

An element u of X is said to have relatively prime partial derivatives if there exist elements $a_1, a_2, \ldots$ in ZX such that $\sum_i (\partial u/\partial x_i)a_i = 1$.

We can now give a necessary condition on the partial derivatives of an element u of X in order that u be a free generator of X.

Theorem 5.

If u is a free generator of X, then the partial derivatives of u are relatively prime.

Proof.

Let X be freely generated by $\{x_i\}$, and let u be a member of some free generating set for X. Then there is an automorphism f of X such that $f(u) = x_1$. By Theorem 4, with $X = Y$, we have

$$\partial f(u)/\partial x_1 = \sum_i f(\partial u/\partial x_i)\partial f(x_i)/\partial x_1 .$$

Now $\partial f(u)/\partial x_1 = \partial x_1/\partial x_1 = 1$, so applying f^{-1} to both sides above, we get

$$1 = f^{-1}(1) = \sum_i \{\partial u/\partial x_i\} f^{-1}\{\partial f(x_i)/\partial x_1\} .$$

II Reduction Modulo the First Commutator Subgroup

From now on, X will be the free group on two generators, x and y. In the last chapter, we showed that if an element u of X is a free generator, then u has relatively prime partial derivatives. In this chapter, we will show that if u has relatively prime partial derivatives, then u must be the product of a free generator of X with an element of the first commutator subgroup of X, that subgroup being denoted by X'.

We will then show that the property of having relatively prime partial derivatives is preserved by automorphisms of X; this will allow us to restrict our attention to elements of the form xc, where c is an element of X'.

<u>Definition 3.</u>

Let u be any element of X. Written as a reduced word, we have $u = \prod_{i=1}^{t} x^{n_i} y^{m_i}$, where no n_i or m_i is zero, except possibly for n_1 and m_t. The length of u is defined to be $\sum_{i=1}^{t} n_i + \sum_{i=1}^{t} m_i$, while the syllable length of u is defined to be $2t$, if neither n_1 nor m_t is zero; $2t - 1$, if precisely one of them is zero; and $2t - 2$, if both n_1 and m_t are zero.

Lemma 1.

Let $u = \prod_{i=1}^{t} x^{n_i} y^{m_i}$ be any element of X. Then $u = x^n y^m c$, where c is an element of X', $n = \sum_{i=1}^{t} n_i$, and $m = \sum_{i=1}^{t} m_i$.

Proof.

By induction on the syllable length of u. The lemma is trivially true for words of syllable length 1. Assuming it is true for words of syllable length less than the syllable length of u, we write

$$u = x^{n_1} y^{m_1} \prod_{i=2}^{t} x^{n_i} y^{m_i} = x^{n_1} y^{m_1} x^{n-n_1} y^{m-m_1} c_1 =$$

$$= x^n y^m (y^{-m} x^{-n+n_1} y^{m_1} x^{n-n_1} y^{m-m_1} c_1),$$ where c_1 belongs to X', and so the entire expression within the parentheses belongs to X'.

In what follows, we shall denote the partial derivatives of an element a of ZX by a_x and a_y, or by $D_x(a)$ and $D_y(a)$, in place of the more cumbersome $\partial a/\partial x$ and $\partial a/\partial y$.

Lemma 2.

If u and v represent the same reduced word in X, then $u_x = v_x$ and $u_y = v_y$.

Proof.

It need only be shown that $D_x(u'u'') = D_x(u'gg^{-1}u'')$, the proof for the partial derivative with respect to y being exactly the same.

By (8.6) we have

$$
\begin{aligned}
D_x(u'gg^{-1}u'') &= D_x u' + u'D_x g + u'gD_x g^{-1} + u'gg^{-1}D_x u'' \\
&= D_x u' + u'D_x g + u'g(-g^{-1}D_x g) + u'D_x u'' \\
&= D_x u' + u'D_x g - u'D_x g + u'D_x u'' \\
&= D_x u' + u'D_x u'' \\
&= D_x(u'u''),
\end{aligned}
$$

where in the second line we used (8.7).

Theorem 6.

If $u = x^n y^m c$, with c in X', then $u_x^* = n$ and $u_y^* = m$.

Proof.

We put u in the form $\prod_{i=1}^{t} x^{n_i} y^{m_i}$, where $n = \sum_{i=1}^{t} n_i$ and $m = \sum_{i=1}^{t} m_i$, and use induction on t. For $t = 1$, we have $u = x^{n_1} y^{m_1}$, so

$u_x = \operatorname{sgn}(n_1) x^{\frac{n_1 - |n_1|}{2}}(1 + x + \cdots + x^{|n_1|-1})$ and

$u_y = \operatorname{sgn}(m_1) x^{n_1} y^{\frac{m_1 - |m_1|}{2}}(1 + y + \cdots + y^{|m_1|-1})$.

Therefore, $u_x^* = \operatorname{sgn}(n_1)|n_1| = n_1$ and $u_y^* = \operatorname{sgn}(m_1)|m_1| = m_1$. Assuming the theorem is true for all words of syllable length less than the syllable length of u, and putting $w = \prod_{i=1}^{t-1} x^{n_i} y^{m_i}$, we have $u = wx^{n_t} y^{m_t}$, so

$u_x = w_x + w \operatorname{sgn}(n_t) x^{\frac{n_t - |n_t|}{2}}(1 + x + \cdots + x^{|n_t|-1})$

whence $u_x^* = w_x^* + n_t = \sum_{i=1}^{t-1} n_i + n_t = n$.

Similarly, $u_y^* = m$.

Corollary 1.

Let $u = x^n y^m c$, c in X', and suppose u has relatively prime partial derivatives. Then $(n,m) = 1$, that is to say, n and m are relatively prime integers.

Proof.

To say u has relatively prime partial derivatives means $u_x a + u_y b = 1$ for some elements a and b of ZX. Applying the augmentation homomorphism to the above equation, we get $u_x^* a^* + u_y^* b^* = 1$, so by Theorem 6 we have $na^* + mb^* = 1$, whence $(n,m) = 1$.

The next theorem shows that, modulo the first commutator subgroup, the converse of Theorem 5 is true.

Theorem 7.

If u has relatively prime partial derivatives, then the coset $\bar{u} = uX'$ is a free generator of $\bar{X} = X/X'$.

Proof.

If $u = x^n y^m c$ has relatively prime partial derivatives, then by Corollary 1, $(n,m) = 1$, and so, as is generally known, $\bar{u} = \bar{x}^n \bar{y}^m$ is a free generator of the free abelian group X/X'.

The result of the following theorem is originally due to Nielsen. The proof given here is mine.

Theorem 8.

If $\tilde{u}$ is a free generator of X/X', then there is an element c of X' such that uc is a free generator of X.

Proof.

If $\tilde{u}$ is a free generator of X/X', then $\tilde{u}$ must equal $\tilde{x}^n\tilde{y}^m$ with $(n,m) = 1$, and so u must equal x^ny^md, where d is in X'. Without loss of generality we assume that n and m are nonnegative, since either x or y could be replaced by its inverse.

We need only show that for some c in X', x^ny^mc is a free generator of X, for then $u(d^{-1}c) = x^ny^mc$ will be a free generator of X, and $d^{-1}c$ belongs to X'. If $n = 1$, just take $c = 1$, since xy^m is a free generator for every m. If $n = 2$, we use induction on m with $(2,m) = 1$:

for $m = 3$, take $c = y^{-3}x^{-1}yxy^2$, for then $x^2y^3c = xyxy^2$, which is mapped, by the automorphism $x \mapsto xy^{-1}$, $y \mapsto y$, to the element x^2y, which is a free generator, and so x^2y^3c is a free generator.

Assuming the theorem true for $n = 2$ and for all k less than m with $(2,k) = 1$, let $u = x^2y^m$. Let F be the automorphism which sends x to xy^{-1} and y to y. Then $F(u) = xy^{-1}xy^{m-1} = x^2y^{m-2}d_1$, d_1 in X', by lemma 1. $(2,m-2) = 1$, since $(2,m) = 1$, so by the induction hypothesis there is an element e of X'

such that $x^2y^{m-2}e = F(u)d_1^{-1}e$ is a free generator, g. Then $uF^{-1}(d_1^{-1}e) = F^{-1}(g)$ is a free generator, and $F^{-1}(d_1^{-1}e)$ belongs to X', since X' is a characteristic subgroup of X.

We now proceed by induction on n. Assume the theorem is true for every k less than n and for every m with $(k,m) = 1$, and let $u = x^n y^m$, $(n,m) = 1$. By symmetry we may assume $n > m$. Let T be the automorphism which sends x to x and y to $x^{-1}y$. Then $T(u) = x^n(x^{-1}y)^m$, which, again by lemma 1, equals $x^{n-m}y^m d_2$, with d_2 in X'. Now $(n,m) = 1$ implies that $(n-m,m) = 1$, and since $n-m < n$, the induction hypothesis applies, so there is an element d_3 of X' with $x^{n-m}y^m d_3 = T(u)d_2^{-1}d_3$ a free generator, h, so $uT^{-1}(d_2^{-1}d_3) = T^{-1}(h)$ is a free generator, and $T^{-1}(d_2^{-1}d_3)$ is an element of X'. This completes the proof.

Lemma 3.

If uc is a free generator of X, c in X', then there is an element d in X' and an automorphism f of X such that $f(u) = xd$.

Proof.

If uc is a free generator, then for some automorphism f of X, $x = f(uc) = f(u)f(c)$, and so $f(u)$ equals $xf(c^{-1})$.

For the following theorem, we use the fact (see , page 169) that the automorphism group of the free group on two generators can be generated by the automorphisms P, S, and U, which are defined by

$$P(x) = y \qquad P(y) = x$$
$$S(x) = x^{-1} \qquad S(y) = y$$
$$U(x) = xy \qquad U(y) = y.$$

Theorem 5.

The property of having relatively prime partial derivatives is preserved under automorphisms of X.

Proof.

Suppose an element u of X has relatively prime partial derivatives. We must show that if $v = f(u)$, where f is one of the automorphisms P, S, or U, then v also has relatively prime partial derivatives. By Theorem 4, we have

$$(22.1) \qquad v_x = f(u_x)D_x(f(x)) + f(u_y)D_x(f(y))$$
$$(22.2) \qquad v_y = f(u_x)D_y(f(x)) + f(u_y)D_y(f(y)).$$

Let a and b be elements of ZX such that $u_x a + u_y b = 1$. For the case $f = P$, we get, using (22.1) and (22.2), $v_x = P(u_y)$ and $v_y = P(u_x)$. Therefore,

$$v_x P(b) + v_y P(a) = P(u_y)P(b) + P(u_x)P(a) = P(1) = 1.$$

For the case $f = S$, we get $v_x = -S(u_x)x^{-1}$ and $v_y = S(u_y)$, and so and so

$$v_x[-xS(a)] + v_y S(b) = [-S(u_x)x^{-1}][-xS(a)] + S(u_y) S(b)$$
$$= S(u_x)S(a) + S(u_y)S(b)$$
$$= 1.$$

Finally, for the case $f = U$, we get $v_x = U(u_x)$ and $v_y = U(u_x)x + U(u_y)$, so

$$v_x [U(a) - xU(b)] + v_y U(b) =$$
$$= U(u_x)U(a) - U(u_x)xU(b) + U(u_x)xU(b) + U(u_y)U(b)$$
$$= U(u_x)U(a) + U(u_y)U(b)$$
$$= 1.$$

Thus, in each case, v also has relatively prime partial derivatives.

Corollary 2.

The problem of showing that if an arbitrary element u of X has relatively prime partial derivatives, then u is a free generator of X, reduces to the problem of showing that if xc, c an arbitrary element of X', has relatively prime partial derivatives, then xc is a free generator of X.

Proof.

Suppose we can show that for any element c of X', if xc has relatively prime partial derivatives, then xc must be a free generator of X, and suppose, furthermore, that u is any element of X with relatively prime partial derivatives. Then, by Lemma 1 and

Corollary 1, $u = x^n y^m d$, where d is in X' and $(n,m) = 1$. Hence, by Theorem 7, Theorem 8, and Lemma 5, there is an element c of X' and an automorphism f of X such that $f(u) = xc$. By Theorem 9, xc has relatively prime partial derivatives. If we could then show that xc is a free generator, then $u = f^{-1}(xc)$ would also be a free generator.

III Reduction Modulo the Second Commutator Subgroup

In this chapter, we will show that if an element u of X has relatively prime partials, then u is the product of a free generator with an element of the second commutator subgroup, X''

Definition 4.

A simple commutator is a commutator of the form $[x^r, y^s]^{\pm 1}$, where r and s are integers.

Theorem 10.

Any commutator can be written as the product of simple commutators.

Proof.

By induction on the syllable length of the commutator. Let $c = x^{n_1} y^{m_1} \cdots x^{n_t} y^{m_t}$ be an element of X', whence $\sum_{i=1}^{t} n_i = \sum_{i=1}^{t} m_i = 0$, and assume the result is true for all commutators of syllable length less than the syllable length of c. Then

$$c = (x^{n_1} y^{m_1} x^{-n_1} y^{-m_1})(y^{m_1} x^{n_1+n_2} y^{m_2} x^{n_3} y^{m_3} \cdots x^{n_t} y^{m_t})$$
$$= [x^{n_1}, y^{m_1}] (y^{m_1} x^{n_1+n_2} y^{-m_1} x^{-n_1-n_2})(x^{n_1+n_2} y^{m_1+m_2} x^{n_3} y^{m_3} \cdots x^{n_t} y^{m_t})$$
$$= [x^{n_1}, y^{m_1}][y^{m_1}, x^{n_1+n_2}](x^{n_1+n_2} y^{m_1+m_2} x^{n_3} y^{m_3} \cdots x^{n_t} y^{m_t}).$$

Now the last factor in parentheses is a commutator of syllable length less than that of c, and so, is the product of simple commutators. Therefore, so is c.

Given an element u with relatively prime partial derivatives, we know we can take u to be of the form xc, with c in X'. By Theorem 10, u is then of the form $xc_1c_2\cdots c_t$, where each c_i is a simple commutator.

Theorem 11.

Let $u = x^n c$, c in X'. Define $F: X \to X$ by $F(x) = 1$, $F(y) = y$ (so $F: ZX \to Z\langle y \rangle$, where $\langle y \rangle$ is the free group on one generator, y). Then $F(u_y) = 0$.

Proof.

We first show that if c is a simple commutator, then $F(c_y) = 0$. Suppose, first, that $c = [x^r, y^s] = x^r y^s x^{-r} y^{-s}$. If $s > 0$, we have

$c_y = x^r(1 + y + \cdots + y^{s-1}) - x^r y^s x^{-r}(y^{-1} + \cdots + y^{-s})$, so

$F(c_y) = 1 + y + \cdots + y^{s-1} - y^s(y^{-1} + \cdots + y^{-s}) = 0.$

A similar calculation holds for $s < 0$.

If now $c = [x^r, y^s]^{-1}$, we see that $F(c_y) = 0$ by using (8.7).

Returning to $u = x^n c = x^n c_1 c_2 \cdots c_t$, where each c_i is a simple commutator, we have, by (8.6)

$u_y = \sum_{i=1}^{t} x^n c_1 \cdots c_{i-1}(\partial c_i/\partial y)$, so

$F(u_y) = \sum_{i=1}^{t} F(x^n c_1 \cdots c_{i-1}) F(\partial c_i/\partial y) = 0.$

Lemma 4.

If $F: X \to X$ by $F(x) = 1$, $F(y) = y$, then $F(\partial x^r/\partial x) = r$.

Proof.

$(\partial x^r/\partial x) = (\operatorname{sgn} r)x^{(r-|r|)/2}(1 + x + \dots + x^{|r|-1})$, so $F(\partial x^r/\partial x) = (\operatorname{sgn} r)(1)|r| = r$.

Corollary 3.

If $u = \prod_{i=1}^{t} x^{n_i}y^{m_i}$ and $F: X \to X$ by $F(x) = 1$, $F(y) = y$, then $F(u_x) = n_1 + n_2y^{m_1} + n_3y^{m_1+m_2} + \dots + n_ty^{m_1+\dots+m_{t-1}}$.

Proof.

By (3.6) and the fact that $D_x(y^m) = 0$, we have $u_x = \sum_{i=1}^{t} x^{n_1}y^{m_1}\cdots x^{n_{i-1}}y^{m_{i-1}}D_x(x^{n_i})$, and so $F(u_x) = \sum_{i=1}^{t} y^{m_1+\dots+m_{i-1}}F(D_x(x^{n_i})) = \sum_{i=1}^{t} n_iy^{m_1+\dots+m_{i-1}}$.

Theorem 12.

In $Z(y)$, the integral group ring of the free group on one generator, the only units are the trivial units.

Proof.

Suppose $p(y)$ and $q(y)$ are any two elements of $Z(y)$ such that $p(y)q(y) = 1$. Then there are nonnegative integers i and j such that $y^ip(y)$ and $y^jq(y)$ are in $Z[y]$, the ring of polynomials over Z, and $(y^ip(y))(y^jq(y)) = y^{i+j}$. But then $y^ip(y) = \pm y^s$ and $y^jq(y) = \pm y^t$, where s and t are nonnegative integers such that $i + j = s + t$, so $p(y) = \pm y^{s-i}$ and $q(y) = \pm y^{t-j}$.

Theorem 13.

If $u = xc$, c in X', has relatively prime partial derivatives, and $F:X \to X$ by $F(x) = 1$, $F(y) = y$, then $F(u_x) = \pm y^t$ for some integer t.

Proof.

By Theorem 11, $F(u_y) = 0$. Since $u_x a + u_y b = 1$ for some elements a and b of ZX, we have $1 = F(1) = F(u_x)F(a) + F(u_y)F(b) = F(u_x)F(a)$, and so $F(u_x)$ is a unit in $Z(y)$. Thus, by Theorem 12, $F(u_x) = \pm y^t$.

Theorem 14.

If c is a simple commutator, then $u = xc$ has relatively prime partial derivatives if and only if u is a free generator of X.

Proof.

We need only show that if $u = x[x^r,y^s]^{\pm 1}$ has relatively prime partial derivatives, then u is a free generator.

Case 1: $u = x[x^r,y^s] = x^{r+1}y^s x^{-r}y^{-s}$. Let $F:X \to X$ by $F(x) = 1$, $F(y) = y$. Then, by Corollary 3, $F(u_x) = r + 1 - ry^s$, and this must equal $\pm y^t$, by Theorem 13. Since we may assume $rs \neq 0$, it follows that ry^s is not an integer, so ry^s cannot cancel with either r or 1. Therefore r and 1 must cancel, so $r = -1$. Thus, $u = y^s x y^{-s}$, and so is a conjugate of x, hence a free generator of X.

Case 2: $u = x[x^r, y^s]^{-1} = xy^s x^r y^{-s} x^{-r}$.

Then $F(u_x) = 1 + ry^s - ry^{s-s} = 1 - r + ry^s$. By the same reasoning as before, we see that $r = 1$, and so $u = xy^s xy^{-s} x^{-1}$, which is again a conjugate of x.

Lemma 5.

Let $c(n,m) = x^n y^m x y^{-m} x^{-n-1}$, and let $c^{-1}(n,m) = x^{n+1} y^m x^{-1} y^{-m} x^{-n}$. Then $\{c(n,m)\}_{n,m \in Z}$ generates X'.

Proof.

By Theorem 10, we need only show that a simple commutator can be written as the product of the $c(n,m)$ and the $c^{-1}(n,m)$.

Let b and p be integers, $p > 0$. A simple commutator can either be of the form $[x^p, y^b]^{\pm 1}$ or $[x^{-p}, y^b]^{\pm 1}$. As can be seen by cancelling, we have

$$[x^p, y^b] = \prod_{i=0}^{p-1} c^{-1}(p-1-i, b)$$
$$[x^p, y^b]^{-1} = \prod_{i=p-1}^{0} c(p-1-i, b)$$
$$[x^{-p}, y^b] = \prod_{i=0}^{p-1} c(-p+i, b)$$
$$[x^{-p}, y^b]^{-1} = \prod_{i=p-1}^{0} c^{-1}(-p+i, b).$$

In the next theorem, the notation $[[h,k]]$ stands for the set of all integers between the two integers h and k, including h and k.

Theorem 15.

Suppose $u = xc$ has relatively prime partial derivatives. By Lemma 5 we have $c = \prod_{i=1} c^{e_i}(n_i, m_i)$, where n_i is any integer, m_i is any integer other than 0, and $e_i = \pm 1$.

If s is even and equals $2k$, then

$e_{i_1} = \cdots = e_{i_k} = -1$, $e_{i_{k+1}} = \cdots = e_{i_{2k}} = 1$, and there is a bijection $T: [1,k] \to [k+1,2k]$ such that for each j in $[1,k]$ we have $n_{i_j} = m_{i_{T(j)}}$; while if s is odd and equals $2k+1$, then

$e_{i_1} = \cdots = e_{i_k} = -1$; $e_{i_{k+1}} = \cdots = e_{i_{2k+1}} = 1$, and there is an injection $I: [1,k] \to [k+1, 2k+1]$ such that for each j in $[1,k]$ we have $m_{i_j} = m_{i_{I(j)}}$.

Proof.

Let $d_i = c^{e_i}(n_i, m_i)$, so $u = xd_1 \cdots d_s$.

Then by (8.6), $u_x = 1 + xD_x(d_1) + xd_1 D_x(d_2) + \cdots$

$$\cdots + xd_1 \cdots d_{s-1} D_x(d_s).$$

Defining $F: X \to X$ by $F(x) = 1$, $F(y) = y$, we have $F(u_x) = \pm y^p$, by Theorem 13. Now, since $F(xd_1 \cdots d_i) = 1$ for each i, we also have

$F(u_x) = 1 + F(D_x(d_1)) + F(D_x(d_2)) + \cdots + F(D_x(d_s))$.

By Corollary 3, $F(D_x(c(n,m))) = F(D_x(x^n y^m x y^{-m} x^{-n-1})) =$

$$= n + y^m + (-n-1)y^{m-m} = y^m - 1$$

and $F(D_x(c^{-1}(n,m))) = F(D_x(x^{n+1} y^m x^{-1} y^{-m} x^{-n})) =$

$$= n + 1 - y^m - ny^{m-m} = 1 - y^m.$$

Therefore,

$$F(D_x(d_i)) = F(D_x(c^{e_i}(n_i, m_i))) = e_i(y^{m_i} - 1)$$

hence

$$F(u_x) = 1 + e_1(y^{m_1} - 1) + \quad + e_s(y^{m_s} - 1).$$

Suppose k of the e_i are equal to -1 and $s - k$ of the e_i are equal to $+1$. Then

$$F(u_x) = 1 - (y^{m_1} - 1) - \quad - (y^{m_k} - 1) + (y^{m_{k+1}} - 1) + \quad + (y^{m_s} - 1)$$

$$= 1 - \sum_{i=1}^{k} y^{m_i} + \sum_{i=k+1}^{s} y^{m_i} + k - (s - k)$$

$$= 1 + 2k - s - \sum_{i=1}^{k} y^{m_i} + \sum_{i=k+1}^{s} y^{m_i},$$

and this must equal $\pm y^p$. Since no m_i equals zero, there are three possibilities for the constant term $1 + 2k - s$: it can equal 0, +1, or -1.

Case 1: $1 + 2k - s = +1$, and so $s = 2k$. Then, from above, $F(u_x) = 1 - \sum_{i=1}^{k} y^{m_i} + \sum_{i=k+1}^{s} y^{m_i} = \pm y^p$. Again, since no m_i equals zero, this can happen only if $p = 0$ and $y^p = +1$, in which case we have

$$y^{m_1} + \cdots + y^{m_k} = y^{m_{k+1}} + \cdots + y^{m_s}.$$

But this can happen only if each term on the left equals some term on the right, and so we get the first conclusion of the theorem.

Case 2: $1 + 2k - s = 0$, and so $s = 2k + 1$. In this case, $F(u_x) = -\sum_{i=1}^{k} y^{m_i} + \sum_{i=k+1}^{s} y^{m_i} = \pm y^p$, and so each of the k terms in the first sum must equal one of the k + 1 terms in the second sum, and there is one term in the second sum left over, this being y^p. This is the second conclusion of the theorem.

Case 3: $1 + 2k - s = -1$, and so $s = 2k + 2$. In this final case, $F(u_x) = -1 - \sum_{i=1}^{k} y^{m_i} + \sum y^{m_j} = \pm y^p$. Again, since no m_i equals zero, we must have $p = 0$ and the coefficient in front of y^p must be -1, in which case we would have $-\sum_{i=1}^{k} y^{m_i} + \sum y^{m_j} = 0$. But this is impossible, since the k terms of the first sum cannot cancel against the $k + 2$ terms of the second sum, and so this case cannot arise. This completes the proof of the theorem.

<u>Theorem 16.</u>

Suppose $u = xc$, with c in X', has relatively prime partial derivatives. Then we may assume that c is an element of the second commutator subgroup, X'', so modulo X'', u is a free generator.

Before we start the main part of the proof, we must deal with some preliminaries.

We have $u = xc_1 \cdots c_t$, where $c_i = [x^{r_i}, y^{s_i}]^{\pm 1}$, and r_i and s_i are nonzero integers. In what follows, we will let a_i be a positive integer, and b_i any nonzero integer. We distinguish four kinds of simple commutators:

1) $[x^{-a}, y^{b}] = c(-a,b)c(-a+1,b)\cdots c(-1,b)$

2) $[y^{b}, x^{a}] = c(0,b)c(1,b)\cdots c(a-1,b)$

3) $[x^{a}, y^{b}] = c^{-1}(a-1,b)c^{-1}(a-2,b)\cdots c^{-1}(0,b)$

4) $[y^{b}, x^{-a}] = c^{-1}(-1,b)c^{-1}(-2,b)\cdots c^{-1}(-a,b)$

Definition 5.

The first two types of simple commutators will be called positive simple commutators, and the last two, negative simple commutators.

Let us put $c_i = \begin{cases} N_i, & \text{if } c_i \text{ is a negative simple commutator} \\ P_i, & \text{if } c_i \text{ is a positive simple commutator} \end{cases}$

Then $u = xc_1\cdots c_t =$ (mod X'') $xN_1\cdots N_r P_{r+1}\cdots P_t$ (with a possible renumbering of subscripts, for ease of notation). Now $N_i = \prod_{k=1}^{a_i} c^{-1}(n_{i,k}, b_i)$ and $P_i = \prod_{k=1}^{a_i} c(n_{i,k}, b_i)$ where the $n_{i,k}$ are integers, a_i is the exponent of x and b_i the exponent of y in the simple commutator N_i or P_i, and so we have

(33.1) $$u = (\text{mod } X'')\ x\left(\prod_{i=1}^{r}\prod_{k=1}^{a_i} c^{-1}(n_{i,k}, b_i)\right)\left(\prod_{i=r+1}^{t}\prod_{k=1}^{a_i} c(n_{i,k}, b_i)\right).$$

Referring back to the notation of Theorem 15 (where s is the number of terms of the form $c^{e}(n,m)$), we have $s = a_1 + \cdots + a_r + a_{r+1} + \cdots + a_t$, which equals either $2q$ or $2q + 1$, and we must have q negative simple commutators and either q or $q + 1$ positive simple commutators (depending upon whether s equals $2q$ or $2q + 1$).

Thus, $a_1 + \cdots + a_r = q$ and $a_{r+1} + \cdots + a_t = q$ or $q + 1$.

Remark 1: By Theorem 15, $r \neq t$. For to say $r = t$ is to say that all of the simple commutators are negative simple commutators, while Theorem 15 says that the number of negative simple commutators cannot exceed the number of positive simple commutators.

Furthermore, if $r = 0$, that is, if there are no negative simple commutators, then q must equal 0, so s equals either 0 (which is $2q$) or 1 (which is $2q + 1$).

If $s = 0$, then all of the a_i equal 0, so we have the trivial case where each simple commutator is the identity, and so modulo X'', $u = x$.

On the other hand, if $s = 1$, then a_{r+1}, say, equals 1 and all the other a_i equal 0, which means $u \equiv (\text{mod } X'')\ xP_{r+1}$, where the exponent of x in the simple commutator P_{r+1} is 1. But this is the situation of Theorem 14, and so u would be a free generator, modulo X''.

Thus, we may assume r is not 0 or t, that is, $1 \leq r \leq t-1$.

Remark 2: Also by Theorem 15, for each b_i in the first bracket in (33.1), there must be a b_j in the second bracket such that $b_i = b_j$. Now b_i occurs a_i times, so in the first bracket there are a_1 occurrences of b_1, ..., and a_r occurrences of b_r, and in the second bracket there are a_{r+1} occurrences of $b_{r+1}, \ldots,$ and a_t occurrences of b_t.

Let us say that $b_1, \ldots, b_{r_1}$ are those b_i's from the first bracket which equal b_1. Since there are $a_1 + \cdots + a_{r_1}$ of them, there must be $a_1 + \cdots + a_{r_1}$ b_j's in the second bracket which equal b_1: call these $b_{k_1}, \ldots, b_{K_1}$. Thus

$$b_1 = \cdots = b_{r_1} = b_{k_1} = \cdots = b_{K_1}$$

and there are $2(a_1 + \cdots + a_{r_1})$ of these b's, half from each bracket.

Now, let n_2 be the least natural number such that $b_{n_2} \neq b_1$, and let $b_{n_2}, \ldots, b_{r_2}$ be those b_i's from the first bracket which equal b_{n_2}. Then there are $a_{n_2} + \cdots + a_{r_2}$ of them, so there are also $a_{n_2} + \cdots + a_{r_2}$ b_j's from the second bracket which equal b_{n_2}: call these $b_{k_2}, \ldots, b_{K_2}$. Thus

$$b_{n_2} = \cdots = b_{r_2} = b_{k_2} = \cdots = b_{K_2}$$

and there are $a_{n_2} + \cdots + a_{r_2}$ of these b's from each bracket.

Continue in this way until all the b_i's from from the first bracket are exhausted; this will either exhaust all the b_j's from the second bracket (if $s = 2q$) or all but one (if $s = 2q + 1$). Let us call the last grouping of b's $b_{n_L}, \dots, b_{r_L}$ from the first bracket and $b_{k_L}, \dots, b_{k'_L}$ from the second. Thus,

$$b_{n_L} = \cdots = b_{r_L} = b_{k_L} = \cdots = b_{k'_L}$$

and there are $\varepsilon_{n_L} + \cdots + \varepsilon_{r_L}$ of these b's from each bracket.

We now relabel the commutators, according to the different groupings of b_i's (there are L different groupings): let $M_1 = N_1 \cdots N_{r_1} P_{k_1} \cdots P_{k'_1}$, $M_2 = N_{n_2} \cdots N_{r_2} P_{k_2} \cdots P_{k'_2}$, ..., $M_L = N_{n_L} \cdots N_{r_L} P_{k_L} \cdots P_{k'_L}$. Then each commutator M_i is the product of simple commutators in such a way that, for a fixed M_i, the y-exponents of all the simple commutators are the same. Thus, if $s = 2q$, then $u \equiv (\text{mod } X'')\ xM_1M_2 \cdots M_L$, and if $s = 2q + 1$, then $u \equiv (\text{mod } X'')\ xM_1M_2 \cdots M_LP$, where P is a positive simple commutator with x-exponent equal to 1.

<u>Proof of Theorem 16.</u>

The idea of the proof is to show, for $u \equiv (\text{mod } X'')\ xM_1 \cdots M_L$ or $u \equiv (\text{mod } X'')\ xM_1 \cdots M_LP$, that modulo X'' we can successively get rid of each M_i, whence we would get $u \equiv (\text{mod } X'')\ x$, a free generator, or $u \equiv (\text{mod } X'')\ xP$, which is a conjugate of x, hence also a free generator.

To do this, it suffices to show that if N_1 is a negative simple commutator with y-exponent b_1 and x-exponent a_1, and P_{K_1} is a positive simple commutator with y-exponent b_1 and x-exponent a_2, then (with E an arbitrary commutator)

$$xN_1P_{K_1}E = (\text{mod } X'') \begin{cases} xNE, & \text{if } a_1 > a_2, \text{ where } N \text{ is a neg. simple commutator with x-exponent } a_1 - a_2 \\ xPE, & \text{if } a_1 < a_2, \text{ where } P \text{ is a pos. simple commutator with x-exponent } a_2 - a_1 \\ xE, & \text{if } a_1 = a_2 \end{cases}$$

The fact that each N_i can be gotten rid of modulo X'' then follows from the fact that the sum of the x-exponents of $N_{n_i}, \ldots, N_{r_i}$ equals the sum of the x-exponents of $P_{K_i}, \ldots, P_{K_i'}$, so that eventually the stage "$a_1 = a_2$" is reached.

Since there are two types of both negative and positive simple commutators, there are four cases:

Case 1. $x[x^a,y^b][x^{-c},y^b]E = (\text{mod } X'')\ x[x^{-c},y^b][x^a,y^b]E =$
$= x^{-c+1}y^bx^cy^{-b}x^ay^bx^{-a}y^{-b}E$ which is conjugate to
$x(y^{-b}x^ay^bx^{-a})(y^{-b}Ex^{-c+1}y^bx^{c-1})$ which equals, modulo X'',
$x(y^{-b}Ex^{-c+1}y^bx^{c-1})(y^{-b}x^ay^bx^{-a})$ which is conjugate to

(simply conjugate by $x^ay^bx^{-a}$)

$x(x^{a-1}y^bx^{-a+1}y^{-b})E(x^{-c+1}y^bx^{c-1}y^{-b})$
$= x[x^{a-1},y^b]E[x^{-c+1},y^b]$ which equals, modulo X'',

$x[x^{a-1},y^b][x^{-c+1},y^b]E$.

Thus, if $a > c$, for example, simply repeat this manipulation $c - 1$ more times, and one is left with $x[x^{a-c},y^b]E$. Similarly, the result holds if $a < c$ or if $a = c$.

In the remaining three cases, we will write $u \sim v$ if u and v are automorphic images of each other (in particular, if they are conjugate), and $u \cong v$ if $u = v$ modulo X''.

Case 2. $x[x^a,y^b][y^b,x^c]E \cong x[x^a,y^b]E[y^b,x^c] =$

$$= x^{a+1}y^bx^{-a}y^{-b}Ey^bx^cy^{-b}x^{-c}$$

$$\sim x(x^{c-1}y^{-b}x^{-c+a+1}y^bx^{-a})(y^{-b}Ey^b)$$

$$\cong x(y^{-b}Ey^b)(x^{c-1}y^{-b}x^{-c+a+1}y^bx^{-a})$$

$$\sim x(x^{a-1}y^bx^{-a+1}y^{-b})E(y^bx^{c-1}y^{-b}x^{-c+1})$$

$$\cong x[x^{a-1},y^b][y^b,x^{c-1}]E$$

Case 3. $x[y^b,x^{-a}][x^{-c},y^b]E$

$$\cong x[x^{-c},y^b][y^b,x^{-a}]E$$

$$= x^{-c+1}y^bx^{c-a}y^{-b}x^aE$$

$$\sim xE(x^{-c+1}y^bx^{c-1})(x^{-a+1}y^{-b}x^{a-1})$$

$$= xE(x^{-c+1}y^bx^{c-1}y^{-b})(y^bx^{-a+1}y^{-b}x^{a-1})$$

$$\cong x[y^b,x^{-a+1}][x^{-c+1},y^b]E$$

Case 4. $x[y^b,x^{-a}][y^b,x^c]E$

$$\cong x[y^b,x^{-a}]E[y^b,x^c]$$

$$= xy^bx^{-a}y^{-b}x^aEy^bx^cy^{-b}x^{-c}$$

$$\sim x(x^{c-1}y^{-b}x^{-c+1}y^b)(x^{-a}y^{-b}x^aEy^b)$$

$$\equiv x(x^{-a}y^{-b}x^{a}Ey^{b})(x^{c-1}y^{-b}x^{-c+1}y^{b})$$

$$\equiv xE(y^{b}x^{c-1}y^{-b}x^{-c+1})(y^{b}x^{-a+1}y^{-b}x^{a-1})$$

$$\equiv x[y^{b},x^{-a+1}][y^{b},x^{c-1}]E.$$

In the last three cases, as with the first case, we see that by repeating the appropriate manipulations either $c - 1$ or $a - 1$ more times, either the negative or the positive simple commutator will drop out, and so modulo X" each M_i will drop out, and we are left with the situation that v equals a free generator modulo the second commutator subgroup. This completes the proof of the theorem.

The results of Section III were derived, in part, by writing a commutator as the product of simple commutators. In the free group on n generators, $n > 2$, this cannot, in general, be done. Of course, this may not be a major obstacle; it may be merely a small inconvenience.

The major obstacle is that there is no analogue to Theorem 13: even in the free group on three generators x, y, and z, if we have an element of the form xc, where c is a commutator, there is, in general, no mapping F under which $D_y(xc)$ and $D_z(xc)$ are sent to zero, so we are unable to make any claims about $F(D_x(xc))$ being a unit.

Bibliography

[1]. Blanchfield, R. C., Applications of Free Differential Calculus to the Theory of Groups. Senior Thesis, Princeton University. 1949.

[2]. Chen, K. T., A Group Ring Method for Finitely Generated Groups. Trans. A. M. S. 76 (1954) pp. 275-287.

[3]. Chen, K. T., Fox, R. H., and Lyndon, R. C., The Quotient Groups of the Lower Central Series. Annals of Math. 68 (1958). pp. 81-95.

[4]. Crowell, R. H., Genus of Alternating Link Types. Annals of Math. 69 (1959). pp. 258-275.

[5]. Crowell, R. H., and Fox, R. H., Introduction to Knot Theory. Ginn and Co., New York. 1963.

[6]. Fox, R. H., Free Differential Calculus I. Derivation in the Free Group Ring. Annals of Math. 57 (1953). pp. 547-560.

[7]. Hall, M., Jr., The Theory of Groups. The Macmillan Co., New York. 1959.

[8]. Kinoshita, S., On the Alexander Polynomial of 2-spheres in a 4-sphere. Annals of Math. 74 (1961). pp. 518-531.

[9]. Lyndon, R. C., Cohomology Theory of Groups with a Single Defining Relation. Annals of Math. 52 (1950). pp. 650-665.

[10]. Lyndon, R. C., On Burnside's Problem. Trans. A. M. S. 77 (1954). pp. 202-215.

[11]. Magnus, W., Karrass, A., and Solitar, D., Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations. John Wiley & Sons, Inc., New York. (1966).

[12]. Milnor, J., Link Groups. Annals of Math. 59 (1954). pp. 177-195.

[13]. Milnor, J., Isotopy of Links. Algebraic Geometry and Topology. A Symposium in Honor of S. Lefschetz. pp. 280-306. Princeton University Press, Princeton, New Jersey. (1957).