The Conjugacy problem in the Lyndon's Group

Jessica Bridson

Department of Mathematics and Statistics

McGill University, Montreal

January, 1998

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment

of the requirements of the degree of Masters of Science.

Abstract

The Lyndon's Group $F^{Z[x]}$ is of great interest to algebraists due to its unique properties. Using Van Kampen diagrams and results already proven for conjugate elements in $F^{Z[x]}$ by Myasnikov and Remeslennikov, this thesis proves that the conjugacy problem in the Lyndon's group is solvable. The concept of being conjugately residually free is introduced and it is shown that a single free extension of a centralizer of a free group is conjugately residually free.

Résumé

Le groupe de Lyndon $F^{Z[x]}$ suscite beaucoup l'interet des algébristes de par ses liens avec des groupes libres. En utilisant les diagrammes de Van Kampen et les resultats déjà prouvés par Myasnikov et Remeslennikov pour des éléments conjugués dans $F^{Z[x]}$, on montre que le problème de conjugaison en $F^{Z[x]}$ est résoluble. Ce document présente le concept de groupes conjugés résiduellement libres, et montre qu'une simple extension libre du centralisateur d'un groupe libre est un groupe conjugé résiduellement libre.

Acknowledgements

Many thanks to my supervisor Dr. O. Kharlampovich for her advice, help and financial support throughout my Masters degree. I am truly grateful for the time and effort she spent explaining and helping me understand concepts and ideas.

Thanks to my family and friends who offered encouragement and support whenever it was needed. In particular I would like to thank Catherine Gustavino for helping me with my french abstract.

Contents

Notation

$[v,t] = v^{-1}t^{-1}vt$

$[V,T]$ is the subgroup generated by all $[v,t]$ for $v \in V, t \in T$.

$u^g = g^{-1}ug$ where $g, u \in G$

$C_G(v)$ is the centralizer of the element v in the group G.

$G\langle v,t\rangle$ is the free extension of the centralizer of v by the element t.

$G\langle V,T\rangle$ is a finite series of free extension of centralizers, where at each step the centralizer of an element $v_i \in V$ is extended by an element $t_i \in T$.

Chapter 1

Introduction

The theory of exponential groups (groups which permit exponents from a ring A) begins with the work of Hall [4], Mal'cev [9], Lyndon [7], and G. Baumslag [1, 2]. In particular, Lyndon's paper introduced the axiomatic idea of an exponential group while Baumslag's papers look at the similarities between groups with unique roots (a type of exponential group) and free groups. The group studied in this thesis, the Lyndon's group, is an exponential group commonly written $F^{Z[x]}$ where $Z[x]$ is the ring of polynomials in one indeterminate with inseparable coefficients and F is a free group. Lyndon introduced this group while attempting to solve Tarski's problem on the elementary equivalence of free groups of different ranks. The group continues to be of interest to algebraists. Recently it has been proved that all finitely generated fully residually free groups are embeddable in this group, the three generator case was shown by Fine et. al. [3] and the complete proof by Kharlampovich and Myasnikov [5, 6]. As a consequence of this result Kharlampovich and Myasnikov have shown that all $\exists$-free groups (groups existentially equivalent to a free group) are embeddable in $F^{Z[x]}$.

Myasnikov and Remeslennikov [11] give an updated description of exponential groups and a construction of $F^{Z[x]}$ which is different from that used in this paper. They also give a description of conjugate elements in $F^{Z[x]}$ which is vital to my work. At the end of their paper they pose several open questions, one of which is

Question 4. Prove that in the A-free group F^A the word problem and the conjugacy problem are algorithmically decidable.

They state that: If the domain A is residually Z, then the answers to questions 5,6, and 7 are affirmative. We assume they meant instead questions 4,5, and 6 as no question 7 is listed. However there is no proof of this statement given in their paper, chapter 2 of this thesis gives such a proof. We also show how to solve the conjugacy problem in a group obtained from a free group by a series of free extensions of centralizers

In order to solve this problem, we introduce Van Kampen diagrams which were first introduced by Van Kampen in 1933 [12]. These diagrams supply a useful tool to prove statements relying on the relations which occur in a group.

The final chapter of this thesis introduces the idea of being conjugately residually G. We will prove that a single free extension of a centralizer of F is in fact conjugately residually F. It should be possible to extend this result to $F^{Z[x]}$, perhaps using free length functions.

Chapter 2

Preliminaries

2.1 Higman-Neumann-Neumann Extensions

In this section we will follow Lyndon and Schupp [8]. We define an HNN extension in the following manner.

Definition 2.1 *Let G be a group, A and B subgroups of the group G and $\phi : A \to B$ an isomorphism. Then the HNN extension of G with respect to A,B and ϕ is the group*

$$G^* = \langle G, t; t^{-1}at = \phi(a), a \in A\rangle.$$

We will deal with a special kind of HNN extension, called a free extension of a centralizer.

Definition 2.2 *Given a group G and an abelian centralizer $C(u)$ the free extension of the centralizer of u is*

$$G\langle u, t\rangle = \langle G, t; t^{-1}vt = v, v \in C(u)\rangle$$

where $C(u)$ is the centralizer of the element u.

In the following we will let ϵ (with or without subscript) denote either 1 or -1, and let A,B,G, t and ϕ be as in the definition of an HNN extension.

Definition 2.3 *A sequence $g_0, t^{\epsilon_1}, g_1, \ldots, t^{\epsilon_n}, g_n$ is reduced if it contains no consecutive subsequence t^{-1}, g_i, t where $g_i \in A$ or t, g_j, t^{-1} where $g_j \in B$.*

Before defining a *normal form* we must choose right coset representatives of A and B in G which will be used throughout the following discussion.

Definition 2.4 *A normal form in G^* is a sequence $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n (n \geq 0)$ where*

(1) $g_0 \in G$,

(2) If $\epsilon_i = -1$ then g_i is a right coset representative of A in G,

(3) If $\epsilon_i = 1$ then g_i is a right coset representative of B in G,

(4) there is no consecutive subsequence $t^{\epsilon}, 1, t^{-\epsilon}$.

The following theorem and proof are based on Theorem 2.1, page 182 in Lyndon and Schupp [8].

Theorem 2.1 (The Normal Form Theorem for HNN extensions) *Let $G^* = \langle G, t; t^{-1}at = \phi(a), a \in A\rangle$ be an HNN extension of the group G. Then*

1. The group G is embedded in G^* by the map $g \rightarrow g$. If $g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n = 1$ in G^* where $n > 0$ then $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ is not reduced.

2. Every element w of G^* has a unique representation as $w = g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n$ where $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ is in normal form.

Proof of Theorem 2.1: First we shall prove that these statements are equivalent. Assume that (2) holds. Clearly the normal form of an element $g \in G$ is g, hence the map $g \to g$ does embed G in G^*. Notice if $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$, where $n \geq 1$, is a reduced sequence then the corresponding normal from found by working from right to left has the same number of occurrences of t and thus $g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n \neq 1$.

Next assume statement (1) to be correct. Suppose we have two sequences which are in normal form such that

$$g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n = h_0 t^{\delta_1} \cdots t^{\delta_m} h_m.$$

If $n = m = 0$ then by statement (1) we have $h_0 = g_0$. Now suppose $m > 0$ then we have

$$1 = g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n h_m^{-1} t^{-\delta_m} \cdots t^{-\delta_1} h_0^{-1}.$$

We know from statement (1) that the expression on the right hand side is not reduced, thus we must have a possible reduction in $t^{\epsilon_n} g_n h_m^{-1} t^{-\delta_m}$ (Notice $n \neq 0$ if $m \neq 0$ as otherwise we would have that $h_0 t^{\delta_1} \cdots t^{\delta_m} h_m$ is not in reduced normal form). Thus $\epsilon_n = \delta_m$ and assuming $\epsilon_n = -1$, we have that $g_n h_m^{-1} \in A$ where g_n and h_m are representatives of cosets of A in G. Thus in fact $g_n = h_m$(Similarly if $\epsilon_n = 1$ we have the same result except that all elements must belong to B). We now have that

$$g_0 t^{\epsilon_1} \cdots t^{\epsilon_{n-1}} g_{n-1} = h_0 t^{\delta_1} \cdots t^{\delta_{m-1}} h_{m-1}$$

and by induction on m the result follows.

To prove the theorem we will use the Artin-van der Waerden idea of making G^* permute normal forms. Let the action of G^* be to multiply on the left and then reduce the expression to normal form. Let W be the set of normal forms on G^* and $S(W)$ be the group of all permutations of W. We define a homomorphism $\sigma : G^* \to S(W)$ by defining its action on G and on t.

First if $g \in G$ we define $\sigma(g)$ by

$$\sigma(g)(g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n) = gg_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}.$$

This is obviously a homomorphism as $\sigma(g'g) = \sigma(g')\sigma(g)$. Further $\sigma(g^{-1})\sigma(g) = \sigma(g)\sigma(g^{-1}) = 1_W$, hence $\sigma(g)$ is a permutation of W and σ is a homomorphism from G into $S(W)$.

We now define $\sigma(t)$. If $g_0 \in B$ and $\epsilon_1 = -1$ then

$$\sigma(t)(g_0, t^{-1}, \ldots, t^{\epsilon_n}, g_n) = \phi^{-1}(g_0)g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n.$$

Otherwise,

$$\sigma(t)(g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n) = \phi^{-1}(b), t, \hat{g}_o, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$$

where $g_0 = b\hat{g}_0$ with $b \in B$ and $\hat{g}_0$ the representative of the right coset of B containing g_0.

In order to show that $\sigma(t)$ is indeed a permutation of W we prove the inverse of $\sigma(t)$ is $\sigma(t^{-1})$. We define $\sigma(t^{-1})$ as follows where $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ is a normal form. If $\epsilon_1 = 1$ and $g_o \in A$ then

$$\sigma(t^{-1})(g_0, t^1, \ldots, t^{\epsilon_n}, g_n) = \phi(g_0)g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n.$$

Otherwise,

$$\sigma(t^{-1})(g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n) = \phi(a), t, \bar{g}_o, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$$

where $g_0 = a\bar{g}_0$ with $a \in A$ and $\bar{g}_0$ the representative of the coset of A containing g_0.

We have two cases to consider in checking that $\sigma(t^{-1})\sigma(t) = 1_W$. Once again let $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ be a normal form. If the first case of $\sigma(t)$ applies then $\epsilon_1 = -1$ and $g_0 \in B$. It is impossible to have $\epsilon_2 = 1$ and $g_1 \in A$ as this sequence is a normal form. Now

$$\sigma(t)(g_0, t^{-1}, \ldots, t^{\epsilon_n}, g_n) = \phi^{-1}(g_0)g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n.$$

By the previous observation we see that we use the second definition of $\sigma(t^{-1})$ and as g_1 is a coset representative and $\phi^{-1}(g_0) \in A$ the coset representative of $A\phi^{-1}(g_0)g_1$ is g_1. Thus

$$\sigma(t^{-1})(g_0, g_1, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n) = g_0, t^{-1}, g_1, t^{\epsilon_2}, \ldots, t^{\epsilon_n}, g_n.$$

If the second part of the definition of $\sigma(t)$ applies then obviously

$$\sigma(t^{-1})\sigma(t)(g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n) = g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n.$$

Thus $\sigma(t^{-1})\sigma(t) = 1_W$ and using the same method we see also that $\sigma(t)\sigma(t^{-1}) = 1_W$. Notice also that if $b \in B, \sigma(b) = \sigma(t^{-1})\sigma(b)\sigma(t)$ and hence σ maps all defining relations to 1. Thus σ is a homomorphism from G^* into $S(W)$.

Finally notice that if $g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n$ is a normal form then

$$\sigma(g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n)(1) = g_0, t^{\epsilon_1}, \ldots, t^{\epsilon_n}, g_n.$$

□

2.1.1 Power normal form

Definition 2.5 (Power Normal Form) *Let $x \in G\langle v, t\rangle$, a free extension of a centralizer in G. x is in power normal form if $x = pc_1c_2 \cdots c_r$ where:*

(1) $p \in C_G(v)$*,*

(2) $c_1, \ldots, c_r$ *are either powers of* t *or right coset representatives (as chosen before for the normal form) and* $\forall i, c_i \neq 1$*,*

(3) $\forall i < r$ *if* c_i *is a power of* t *then* c_{i+1} *is a right coset representative, and vice versa.*

The power normal form of x can be found uniquely from the normal form of x. If in normal form $x = g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n$ then we may write $x = pc_1c_2 \cdots c_r$ calculating as follows:

(1)If $g_0 \in C_G(v)$ then $p = g_O$. Otherwise c_1 is the coset representative for g_0 and $g_0 = pc_1$ where $p \in C_G(v)$.

(2)Thus if $g_0 \in C(v)$, c_1 is a power of t. Let $i = 1$. Otherwise we have already calculated a value for c_1 and thus c_2 is a power of t, let $i = 2$. Powers of t and coset representatives alternate from then on. If $g_1 \neq 1$ then $c_i = t^{\epsilon_1}$ and let $k = 0$. Otherwise $g_j = 1$ for $j = 1, \ldots, k$ and $g_{k+1} \neq 1$ and we set $c_i = t^{\epsilon_1 + \cdots + \epsilon_{k+1}}$. Let $i = i + 1$.

(3) If $n > k$ then $c_i = g_{k+1}$ and let $i = i + 1, k = k + 2$.

(4) If $n \geq k$ and $g_k \neq 1$ then $c_i = t^{\epsilon_k}, l = 0$. Otherwise $g_j = 1, j = k, \cdots, k + l - 1$; $g_{k+l} \neq 1$ and $c_i = t^{\epsilon_k + \cdots + \epsilon_{k+l}}$. Let $i = i + 1, k = k + l - 1$ and go to step 3.

Hence we see that each normal form induces a unique power normal form. Further each power normal form induces a unique normal form $g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n$ by the following method where the power normal form of x is $pc_1c_2 \cdots c_r$:

(1)If c_1 is a right coset representative then $g_0 = pc_1$ otherwise $g_0 = p$. Let i be the index of the first c_i which is a power of t. Let $j = 1$.

(2) If $i \leq r$ we have $c_i = t^\alpha$ for some α. If $\alpha = \pm 1$ then $\epsilon_j = \alpha$. Otherwise $\epsilon_k = \alpha / \mid \alpha \mid$; $k = j, \ldots, j+\alpha-1$ and $g_k = 1, k = j, \ldots, j+\alpha-2$. Let $i = i+1, j = j+\alpha-1$.

(3) If $i \leq r$ we have $g_j = c_i$. Let $i = i+1, j = j+1$, go back to step 2.

(4) If $i > r$ and c_{i-1} is a power of t, let $g_j = 1$.

Thus clearly all elements in the group can be uniquely identified by a power normal form. We now define length for a power normal form.

Definition 2.6 *Given $x \in G\langle v, t\rangle$, such that the power normal form is $x = pc_1c_2\cdots c_r$, then the power normal length of x, $|x|_p = r$.*

2.1.2 Commutation in free extensions of centralizers

Next we introduce a theorem about commutation in a free extension of a centralizer. This theorem is based on Theorem 4.5 on page 209 of Magnus, Karras and Solitar [10].

Theorem 2.2 *Let $H = \langle G, t \mid [C(v), t] = 1\rangle$ and suppose $x, y \in G$ and $[x, y] = 1$. Then*

(1) x or y may be in a conjugate of $C(v)$;

(2) if neither x nor y is in a conjugate of $C(v)$ but x is in a conjugate of G then y is in the same conjugate of G;

(3) if neither x nor y is in a conjugate of G or $C(v)$, then $x = huh^{-1} \cdot W^j$ and $y =$

$hu'h^{-1} \cdot W^k$, where $h, W \in H$, $u, u' \in H$ and $huh^{-1}, hu'h^{-1}$, and W commute in pairs.

Proof of Theorem 2.2: If x or y is in a conjugate of $C(v)$ there is nothing to prove. Thus assume neither x nor y is in a conjugate of $C(v)$. Let x be in a conjugate of G, thus $hxh^{-1} = g \in G, g \notin C(v)$. Thus hyh^{-1} commutes with g. We have that $hyh^{-1} \notin C(v)$, and we will take the normal form of hyh^{-1} to be $h_0 t^{\epsilon_1} h_1 \dots t^{\epsilon_n} h_n$. Now

$$h_0 t^{\epsilon_1} h_1 \dots t^{\epsilon_n} h_n \cdot g \cdot h_n^{-1} t^{-\epsilon_n} \dots t^{-\epsilon_1} h_0^{-1} = g.$$

If $h_n g h_n^{-1} \notin C(v)$ then the expression on the left has length $2n$ but g has length zero. Hence if $n > 0$ then $h_n g h_n^{-1} \in C(v)$. But this would mean x is in a conjugate of $C(v)$ hence $n = 0$ and thus $hyh^{-1} \in G$. Hence, x and y are both in $h^{-1}Gh$, a conjugate of G.

Now to finish the proof we shall assume the theorem is false and obtain a contradiction. Let x be an element of shortest power length for which there exists a y which contradicts the theorem. Pick y to be an element of minimal power length which leads to a contradiction for the x chosen. By the above neither x nor y can be in a conjugate of G or $C(v)$. Thus we have $x = pc_1 \dots c_r, r > 1$ and $y = p'd_1 \dots d_s, s > 1$ are the power normal forms of the elements, notice also that $s \geq r$ as otherwise x would not be of minimal power length. Notice that c_r and c_1 cannot be of the same form, i.e. one is a power of t while the other is a right coset representative. Otherwise $c_r x c_r^{-1} = (c_r p c_1) c_2 \dots c_{r-1}$. If c_r, c_1 are powers of t then this gives $c_r x c_r^{-1} = p(c_r c_1) c_2 \cdots c_{r-1}$ which has length $r - 1$, and if c_r, c_1 are both right coset representatives then $c_r x c_r^{-1} = p'' c_1' c_2 \dots c_{r-1}$ which also has length $r - 1$. Further as c_1 and c_r have different form, they cannot both have the same form as d_s.

Without loss of generality we will assume c_1 and d_s do not have the same form, the proof works in exactly the same way if c_r and d_s do not have the same form, replacing x by x^{-1} throughout the proof.

Thus we know that $yx = p'd_1 \cdots d_s p c_1 \cdots c_r$ has power length $s + r$. Hence $xy = yx = pc_1 \cdots c_r p' d_1 \cdots d_s$ also has power length $s + r$ which gives that c_r and d_1 have different forms. Notice that in $yx, c_1, \ldots, c_r$ occur as the r last representatives, while in $xy, d_1, \ldots, d_s$ occur as the last s representatives. Thus as $r \leq s$ we have that $c_r = d_s, c_{r-1} = d_{s-1}, \ldots, c_1 = d_{s-r+1}$. So now $yx^{-1} = p'd_1 \cdots d_{s-r}p^{-1}$ and as it is an element which commutes with x but which has shorter power length than y, it must be that yx^{-1} and x satisfy the assertions of the theorem. We have three cases, in the first case yx^{-1} is in a conjugate of C(v), thus $yx^{-1} = gug^{-1}$ where $u \in C(v)$. Then as $x = g1g^{-1} \cdot x$ and $y = yx^{-1}x = gug^{-1}x$ we have that x and y would satisfy the theorem contrary to our assumption. Next if yx^{-1} is in a conjugate of G then from above x is in the same conjugate of G, and hence $y = yx^{-1}x$ is also, again contradicting the assumptions made. Thus only one case is left and we have that $x = huh^{-1} \cdot W^j, yx^{-1} = hu'h^{-1}W^k$ where $huh^{-1}, hu\prime h^{-1}$,and W commute in pairs. But $y = yx^{-1} \cdot x = hu'h^{-1}W^k \cdot huh^{-1}W^j = hu'uh^{-1}W^{j+k}$ and thus x and y satisfy the assumptions of the theorem. Thus assuming c_1 and d_s are not of the same form leads to a contradiction, and as mentioned above so does assuming c_r and d_s are not of the same form.

□

2.2 CSA groups

In this section we follow the work of Myasnikov and Remeslennikov in section 6 of [11]. We begin by giving two definitions.

Definition 2.7 *A subgroup A of a group G is called malnormal if $A \cap A^g = 1$ for all $g \in G \setminus A$.*

Definition 2.8 *G is a CSA group if all of the centralizers of nontrivial elements in G are abelian and malnormal.*

Clearly a free group is a CSA group as all of its elements have cyclic centralizers and $g^{-1}a^i g = a^j$ in a free group if and only if g is a power of a (in which case $i = j$).

Definition 2.9 *A group G is said to have commutation transitivity if for all x, y, z, $[x, y] = 1$ and $[y, z] = 1$ implies that $[x, z] = 1$.*

Lemma 2.1 *CSA groups have the property of commutation transitivity.*

Proof: Let G be a CSA group and $x, y, z \in G$ be non trivial elements with the property that $[x, y] = 1, [y, z] = 1$. Then $y \in C(x)$ as y commutes with x. But notice $y \in C(x)^z \cap C(x)$. Hence as G is CSA we have that $z \in C(x)$ or that $[x, z] = 1$.

Theorem 2.3 *The property of being a nonabelian CSA group is preserved by free extension of centralizers.*

The proof of this theorem is based on work found in Myasnikov and Remeslennikov[11], with additional proof based on work by Magnus, Karras and Solitar[10]. First we will introduce some lemmas which will be useful in proving this result, the first of these is similar to Lemma 1 in [11]. Let G be a nonabelian CSA group.

Lemma 2.2 *Let $x \in G^* = G\langle v, t\rangle$. Then:*

(1) if $x \in C(v)^g$ then $C(x) = C(v)^g$,

(2) if $x \notin C(v)^g$ but $x \in G^g$ then $C(x) \leq G^g$,

(3) if $x \notin C(v)^g, x \notin G$ then $C(x) = \langle z\rangle$ where z is not in a conjugate of $C(v)$, and z is not a proper power.

We will use the description of conjugate elements in a free extension of centralizers as given in section 2.1.2.

Proof: Let $x \in C(v)^g$. Clearly if $y \in C(v)^g$ then $[x, y] = [gug^{-1}, gu'g^{-1}] = 1$ where $u, u' \in C(v)$. Now assume $y \in G^*$ and $[x, y] = 1$. Conjugating by g^{-1} if necessary we may assume that $x \in C(v)$. In power normal form $y = pd_1d_2 \cdots d_n$ and $x = p't^{\alpha}$(where $p' \in C_G(v)$) thus $xy = yx$ implies

$$xpd_1 \cdots d_n = pd_1 \cdots d_n x.$$

If d_n is not a power of t then we get that $d_np' = x_1d_n$ where $x_1 \in C_G(v)$, or $d_np'd_n^{-1} = x_1$. Otherwise d_n commutes with x but we see that d_{n-1} does not and hence we have $d_{n-1}p' = x_1d_{n-1}$ or $d_{n-1}p'd_{n-1}^{-1} = x_1$ where $x_1 \in C_G(v)$. However both statements provide a contradiction as G is a CSA group.

If $x \in G^g$ then from theorem 2.2, if $[x, y] = 1$ then $y \in G^g$ and thus we have case (2).

Finally suppose x is not in a conjugate of either G or $C(v)$ and $[x, y] = 1$ for $y \in G^*$. From the above description $y \notin G^g$ and also from the proof above $y \notin C(v)^g$. Hence from theorem 2.2, $x = huh^{-1} \cdot z^j$ and $y = hu'h^{-1} \cdot z^k$, where $h, z \in g'$, $u, u' \in C(v)$ and $gug^{-1}, gu'g^{-1}$, and z commute in pairs. If we conjugate by h we reduce the problem to the case $x = uz_1^j, y = u'z_1^k, z_1 = h^{-1}zh$. If $u \neq 1$ or $u' \neq 1$ then from above $z_1 \in C(v)$, but this contradicts that z is not in a conjugate of $C(v)$. Thus $u = 1, u' = 1$ and we have proved case (3).

Corollary 2.1 *All centralizers of elements in $G\langle v, t\rangle$ are abelian and $G\langle v, t\rangle$ has commutation transitivity.*

Proof: We first remember that G is a CSA group and hence it has commutation transitivity and the property that all centralizers of its elements are abelian. From above we have three different types of centralizers. The corollary is obvious for centralizers of types 1 and 3. If $C(x)$ is a centralizer of type 2 notice that it is the conjugate of a centralizer in G, and hence the theorem holds.

Corollary 2.2 *There are three types of maximal abelian subgroups of $G^* = G\langle v, t\rangle$:*

(1) M^g where M is a maximal abelian subgroup of G, $g \in G\langle v, t\rangle$ and M is not a conjugate of $C_G(v)$,

(2) $C(v)^g, g \in G\langle v, t\rangle$,

(3) $< z >$ where z is not a proper power and $z \notin C(v)^g, z \notin G^g$.

Proof: Due to commutation transitivity this is straightforward.

Next we give a theorem on conjugacy in a free extension of centralizers, this is based on lemma 2 in Myasnikov and Remeslennikov [11] and page 185 of Lyndon and Schupp [8].

Theorem 2.4 *Let g be a cyclically reduced element of* $G^* = \langle G, t | t^{-1}zt = z, z \in C(v) \rangle$ *then*

(1) If g *is conjugate to an element* h *in* G *then* g *is also in* G *and is conjugate to* h *in* G.

(2) If $g = g_0 t^{\epsilon_1} g_1 \cdots t^{\epsilon_n}$, $n \geq 1$ *and v is a conjugate cyclically reduced element then* $|g| = |v|$ *and* g *is a conjugate of some appropriate cyclic permutation* v^* *of* v *by some element* $c \in C_G(z)$.

Proof of Theorem 2.4: Case (1): We have that $g = chc^{-1}$ for some c, if $c \in G$ then $|g| = 0$, hence $g \in G$ and we are done. Suppose $c \notin G$ i.e. $|c| \geq 1$, then notice that $|hc^{-1}c| < |chc^{-1}|$ implying that g is not cyclically reduced. Thus $c \in G$, and $g, h \in G$ and are conjugate in G.

Case (2): We will prove by induction on $|c|$ that if $v^* = h_0 t^{\delta_1} \cdots t^{\delta_m}$ is any cyclic permutation of v which ends in a power of t and $cv^*c = g$ then the theorem holds. First let $|c| = 0$. Then

$$ch_0 t^{\delta_1} \cdots t^{\delta_m} c^{-1} = g_0 t^{\epsilon_1} \cdots t^{\epsilon_n}$$

and thus

$$1 = g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} c t^{-\delta_m} \cdots t^{-\delta_1} h_0^{-1} c^{-1}.$$

The only possible reduction on the right hand side is $t^{\epsilon_n} c t^{\delta_m}$, thus $c \in C(z)$ and $\epsilon_n = \delta_m$. As before, in the proof of a unique normal form, we must have that $n = m$ and $\forall i, \epsilon_i = \delta_i$.

Next let $|c| = k \geq 1$, where $c = c_0 t^{\lambda_1} \cdots t^{\lambda_k} c_k$. We now have

$$g = c_0 t^{\lambda_1} \cdots t^{\lambda_k} c_k h_0 t^{\delta_1} \cdots t^{\delta_m} c_k^{-1} t^{-\lambda_k} \cdots t^{-\lambda_1} c_0^{-1}.$$

However g is cyclically reduced, thus there must be some possible reduction of the right hand side so that this element is also cyclically reduced. The only places where such a reduction can occur are $t^{\lambda_k} c_k h_0 t^{\delta_1}$ or $t_m^{\delta} c_k^{-1} t^{-\lambda_k}$.

First assume that the reduction takes place at $t^{\lambda_k} c_k h_0 t^{\delta_1}$. Then $\lambda_k = -\delta_1$ and $c_k h_0 \in C(z)$. Thus $t^{\lambda_k} c_k h_0 t^{\delta_1} = c_k h_0$ and hence adding $(c_k h_0 h_0^{-1} c_k^{-1}) = 1$ to the sequence

$$g = c_0 t^{\lambda_1} \cdots t^{\lambda_{k-1}} c_{k-1} c_k h_0 h_1 t^{\delta_2} \cdots t^{\delta_m} c_k^{-1} t^{-\lambda_k} (c_k h_0 h_0^{-1} c_k^{-1}) c_{k-1}^{-1} t^{-\lambda_{k-1}} \cdots t^{-\lambda_1} c_0^{-1}.$$

We know from above that $t^{-\lambda_k} c_k h_0 = c_k h_0 t^{\delta_1}$ and thus

$$g = c_0 t^{\lambda_1} \cdots t^{\lambda_{k-1}} c_{k-1} c_k h_0 (h_1 t^{\delta_2} \cdots t^{\delta_m} h_0 t^{\delta_1}) h_0^{-1} c_k^{-1} c_{k-1}^{-1} t^{-\lambda_{k-1}} \cdots t^{-\lambda_1} c_0^{-1}.$$

Notice the expression in the brackets is a cyclic permutation of v and that now we have $g = a v^* a^{-1}$ where $|a| < |c|$. The result follows by the induction hypothesis.

If instead the reduction takes place at $t^{\delta_m} c_k^{-1} t^{-\lambda_k}$ we can use the same idea. We now have that $\delta_m = \lambda_k$ and $c_k^{-1} \in C_G(z)$, thus $t^{\delta_m} c_k^{-1} t^{-\lambda_k} = c_k^{-1}$. Hence

$$g = c_0 t^{\lambda_1} \cdots t^{\lambda_{k-1}} c_{k-1} (c_k c_k^{-1}) t^{\lambda_k} c_k h_0 t^{\delta_1} \cdots t^{\delta_{m-1}} h_{m-1} c_k^{-1} c_{k-1}^{-1} t^{-\lambda_{k-1}} \cdots t^{-\lambda_1} c_0^{-1}.$$

But now we reduce again as above and

$$g = c_0 t^{\lambda_1} \cdots t^{\lambda_{k-1}} c_{k-1} c_k (t^{\delta_m} h_0 t^{\delta_1} \cdots t^{\delta_{m-1}} h_{m-1}) c_k^{-1} c_{k-1}^{-1} t^{-\lambda_{k-1}} \cdots t^{-\lambda_1} c_0^{-1}.$$

Once again we have that the section within the brackets is a cyclic permutation of v and the result follows by the induction hypothesis.

Finally notice that when $g = cv^* c^{-1}$ where $c \in C(z)$ it follows by the same logic as in the proof of unique normal form, that the order of powers of t is exactly the same in both g and v^*.

Proof of Theorem 2.3: Once again we have three cases due to corollary 2.2. First let $N = M^g$ be a maximal abelian subgroup of G^* of type (1). We can reduce to the case where $N = M < G$ by conjugating if necessary. Now consider for which values of $x, M^x \cap M = z \neq 1$, i.e. for which values of x there are non trivial elements $f, h \in M$ such that $f^x = h$. But f written in normal form is cyclically reduced, hence there exists a $y \in G$ such that $f^y = h$ from part (1) of the preceding theorem. But this gives that $M \cap M^y \neq 1$ and hence $y \in M$ as G is a CSA group, and so $f = h$ as M is abelian. Hence $[h, x] = [f, x] = 1$ and from lemma 2 we have that $x \in G$. But this in turn implies that $x \in M$.

Next we look at centralizers of type 2, i.e. $N = C(v)^g, g \in G^*$. Once again, by conjugating if necessary, we only need examine the case $N = C(v)$. Suppose $C(v) \cap C(v)^x \neq 1$ then there are $f, h \in C(v)$ such that $f^x = h$. Notice all elements in $C(v)$ are cyclically reduced when written in normal form hence theorem 4 applies. If $h \in G$ then $f \in G$ and thus there exists $y \in G$ such that $f^y = h$ as above. But this gives that

$C_G(v) \cap C_G(v)^y \neq 1$ and hence $y \in C_G(v)$. Thus as above $f = h$ and we have $[f, x] = 1$ and thus $x \in C_G(v)$. Otherwise we have the case that $|f| \geq 1$ and thus from part (2) of theorem 4 $|f| = |h|$. Further the normal form of an element in $C(v)$ has the form $gt^{\epsilon}1t^{\epsilon} \cdots t^{\epsilon}1$ where $\epsilon = \pm 1$ and $g \in C_G(v)$. Thus from the commutativity of g with t^{ϵ} we see that all cyclic permutations of h are in fact equal to h, thus we have $f = h^y$ where $y \in C(v)$. But now we have $f = h$ and hence $f^x = h^x = h$ and thus as $C(v) = C(h)$ from lemma 2 we have that $x \in C(v)$.

Finally we look at centralizers of type 3, i.e. $N = \langle z \rangle$.We introduce the notation $||z|| = \min\{|y| \ \ |y$ is cyclically reduced and conjugate to $z\}$. As we are given that $z \notin C_G(v)^g, z \notin G^g$ we have that $||z|| \geq 1$. Thus if $N \cap N^x \neq 1$ we have that $(z^n)^x = z^m$ for some integers n, m. Hence $||z^n|| = ||z^m||$, but we see easily that $||z^n|| = |n| \cdot ||z||$ and thus we now have that $|m| = |n|$. If $n = m$ then $[x, z^n] = 1$ which implies by commutation transitivity that $[x, z] = 1$ and thus $x \in \langle z \rangle$. If $n = -m$, then $x^{-1}z^n x = z^{-n}$ and thus $x^{-2}z^n x^2 = x^{-1}z^{-n}x = z^n$. Thus $[x^2, z^n] = 1$ and by commutation transitivity $[x, z] = 1$ and $x \in \langle z \rangle$.

□

2.2.1 Direct limits of CSA groups

Next we will introduce a theorem which is necessary for the proof of the construction of the Lyndon's group. The work in this section is found in lemma 3 and theorem 6 in

Myasnikov and Remeslennikov [11].

Theorem 2.5 *Let $G = \{G_i, \phi_j^i, I\}$ be an inductive system of non-abelian CSA groups, $i \in I$ and $G^* = \lim_{\rightarrow} G_i$. Then G^* is a non-abelian CSA group.*

First we prove a lemma about centralizers in G_i^*.

Lemma 2.3 *Let $G^* = \lim_{\rightarrow} G_i$ be a direct limit of CSA groups $G_i, i \in I$. If M is a maximal abelian subgroup of G^*, then $\forall i\ G_i \cap M = M_i$ is either maximal abelian in G_i or trivial. Further $M = lim_{\rightarrow} M_i$.*

Proof of Lemma 2.3: The first point to notice is that G^* has the property of commutation transitivity. This is because any three elements $x, y, z \in G^*$ such that $[x, y] = [y, z] = 1$, have the property that $x, y, z \in G_k$ for some k, but we have that all G_k are CSA groups, thus $[x, z] = 1$.

Assume M_i is nontrivial and not maximal in G_i. As M_i is not maximal there exists an $x \notin M_i$ such that $[M_i, x] = 1$. Now by commutation transitivity, M is the centralizer of some element $z \in G^*$. Hence there exists a $k, i \leq k$ such that $x, z \in G_k$. From commutation transitivity $[x, z] = 1$, and hence $x \in M$, providing a contradiction.

From the definition given it is obvious that

$$M = \lim_{\rightarrow} M_i$$

Now to finish proving Theorem 2.5. Take M a maximal abelian subgroup of G^* and suppose $M \cap M^g \neq 1$. Then $x = y^g$ for some $x, y \in M$. We chose $k \in I$ such that

$x, y, g \in G_k$ and from above $M_k \cap M_k^g \neq 1$ in G_k. But G_k is a CSA group and hence $g \in M_k < M$.

□

2.3 The Lyndon's Group

We first define A groups as defined in Myasnikov and Remeslennikov [11]. Let A be any associative ring with identity and let G be a group. Then we have a map $G \times A \to G$, and we write the action of $\alpha \in A$ on $g \in G$ as g^α. In order for G to be an A group the action of A on G must have the following 4 properties where $\alpha, \beta \in A$ and $g, h \in G$:

(1) $g^1 = g, g^0 = 1, 1^\alpha = 1$

(2) $g^{\alpha+\beta} = g^\alpha \cdot g^\beta, g^{\alpha\beta} = (g^\alpha)^\beta$

(3) $(h^{-1}gh)^\alpha = h^{-1}g^\alpha h$

(4) $[g, h] = 1 \Rightarrow (gh)^\alpha = g^\alpha h^\alpha$

Another important notion is that of the A completion of a group G. The A group G^A and a homomorphism λ from $G \to G^A$ is called a tensor A completion of G if G^A satisfies the universal property that for any A group H and any homomorphism $\psi : G \to H$ there exists a unique A-homomorphism $\phi : G^A \to H$ such that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "\lambda"] \arrow[d, "\psi"'] & G^A \arrow[dl, "\phi"] \\
H &
\end{tikzcd}$$

The Lyndon's group is such a completion where G is a free group, and A is the ring of polynomials with inseparable coefficients in one indeterminate.

In order to make the development of later ideas simple it is now necessary to construct the Lyndon's group $F^{Z[x]}$. Note that length will be defined differently from in previous sections, rather the length of a word W, will be the length in letters of the reduced word equivalent to W. Another construction for this group can be found in Myasnikov and Remeslennikov [11]. We will proceed in the following manner.

Let F_1 be F. Let V_{i+1} be a maximal set of primitive reduced elements which have nonconjugate centralizers and length less than $i+1$ in F_i (length is well defined as these are reduced elements). We now form F_{i+1} from F_i and V_{i+1} by extending the centralizers of each element in V_{i+1}, i.e.

$$V_{i+1} = \{a_{i1}, a_{i2}, \ldots, a_{in}\}$$

and

$$\cdots \leq F_i \leq F_{i_1} = \langle F_i, t_{i_1} | t_{i_1} a t_{i_1}^{-1} = a, \forall a \in C(a_{i_1}) \rangle \leq F_{i_2} \cdots \leq$$

$$\leq F_{i_n} = \langle F_{i_{n-1}}, t_{i_n} | t_{i_n} a t_{i_n}^{-1} = a, \forall a \in C(a_{i_n}) \rangle = F_{i+1} \leq \cdots$$

where t_{ik} extends the centralizer of a_{ik}.

Notice from the previous section that we have $\bigcup_{i=1}^{\infty} F_i$ is a CSA group, and hence all of its centralizers are abelian and malnormal. Further due to commutation transitivity all intersections of centralizers are trivial.

Claim 2.1 $F^{Z[x]} = \bigcup_{i=1}^{\infty} F_i$.

Proof of Claim 2.1: The first step is to show that $\bigcup F_i$ is in fact a $Z[x]$ group. We see that every centralizer in $\bigcup F_i$ is in fact isomorphic to $Z[x]$. From the construction we see we have a map ϕ of the generators of $Z[x]$ to the generators of the centralizer of each element v equal to $\langle v, t_1, t_2, t_3, \ldots \rangle$ in the following manner $\phi(1) = v, \phi(x) = t_1, \phi(x^2) = t_2$. Thus every centralizer admits the action of $Z[x]$.

Define a root element to be an element of F_i which occurs for the first time in F_i and is not in the centralizer of any element occurring in an earlier extension. Notice that by the construction every centralizer in $\bigcup F_i$ is conjugate to the centralizer of some root element in $\bigcup F_i$. All centralizers in $\bigcup F_i$ have trivial intersection as $\bigcup F_i$ is a CSA group due to theorem 2.5, thus we see that the action of $Z[x]$ can be well defined on $\bigcup F_i$. Simply define the action of $Z[x]$ on centralizer's of root elements and then use conjugation to define the action on the whole of $\bigcup F_i$. We can define this action in the following manner, where our centralizer is as above, $v^1 = v, v^x = t_1, v^{x^2} = t_2$, etc. Hence $\bigcup F_i$ is a $Z[x]$ group.

It remains to show that this group satisfies the universal property previously mentioned. Let H be a $Z[x]$ group and $\phi : F \to H$ a homomorphism. We can embed F in $\bigcup F_i$ (after all F is F_1), and so define $\gamma : \bigcup F_i \to H$ such that all elements in F are mapped to the correct element in H. Then by letting γ be a $Z[x]$ homomorphism (i.e. having its action commute with that of $Z[x]$) we arrive at a well defined homomorphism which makes the diagram commute. γ is clearly defined uniquely, hence $\bigcup F_i$ is indeed the Lyndon's group $F^{Z[x]}$.

$$\begin{tikzcd}
F \arrow[r, two heads] \arrow[d, "\phi"'] & \bigcup F_i \arrow[dl, "\gamma"] \\
H &
\end{tikzcd}$$

It also follows now that any subgroup of $F^{Z[x]}$ is a subgroup of a countable extension of centralizers of F. Further any finitely generated subgroup is a subgroup of a finite extension of centralizers.

2.4 Van Kampen diagrams

The ideas in this section can be found in Lyndon and Schupp [8] and Van Kampen [12].

In order to prove the Van Kampen lemma and discuss Van Kampen diagrams it is first necessary to establish some definitions. These diagrams are two dimensional in the

Euclidean plane E^2. If $S \subseteq E^2$ then the boundary of S will be denoted by δS while the topological closure is written $\bar{S}$. A map M in E^2 consists of 3 distinct parts; vertices, edges and cells which are pairwise disjoint in the map. A vertex is a point in E^2, an edge is a bounded subset of E^2 homeomorphic to the open unit interval, while a cell is a bounded set homeomorphic to the open unit disk. Any map must have the property that for each edge in M there are 2 vertices a, b in M such that $\bar{e} = e \cup \{a\} \cup \{b\}$. Also if any cell C is in M then δC is connected and there is a set of edges $e_1, \ldots, e_n$ all in M such that $\delta C = \bar{e}_1 \cup \cdots \cup \bar{e}_n$.

We can now add the idea of direction to our concept of a map. For an edge e such that $\bar{e} = e \cup \{a\} \cup \{b\}$ the two endpoints $\{a\}$ and $\{b\}$ are thought of as being initial and terminal vertices. Thus if a is the initial vertex, e runs from a to b, and e^{-1}, the inverse of e, runs from b to a. Henceforth $\bar{e}$ will be known as a closed edge.

A path in M is a sequence of closed edges in M such that the terminal vertex of e_i is the initial vertex of e_{i+1}. A reduced path is a path in which no cancellations occur, i.e. if e is an edge in the path then e and e^{-1} will never occur adjacently. Further a simple path is a reduced path where all edges in the path have different initial vertices. A closed path of length n is a path such that the initial vertex of e_1 is the terminal vertex of e_n, such a path is also called a cycle.

By giving each edge in a map M an orientation we create an oriented map M'. We now define a boundary cycle of a cell C to be a reduced closed path of minimal length which includes all edges of δC with their orientations in accordance with the oriented map

M'. If M' is connected and simply connected, a boundary cycle of M' can be defined as a reduced closed path α of minimal length which contains all edges in $\delta M'$ in accordance with the orientation of M' such that, if e_i and e_{i+1} are consecutive edges in α with e_i terminating at v, then e_i^{-1} and e_{i+1} are adjacent in the cyclically ordered path of all edges of M beginning at v.

Definition 2.10 *Let $G = \langle a_1, \ldots, a_n | R = 1\rangle$ be a group with the relations R on $\{a_1, \ldots, a_n\}$ and $F = \langle a_1, \ldots, a_n\rangle$ be the corresponding free group. Then a Van Kampen diagram over G is an oriented map, as described above such that each edge e_i of the map has an associated label $\phi(e_i) \in F$ with the following 4 properties:*

1. If e is an edge in M then $\phi(e) \neq 1$,

2. If e is an edge and e^{-1} is the oppositely oriented edge then $\phi(e^{-1}) = \phi(e)^{-1}$,

3. If C is a cell then any boundary cycle of C, $e_1, e_2, \ldots, e_k$ has the property that $\phi(e_1)\cdots\phi(e_k)$ is reduced without cancellation and also $\phi(e_1)\cdots\phi(e_k)$ is cyclically equivalent to an element of R,

4. M is connected and simply connected. Further M has a boundary cycle $e_1, \ldots, e_k$ such that $\phi(e_1)\cdots\phi(e_k)$ is cyclically reduced without cancellation, i.e. $\phi(e_1)\cdots\phi(e_k)$ and all cyclic permutations of this word have the property that $\forall f \in F$ there is no occurrence of ff^{-1} in the word.

2.4.1 Van Kampen's Lemma

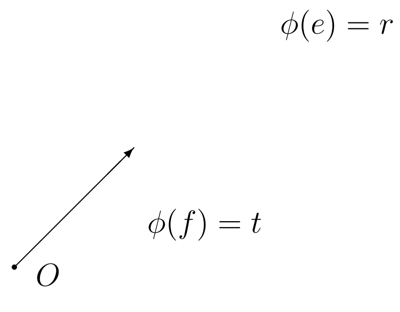
We are now ready to prove Van Kampen's Lemma, we follow the work in Lyndon and Schupp [8]. Let R be a set of relations over a free group F. Expand R to contain all cyclically equivalent expressions. Let N be the normal closure of this expanded R.

Lemma 2.4 *If $w \in F$, $w \in N$ if and only if there exists a connected, simply connected Van Kampen diagram M such that $\phi(\alpha) = w$ where α is a boundary cycle of M.*

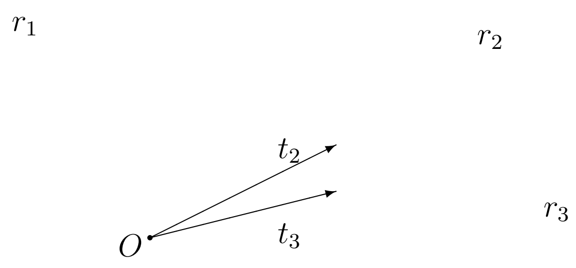
Proof: Assume $w \in N$, i.e.

$$w = \prod_{i=1}^{n} t_i r_i t_i^{-1}$$

where $r_i \in R$ (R defined as above), $t_i \in F$. If $n = 0$ then the diagram M is a single vertex O. If $n = 1$ we take an edge e and vertex v such that both the initial and terminal vertices of e are v and $\phi(e_1) = r_1$. If $t_1 = 1$ this is the complete diagram and for consistency we rename v as O. If $t_1 \neq 1$ then add an extra vertex O to the diagram outside the loop formed by e and connect O to v. The edge f running from O to v is labeled such that $\phi(f) = t$.



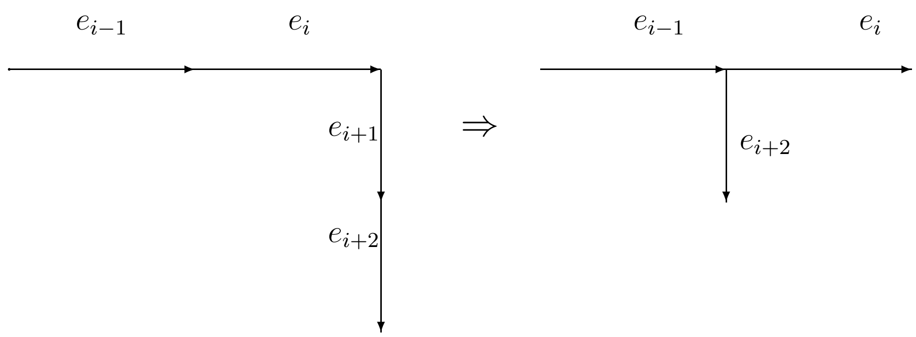
Now if $n > 1$ construct the diagram in the following manner. For each i construct a diagram as above and link these diagrams in order to a common vertex O as below.



If

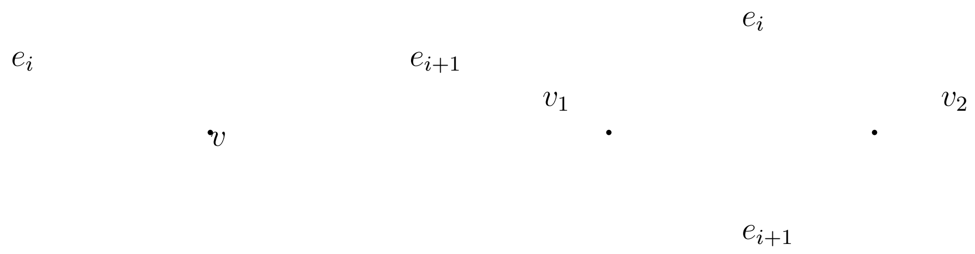
$$\prod_{i=1}^{n} t_i r_i t_i^{-1}$$

is cyclically reduced without cancellation we are finished. However it is possible that cancellations can be made in this word, in this case break down each edge in the diagram creating M' so that every edge is labeled by a generator of F. For example if $\phi(e_1) = x_1 x_2 x_1^{-1}$, then in M' there are 3 edges, e_{11}, e_{12}, e_{13} such that $\phi(e_{11}) = x_1, \phi(e_{12}) = x_2, \phi(e_{13}) = x_1^{-1}$. Now consider successive pairs of edges e_i, e_{i+1} in the diagram such that $\phi(e_i) = \phi(e_{i+1})^{-1}$. Let e_i run from v_1 to v_2, and e_{i+1} run from v_2 to v_3. If v_3 is distinct from v_1 and v_2 (or v_1 is distinct from v_2 and v_3) identify e_{i+1} with e_i and glue them together as below to achieve a new diagram M''. Notice we have simplified our diagram and $\delta M''$ contains



fewer edges than $\delta M'$.

If $v_1 = v_3$ we have the situation of either one or two loops.



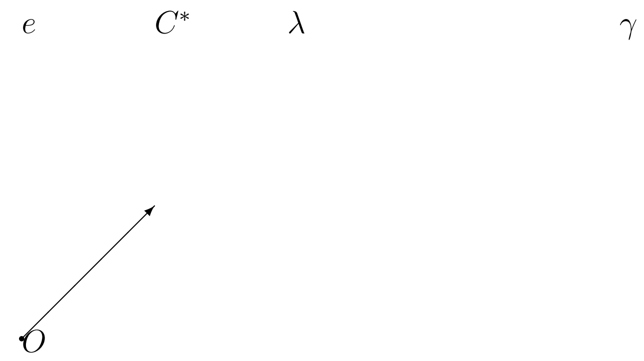
In this case to arrive at a simpler diagram M'' eliminate the loop(s) formed by e_i and e_{i+1} and all of M' interior to the loop(s) leaving only the vertex v_i. By iterating this process we eventually eliminate all possible cancellations and arrive at a diagram which satisfies the properties of a Van Kampen diagram. Hence if $w = 1$ it forms the boundary of a Van Kampen diagram.

Next assume M is a Van Kampen diagram with boundary δM such that α is a boundary cycle of the diagram and $\phi(\alpha) = w$. We need to show that if M consists of cells $C_1, C_2, \ldots, C_k$ then there exist labels $r_1, \ldots, r_k \in R$ of the cells and elements u_i $(1 \leq i \leq k)$ of F such that

$$w = (u_1 r_1 u_1^{-1}) \cdots (u_k r_k u_k^{-1}) = 1.$$

If $k = 0$ then there are no cells in M, thus M is a tree and hence trivially $\phi(\alpha) = 1$.

We shall use proof by induction. Assume the result is true for diagrams with k cells and let M be a diagram with $k+1$ cells. Clearly M contains a cell C^* such that $\delta M \cap \delta C^* \neq \emptyset$. Let $\{e_i\}$ be the set of edges e_i such that $e_i \in (\delta M \cap \delta C^*)$ and form M' from M by deleting $\{e_i\}$ from M.



We have that M' is a Van Kampen diagram with k cells. Let e be the ordered list of edges in $\{e_i\}$ and let the boundary cycle of C^* be $e\lambda$ and the boundary cycle α of M be $e\gamma$ such that $\phi(\lambda) = l, \phi(\gamma) = g, \phi(e) = x$. Then $\phi(\alpha) = xg = w$ and the label of M' is

$$\phi(\alpha') = \phi(\lambda^{-1}\gamma) = l^{-1}g = \prod_{i=1}^{k-1}(u_i r_i u_i^{-1})$$

by the induction hypothesis. But notice we may write $w = l^{-1}gg^{-1}xg = (l^{-1}g)(g^{-1}lxg)$. Hence from above $w = (u_1 r_1 u_1^{-1}) \dots (u_{k-1} r_{k-1} u_{k-1}^{-1})g^{-1}lxg$. By letting $g^{-1} = u_k$ and noticing lx is a label for C^* we can set $r_k = lx$ and have $w = (u_1 r_1 u_1^{-1}) \dots (u_k r_k u_k^{-1})$. Thus w is a label for a boundary cycle of a Van Kampen diagram if and only if $w \in N$, N as described above.

$\square$

Chapter 3

The conjugacy problem in $F^{Z[x]}$

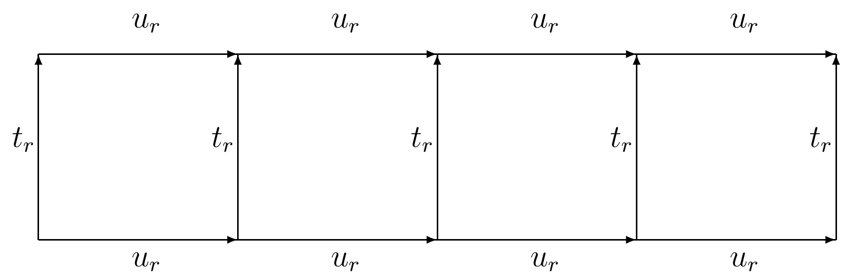
3.1 Reduction of the conjugacy problem from $F^{Z[x]}$ to groups of the type $F\langle U, T\rangle$

We have previously constructed the Lyndon's group $F^{Z[x]}$ such that $F^{Z[x]} = \cup F_i$ where

$$\cdots \leq F_i \leq F_{i+1} = \langle F_i, \{t_{i_1}\} | [a_{i_1}, t_{i_1}] = 1\rangle \leq F_{i+2} \leq \cdots$$

Definition 3.1 *A cell with boundary label $t_r u_r t_r^{-1} u_r^{-1}$ such that $t_r u_r t_r^{-1} u_r^{-1}$ is a relation added in F_r is a t_r cell.*

Definition 3.2 *A diagram consisting only of t_r cells connected by their t_r edges as pictured below is called a t_r strip.*

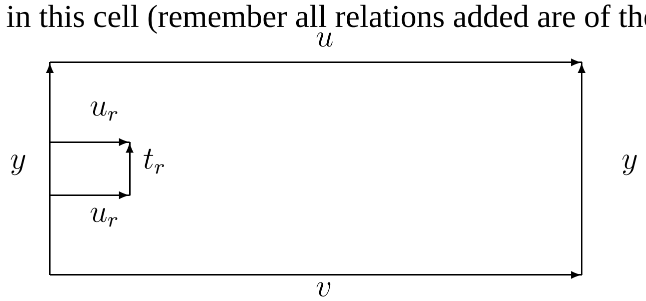


Notice two t_r strips cannot intersect as u_r does not contain t_r and vice versa.

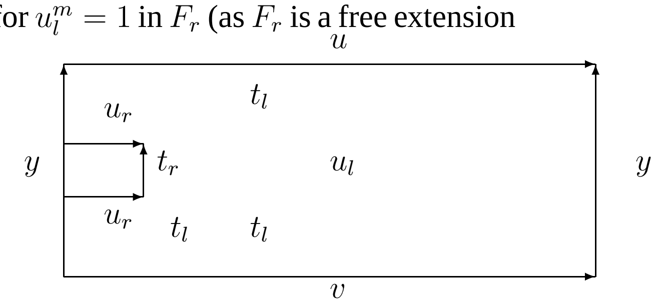
Lemma 3.1 *If u and v are conjugate in $F^{Z[x]}$ and both $u, v \in F_n$ then u and v are conjugate in F_n.*

Proof: We will assume that F_n is the first extension to contain both u and v and that u contains t_n. We have that u and v are conjugate hence there exists a $y \in F^{Z[x]}$ such that $yuy^{-1} = v$. We know in fact that $y \in F_r$ for some r, as words have finite length and thus contain only finitely many of the variables added through extensions.

From the Van Kampen lemma we have that there exists a Van Kampen diagram which has $yuy^{-1}v^{-1}$ for its boundary cycle label (from now on edges will be known by their labels). If the maximum i such that t_i is a letter in y is less than or equal to n then we are done. Suppose not, then t_r is a letter in y for some $r > n$. Thus we have the following picture, our diagram must include a t_r cell. It remains to show what is to be done with the other t_r involved in this cell (remember all relations added are of the form $xyx^{-1}y^{-1}$).

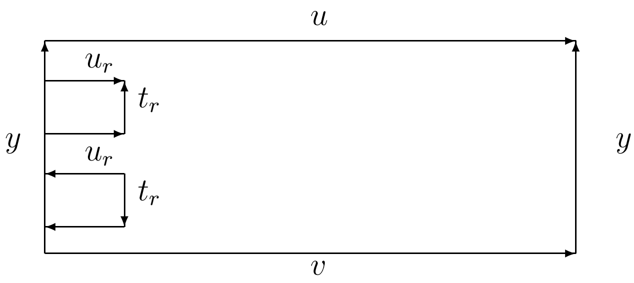


Notice first, any cell containing t_r which is not a t_r cell must contain an added variable t_l of index greater than r. But an edge t_l cannot link with any of the edges in the diagram as r is the maximum added variable index in $u, v,$ and y. Hence an annulus must be formed by the cells involving t_l as below. But this creates a region with boundary cycle u_l^m for some m, which clearly cannot exist as it is not possible for $u_l^m = 1$ in F_r (as F_r is a free extension of centralizers over a free group).

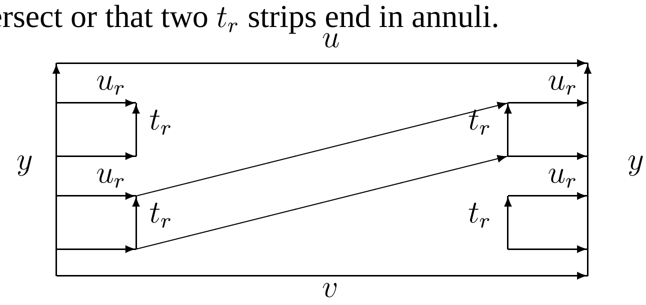


Hence we must have that the cell involving t_r is a t_r cell and that it is joined to other such cells. Notice that this cell cannot be joined to a mirror image of itself as then we would not have a Van Kampen diagram (in a Van Kampen diagram all boundary cycles are cyclically reduced without cancellation), hence we have a t_r strip. Following the same logic as above we see that we cannot have the formation of an annulus, and as neither u nor v contains t_r, a t_r strip can link to neither the u nor v edge.

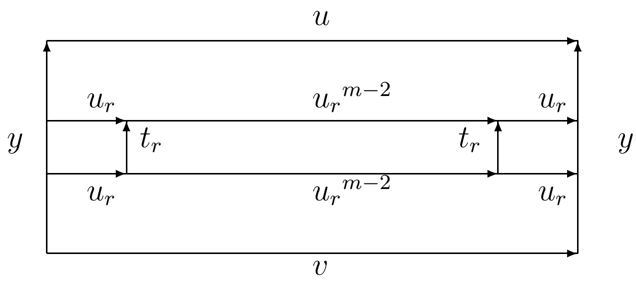
Thus we know the diagram contains a t_r strip which must be linked at both ends to edges of the diagram which are labeled with y. One possibility is that the t_r strip will link to the same side if y contains t_r^{-1}. In this case y may be replaced with an expression not involving these 2 incidences of t_r. Labeling the sections of y such that $y = x_1 t_r^{\epsilon} x_2 t_r^{-\epsilon} x_3$ where $\epsilon = \pm 1$, then y may be replaced with $x_1 u_r^m x_3$ for some n, as shown by the diagram below.



We also have the possibility that the t_r strip attaches to both y-edges of the diagram. There are now two possibilities, the chain may attach at the same spot on both y-edges or it may attach at different spots. If it attaches at different spots then we have a diagram as below, we assume there is no possible way of making arches on either side, otherwise we could simplify our problem as above by replacing y with a word containing less incidences of t_r. The diagram below cannot possibly exist as this diagram would require either that two t_r strips intersect or that two t_r strips end in annuli.



Thus there is one possibility left, that the t_r strip connects to both sides at the same location. Hence one can see from the diagram below that u is conjugate to u_r^m as is v, i.e. we have that $x_1 u x_1^{-1} = u_r^m$ and $x_2 u_r^m x_2^{-1} = v$. Thus $x_2 x_1 u x_1^{-1} x_2 {-} 1 = v$ and we now have that u and v are conjugate by a word y' which has one less incidence of t_r. Clearly by iterating this process we can further simplify y' to the point where y' is an element in F_n.



3.2 The Conjugacy Problem in $F\langle U, T\rangle$

We shall use the conjugacy theorem for free extensions of centralizers(Theorem 2.4) and the construction of $F^{Z[x]}$ (Claim 2.1) as already stated.

3.2.1 Solving a word problem

In order to prove that the conjugacy problem is solvable in $F\langle U, T\rangle$ it will be necessary to show that there exists an algorithm, solving equations of the type

$$bg_0t^{\epsilon_1}\cdots t^{\epsilon_n}g_na = h_0t^{\delta_1}\cdots t^{\delta_m}$$

where we are given $g_0t^{\epsilon_1}\cdots t^{\epsilon_n}g_n$ and $h_0t^{\delta_1}\cdots t^{\delta_m}$ and the centralizers to which a and b belong (notice these are not necessarily the same centralizer). We will do this proof by induction and thus it is first necessary to prove that there exists an algorithm solving such equations in a free group.

We begin with a lemma.

Lemma 3.2 *Given G a CSA group, then if A and B are maximal abelian subgroups $B^g \cap A = 1$ unless $B^g = A$.*

This lemma is obvious as CSA groups have commutation transitivity.

Using this lemma we see that there is a limited number of cases where the equation above can have multiple solutions. If

$$b_1 g a_1 = h = b_2 g a_2,$$

then

$$g^{-1} b_2^{-1} b_1^{-1} g = a_2 a_1^{-1}$$

which implies there are infinitely many solutions if $C(a) = C(b)^g$, but otherwise there can be at most one solution.

Theorem 3.1 *Let F be a free group with generators* $\{x_1, \ldots, x_n\}$. *Given two elements* $g, h \in F$ *and two centralizers* $C(z), C(y) \in F$ *then there is an algorithm solving the following equation for* $a \in C(z)$, $b \in C(y)$

$$gah = b.$$

Proof of Theorem 3.1: First notice that all centralizers in a free group are cyclic. We will consider three cases for this problem. In the following the use of the symbol $\{\cdot\}$ implies multiplication where no reduction is possible.

Case 1: $z = x^n, y = x^m$, i.e. a and b belong to the same centralizer $C(x)$. Then we have that if $g \in C(x)$ there are infinitely many solution pairs if $h \in C(x)$ and that for any choice of a we can find a b which will satisfy the equation. If $g \in C(x), h \notin C(x)$ then there is no solution to this equation. Thus we must only consider what happens if

$g \notin C(x)$ and $h \notin C(x)$, we use the following steps to calculate a, b. Notice that in this case there can be at most one solution. Let $a = 1$, then

(1) If $g = g' \cdot x^i, i \neq 0, |i|$ maximal, then as $g \notin C(x)$ we know this power of x must be cancelled so that the terms in g' which are not in $C(x)$ may also be cancelled. Hence as $g = g'x^i$ let $a = x^{-i}a, g = g'$ and continue with these new values of a and g.

(2) If $g = g' \cdot r, r \neq x^i \ \forall i$ then there are two possibilities. If $x^i = rl$ and $g' \in C(x), h = x^j lh', h' \in C(x)$ then the solution is $a = ax^{-j}, b = glh'$. Otherwise if there is a solution the term r must be cancelled by a term in h. Hence we must be able to write $h = x^i r^{-1} h'$ where $g'h' \in C(x)$. If this is the case then the solution is $a = ax^{-i}, b = g'h'$ if $g'h' \in C(x)$. If neither of these two offers a solution, there is no solution as there are terms in g which are not powers of x and which cannot be cancelled.

Case 2: $a \in C(z), b \in C(y), y = z^x, x \neq z^i \, \forall i$. Notice from the earlier lemma there is the possibility that such an equation has an infinite number of solutions, we will give an algorithm to find one solution (or show there is none if that is the case). Let $a = 1$ and use the following steps:

(1) $g = g' \cdot z^i$, $|i|$ maximal. If $g' = g''x, g'' \in C(y)$ then if $h = z^k x^{-1} h', h' \in C(y)(k$ may be 0) we may take as a solution $a = 1, b = gh$ (Notice this is a case where any value of a has a corresponding value of b which solves the equation). If h cannot be written in such a way then clearly there is no solution for such a g' . If $g \in C(z)$ then

if $h = z^k h'$ where $h' \in C(y)$ then there is the solution $a = g^{-1} \cdot a \cdot z^{-k}, b = h'$, if h cannot be written like this there is no solution. If g' suits neither of these subcases, let $g = g', a = z^{-i}a$ and continue with these new values.

(2) $g = g' \cdot x^{-1}$. If $g \in C(y)$ (i.e. $g' = xz^i$) then if $h = z^k h', h' \in C(y)$ we have the solution $a = az^{-k}, b = gah$, if h cannot be written this way then there is no solution. If $g \notin C(y)$ then if there is a solution we must have that $h = z^i x h'$ and then we have the solution $a = az^{-i}, b = g'h'$ if $g' \cdot h' \in C(y)$, otherwise there is no solution.

(3) $g = g' \cdot x$. If $g' = 1$ then there is a solution only if $h = z^i x^{-1} h', h' \in C(y)$ (i may be 0) and notice this is a case where there are infinitely many solutions as a can be any power of z. If $g' \neq 1$ then there is only a solution if $h = z^i x^{-1} h', g'h' \in C(y)$ in which case take $a = az^{-i}, b = g'h'$.

(4) $g = g'r, r \neq x^{\pm 1}, r \neq z^i$. Then there can only be a solution if $h = z^i r^{-1} h', g'h' \in C(y)$, set $a = a \cdot z^{-i}, b = g'h'$, otherwise there is no solution.

Case 3: In this case we have $a \in C(z)$, $b \in C(y)$ and that these centralizers are not conjugates of one another or equal to one another. We once again let $a = 1$ to begin and use the following method to calculate the solution.

(1) $g = g' \cdot z^i, |i|$ maximal. Then if $y = rz^k$ and $g' = lr, l \in C(y)$ there is a solution only if $h = z^n h', h' \in C(y)$ with $a = z^{k-i} a z^{-n}$. If $g' \in C(z)$ then there are two possibilities for solutions. Either $h = z^j h', h' \in C(y)$ in which case $a = g^{-1} a z^{-j}, b = h'$, or $y^n = z^l h$ in which case $a = g^{-1} z^l, b = y^n$ otherwise for such a

g' there is no solution. If g' is not as above then set $a = z^{-i}a$, $g = g'$ and continue with these new values.

(2) $g = g' \cdot y^i, |i|$ is maximal. If $g \in C(y)$ then there is a solution if $h = z^i y^k$ giving that $a = az^{-i}$. If $g \notin C(y)$ then if $h = z^i y^{-i} h'$ there is a solution $a = az^{-i}, b = g'h'$ if $g'h' \in C(y)$, otherwise there is no solution.

(3) $g = g' \cdot j, j \neq y^i, j \neq z^i$. Then if $y = rj$ and $g' = lr, l \in C(y)$ there is a solution if $h = z^n h', h' \in C(y)$ where $a = az^{-n}$. There is also a solution if $h = z^i j^{-1} h'$ and $g'h' \in C(y)$ in which case $a = az^{-i}, b = g'h'$, otherwise there is no solution.

$\square$

Theorem 3.2 *Given a group of type* $F\langle U, T\rangle$*, elements* $g, h \in F\langle U, T\rangle$ *and two centralizers* $C(z), C(y) \leq F\langle U, T\rangle$ *there is an algorithm solving the equation below for* $a \in C(z), b \in C(y)$*:*

$$gah = b.$$

Proof of Theorem 3.2 : Using the previous theorem we now procede by using the induction step. Given $g, h \in F_i$, F_i a finite series of free extensions of centralizers, we consider the solution of

$$bg_o t^{\epsilon_1} \cdots t^{\epsilon_n} g_n a = h_0 t^{\delta_1} \cdots t^{\epsilon_m} h_m$$

assuming that there is an algorithm to solve all such equations in previous extensions.

Case 1: If $C(a)$ and $C(b)$ do not involve t, the latest extension, then we notice that from the proof of theorem 2.1 we have that there is a solution to this equation only if $m = n$

and $\epsilon_i = \delta_i,\ \forall i$. If the above equation has a solution then we can solve the following set of equations where, $a_i \in C(x)$ where $C(x)$ is extended by t.

$$\begin{aligned}
g_n a &= a_1^{-1} h_n \\
a_2^{-1} g_{n-1} &= h_{n-1} a_1 \\
&\vdots \\
g_0 a_n &= b^{-1} h_0.
\end{aligned}$$

As all of these equations are in an earlier level, by induction there is an algorithm to solve each of the equations. If any equation has no solution, then this implies that the original equation has no solution.If all equations have infinitely many solutions, then plugging in any solution for the first of the above equations will lead to a solution for the system, and thus a solution for the original equation. Otherwise we use the first equation which has a unique solution and then solve the remaining equations using the values found for this equation. If at any point an equation has no solution after substituting in the value for one of its a_i's then the original equation has no solution.

Now we must look at what happens if a or b (or possibly both) belong to centralizers which involve the element t. There are four possible cases to examine. We will assume a belongs to a centralizer involving t, and mention what happens in the case that b does also. When considering the same problem with respect to b the same ideas may be used, only g_0 is used rather than g_n and we try to remove powers of t with the left end of b rather than the right end of a.

Case 2: $a \in C(t)$. Assume b is either not in a centralizer which involves t or $b \in C(t)$.

Three distinct possibilities are provided by h. If $m > n$ then a or b must contain a power of t. If $b \notin C(t)$ then $a = t^{m-n}a'$ or $a = t^{n-m}a'$ where a' is in the centralizer extended by t. If the last $m - n$ powers of t in h are of the same sign, assume positive, we may then solve the equation

$$bg_o t^{\epsilon_1} \cdots t^{\epsilon_n} g_n t^{m-n} a' = h_0 t^{\delta_1} \cdots t^{\epsilon_m} h_m$$

for a' and b as it fits case 1 (unless $\epsilon_n = -1$ and $g_n \in C(t)$ in which case no solution is possible). Otherwise there can be no solution as we have either that the left side is unreduced while the right hand side is reduced, or else the left hand side will have different powers of t from that of h. If $b \in C(t)$ then we need to be more careful as powers of t can be added by either a or b. Once again we can do as above checking all combinations $b = b't^r, a = t^s a'$ such that $|r| + |s| = m - n$ and solving for a', b' in the case where the signs of the powers of t in g and h match. There is also the possibility that t-reductions are possible using either a or b if g_0 or g_r belong to C(t), this will give us a maximum of $2n + m - n + 1 = m + n + 1$ equations which need to be checked, all of which fit case 1.

If $m < n$ then in order to remove powers of t from the left hand side we must have that $g_n \in C(t)$ so that a t reduction can be made (Similarly $g_0 \in C(t)$ if we are considering that the centralizer of b contain t). If no such reduction is possible and b is not in a centralizer involving t then there is no solution to the equation. If such a reduction is possible then we take $a = t^l a'$ where l is of the opposite sign from ϵ_n and $|l| = n - m$. We now examine the resulting equation

$$bg_0 t^{\epsilon_1} \cdots t^{\epsilon_m} g_n a' = h_0 t^{\delta_1} \cdots t^{\epsilon_m} h_m$$

which is in case 1. If $b \in C(t)$ and $g_0 \in C(t)$ then reductions may occur at the beginning of the left side and we are left with $n + l$ equations to consider, arising from different amounts of reduction occurring at each end. However these equations fit Case 1 and hence a solution, if one exists, can be found.

Finally the third case is where $m = n$. If $b \notin C(t)$ then clearly a cannot involve t as this would lengthen the left hand side and mean there was no solution. Hence a belongs to the centralizer extended by t, and thus we are in fact in case 1. If $b \in C(t)$ then if the powers of t in g and h do not match we have the possibility of making them match through reducing powers of t with a or b if either $g_0 \in C(t)$ or $g_n \in C(t)$ and adding powers of t at the other end. Once again only finitely many possibilities need be checked, i.e. $b = b't^s, a = t^l a'$ where $|l| = |s|$ and $0 \leq |l| \leq m$.

Case 3: Assume $a \in C(t)^r, r \notin C(t)$, and either b does not involve t, $b \in C(t)$ or $b \in C(t)^r$. This case is similar to Case 2. If $m > n$ then if the centralizer of b does not contain t, we have that $a = rt^{m-n}a'r^{-1}$ or $a = rt^{n-m}a'r^{-1}$, i.e. we must solve the equations

$$bg_o t^{\epsilon_1} \cdots t^{\epsilon_n} g_n r t^{\pm|m-n|} a' = h_0 t^{\delta_1} \cdots t^{\epsilon_m} h_m r$$

which is back to case 1 (Notice if $g_n r \in C(t)$ and $\epsilon_n = -1$ then there can be no solution). If b can involve powers of t then once again it is a matter of checking a finite number of different equations with different powers of t added on either side. If g_n or g_0 are such that t-reductions are possible with either a or b, then this implies we must check a greater number of powers of t, as above there is a maximum of $m + n + 1$ equations which need to be checked.

If $m < n$, then we must be able to make t-reductions if this equation is to have a solution. Once again this is very similar to case 2, only we require that $g_n r^{-1} \in C(t)$ if we are to make a reduction with a. We then arrive at an equation which fits case 1, by moving the r to the right hand side as above and looking for values of a' which are in the centralizer extended by t. If $b \in C(t)^r$($r = 1$ is a possibility) then it is possible that t-reductions may also be made on the left hand side, if $rg_0 \in C(t)$. This once again increases the number of equations which must be solved, however we still have finitely many equations to check, all of which are solvable by the induction hypothesis.

Finally if $m = n$ then if b does not involve t we must have that $a \in C(x)^r$ where t extends $C(x)$(thus we can use case 1). Otherwise as before we can also try reducing powers of t with one of a and b and adding an equal number of powers with the other. This gives a maximum of $2m$ equations which need to be checked, all of which fit case 1.

Case 4: Assume $a \in C(s)$ where s is a root element at the level i, and hence has a cyclic centralizer. Consider the cases where the centralizer of b does not involve t, where the centralizer of b is $C(t)^r$, and where $b \in C(r)$ where r is a root element at the level i.

As above we first consider the possibilities if $m > n$. If no t-reductions happen involving b then the this case can be solved by calculating $hs^i g^{-1}$ for $n - m \leq i \leq m - n$ and checking if the value is in the correct centralizer. If a t-reduction can happen involving b then we simply check powers of s in a wider range, so solving the above for $-(m + n + 1) \leq i \leq m + n + 1$. (Note in the case where s involves more than one power of t, the above checks more values than necessary)

Similarly if $m \leq n$ we only need check a finite number of powers of s in the equation above.Thus check if $hs^i g^{-1} \in C(b)$ for $-2n < i < 2n$.

Case 5: Assume $a \in C(r)^W, [r,t] \neq 1, W$ involves t. Letting $a' \in C(r)$ we have that

$$bg_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n W^{-1} a' W = h_0 t^{\delta_1} \cdots t^{\delta_n} h_n$$

hence

$$bg_0 t^{\epsilon_1} \cdots t^{\epsilon_n} g_n W^{-1} a' = h_0 t^{\delta_1} \cdots t^{\delta_n} h_n W^{-1}.$$

We have that a' is in a centralizer not involving t, hence we may now consider this equation from the perspective of b and fit it into one of the previous cases.

$\square$

3.2.2 The Conjugacy problem in the Lyndon's group

Theorem 3.3 *For all i, F_i has solvable conjugacy problem.*

Proof of Theorem 3.3: We shall do this proof by induction. The first step is to show that the conjugacy problem is solvable in F, a free group. We follow the proof of theorem 1.3 in Magnus, Karras, Solitar [10].

Let $F = \langle x_1, x_2, \ldots, x_n \rangle$ be a free group, and W be a word in the free group. We define $\rho(W)$ which will reduce a word working from left to right. We define ρ inductively as follows:

$$\rho(1) = 1, p(x_i^\epsilon) = x_i^\epsilon \qquad (\epsilon = \pm 1, i = 1, \ldots n)$$

and if

$$p(W) = x_{k_1}^{\epsilon_1} \cdots x_{k_l}^{\epsilon_l} \qquad (\epsilon_i = \pm 1, k_i = 1, 2, \ldots, n)$$

then

$$\rho(Wx_r^{\epsilon}) = \begin{cases} x_{k_1}^{\epsilon_1} \cdots x_{k_l}^{\epsilon_l} x_v^{\epsilon} & \text{if} \quad k_l \neq v \quad \text{or} \quad \epsilon_l \neq -\epsilon \\ x_{k_1}^{\epsilon_1} \cdots x_{k_{l-1}}^{\epsilon_{l-1}} & \text{if} \quad k_l = v \quad \text{and} \quad \epsilon_l = -\epsilon \end{cases}$$

Let W be a reduced word. We define $\sigma(W)$ to be the cyclic reduction of W inductively as follows

$$\sigma(1) = 1, \sigma(x_i^{\epsilon}) = x_i^{\epsilon} \qquad (\epsilon = \pm 1, i = 1, \ldots n)$$

$$\sigma(x_i^{\epsilon} W x_j^{\nu}) = \begin{cases} x_i^{\epsilon} W x_j^{\nu} & \text{if} \quad i \neq j \quad \text{or} \quad \epsilon \neq -\nu \\ \sigma(W) & \text{if} \quad i = j \quad \text{and} \quad \epsilon = -\nu \end{cases}$$

If W is not reduced then we define $\sigma(W) = \sigma(\rho(W))$.

Theorem 3.4 *Let F be a free group with generators $x_1, \ldots, x_n$. Two words $W_1, W_2 \in F$ are conjugate if and only if their cyclic reductions are cyclic permutations of each other.*

Proof of theorem 3.4: First suppose $\sigma(W_2)$ is a cyclic permutation of $\sigma(W_1)$, i.e.

$$\begin{aligned} \sigma(W_1) &= x_{s_1}^{t_1} \cdots x_{s_k}^{t_k} x_{s_{k+1}}^{t_{k+1}} \cdots x_{s_p}^{t_p} \\ \sigma(W_2) &= x_{s_{k+1}}^{t_{k+1}} \cdots x_{s_p}^{t_p} x_{s_1}^{t_1} \cdots x_{s_k}^{t_k}. \end{aligned}$$

Notice that $\sigma(W_1) = K\sigma(W_2)K^{-1}$ where $K = x_{s_1}^{t_1} \cdots a_{s_k}^{t_k}$. Thus as W_1 and $\sigma(W_1)$ and W_2 and $\sigma(W_2)$ are obviously conjugate pairs we have that W_1 and W_2 are conjugate.

Assuming that we know that W_1 and W_2 are conjugate, we must show that $\sigma(W_1)$ and $\sigma(W_2)$ are cyclic permutations of each other. We have that $W_1 = KW_2K^{-1}$ thus $\rho(W_1) = \rho(KW_2K^{-1})$. Hence

$$\sigma(W_1) = \sigma(\rho(W_1)) = \sigma(\rho(KW_2K^{-1})) = \sigma(KW_2K^{-1})$$

and thus our proof is finished if we can show that $\sigma(KW_2K^{-1})$ is a cyclic permutation of $\sigma(W_2)$. We will do this by induction on the length of K. Let $K = x_i^\epsilon$ where $i = 1, \dots, n$ and $\epsilon = \pm 1$. Notice that

$$\sigma(x_i^\epsilon W_2 x_i^{-\epsilon}) = \sigma(\rho(x_i^\epsilon W_2 x_i^{-\epsilon})) = \sigma(\rho(x_i^\epsilon \rho(W_2) x_i^{-\epsilon})).$$

Suppose that

$$p(W_2) = x_{j_1}^{t_1} \dots x_{j_n}^{t_n},$$

thus we must find the value of

$$\rho(x_i^\epsilon x_{j_1}^{t_1} \dots x_{j_n}^{t_n} x_i^{-\epsilon}).$$

There are three cases we must examine, either no cancellation is possible, cancellation occurs at both ends of the element, or cancellation occurs at only one end of the element.

In the first case we have that

$$\rho(x_i^\epsilon x_{j_1}^{t_1} \dots x_{j_n}^{t_n} x_i^{-\epsilon}) = x_i^\epsilon x_{j_1}^{t_1} \dots x_{j_n}^{t_n} x_i^{-\epsilon}.$$

And thus

$$\sigma(x_i^\epsilon \rho(W_2) x_i^{-\epsilon}) = \sigma(x_i^\epsilon x_{j_1}^{t_1} \dots x_{j_n}^{t_n} x_i^{-\epsilon}) = \sigma(x_{j_1}^{t_1} \dots x_{j_n}^{t_n}) = \sigma(W_2).$$

When cancellation occurs at both ends we have that $i = j_1 = j_n$ and that $\epsilon = -t_1 = t_n$, hence

$$\rho(x_i^\epsilon \rho(W_2) x_i^{-\epsilon}) = x_{j_2}^{t_2} \dots x_{j_{n-1}}^{t_{n-1}},$$

and

$$\sigma(x_i^\epsilon W_2 x_i^{-\epsilon}) = \sigma(x_{j_2}^{t_2} \dots x_{j_{n-1}}^{t_{n-1}}).$$

But we know from above that

$$\sigma(W_2) = \sigma(x_{j_1}^{t_1} x_{j_2}^{t_2} \dots x_{j_{n-1}}^{t_{n-1}} x_{j_1}^{-t_1}) = \sigma(x_{j_2}^{t_2} \dots x_{j_{n-1}}^{t_{n-1}}).$$

The third case is when cancellation takes place at only one end, we will treat the case where cancellation takes place at the left end, but a similar argument works for when the cancellation is at the right end . As cancellation takes place at the left end we have that $j_1 = i, \epsilon = -t_1$ and that

$$\rho(x_i^\epsilon \rho(W_2) x_i^{-\epsilon}) = x_{j_2}^{t_2} \dots x_{j_n}^{t_n} x_{j_1}^{t_1}.$$

But now as both $x_{j_2}^{t_2} \dots x_{j_n}^{t_n} x_{j_1}^{t_1}$ and $x_{j_1}^{t_1} x_{j_2}^{t_2} \dots x_{j_n}^{t_n}$ are reduced, we know that both are cyclically reduced. Hence $\sigma(x_i^\epsilon \rho(W_2) x_i^{-\epsilon}) = x_{j_2}^{t_2} \dots x_{j_n}^{t_n} x_{j_1}^{t_1}$ is a cyclic permutation of $\sigma(W_2) = x_{j_1}^{t_1} x_{j_2}^{t_2} \dots x_{j_n}^{t_n}$. Hence we have that for all cases $\sigma(x_i^\epsilon \rho(W_2) x_i^{-\epsilon})$ is a cyclic permutation of $\sigma(W_2)$.

Assume using the induction hypothesis that $\sigma(TW_2T^{-1})$ is a cyclic permutation of $\sigma(W_2)$, and consider $\sigma(x_j^\nu TW_2T^{-1} x_j^{-\nu})$. By the above $\sigma(x_j^\nu TW_2T^{-1} x_j^{-\nu})$ is a cyclic permutation of $\sigma(TW_2T^{-1})$ and hence of $\sigma(W_2)$. Thus if W_1 and W_2 are conjugate then $\sigma(W_1)$ and $\sigma(W_2)$, their cyclic reductions, are cyclic permutations of each other. Thus the theorem is proved, an obvious consequence is that for a free group the conjugacy problem is solvable.

Proof of Theorem 3.3: We shall now use the induction hypothesis and assume for all $i < n$ that the conjugacy problem in F_i is solvable. Let $F_n = \langle F_{n-1}, t | t^{-1}vt = v, v \in C(z) \rangle$. We shall use theorem 2.4. We have $u = g_0 t^{\epsilon_1} \ldots t^{\epsilon_n}$ a cyclically reduced element and an element v. If $n < 1$ then either both u and v are in F_{n-1}, in which case by induction this problem is already solved, or v is in F_n and if v is conjugate to u then when cyclically reduced v is equal to u.

Otherwise, $n \geq 1$ and

$$u = g_o t^{\epsilon_1} \ldots t^{\epsilon_n}$$

$$v^* = h_o t^{\epsilon_1} \ldots t^{\epsilon_n}$$

where v^* is a cyclic permutation of v. Notice that if the two elements are to be conjugate, the powers of t must be the same in both u and v^*. From theorem 2.4 if u and v are conjugate there is an element $a \in C_G(z)$ such that

$$g_0 t^{\epsilon_1} \cdots t^{\epsilon_n} = a h_0 t^{\epsilon_1} \cdots t^{\epsilon_n} a^{-1}$$

i.e.

$$g_0 t^{\epsilon_1} g_1 \cdots t^{\epsilon_n} a = a h_0 t^{\epsilon_1} \cdots t^{\epsilon_n}.$$

This gives rise to the following set of equations [$*$] where $a_i \in C_G(z)$, $\forall i$:

$$g_{n-1} a = a_1 h_{n-1}$$

$$a_2 g_{n-2} = h_{n-2} a_1^{-1}$$

$$\vdots$$

$$g_0 a_{n-1}^{-1} = a h_0$$

where $a_i \in C(z)\,\forall i$, as the a_i must commute with t^{ϵ_i}. By substituting these equations into each other we arrive at:

$$\begin{aligned}
a &= g_{n-1}^{-1} a_1 h_{n-1} \\
&= g_{n-2}^{-1} g_{n-1}^{-1} a_2^{-1} h_{n-1} h_{n-2} \\
&\vdots \\
&= g_0^{-1} \cdots g_{n-1}^{-1} a h_0 \cdots h_{n-1}.
\end{aligned}$$

And thus finally

$$g_0 g_1 g_2 \cdots g_{n-1} = a h_0 \cdots h_{n-1} a^{-1}.$$

As both $g = g_0 \cdots g_n$ and $h = h_0 \cdots h_n$ are in F_{n-1} and by induction the conjugacy problem in F_{n-1} is solved, we know that if such an a exists in F_{n-1} we can solve for this element.

If no such a exists then from the conjugacy theorem we know that u and v are not conjugate. If such an a does exist then we must check to see whether there exists an $a \in C(z)$ such that u and v^* are conjugate.

The first case is if $h \in C_G(z)$. Then if the necessary a exists, $g \in C(z)$ also, and as $C(z)$ is abelian this implies that $g = h$ which is easily checked. In this case any $a \in C(z)$ will commute g and h. Now we must examine the elements u and v, clearly if

$g_i = h_i, \forall i$ then we have $u = v^*$, and thus u and v are conjugate. Another simple case is if $g_i, h_i \in C_G(z) \forall i$ then $u, v \in C(z)$. As the $g_i, h_i, i \neq 0$ are right coset representatives we know that for $i \neq 0, g_i = 1$ and $h_i = 1$. Hence as $g = h$ we have that $g_0 = h_0$ and $u = v^*$ and therefore that u and v are conjugate.

If the above case is not valid then we examine the system of equations[$*$]. From theorem 3.1 we have that each equation in the system is solvable, hence as shown in the proof of the theorem we can solve for an answer to the system. As at least one of the equations has $g_{n-r}, h_{n-r} \notin C(z)$ we know there is at most one solution to the system, if the value of a found in the first and last equations is the same then u and v are conjugate, otherwise they are not conjugate.

Thus we now assume that $h \notin C(z)$, from above we may assume $g \notin C(z)$ as otherwise there is no solution. Now we simply solve the system of equations [$*$], knowing that there is at most one answer as neither g nor h is in C(z). This system of equations is solvable as argued for the previous case.

$\square$

Thus the conjugacy problem is solvable in the Lyndon's Group.

Chapter 4

$F\langle u, t\rangle$ is conjugately residually F

We first introduce the notion of being conjugately residually G.

Definition 4.1 *Given a group G^* and a group G we say that G^* is conjugately residually G if for any nonconjugate $u, v \in G^*$ there exists a homomorphism ϕ, $\phi : G^* \to G$ such that $\phi(u)$ and $\phi(v)$ are not conjugate in G.*

Theorem 4.1 *Let F be the free group with generators $\{x_1, \ldots, x_n\}$. Then any group $F\langle a, t\rangle = \langle F, t | [v, t] = 1, v \in C(a)\rangle$ is conjugately residually F.*

Proof of Theorem 4.1: Take any $u, v \in F\langle a, t\rangle$, such that u, v are not conjugate. We may assume that both u and v are cyclically reduced, as u and v are conjugate if and only if their cyclic reductions are conjugate. There are three cases to consider. In the following we will write u, v in power normal form.

In the first case $u = g_0 t^{k_1} g_1 \cdots t^{k_n}, v = h_0 t^{l_1} h_1 \cdots t^{l_m}$ where $n \neq m$. We will pick our homomorphism ϕ to be such that the generators of the free group are mapped to themselves and $\phi(t) = a^z$ where z is some large integer. Notice that $g_1, \ldots, g_n, h_1, \ldots, h_m \notin C(u)$ as we are in power normal form, and that if $g_0 \in C(a)$ ($h_0 \in C(a)$) then we must have that $n = 1$ ($m = 1$) otherwise $|u^{g_0 t^{k_1}}|_p < |u|_p$ (similarly $|v^{h_0 t^{l_1}}|_p < |v|_p$). Thus if we write g_i, h_i so that all powers of a at either end have been separated out we have $g_i = a^{r_i} g_i' a^{s_i}, h_i = a^{x_i} h_i' a^{y_i}$ and thus

$$\phi(u) = a^{r_0} g_0' a^{k_1 * z + s_0 + r_1} g_1' a^{k_2 * z + s_1 + r_2} \cdots g_{n-1}' a^{k_n * z + s_{n-1}}$$

$$\phi(v) = a^{x_0} h_0' a^{l_1 * z + y_0 + x_1} h_1' a^{l_2 * z + y_1 + x_2} \cdots h_{m-1}' a^{l_m * z + y_{n-1}}$$

where if z is chosen large enough no power of a is zero.

We now examine the cyclic reductions and see that if r_0 is the opposite sign from $k_n * z + s_{n-1}$ the cyclic reduction of $\phi(u)$ is

$$\sigma(\phi(u)) = g_0' a^{k_1 * z + s_0 + r_1} g_1' a^{k_2 * z + s_1 + r_2} \cdots g_{n-1}' a^{k_n * z + s_{n-1} + r_0}$$

otherwise u was already cyclically reduced. Similarly for v, if the signs of x_0 and $l_m * z + y_{n-1}$ are the same then $\phi(v)$ is already cyclically reduced, otherwise the cyclic reduction is

$$\sigma(\phi(v)) = h_0' a^{l_1 * z + y_0 + x_1} h_1' a^{l_2 * z + y_1 + x_2} \cdots h_{m-1}' a^{l_m * z + y_{n-1} + x_0}.$$

Notice if z is large enough none of the powers of a in the cyclic reductions is zero, hence the two cyclic reductions of $\phi(u)$, $\phi(v)$ are not cyclic permutations of one another as one has more occurrences of powers of a than the other. Hence from theorem 3.4 we have that $\phi(u)$ is not a conjugate of $\phi(v)$.

In the second case u and v have the same lengths but the powers of t in u and v are different no matter which cyclic permutations of the elements are taken. We will write u and v as above only now consider that $n = m$. Thus depending on the sign of r_0 we have that the cyclic reduction of u is

$$\sigma(\phi(u)) = a^{r_0} g'_0 a^{k_1 * z + s_0 + r_1} g'_1 a^{k_2 * z + s_1 + r_2} \cdots g'_{n-1} a^{k_n * z + s_{n-1}}$$

or

$$\sigma(\phi(u)) = g'_0 a^{k_1 * z + s_0 + r_1} g'_1 a^{k_2 * z + s_1 + r_2} \cdots g'_{n-1} a^{k_n * z + s_{n-1} + r_0}$$

and similarly for v. Clearly if z is very large the $k_i * z$ ($l_i * z$) terms dominate in the powers of a, and thus by picking a large enough value of z we can ensure that any two powers of a in u and v are different if the coefficients k_i and l_i are different. Hence looking at each cyclic permutation u^* of u we can choose a value of z which ensures that the powers of a in u^* do not match the powers of a in v, thus picking the largest such value of z we find that the powers of a do not match in any cyclic permutation of u and v. Hence as the cyclic reductions cannot be cyclic permutations of one another we have from theorem 3.4 that $\phi(u)$ is not conjugate to $\phi(v)$.

The third case is when the elements u and v have the same length and the same powers of t for some cyclic permutation (we will write them so that we use one of these permutations). Once again we will map t to a large power of a

$$\phi(u) = g_0 a^{z_1} g_1 a^{z_2} \cdots g_{n-1} a^{z_n}$$

$$\phi(v) = h_0 a^{z_1} h_1 a^{z_2} \cdots h_{n-1} a^{z_n}$$

where $z_i = k_i * z$.

If these two elements are conjugate then we must have a $c \in F$ such that

$$g_0 a^{z_1} g_1 a^{z_2} \cdots a^{z_{n-1}} g_{n-1} a^{z_n} c a^{-z_n} h_{n-1}^{-1} a^{-z_{n-1}} \ldots a^{-z_2} h_1^{-1} a^{-z_1} h_0^{-1} c^{-1} = 1.$$

We can now consider two cases, either $c \in C(a)$ or $c \notin C(a)$.

First if $c \in C(a)$ then notice in order for the $a^{z_{n-1}}$ terms to be cancelled we must have that $g_{n-1} a^{z_n} c a^{-z_n} h_{n-1}^{-1} \in C(a)$, i.e. as $c \in C(a)$,

$$g_{n-1} c h_{n-1}^{-1} = c_1$$

where $c_1 \in C(a)$. Continuing on, to cancel the terms $a^{\pm z_{n-2}}$ we must have that

$$\begin{aligned} g_{n-2} c_1 h_{n-2}^{-1} &= c_2 \\ &\vdots \\ g_0 c_n h_0 c^{-1} &= 1. \end{aligned}$$

However notice from the proof of the theorem 3.3 if these equations are solvable then this means that the original u and v were in fact conjugate, hence if $\phi(u)$ and $\phi(v)$ are conjugate, they can not be conjugated by an element in $C(a)$.

Thus if the two elements are conjugated by c we must have that $c \notin C(a)$. We will assume that h_0^{-1} is not cancelled by c^{-1}, if this is not the case a similar argument to the one below applies. We consider what happens if the term c cancels all or part of the term $\phi(u)$ before it and all or part of $\phi(v)$ which occurs after the c term. We will write $\phi(u) = u_1 u_2, \phi(v) = v_1 v_2$ and assume $c = u_2^{-1} v_2$. Then we have from theorem 3.4 the two conjugate cyclically reduced elements in the free group are cyclic permutations of one another, i.e.

$$\phi(u)c\phi(v)^{-1}c^{-1} = 1$$

simplifies to

$$u_1 v_1^{-1} v_2^{-1} u_2 = 1$$

and thus

$$u_2 u_1 = v_2 v_1$$

(where u_1, u_2, v_1, v_2 can be 1). There are now three cases to consider, in case 1 both u_1, v_1 end in a power of a, in case 2 both u_1, v_1 end in a coset coefficient, and in case 3 either $u_1 = g_0$ or $v_1 = h_0$ while the other ends in a power of a. Notice that in the following, powers of a must occur in the same order in both cyclic permutations of the elements due to theorem 3.4 (i.e. in the following although it is possible that $r \neq s$ we do have that $a^z_{r+i} = a^z_{s+i} \forall i$ where we consider $a^{z_1} = a^{z_{r+(n-r)+1}} = a^{z_{s+(n-s)+1}}$). In the first case we have

$$g_r \cdots g_{n-1} a^{z_n} g_0 \cdots a^{z_{r-1}} g_{r-1} a^{z_r} a^{-z_s} h_{s-1}^{-1} a^{-z_{s-1}} \cdots h_0^{-1} a^{-z_n} h_{n-1}^{-1} \cdots h_s^{-1} = 1$$

while in the second

$$a^{z_r} \cdots g_{n-1} a^{z_n} g_0 a^{z_1} \cdots g_{r-1} h_{s-1}^{-1} \cdots a^{-z_1} h_0^{-1} a^{-z_n} h_{n-1}^{-1} \cdots a^{-z_s} = 1.$$

In both cases in order for this to be true we must have that the following system of equations holds for $a_i \in C(a)$:

$$g_{r-1} 1 h_{s-1}^{-1} \quad = \quad a_1$$

$$
\begin{aligned}
g_{r-2}a_1h_{s-2}^{-1} &= a_2 \\
&\vdots \\
g_ra_nh_s^{-1} &= 1.
\end{aligned}
$$

However notice from the theorem 3.3 we have that this implies the elements

$$u^* = g_rt^{z_r+1}\cdots g_{n-1}t^{z_n}g_0t^{z_1}\cdots g_{r-1}t^{z_r}$$

and

$$v^* = h_st^{z_s+1}\cdots h_{n-1}t^{z_n}h_0t^{z_1}\cdots s_{s-1}t^{z_s}$$

are conjugate, and hence it follows that u and v are conjugate as cyclic permutations of the elements are conjugate, hence in the above two cases $\phi(u)$ and $\phi(v)$ cannot be conjugate.

In case 3 we will look at the case when $u_1 = g_0$, the case $v_1 = h_0$ is similar. Once again the equality of powers of a follows as above. Then we have the equation

$$a^{z_1}g_1a^{z_2}\cdots a^{z_n}g_0a^{-z_s}h_{s-1}^{-1}\cdots a^{-z_1}h_0^{-1}a^{-z_n}h_{n-1}^{-1}\cdots a^{-z_{s+1}}h_s^{-1} = 1.$$

We now arrive at the following system of equations where $a_i \in C(a)$

$$
\begin{aligned}
g_0 &= a_1 \\
g_{n-1}a_1h_{s-1}^{-1} &= a_2 \\
&\vdots \\
g_1a_{n-1}h_{s+1}^{-1} &= a_n \\
h_s &= a_n.
\end{aligned}
$$

This means that $h_s = h_0$ as only h_0 may belong to $C(a)$(It also implies that both u, v have power length 1). But we now have that in fact $c \in C(a)$, a contradiction, hence $\phi(u), \phi(v)$ are not conjugate. Thus $F\langle a, t\rangle$is conjugately residually F.

□

Chapter 5

Conclusions

The purpose of this thesis was to examine the conjugacy problem in the Lyndon's group $F^{Z[x]}$. This problem is in fact solvable and my proof of this problem used a variety of different tools. Van Kampen diagrams were used to reduce the problem to that of the conjugacy problem in a group of type $F\langle U, T\rangle$, a finite series of free extensions of centralizers. Using a theorem on the conjugacy of elements in free extensions and a proof of the solvability of a particular type of word problem it was possible to show that the conjugacy problem is indeed solvable.

The question then arose as to whether or not it would be possible to map $F^{Z[x]}$ to the free group F preserving the nonconjugacy of two elements. The first natural step was to look at a single free extension, as is done in chapter 4 of this thesis. This is indeed possible, thus $F\langle U, T\rangle$ is conjugately residually F. The next step is to show this is true for any finite number of such extensions (in which case it is also true for the Lyndon's group). Work continues on this idea, length functions introduced by Lyndon should provide the means necessary for such a proof.

Bibliography

[1] Gilbert Baumslag. On Free $\mathcal{D}$-Groups *Comm. Pure Appl. Math.*, 18: 25-30, 1965.

[2] Gilbert Baumslag. Some Aspects of Groups with Unique Roots. *Acta Math.*, 104:217-303, 1960.

[3] B. Fine, A.M. Gaglione, A. Myasnikov, G. Rosenberger, and D. Spellman. A classification of fully residually free groups. 1994. accepted by the Journal of Algebra.

[4] P. Hall. Nilpotent groups. *Canad. Math. Congress*, Edmonton, 1957.

[5] O. Kharlampovich and A. Myasnikov. Irreducible Affine Varieties over a Free Group. I: Irreducibility of Quadratic Equations and Nullstellensatz. *Journal of Algebra.*, 200: 472-516, 1998.

[6] O. Kharlampovich and A. Myasnikov. Irreducible Affine Varieties over a Free Group. II: Systems in Triangular Quasi-quadratic Form and Description of Residually Free Groups. *Journal of Algebra.*, 200: 517-570, 1998.

[7] R. C. Lyndon. Groups with parametric exponents. *Trans. Amer. Math. Soc.*, 96:518–533, 1960.

[8] Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Springer-Verlag, 1977.

[9] A.I. Mal'cev. Torsion free nilpotent groups. *Izv. AN SSSR, Ser. Math.* 1949-13, N3, p201-212.

[10] W. Magnus, A. Karras, D. Solitar. *Combinatorial Group Theory*. John Wiley & Sons inc., 1966.

[11] A. G. Myasnikov and V. N. Remeslennikov. Exponential groups 2: extension of centralizers and tensor completion of csa-groups. *International Journal of Algebra and Computation*, 6(6):687–711, 1996.

[12] Egbert R. van Kampen On Some Lemmas in the Theory of Groups *Amer. J. Math.*, 55: 268-273, 1933.