12-15-2010 12:00 AM

Descending Central Series of Free Pro-p-Groups

German A. Combariza
University of Western Ontario

Supervisor
Jan Minac
The University of Western Ontario

Graduate Program in Mathematics
A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Descending Central Series of Free Pro-p-Groups

(Spine title: Descending Central Series of Free Pro-p-Groups)

(Thesis format: Monograph)

by

German Combariza

Graduate Program
in
Mathematics

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Certificate of Examination

THE UNIVERSITY OF WESTERN ONTARIO
SCHOOL OF GRADUATE AND POSTDOCTORAL STUDIES

Chief Adviser:	**Examining Board:**
Professor Jan Minac	Professor Martin Pinsonnault
Advisory Committee:	Professor Nicole Lemire
	Professor Eric Schost
	Professor Sunil Chebolu

The thesis by

German Combariza

entitled:

Descending Central Series of Free Pro-p-Groups

is accepted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

Date: ____________________

Chair of Examining Board
Firstname Lastname

Abstract

In this thesis, we study the first three cohomology groups of the quotients of the descending central series of a free pro-p-group. We analyse the Lyndon-Hochschild-Serre spectral sequence up to degree three and develop what we believe is a new technique to compute the third cohomology group. Using Fox-Calculus we express the cocycles of a finite p-group G with coefficients on a certain module M as the kernel of a matrix composed by the derivatives of the relations of a minimal presentation for G. We also show a relation between free groups and finite fields, this is a new exiting recent development. We do this by showing the explicit bijection between basic commutators and the irreducible polynomials over a certain finite field.
Keywords: cohomology, spectral sequences, central series, profinite groups, Fox calculus, irreducible polynomials, basic commutators.

Acknowledgements

First, I want to thank God for giving me the life to reach this goal. I want to thank my wife, for her great patience, support and love all these years. I Also want to thank to my kids for lighting the path to my goal through giving me happiness. I want to thank my parents and the rest of my family for giving me their support and love.

I Also want to thank all the people that helped us all this time and who I really appreciate: The Mantillas in Vancouver, The Forgets in London and The Gonzalez in Seattle.

I want to thank to my advisor Jan Mináč for his good ideas, fascinating project,constant support, great optimism about this work and belief in me. I want to thank my co-advisor Alejandro Adem for his kind support and help as well as for introducing me to Jan Mináč and arranging my work both in University of British Columbia and The University of Western Ontario. I want to thank to Sunil Chebolu, Nicole Lemire, Martin Pinsonnault and Eric Schost for their comments about this work.

To Samuel Joaquín Flores:

1 Corinthians 9:2 “Even though I may not be an apostle to others, surely I am to you! For you are the seal of my apostleship in the Lord”.

Table of Contents

Introduction

We start this thesis by recalling the concept of a profinite group in the first chapter. We follow the basic references of L. Ribes [24] and J. Wilson [29]. The profinite groups, first called "Groups of Galois Type", appear early in particular examples in number theory as the p-adic integers that were defined by Hensel in 1908. The Galois groups are equipped with a natural topology called "the Krull Topology".

In chapter two we recall the definition of cohomology of groups and the Lyndon-Hochschild-Serre spectral sequence. For more details about the cohomology of profinite groups we refer the reader to the book of J. Neukirch, A. Schmidt, K. Wingberg [22]. If S is a free pro-2-group and $S^{(m)}$ is the m-th term in its lower 2-central series the cohomology groups $H^i(S/S^{(m)}, \mathbb{F}_2)$, $i = 1, 2, 3$, together with their multiplicative structure, appear as the key obstruction in proving the conjecture established in [18], by Karagueuzian, Labute and Mináč, about a special case of central series for minimal presentations. This conjecture is related to the Bloch-Kato Conjecture, also known for $p = 2$ as the Milnor conjecture. Computing the cohomology groups $H^i(S/S^{(m)}, \mathbb{F}_2)$ was our first motivation and the goal of this project.

We proceed to define in chapter three the lower 2-central series of a pro-2-group. In this chapter we concentrate on the case $p = 2$. In 1996, Mináč and Spira published [21] in the *Annals of Mathematics*, which showed the importance of the third quotient group $S/S^{(3)}$ of the lower 2-central series, and its connection with Galois cohomology and quadratic forms. In the paper [6] written by S. Chebolu, I. Efrat and J. Mináč it is shown how this group determines the Galois Cohomology of the absolute Galois Group. In this chapter we give a partial solution to our original problem. We prove in 3.3.3 that the inflation map between the groups $H^3(S^{[m]}) \to H^3(S^{[m+1]})$ is not trivial but based on calculations done in the example 3.3.7 for $m = 3$ we conjecture that the composition of two of these inflation maps is in fact trivial. In 3.3.2 we compute the dimension over $\mathbb{F}_2$ of the vector space of decomposable elements of $H^3(S^{[m]}, \mathbb{F}_2)$ is

$$n(d_1 + \cdots + d_m) - d_{m+1}$$

where the d_i's are the Witt numbers define in the chapter three.

In chapter four we show a relation between elements of free groups and finite extensions of the field $\mathbb{F}_p$ for any prime p. This is a new exiting recent development. We do this by showing the explicit bijection between basic commutators and the irreducible polynomials over a certain finite field. The basic commutators were described by Marshall Hall in his book [12] which form a natural basis for the quotients of the lower p-central series. The main theorem 4.3.1 of chapter four is the explicit bijections

$$\text{Top Elements} \xrightarrow{\text{Wording}} \text{Circular Words} \xrightarrow{\text{Bracketing}} \text{Basic Commutators},$$

where for a given finite extension $F/\mathbb{F}_p$ of finite fields the top elements are the elements in F that are not in any proper intermediate field. In this case there is always a normal basis determined for a special element α. The *Wording* bijection relies on expressing top elements in this normal basis. The *Bracketing* is defined in [12] and recalled in chapter four.

In chapter five, we use Fox Calculus to give a new interpretation of the third cohomology group $H^3(G, \mathbb{F}_p)$, for a finite p-group G and a prime number p, as the kernel of a certain matrix. Let $1 \to R \to S \to G \to 1$ be a minimal presentation for G. We showed that the module $H^1(R, \mathbb{F}_p)$ is the dual of the module generated by the image of R under the Fox derivatives where the action of G over this image is left multiplication. It follows from Llyndon-Hochschild-Serre spectral sequence applied to the minimal presentation of $H^3(G, \mathbb{F}_p) \simeq H^1(G, H^1(R, \mathbb{F}_p))$. With the notation above we proved in 5.3.1 that the dimension over $\mathbb{F}_p$ of the coboundaries

$B^1(G, H^1(R, \mathbb{F}_p))$ of G with coefficients in $H^1(R, \mathbb{F}_p)$ is

$$\dim B^1(G, H^1(R, \mathbb{F}_p)) = 1 + |G|(\dim H^1(G, \mathbb{F}_p) - 1) - \dim H^2(G, \mathbb{F}_p).$$

Our main theorem 5.3.2 gives an explicit description for the cocycles in terms of the kernel of the matrix given by the Fox derivatives of the relations acting on copies of the module $H^1(R, \mathbb{F}_p)$. The set of cocycles $Z^1(G, H^1(R, \mathbb{F}_p))$ is the kernel of the matrix

$$D = \left(\frac{\partial r_i}{\partial x_j}\right)_{ij} : \bigoplus^{d} H^1(R, \mathbb{F}_p) \to \bigoplus^{l} \mathbb{F}_p[G].$$

Where $d = \dim H^1(G, \mathbb{F}_p)$ and $l = \dim H^2(G, \mathbb{F}_p)$. It is expected that the method in this thesis can be refined and used to give a the full structure of the cohomology groups $H^i(S^{[m]}, \mathbb{F}_p)$ for $i = 1, 2, 3$ and their multiplicative structure.

Chapter 1

Profinite groups

In this chapter we describe the notion and basic properties of profinite groups, free pro-p-groups, which will be used throughout this thesis. We also show its connection with Galois groups. We will follow [29] and [24].

1.1 Projective limits

Let I denote a *directed set*, that is, I is a set with a binary relation "$\preceq$" satisfying the following conditions:

(1) $i \preceq i$ for $i \in I$;

(2) $i \preceq j$ and $j \preceq k$ imply $i \preceq k$ for $i, j, k \in I$;

(3) $i \preceq j$ and $j \preceq i$ imply $i = j$ for $i, j \in I$;

(4) if $i, j \in I$ there exists some $k \in I$ such that $i, j \preceq k$.

A *projective system* of topological groups over I, consists of a collection $\{X_i | i \in I\}$ of topological groups indexed by I, and a collection of continuous group homomorphisms $\varphi_{ij} : X_i \to X_j$ defined whenever $j \preceq i$, such that for all $i, j, k \in I$ with $k \preceq j \preceq i$ the following diagram is commutative.

$$\begin{tikzcd} X_i \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & X_k \\ & X_j \arrow[ur, "\varphi_{jk}"'] & \end{tikzcd} \tag{1.1}$$

In addition we assume that φ_{ii} is the identity mapping id_{X_i} on X_i. We shall denote such a system by $\{X_i, \varphi_{ij}, I\}$.

Let Y be a topological group, and let $\psi_i : Y \to X_i$ be a continuous homomorphism for each $i \in I$. The maps ψ_i are said to be *compatible* if $\varphi_{ij}\psi_i = \psi_j$, $\forall i, j \in I$.

A topological group X together with a compatible set of continuous homomorphisms $\varphi_i : X \to X_i$, $i \in I$ is called a *projective limit* of the inverse system $\{X_i, \varphi_{ij}, I\}$ if whenever Y is a topological group and $\psi_i : Y \to X_i$, $i \in I$, is a set of compatible continuous homomorphisms, then there is a unique continuous homomorphism $\psi : Y \to X$ such that $\varphi_i\psi = \psi_i$ for all $i \in I$. i.e. the following diagram is commutative.

$$\begin{tikzcd} Y \arrow[r, dashed, "\psi!"] \arrow[dr, "\psi_i"'] & X \arrow[d, "\varphi_i"] \\ & X_i. \end{tikzcd} \tag{1.2}$$

Theorem 1.1.1. *Let $\{X_i, \varphi_{ij}, I\}$ be an inverse system of topological groups over a directed set I. Then*

(1) *There exists an inverse limit of the inverse system $\{X_i, \varphi_{ij}, I\}$;*

(2) *This limit is unique in the following sense: If (X, φ_i) and (Y, ψ_i) are two limits of the inverse system $\{X, \varphi_{ij}, I\}$, then there is a unique topological isomorphism $\varphi : X \to Y$ such that $\psi_i\psi = \varphi_i$ for every $i \in I$.*

Proof. (1) Define X as the subgroup of the direct product

$$\prod_{i \in I} X_i$$

of topological groups consisting of those tuples (x_i) that satisfy the condition $\varphi_{ij}(x_i) = x_j$ if $j \preceq i$. Let $\varphi_i : X \to X_i$ to denote the restriction of the canonical projection. Then one easily checks that each φ_i is a continuous homomorphism and that (X, φ_i) is an inverse limit.

(2) Suppose (X, φ_i) and (Y, φ_i) are two inverse limits of the inverse system $\{X_i, \varphi_{ij}, I\}$.

$$\begin{tikzcd} X \arrow[rr, dashed, shift left, "\varphi"] \arrow[dr, "\varphi_i"'] & & Y \arrow[ll, dashed, shift left, "\psi"] \arrow[dl, "\psi_i"] \\ & X_i & \end{tikzcd} \tag{1.3}$$

Since the maps $\psi_i : Y \to X_i$ are compatible, the universal property of the inverse limit (X, φ_i) shows that there exists a unique continuous homomorphism $\psi : Y \to X$ such that $\varphi_i \psi = \psi_i$ for all $i \in I$. Similarly, there is a unique continuous homomorphism $\varphi : X \to Y$ such that $\psi_i \varphi = \varphi_i$ for all $i \in I$. Observe that

$$\begin{tikzcd} X \arrow[rr, dashed, shift left, "\varphi\psi"] \arrow[rr, dashed, shift right, "id_X"'] \arrow[dr, "\varphi_i"'] & & X \arrow[dl, "\varphi_i"] \\ & X_i & \end{tikzcd} \tag{1.4}$$

commutes for each $i \in I$. Then by definition $\varphi\psi = id_X$, similarly $\psi\varphi = id_Y$.

$\square$

We shall denote the inverse system of $\{X_i, \varphi ij, I\}$ by $\varprojlim_{i \in I} X_i$ or just $\varprojlim X_i$.

Proposition 1.1.2. *If $\{X_i, \varphi_{ij}, I\}$ is an inverse system of Hausdorff topological groups, then $\varprojlim X_i$ is isomorphic to a closed subgroup of $\prod_{i \in I} X_i$.*

Proof. Let $(x_i) \in (\prod X_i) \setminus \left(\varprojlim X_i\right)$. Then there are $r, s \in I$ with $s \preceq r$ and $\varphi_{rs}(x_r) \neq x_s$. Choose open disjoint neighbourhoods U and V of $\varphi_{rs}(x_r)$ and x_s in X_s, respectively. Let U' be an open neighbourhood of x_r in X_r, such that $\varphi_{rs}(U') \subseteq U$.

Consider the open neighbourhood of (x_i) in $\prod X_i$, $W = \prod_{i\in I} V_i$ where $V_r = U'$, $V_s = V$ and $V_i = X_i$ for $i \neq r, s$. Note that $W \bigcap \varprojlim X_i = \varnothing$. $\square$

Proposition 1.1.3. *A projective limit of non-empty finite sets is not empty.*

Proof. For each $j \in I$ define a subset Y_j of $\prod X_i$ to consist of those (x_i) with the property $\psi_{jk}(x_j) = x_k$ whenever $k \preceq j$. Using the axiom of choice and an argument similar to the one used above, one easily checks that each Y_j is a non-empty closed subset of $\prod X_i$ where the topology of $\prod X_i$ is the product topology. Observe that if $j \preceq k$ then $Y_j \supseteq Y_k$, it follows that the collection of subsets $\{Y_j | j \in I\}$ has the finite intersection property. Then from Tychonoff and the compactness of X_i one deduces that

$$\varprojlim X_i = \bigcap_{j\in I} Y_j$$

is non-empty. $\square$

1.2 Profinite groups

A topological group which is the projective limit of finite groups, each given the discrete topology, is called a *profinite group*. Such group is totally disconnected and compact by Tychonoff's theorem and Proposition 1.1.2.

Proposition 1.2.1. *A compact totally disconnected topological group is profinite.*

Proof. Let G be such a group. Since G is totally disconnected and locally compact, the open subgroups of G form a base of neighbourhoods of 1. Such a group U has finite index because G is compact; hence its conjugates gUg^{-1} $(g \in G)$ are finite in number and their intersection V is both normal and open in G. Such V's are thus a base of neighbourhood's of 1; the map $G \to \varprojlim G/V$ is injective, continuous, and its image is dense, then by the compactness of G is clear that it is an isomorphism. $\square$

Example 1.2.2. (1) *Let L/K be a Galois extension of fields. The Galois group $G(L/K)$ of this extension is, as we will see later, the projective limit of the Galois groups $G(L_i/K)$ of the finite Galois extensions L_i/K which are contained in L/K; thus it is a profinite group.*

(2) *Let G be a discrete topological group, and let $\hat{G}$ be the projective limit of the finite quotients of G. The profinite group $\hat{G}$ is called the completion of G, the kernel of $G \to \hat{G}$ is the intersection of all subgroups of finite index in G.*

(3) *If M is a torsion abelian group, its dual $M^* = Hom(M, \mathbb{Q}/\mathbb{Z})$, given the topology of pointwise convergence, is a commutative profinite group. Thus one obtains the anti-equivalence between torsion abelian groups and commutative profinite groups.*

1.3 Free pro-p-groups

Let p be a prime number. A profinite group G is called a *pro-p-group* if it is a projective limit of p-groups. A map $\alpha : I \to G$ from a set I to a profinite group G is said to be 1-*convergent* if the set $\{x \in I | \alpha(x) \notin N\}$ is finite for each open normal subgroup N of G.

Definition 1.3.1. *The free pro-p-group on a set I is a pro-p-group S together with a* 1*-convergent map $j : I \to S$ with the following universal property: whenever $\xi : I \to G$ is a* 1*-convergent map to a profinite group G, there is a unique homomorphism $\bar{\xi} : S \to G$ such that $\xi = \bar{\xi} j$.*

$$\begin{tikzcd} S \arrow[r, dashed, "\bar{\xi}"] & G \\ I \arrow[u, "j"] \arrow[ur, "\xi"'] & \end{tikzcd} \tag{1.5}$$

Let X be a set, and let $S(X)$ be the free discrete group generated by the elements $x \in X$. Consider the family I of normal subgroups N of $S(X)$ such that:

- $S(X)/N$ is a finite p-group,
- N contains all the x's but finitely many.

Let S_X be the inverse limit $\varprojlim S(X)/N$ over the set I.

Proposition 1.3.2. *The group S_X is the free pro-p-group on the set I, with the map $j : x \mapsto (Nx)$*

Proof. The kernels of the projections $p_N : S_X \to S(X)/N$ form a base of open neighbourhoods of 1 in S_X and $j(x) \in \ker p_N$ if and only if $x \in N$, therefore j is 1-convergent.

We have $j = \varepsilon\iota$, where $\iota : X \to E$ is the inclusion map and ε is the canonical map from $S(X)$ to its completion S_X. Now let $\xi : X \to H$ be a 1-convergent map to a pro-p-group H. By the universal property of the free abstract group, there is a unique homomorphism $\mu : S(X) \to H$ with $\xi = \mu\iota$. Since all but finitely many elements of X map to 1 in H, we have that $\ker\mu \in I$, and so μ in continuous with respect to the topology on $S(X)$ having I as a base of open neighbourhoods of 1. Therefore the universal property of the completion S_X gives a map $\bar{\xi} : S_X \to H$ completing the commutative diagram

$$\begin{tikzcd}
X \arrow[r, "\iota"] \arrow[dr, "\xi"'] & S(X) \arrow[r, "\varepsilon"'] \arrow[d, "\mu"] & S_X \arrow[dl, "\bar{\xi}"] \\
& H &
\end{tikzcd} \tag{1.6}$$

and so satisfying $\bar{\xi}j = \xi$. However if $\bar{\xi}_1 : S_X \to H$ is a homomorphism satisfying $\bar{\xi}_1 = \xi$ then we have $(\bar{\xi}\varepsilon)\iota = \xi$. It follows from the universal property of $S(X)$ that $\bar{\xi}_1\varepsilon = \xi\varepsilon$, and hence from the universal property of S_X that $\bar{\xi}_1 = \bar{\xi}$. The uniqueness is a routine argument.

□

Example 1.3.3.

- *Let I be a set containing just one element, then $S_I \cong \mathbb{Z}_p$*

- *Let k be a field of prime characteristic p, with algebraic closure $\bar{k}$, and write $k(p)$ for the join of all finite Galois extensions L/k of p-power degree with $L \leq \bar{k}$. Let I be a basis of the $\mathbb{F}_p$-space $\{x_i^p - x_i | x_i \in k\}$ of k. Then $G(k(p)/k)$ is the free pro-p-group on I.*

- *Let k be a field extension of finite degree n of the field of p-adics numbers $\mathbb{Q}_p$, suppose that k does not contain p^{th} roots of 1, and write $k(p)$ for the subfield of an algebraic closure of k generated by all Galois extensions of k of p-power degree. Shafarevich [27] proved that $G(k(p)/k)$ is the free pro-p-group on a set with $n+1$ elements.*

- *Let k be an algebraically closed field and let $\overline{k(t)}$ be the algebraic closure of the field of rational functions over k. Then $G(\overline{k(t)}/k(t))$ is the free profinite group on the set k. This was proved by Douady [8] when char $k = 0$ and by Harbater [13] for char $k \neq 0$.*

1.4 Galois extensions

Let K/k be an algebraic extension, finite or infinite. K/k is called a Galois extension if it is both normal and separable. The Galois group $G(K/k)$ of an algebraic extension is defined to be the group of all automorphisms of K fixing each element of k. Write

$$\mathcal{F} = \{L | L \text{ is a subfield of } K \text{ such that } L/k \text{ is a finite Galois extension}\}.$$

We define a topology in $G(K/k)$ by taking as a base of open neighbourhoods of 1 the family of subgroups

$$\mathcal{N} = \{G(K/L) | L \in \mathcal{F}\}.$$

Proposition 1.4.1. *$G(K/k)$ is the inverse limit of the finite groups $G(L/k)$ with $L \in \mathcal{F}$; in particular, $G(K/k)$ is a profinite subgroup.*

Proof. Observe that each group $G(L/k)$ is finite for $L \in \mathcal{F}$, now if $L_1, L_2 \in \mathcal{F}$ with $L_1 \subset L_2$, then the restriction map $\sigma \mapsto \sigma_{\restriction L_1}$ from $G(L_2/k)$ to $G(L_1/k)$ is an epimorphism, and the groups $G(L/k)$ together with these restriction maps clearly form an inverse system over $\mathcal{F}$.

The restriction maps $G(K/k) \to G(L/k)$ yield a group homomorphism

$$\varphi : G(K/k) \to \prod_{L \in \mathcal{F}} G(L/k)$$

clearly the image of φ is contained in $\varprojlim G(L/k)$. Let $(\sigma_L) \in \varprojlim G(L/k)$, for $x \in K$ define

$$\psi : \varprojlim G(L/k) \to G(K/k)$$

by $\psi((\sigma_L))(x) = \sigma_M(x)$, for some $M \in \mathcal{F}$ with $x \in M$; this is well defined. It is easy to check that $\psi((\sigma_L)) \in G(K/k)$ and that ψ is the inverse of the map φ, so that φ is an isomorphism of abstract groups. Now, for $N \in \mathcal{F}$, the subgroup $\varphi(G(K/N))$ consists of the elements of $\varprojlim G(L/k)$ whose projection in $G(N/k)$ is trivial, and so φ maps the base $\mathcal{N}$ of open neighbourhoods of 1 in $G(K/k)$ to a base of open neighbourhoods of 1 in the inverse limit $\varprojlim G(L/k)$. It follows that φ is also an isomorphism of topological groups. $\square$

Theorem 1.4.2 (The Fundamental Theorem of Galois Theory)**.** *Let K/k be a Galois extension. Then the map Φ defined by*

$$\Phi(M) = Gal(K/M)$$

is an inclusion-reversing bijection from the set of intermediate fields M of K/k to the *set of closed subgroups of $G(K/k)$. Its inverse Φ^{-1} is defined by*

$$\Phi^{-1}(H) = K^H = \{\textit{the field of all elements fixed by } H\}.$$

Proof. Since every intermediate field is a union of finite field extensions of k, and $G(K/N)$ is an open subgroup of $G(K/k)$ for any finite extension of k, it follows that the image of Φ is closed with respect to intersections and that the members of this image are closed in $G(K/k)$. If M_1, M_2 are intermediate fields satisfying $M_1 \leq M_2$ then clearly $\Phi(M_2) \leq \Phi(M_1)$.

Let M be an intermediate field. From above, $G(K/M) \leq G(K/k)$, and clearly $M \leq K^{G(K/M)}$. Let $x \in K - M$, then x is the zero of an irreducible polynomial of degree greater than 1 over M; let y be another zero in K. The two fields generated by x, y over M are isomorphic, under an isomorphism mapping x to y and fixing all elements of M. It follows that x is not fixed by $G(K/M)$, then $M = K^{G(K/M)}$.

It remains now to show that $H = G(K/K^H)$ for each subgroup H of $G(K/k)$. However if $H = G(K/M)$ for some intermediate field M then $K^H = M$ from the above and then $H = G(K/K^H)$. Therefore is sufficient to show that every subgroup of $G(K/k)$ is of the form $G(K/M)$. Indeed, since the image of Φ is closed with respect to intersections of subgroups, it is enough to show that if H is an open subgroup then $H = G(K/M)$. Since H is open, it contains $G(K/L)$ for some intermediate field L with L/k a finite Galois extension. Then, by classic Galois theory results we can conclude that $H = G(K/M)$ for some subfield M of L.

□

Lemma 1.4.3. *Let θ be a homomorphism from a profinite group G to the Galois group $G(K/k)$ for some algebraic extension K/k. For $x \in K$ suppose that G_x [1] is open for each x, and that the subfield fixed by $\theta(G)$ is k. Then K/k is a Galois extension, and θ is continuous and surjective.*

1. For each x write G_x for the group of elements of G whose images under θ fix x.

Proof. Write R_x for the intersection of the conjugates of G_x in G, for each $x \in K$. Since G_x is open, it contains a open normal subgroup, and so R_x is open. Let $x_1, \cdots, x_r \in K$ and write L for the subfield generated by k and all images of $x_1, \cdots, x_r$ under the elements of $\theta(G)$. Thus G induces automorphisms of L, and if $g \in G$ then $\theta(g)$ fixes each element of L if and only if $g \in R_{x_1}, \cdots, R_{x_r}$. It follows that the image of G in $G(L/k)$ is finite and that its fixed field is k. A result of Artin in classical Galois theory states that H is a finite group automorphisms of a field F and if the fixed field is F_0, then the extension F/F_0 is Galois and $H = G(F/F_0)$. From here it follows that L/k is a finite Galois extension, and that G maps onto $G(L/k)$.

Since K is a union of such fields L, K/k is a Galois extension. The image of $\theta(G)$ in $G(L/k)$ under the map $G(K/k) \to G(L/k)$ is $G(L/k)$; since this map has kernel $G(K/L)$ it follows that

$$G(K/k) = \theta(G)G(K/L)$$

for each L. Each subgroup $\theta^{-1}(G(K/L))$ is open and because the subgroups $G(K/L)$ form a base of neighbourhoods of 1 in $G(K/k)$, the map θ is continuous. Therefore θ is closed and surjective. □

Theorem 1.4.4. *Every profinite group G is isomorphic as a topological group, to a Galois group.*

Proof. Let F be an arbitrary field. Write S for the disjoint union of the sets G/N with N an open normal subgroup of G. Let $K = F(X_s | s \in S)$, where the elements X_s are independent transcendentals over F in bijective correspondence with the elements of S. The natural action of G on S induces a homomorphism $\theta : G \to \mathrm{aut}(K)$. If $u \in K$ suppose $u \in F(X_{s_1}, \cdots, X_{s_r})$, and if $s_i = g_i N_i$, for $i = 1, \cdots r$ then

$$G_u \geq N_1 \cap \cdots \cap N_r$$

which is open. Let k be the fixed field of G. The map $\theta : G \to G(K/k)$ is clearly an injective homomorphism, and by the lemma above an isomorphism of profinite groups. $\square$

Chapter 2

Cohomology of profinite groups

In this chapter we recall the definition of cohomology of groups and the Lyndon-Hochschild-Serre spectral sequence. For more details we refer the reader to [22]. Although cohomology is fundamental for mathematicians today, it was not until 1935, that the first ideas appeared in three papers in a Moscow conference. Later on in the mid-40's, Eilenberg and Mac Lane defined cohomology groups in their influences series of papers published in annals of mathematics.

2.1 Definitions

Let G be a profinite group, A a G-module and n a positive integer. By a G-module A we mean an abelian topological group which is also a G-module and the map $G \times A \to A$ defining the module structure on A is continuous. We assume that all G-modules are discrete.

(1) Consider the map $d_i : G^{n+1} \to G^n$ by

$$(g_0, \cdots, g_n) \mapsto (g_0, \cdots, \hat{g}_i, \cdots, g_n)$$

where by $\hat{g}_i$ we indicate that we have omitted g_i from the $(n+1)$-tuple $(g_0, \cdots, g_n)$. G acts on G^n by left multiplication.

(2) Define the G-modules $X^n = Map(G^{n+1}, A)$ with the G action is given by

$$(g \cdot \sigma)(g_0, \cdots, g_n) := g\sigma(g^{-1}g_0, \cdots, g^{-1}g_n)$$

(3) The maps d_i induce G-homomorphisms $d_i^* : X^{n-1} \to X^n$ and we form the alternating sum

$$\partial^n = \sum_{i=0}^{n} (-1)^n d_i^*.$$

(4) To the exact sequence of G-modules $0 \to A \to X^0 \to X^1 \to \cdots$ we now apply the fixed module functor. We set for $n \geq 0$

$$C^n(G, A) = X^n(G, A)^G.$$

(5) We obtain the **homogeneous cochain complex** of G with coefficients in A

$$C^0(G, A) \to C^1(G, A) \to C^2(G, A) \to \cdots$$

which in general is no longer exact. We now set:

- The n-**cocycles** $Z^n(G, A) = \ker(C^n(G, A) \to C^{n+1}(G, A))$.
- The n-**coboundaries** $B^n(G, A) = \operatorname{im}(C^{n-1}(G, A) \to C^n(G, A))$.
- and finally the n-**dimensional cohomology group** of G with coefficients in A

$$H^n(G, A) = Z^n(G, A)/B^n(G, A).$$

Let A be a R module then the short exact sequence $1 \to R \to S \to G \to 1$ induce an action of G over R by conjugation and this action also induce and action of G over $H^*(R, A)$ by action over the cocycles $f : R^n \to A$ by the rule $(g \cdot f)(r) = gf(g^{-1}r)$.

2.1.1 An alternative definition

Let G be a profinite group, A a G-module and n a positive integer. We denote $\mathcal{C}^n$ the set of all continuous maps from G^n to A.[1] The elements of $\mathcal{C}$ are called the

1. G^n equipped with the product topology.

inhomogeneous n-cochains.

(1) We have then the isomorphism $C^n(G,A) \to \mathcal{C}^n(G,A)$,

$$\sigma(g_0, \cdots, g_n) \mapsto \tilde{\sigma}(g_1, \cdots, g_n) = \sigma(1, g_1, g_1g_2, \cdots, g_1g_2\cdots g_n)$$

with inverse given by

$$\tilde{\sigma}(g_1, \cdots, g_n) \mapsto \sigma(g_0, \cdots, g_n) = g_0\tilde{\sigma}(g_0^{-1}g_1, g_1^{-1}g_2, \cdots, g_{n-1}^{-1}g_n).$$

(2) With these isomorphisms the coboundary operators ∂^n are transformed into the homomorphisms $\partial^{n+1} : \mathcal{C}^n(G,A) \to \mathcal{C}^{n+1}(G,A)$ given by:

$$\begin{aligned}(\partial f)(g_1, \cdots, g_{n+1}) &= g_1 \cdot f(g_2, \cdots, g_{n+1}) \\ &\quad + \sum_{i=1}^{n}(-1)^i f(g_1, \cdots, g_ig_{i+1}, \cdots, g_{n+1}) \\ &\quad +(-1)^{n+1} f(g_1, \cdots, g_n).\end{aligned}$$

(3) Setting

- The **inhomogeneous n-cocycles** $\mathcal{Z}^n(G,A) = \ker(\mathcal{C}^n(G,A) \to \mathcal{C}^{n+1}(G,A))$.
- The **inhomogeneous n-coboundaries** $\mathcal{B}^n(G,A) = \operatorname{im}(C^{n-1}(G,A) \to C^n(G,A))$.
- We have induced isomorphisms

$$H^n(G,A) \simeq \mathcal{Z}^n(G,A)/\mathcal{B}^n(G,A).$$

As usual, $H^0(G,A) = A^G$ is the subgroup of fixed points of G in A. $H^1(G,A)$ is the group of classes of continuous crossed-homomorphism of G into A and $H^2(G,A)$ is the group of classes of continuous factor systems from G to A. If G a pro-p-group, then $\dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p)$ is the minimum numbers of topological generators of G and $\dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p)$ is the number of relations. [25]

We shall say that a short exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ of abelian topological groups is *well adjusted* if

- the map i induces a homeomorphism from A to its image and
- there is a continuous section τ for j.

The following theorem shows us how to recover the cohomology of profinite groups from the cohomology of finite groups.

Theorem 2.1.1. *Let $\{G_i, \varphi_{ij}, i\}$ be an inverse system of topological groups over a directed poset I with projective limit $G = \varprojlim G_i$, and let $\{A_i, \tau_{ij}, i\}$ be a direct system of discrete abelian groups over I, with direct limit $A = \varinjlim A_i$. Suppose that A_i is a G_i-module for each i and that each pair $(\varphi_{ij}, \tau_{ij})$ is compatible. Then*

$$H^n(G, A) = \varinjlim H^n(G_i, A_i).$$

Proof. Note that the abelian groups $C^n(G_i, A_i)$ together with the induced maps

$$\gamma_{ji} = (\varphi_{ij}, \tau_{ji})^* : C^n(G_i, A_i) \to C^n(G_j, A_j)$$

form a direct system, with direct limit $C^n(G, A)$ and induced maps

$$\gamma_i = (\varphi_i, \tau_i)^* : C^n(G_i, A_i) \to C^n(G, A).$$

The abelian groups $H^n(G_i, A_i)$ together with the induced map

$$\eta_{ji} = (\varphi_{ij}, \tau_{ji})^* : H^n(G_i, A_i) \to H^n(G_j, A_j)$$

comprise a direct system, and the induced maps

$$\eta_i = (\varphi_i, \tau_i)^* : H^n(G_i, A_i) \to H^n(G, A)$$

satisfy $\eta_j \eta_{ji} = \eta_i$ for $i \leq j$. First let us prove that $H^n(G, A) = \cup_i \mathrm{im}(\eta_i)$

Let $f + B^n(G, A) \in H^n(G, A)$. Thus $f \in Z^n(G, A)$; say $f = \gamma_i(f_i)$ where $f_i \in C^n(G_i, A_i)$. Then $0 = \delta f = \gamma_i(\delta f_i)$, so that $0 = \gamma_{ji}(\delta f_j) = \delta(\gamma_{ij(f_i)})$ for some $j \geq i$. Hence the element

$$h_j = \gamma_{ji}(f_i) + B^n(G_j, A_j)$$

lies in $H^n(G_j, A_j)$ and we have

$$\eta_j(h_j) = \gamma_j \gamma_{ji}(f_i) + B^n(G, A) = f + B^n(G, A).$$

This shows that $H^n(G, A) = \cup \mathrm{im} \eta_i$.

Now let $g_i + B^n(G_i, A_i)$ be an element of $H^n(G_i, A_i)$ which is mapped to zero by η_i. Thus $\gamma_i(g_i) \in B^n(G, A)$. Write $\gamma_i(g_i) = \delta g \in C^{n-1}(G, A)$ and $g = \gamma_j(g'_j)$ with $g'_j \in C^{n-1}(G, A)$. For $k \geq i, j$ we have $\gamma_k(\gamma_{ki}(g_i) - \delta\gamma_{kj}(g'_j)) = \gamma_i(g_i) - \delta\gamma_j(g'_j) = 0$, and so there is an index $l \geq k$ such that

$$0 = \gamma_{lk}(\gamma_{ki}(g_i) - \delta\gamma_{kj}(g'_j)) = \gamma_{li}(g_i) - \delta\gamma_{lj}(g'_j).$$

Hence

$$\eta_i(g_i + B^n(G_i, A_i)) = \gamma_{li}(g_i) + B^n(G_l, A_l) = B^n(G_l, A_l).$$

$\square$

2.2 The LHS spectral sequence

Given a 2-group G we will illustrate by some examples how to compute $H^*(G) = H^*(G, \mathbb{F}_2)$ using the Lyndon-Hochschild-Serre (LHS) spectral sequence. Given a short exact central sequence $1 \to N \to G \to Q \to 1$, where N is a normal closed subgroup of G, the second page of the LHS spectral sequence is the bigraded differential algebra

$$E_2^{s,t} = H^s(Q, H^t(N, \mathbb{F}_2)).$$

The spectral sequence consists of a series of differential algebras

$$\{E_r^{s,t}, \partial_r, r \geq 2\}$$

such that

(1) $\partial_r \circ \partial_r = 0$.

(2) $E_{r+1}^{s,t} = \frac{\ker(\partial_r : E_r^{s,t} \to E_r^{s+r,t-r+1})}{\operatorname{im}(\partial_r : E_r^{s-r,t+r-1} \to E_r^{s,t})}$.

(3) If $a \in E_r^{s,t}$, $b \in E_r^{p,q}$ then

$$\partial_r(ab) = \partial_r(a)b + a\partial_r(b). \tag{2.1}$$

(4) There is a filtration of $H^*(G)$

$$H^n(G) = F^0 \supset \cdots \supset F^n = 0$$

such that

$$E_\infty^{s,t} \simeq F^s/F^{s+1}. \tag{2.2}$$

Example 2.2.1. *We compute in detail the mod 2 cohomology of the 2-adics integers $\mathbb{Z}_2$. We know that*

$$\mathbb{Z}_2 = \varprojlim_n C_{2^n}$$

where C_m is the cyclic group of order m. The projective system is then

$$\cdots \to C_{2^n} \to \cdots \to C_4 \to C_2$$

which induces the injective system in cohomology

$$H^*(C_2) \to H^*(C_4) \to \cdots \to H^*(C_{2^n}) \to \cdots$$

Let's compute the cohomology groups using the LHS spectral Sequence and denote $H^*(C_2) = \mathbb{F}_2[x]$.

C_4 is determined by the extension associated to $y^2 \in H^2(C_2)$ where the second copy of C_2 has cohomology $\mathbb{F}_2[y]$

$$1 \to C_2 \to C_4 \to C_2 \to 1$$

in this case the second page of the spectral sequence looks like

$$\begin{tikzcd}
2 & x^2 & x^2y & x^2y^2 \\
1 & x \arrow[drr] & xy & xy^2 \\
0 & 1 & y & y^2 \\
 & 0 & 1 & 2
\end{tikzcd} \tag{2.3}$$

Then the third page is

$$\begin{tikzcd}
2 & x^2 \arrow[ddrrr] & x^2y & & \\
1 & & & & \\
0 & 1 & y & & \\
 & 0 & 1 & 2 & 3
\end{tikzcd} \tag{2.4}$$

Therefore $E_3 = E_\infty$ *and*

$$H^*(C_4) = \mathbb{F}_2[z_2, y_2]/(y_2^2)$$

with $|y_2| = 1, |z_2| = 2.$

Now, C_8 *is determined by an element* $z_2 \in H^2(C_4)$ *in*

$$1 \to C_2 \to C_8 \to C_4 \to 1$$

then the second page of the spectral sequence is

$$\begin{tikzcd}
2 & x^2 & xy_2^2 & x^2z_2 \\
1 & x \arrow[drr] & xy_2 & xz_2 \\
0 & 1 & y_2 & z_2 \\
 & 0 & 1 & 2
\end{tikzcd} \tag{2.5}$$

and the third page is

$$
\begin{array}{c|c|c|c|c}
2 & x^2 & x^2y_2 & & \\
\hline
1 & & & & \\
\hline
0 & 1 & y_2 & & \\
\hline
 & 0 & 1 & 2 & 3
\end{array}
\tag{2.6}
$$

Therefore $E_3 = E_\infty$ *and*

$$H^*(C_8) = \mathbb{F}_2[z_3, y_3]/(y^2)$$

with $|y_3| = 1, |z_3| = 2$. *It follows that*

$$H^*(C_{2^n}) = \mathbb{F}_2[z_n, y_n]/(y_n^2)$$

with $|y_n| = 1, |z_n| = 2$.

Note that in the Spectral Sequence of C_8 (2.5) *and* (2.6)

$$H^*(C_4) = E_2^{0,*} \to E_3^{0,*} \subset H^*(C_8)$$

then we have the well known inflation function

$$inf : H^*(C_4) \to H^*(C_8)$$

$$y_2 \mapsto y_3$$

$$z_2 \mapsto 0$$

and obviously

$$inf : H^*(C_{2^n}) \to H^*(C_{2^{n+1}})$$
$$y_n \mapsto y_{n+1}$$
$$z_n \mapsto 0$$

then for the cohomology of the 2-adics integers we have

$$H^*(\mathbb{Z}_2) = \varinjlim_n H^*(C_{2^n}) = \varinjlim \mathbb{F}_2[z_n, y_n]/(y_n^2) = \mathbb{F}_2[y]/(y^2)$$

With $|y| = 1$.

Example 2.2.2. *Let* D_8 *denote the dihedral group of order eight given by the central extension*

$$1 \to C_2 \to D_8 \to C_2 \times C_2 \to 1$$

Here the second page of the LHS spectral sequence is given by $E_2 = \mathbb{F}_2[x, y, z]$ *with differential*

$$\partial_2(z) = xy$$

where $H^*(C_2) = \mathbb{F}_2[z]$, $H^*(C_2 \times C_2) = \mathbb{F}_2[x, y]$ *and the extension is associated to the element* $xy \in H^2(C_2 \times C_2)$ *then the spectral sequence collapses in the third page this is*

$$E_3 = E_\infty = \mathbb{F}_2[x, y, w]/(xy)$$

with $|x| = |y| = 1$ *and* $|w| = 2$.

Example 2.2.3. *Consider* Q_8 *the quaternion group with extension*

$$1 \to C_2 \to Q_8 \to C_2 \times C_2 \to 1$$

associated to the element $x^2 + xy + y^2 \in H^2(C_2 \times C_2)$. *This example is a little bit* *more complicated because the LHS spectral sequence collapse at the fourth page and*

$$H^*(Q_8) = E_4 = E_\infty = \mathbb{F}_2[x, y, w]/(x^2 + xy + y^2, xy^2 + yx^2)$$

with $|x| = |y| = 1$ *and* $|w| = 4$.

Example 2.2.4. *Consider the central extension*

$$1 \to \bigoplus^3 C_2 \to G \to \bigoplus^2 C_2 \to 1.$$

defined by the quadratic forms

$$\begin{aligned} H^*(\bigoplus^3 C_2) = \mathbb{F}_2[a, b, c] \quad &\to \quad H^*(\bigoplus^2 C_2) = \mathbb{F}_2[x, y] \\ a \quad &\mapsto \quad x^2 \\ b \quad &\mapsto \quad y^2 \\ c \quad &\mapsto \quad xy. \end{aligned}$$

This group can be viewed as the finitely presented group

$$G = \langle x, y | x^4 = y^4 = [x, y]^2 = [x, x, y] = [y, x, y] = 1 \rangle$$

and its LHS spectral sequence collapses in the third page

$$H^*(G) = E_3 = E_\infty = \frac{\mathbb{F}_2[\alpha, \beta, \gamma, x, y, u, v]}{(x^2, y^2, xy, xu, yv, xv + yu, u^2, v^2, uv)}.$$

A generalization of this result can be found in [2] and [19].

Chapter 3

The 2-descending central series

We recall in this chapter the lower 2-central series of a pro-2-group. In this chapter we concentrate on the case $p = 2$ because of the connection in the case $p = 2$ with the W-group and quadratic forms as explained in [21]. For any prime p the lower p-central series arises most frequently in computational group theory. In particular, when computing with finite p-groups, there is a very efficient algorithm known as *the nilpotent quotient*, which takes a finite p-group and computes the terms of its lower p-central series. This series can also be used to compute the automorphism group of a finite p-group inductively.

Our first attempt to compute the cohomology groups use the Lyndon-Hochschild-Serre spectral sequence[1]. We illustrate the spectral sequences in some cases and then, we apply these sequences to the quotients of the 2-descending central series of a free pro-2-group.

Let S a free pro-2-group. Denoted its 2-descending central series by

$$S = S^{(1)} \supset S^{(2)} \supset \cdots \supset S^{(m)} \supset \cdots$$

1. In 1954, spectral sequences enabled Jean-Pierre Serre to discover connections between the homotopy groups of a space and homology groups and to prove important results on the homotopy groups of spheres. He was awarded the Fields Medal for this work. A decade before, in 1946, the hydrodynamics expert Jean Leray introduced the notion of spectral sequence. This French mathematician made substantial contributions to the mathematical study of fluid dynamics before the second world war and served as an army officer in 1939. In 1940 he was captured by the Germans and was taken to an officer's prison camp in Austria until the end of the war in 1945. He hid his skill in applied mathematics from his captors because he feared that if they knew of it he would be forced to work for the war. Instead, he claimed to be a topologist and worked on this new subject for him.

given by

$$S^{(1)} = S$$
$$S^{(m+1)} = [S, S^{(m)}](S^{(m)})^2.$$

Observe that $S^{(m)}/S^{(m+1)}$ is the elementary abelian 2-group of dimension k_m

$$S^{(m)}/S^{(m+1)} = \bigoplus^{k_m} C_2$$

with $k_m = d_1 + \cdots + d_m$ and $d_a = \frac{1}{a}\sum_{b|a} n^{a/b}\mu(b)$ where μ is the Moebius function. This was proved by Shafarevich in [26]. These numbers d_i above are known as the Witt numbers.

Define the quotient groups

$$S^{[m]} = S/S^{(m)}.$$

We have the extension

$$1 \to \frac{S^{(m)}}{S^{(m+1)}} \to S^{[m+1]} \to S^{[m]} \to 1. \tag{3.1}$$

which implies that $|S^{[m+1]}| = 2^{k_1+\cdots+k_m}$. [2]

These quotient groups have been introduced as the Galois Groups of certain extension of fields $F^{(3)}/F$ in [21]. In fact for $m = 3$ the group $S^{[m]}$ is called the W-group of F and determines the Galois extension. Also in [2] they show that the absolute Galois group characterize the W-group and reflect important properties of the field. In [2] they construct a topological model to compute its cohomology.

2. This quotient group $S^{[m]}$ is isomorphic to the quotient $H^{[m]}$ of a free abstract group H, see 3.2.2 [24]

Theorem 3.0.5. *[9.20 in Holt] If $S/S^{(2)}$ is generated by the images of $a_1, \cdots, a_d$, then $S^{(2)}/S^{(3)}$ is generated by the images of a_i^2 where $1 \leq i \leq d$ and $[a_j, a_i]$ where $1 \leq i < j \leq d$. More generally, for $m > 0$, let X be a subset of S which generates S modulo $S^{(2)}$ and let T generates $S^{(m)}$ modulo $S^{(m+1)}$. Then $S^{(m+1)}$ is generated modulo $S^{(m+2)}$ by $[x, t]$ for $x \in X, t \in T$ and t^2 for $t \in T$*

These generators are know as Basic Commutators. We will talk about them in the next chapter.

Example 3.0.6. *In two generators the presentation for the first four groups and the Witt numbers are*

$d_1 = 2, d_2 = 1, d_3 = 2, d_4 = 3$ *and*

- $S/S^{(2)} = \langle x, y \rangle$
- $S^{(2)}/S^{(3)} = \langle x^2, y^2, [x, y] \rangle$
- $S^{(3)}/S^{(4)} = \langle x^4, y^4, [x, y]^2, [x, [x, y]], [y, [x, y]] \rangle$
- $S^{(4)}/S^{(5)} = \langle x^8, y^8, [x, y]^4, [x, x, y]^2, [y, x, y]^2, [x, x, x, y], [y, y, x, y], [y, x, x, y] \rangle$

In this chapter we will try to give a good description of the first three cohomology groups of $S^{[m]}$.

3.1 The first cohomology group

Lemma 3.1.1. *Let A, B, C be pro-p-groups. Denote by $d(B)$ the minimal number of topological generators of B. Let*

$$1 \to A \to B \xrightarrow{\varphi} C \to 1$$

be a short exact sequence. Then $d(C) \leq d(B)$.

Proof. Let $\mathcal{B} = \{b_i | i \in I\}$ be a set of minimal topological generators of B. Consider the set

$$\mathcal{C} = \{c_i | c_i = \varphi(b_i), i \in I\}.$$

We will show that the abstract group $\hat{C}$ generated by the set $\mathcal{C}$ is dense in C. Let $c \in C$, then there is an element $b \in B$ such that $\varphi(b) = c$. Let U be an open neighbourhood of $c = \varphi(b)$. Because φ is continuous $\varphi^{-1}(U)$ is an open neighbourhood of b. Since the subgroup $\hat{B}$ generated by $\mathcal{B}$ is dense in B there is an element $\hat{b}$ such that

$$\hat{b} \in \varphi^{-1}(U) \cap \hat{B}$$

then $\varphi(\hat{b}) = \hat{c} \in \hat{C} \cap U$ as required. $\square$

Theorem 3.1.2. *Let S be a pro-2-group, and $S^{[m]}$ as above. Then*

$$\dim_{\mathbb{F}_2} H^1(S^{[m]}) = \dim_{\mathbb{F}_2} H^1(S^{[m+1]})$$

for $m \geq 2$.

Proof. It suffices to prove that $d(S^{[m]}) = d(S^{[m+1]})$. Consider the exact sequence

$$1 \to \frac{S^{(m)}}{S^{(m+1)}} \to S^{[m+1]} \to S^{[m]} \to 1.$$

By the lemma above we have that $d(S^{[m+1]}) \geq d(S^{[m]})$. From the extension

$$1 \to S^{(m)} \to S \to S^{[m]} \to 1. \tag{3.2}$$

we have $d(S) \geq d(S^{[m]})$. Clearly $d(S) = d(S^{[2]})$ therefore

$$n = d(S) \geq d(S^{[m+1]}) \geq d(S^{[m]}) \geq \cdots \geq d(S^{[2]}) = n.$$

$\square$

3.2 The second cohomology group

Theorem 3.2.1. *From the short exact sequence* (3.1) *consider its associated five term exact sequence*

$$0 \to H^1(S^{[m]}) \xrightarrow{inf} H^1(S^{[m+1]}) \xrightarrow{res} H^1\left(\frac{S^{(m)}}{S^{(m+1)}}\right)^{S^{[m]}} \xrightarrow{tr} H^2(S^{[m]}) \xrightarrow{inf} H^2(S^{[m+1]}).$$

Then the homomorphism

$$tr : H^1\left(\frac{S^{(m)}}{S^{(m+1)}}\right)^{S^{[m]}} \to H^2(S^{[m]})$$

is an isomorphism.

Proof. Let $\beta \in H^2(S^{[m]})$. Then β is represented by an extension

$$1 \to \mathbb{F}_2 \to G \to S^{[m]} \to 1$$

for some group G. Because S is a free pro-2-group there is a morphism

$$\alpha : \frac{S^{(m)}}{S^{(m+1)}} \to \mathbb{F}_2$$

such that the following diagram is commutative:

$$\begin{tikzcd}
1 \arrow[r] & \frac{S^{(m)}}{S^{(m+1)}} \arrow[r] \arrow[d] & S^{[m+1]} \arrow[r] \arrow[d] & S^{[m]} \arrow[r] \arrow[d, equal] & 1 \\
1. \arrow[r] & \mathbb{F}_2 \arrow[r] & G \arrow[r] & S^{[m]} \arrow[r] & 1
\end{tikzcd} \tag{3.3}$$

Hence $tr(\beta) = \alpha$, therefore surjective. Because

$$\inf : H^1(S^{[m]}) \to H^1(S^{[m+1]})$$

is an isomorphism from the theorem 3.1.2 it follows that

$$tr : H^1\left(\frac{S^{(m)}}{S^{(m+1)}}\right)^{S^{[m]}} \to H^2(S^{[m]})$$

is injective. $\square$

Observe that the induce action of $S^{[m]}$ on $\frac{S^{(m)}}{S^{(m+1)}}$ is trivial because the extension of groups 3.1 is a central extension.

Corollary 3.2.2. *With the hypothesis of the last theorem*

$$\dim_{\mathbb{F}_2} H^2(S^{[m]}) = \dim_{\mathbb{F}_2}\left(\frac{S^{(m)}}{S^{(m+1)}}\right) = k_m = d_1 + \cdots + d_m.$$

Corollary 3.2.3. *With the hypothesis of the last theorem we also have that*

$$inf : H^2(S^{[m]}) \to H^2(S^{[m+1]})$$

is trivial.

We have now a description for first three columns in the second page $E_2(S^{[m+1]})$ in the LHS spectral sequence associated to (3.1)

2			
1	k_m		
0	1	n	k_m
	0	1	2

(3.4)

Proposition 3.2.4. *For $m = 3$*

$$1 \to \frac{S^{(2)}}{S^3} \to S^{[3]} \to S^{[2]} \to 1$$

the morphisms $\partial^{t,1}$, for $t = 1, 2, \cdots$ is always surjective.

Proof. Let $E_2^{t,0}(S^{[3]}) = H^t(S^{(2)}) = \mathbb{F}_2[x_1, \cdots, x_n]$ then for $w \in H^k(S^{(2)})$ we have that $w = w_1 w_2$ with w_1, w_2 in $H^2(S^{(2)})$, $H^{k-2}(S^{(2)})$ respectively. Then there is an element $\alpha \in E_2^{0,1}$ such that $\partial^{0,1}(\alpha) = w_1$ therefore $\partial^{k-2,1}(\alpha \otimes w_2) = w_1 w_2 = w$. $\square$

This group $S^{[3]}$ have been studied in [2] and example 2.2.4 there are conclusions about its cohomology using the fact that is an extension of two elementary abelian groups. We can also say something about the second cohomology groups in general.

Lemma 3.2.5. *In the $E(S^{[m+1]})$ LHS Spectral Sequence associated to extension 3.1. Then* $\dim(E_3^{0,2}(S^{[m]}))$ *is k_m.*

Proof. Let $E_2^{0,*} = H^*(S^{(m)}/S^{(m+1)}) = \mathbb{F}_2[y_1, \cdots, y_{k_m}]$. Then $E_2^{0,2}$ is generated as $\mathbb{F}_2$-module by the products $y_i y_j$ for $i, j = 1, \cdots, k_m$. Observe that

- $\partial^{0,2}(y_i^2) = 0$
- $\partial^{0,2}(y_i y_j) = \partial^{0,2}(y_i) \otimes y_j + \partial^{0,2}(y_j) \otimes y_i$

but the set $\{\partial^{0,2}(y_i) : i = 1, \cdots, k_m\}$ is linearly independent. Therefore $E_3^{0,2}$ is generated by the $\{y_i^2 : i = 1, \cdots, k_m\}$. $\square$

This result is showing a beautiful conclusion about the second cohomology group of $S^{[m]}$ and its maps. We will see that this k_m elements are indecomposable elements of degree two.

Theorem 3.2.6. *Let*

$$res : H^2(S^{[m+1]}) \to H^2\left(\frac{S^{(m)}}{S^{(m+1)}}\right)$$

be the restriction map associated to the extension 3.1. Then the image of the map res has dimension k_m.

Proof. We will start from the two following well known facts. First the image of the restriction of $S^{[m+1]}$ is just $E_\infty^{0,2}$ which is a submodule of $E_3^{0,2}$. By the lemma above we know that $\dim(E_3^{0,2}) = k_m$. The second fact is that we can associate to each generator α_i of $H^2(S^{(m+1)}/S^{(m+1)})$ an extension

$$1 \to C_2 \to H_i \to S^{[m+1]} \to 1.$$

With the notation of the lemma above, we will show that for every group H_i associated to the element $y_i^2 \in H^2(S^{(m)}/S^{(m+1)})$ this means that

$$H_i = \left(\bigoplus_{1}^{k_m - 1} C_2 \right) \oplus C_4$$

there is a group G_i associated to an element $\beta_i \in H^2(S^{[m+1]})$ such that the following diagram is commutative

$$\begin{tikzcd}
C_2 \arrow[r, tail] \arrow[d, equal] & G_i \arrow[r, two heads] & S^{[m+1]} \\
C_2 \arrow[r, tail] & H_i \arrow[r, two heads] \arrow[u, dashed] & \frac{S^{(m)}}{S^{(m+1)}} \arrow[u, hook]
\end{tikzcd}$$

Suppose that $S^{[m+1]} = \langle x_1, \cdots, x_n | r_1^2, \cdots r_{k_{m-1}}^2, t_1, \cdots, t_{d_{m+1}} \rangle$ is a presentation for $S^{[m+1]}$ with the r's the relations for $S^{[m]}$ and the t's are the new or higher basic commutators. Let the group G_i be the group define by the presentation

$$G_i = \langle x_1, \cdots, x_n | r_1^2, \cdots, r_i^4, \cdots, r_{k_{m-1}}^2, t_1, \cdots, t_{d_{m+1}} \rangle$$

The we have a short exact sequence $1 \to C_2 \to G_i \to S^{[m+1]} \to 1$ were $C_2 = \langle r_i^2 | r_i^4 \rangle$. Observe that $S^{(m)}/S^{(m+1)}$ is the subgroup of $S^{[m+1]}$ generated by the set $\{r_i : i = 1, \cdots, k_{m-1}\}$. Therefore the restriction of G_i is the subgroup H_i of G_i generated by $\{r_i : i = 1, \cdots, k_{m-1}\}$. This is the sequence $1 \to C_2 \to H_i \to S^{(m)}/S^{(m+1)} \to 1$ and then the diagram is commutative. ☐

Example 3.2.7. *Consider the free group on two generators and the third element of the* 2*-descending central series, this is* $m = 3$ *and* $n = 2$ *then the* r*'s are* $\{x^2, y^2, [x,y]\}$ *and the* t*'s are* $\{[x,[x,y]], [y,[x,y]]\}$ *with the notation of the theorem* 3.2.6 *we have*

- $S^{[3]} = \langle x, y | x^4, y^4, [x,y]^2, [x,[x,y]], [y,[x,y]]\rangle$.
- S^2/S^3 *is the subgroup of* $S^{[3]}$ *generated by* $\{x^2, y^2, [x,y]\}$.
- $G_1 = \langle x, y | x^8, y^4, [x,y]^2, [x,[x,y]], [y,[x,y]]\rangle$.
- H_1 *is the subgroup of* G_1 *generated by* $\{x^2, y^2, [x,y]\}$.
- *The cyclic group with two elements is generated by* x^4 *in* G_1.

For the following corollaries $E(S^{[m+1]})$ is the LHS spectral sequences associated to 3.1. We are now given a precise description of the second cohomology group of $S^{[m+1]}$ in the LHS spectral sequence.

Corollary 3.2.8. *The* $\mathbb{F}_2$*-dimension of* $E_\infty^{0,2}(S^{[m+1]})$ *is* k_m.

Proof. The proposition 3.2.6 show that the dimension is at least k_m and the Lemma 3.2.5 shows the other inequality. ☐

The theorem 3.2.1 with corollaries 3.2.2 and 3.2.8 proved the following result.

Corollary 3.2.9. *The* $\mathbb{F}_2$*-dimension of* $E_\infty^{1,1}(S^{[m+1]})$ *is* d_{m+1}.

This can be prove it directly for $m = 3$ by the proposition 3.2.4, in fact

$$\begin{aligned}
\dim \ker(\partial_2^{1,1}) &= \dim E_2^{1,1}(S^{[3]}) - \dim\{\mathrm{im}(\partial_2^{1,1})\} \\
&= nk_2 - \binom{n+2}{3} \\
&= \frac{n^3 - n}{3} \\
&= d_3.
\end{aligned}$$

Corollary 3.2.10. *The morphism $\partial_3^{0,2}$ in the third page of the LHS spectral sequence is trivial and therefore $E_3^{3,0}(S^{[m+1]}) = E_\infty^{3,0} S^{[m+1]}$.*

Proof. By Lemmas 3.2.5 and 3.2.8. ☐

3.3 The third cohomology Group

Theorem 3.3.1. *An element $w \in H^3(S^{[m]})$ is decomposable if and only if is in the image of $d_2^{1,1}$.*

Proof. Suppose $w = x_1 x_2$ with $x_i \in H^i(S^{[m]})$ then there is an element $y \in H^1(S^{(m)}/S^{(m+1)})$ such that $d_2^{1,1}(y) = x_2$ then $w = d_2^{1,1}(x_1 y)$. On the other hand if $w = d_2^{1,1}(xy) = x d_2^{1,1}(y)$ which complete the proof. ☐

Therefore the third page of the LHS spectral sequence $E_3(S^{[m+1]})$ is

2				
1	0	d_{m+1}		
0	1	n	0	I_m
	0	1	2	

(3.5)

Where I_m is the number of indecomposable elements in $H^3(S^{[m]})$.

Corollary 3.3.2. *The $\mathbb{F}_2$-dimension of the decomposable elements D_m of $H^3(S^{[m]})$ is $n * k_m - d_{m+1}$.*

Proof. It follows from theorem 3.3.1 and the corollaries 3.2.8 and 3.2.9. ☐

Corollary 3.3.3. *The inflation map $inf \colon H^3(S^{[m]}) \to H^3(S^{[m+1]})$ is not trivial.*

Proof. By corollary 3.2.10 we know that dimension of $E_\infty^{3,0}$ is I_m, i.e. the number of indecomposable elements in $H^3(S^{[m]})$ that is the image of the inflation map. $\square$

In the following propositions we will try to give a brief description of the third cohomology group of $S^{[m+1]}$ in the LHS spectral sequence $E(S^{[m+1]})$ associated associated to the extension 3.1 with $E_2^{0,*} = \mathbb{F}_2[x_1, \cdots, x_{k_{m-1}}]$.

Proposition 3.3.4. *The $\mathbb{F}_2$-dimension of $E_3^{0,3}(S^{[m+1]})$ is zero.*

Proof. For $\partial_2^{0,3} : E_2^{0,3}(S^{[m+1]}) \to E_2^{2,2}(S^{[m+1]})$ observe that

- $\partial_2^{0,3}(x_i^2 x_j) = x_i^2 \otimes \partial_2^{0,3}(x_j)$ for $1 \leq i \leq j \leq k_{m-1}$
- $\partial_2^{0,3}(x_i x_j x_k) = x_i x_j \otimes \partial_2^{0,3}(x_k) + x_i x_k \otimes \partial_2^{0,3}(x_j) + x_j x_k \otimes \partial_2^{0,3}(x_i)$

where the $\partial_2^{0,3}(x_i)$ are linearly independent, then $\partial_2^{0,3}$ is injective. $\square$

Proposition 3.3.5. *The $\mathbb{F}_2$-dimension of $E_3^{1,2}(S^{[m+1]})$ is at least $n * k_m$.*

Proof. We showed that $E_\infty^{1,0}(S^{[m+1]}) = n$ and $E_\infty^{0,2}(S^{[m+1]}) = k_m$ therefore by the filtration of the spectral sequence its product $E_\infty^{1,0}(S^{[m+1]}) \otimes E_\infty^{0,2}(S^{[m+1]})$ should be in

$$E_\infty^{1,2}(S^{[m+1]}) \bigcup E_\infty^{2,1}(S^{[m+1]}) \bigcup E_\infty^{3,0}(S^{[m+1]})$$

but they are already in $E_3^{1,2}(S^{[m+1]})$ because they are permanent cocycles. $\square$

We conclude that the dimension of $E_\infty^{1,2}(S^{[m+1]})$ id nk_m plus maybe some indecomposable elements, also in $E_\infty^{2,1}(S^{[m+1]})$ we only will have indecomposable elements and $E_\infty^{3,0}(S^{[m+1]})$ will be just I_m.

Conjecture 3.3.6. *The composition of the two inflation maps*

$$H^3(S^{[m]}) \xrightarrow{inf} H^3(S^{[m+1]}) \xrightarrow{inf} H^3(S^{[m+2]})$$

is trivial.

There are some reasons why this could be true. In fact

$$S = \varprojlim S^{[m]}. \implies H^*(S) = \varinjlim H^*(S^{[m]}).$$

and $H^n(S)$ is trivial for $n > 1$ for S a free pro-2-group. We also proved in theorem 3.2.1 that $\inf_1 : H^1(S^{[m]}) \to H^1(S^{[m+1]})$ is a bijection and that $\inf_2 : H^2(S^{[m]}) \to H^2(S^{[m+1]})$ is trivial, we can say that $\inf_3 : H^3(S^{[m]}) \to H^3(S^{[n+?]})$ will be eventually trivial.

In theorem 3.3.1 we proved that $\inf_3$ kills all the decomposable elements of $H^3(S^{[m]})$ and is injective in the indecomposable elements of $H^3(S^{[m]})$ this suggests that the indecomposable elements of $H^3(S^{[m]})$ eventually became decomposable. The conjecture is saying that this happens in the first step i.e. in $H^3(S^{[m+1]})$. This appears to be clear for $m = 3$ in the following example.

Example 3.3.7. *From the description of $S^{[3]}$ given in [2] and the work above we know that the dimension of $H^3(S^{[m]})$ is $nk_2 + \frac{d_4}{3}$ decomposable elements plus $nd_4 - d_5$ indecomposable.*

We saw in corollary 3.3.2 that there are $nk_4 - d_5$ decomposable elements in $H^3(S^{[4]})$ where nk_3 elements are in $E_\infty^{1,2}(S^{[4]})$, note that

$$nk_4 - d_5 = nk_3 + (nd_4 - d_5)$$

therefore we have $nd_4 - d_5$ "new" decomposable elements in $H^3(S^{[4]})$ theses elements have to be the image of the map $\inf_3 : H^3(S^{[3]}) \to H^3(S^{[4]})$ and therefore the composition of the inflation maps in the conjecture is trivial.

Proposition 3.3.8. *The $\mathbb{F}_2$-dimension of $H^3(S^{(m)})$ is at most $nk_{m+1} - d_{m+1} - d_{m+2}$ for $m > 3$.*

Proof. By the conjecture 3.3.6 the indecomposable elements I_m in $H^3(S^{(m)})$ became decomposable in $H^3(S^{(m+1)})$. The dimension of decomposable elements in

$H^3(S^{[m+1]})$ is $nk_{m+1} - d_{m+2}$, Corollary 3.3.2, but there are at least nk_m decomposable elements in $H^3(S^{[m+1]})$ by proposition 3.3.5 therefore $I_m \leq nk_{m+1} - d_{m+2} - nk_m$ and then

$$\begin{aligned} \dim H^3(S^{[m]}) &= D_m + I_m \\ &\leq (nk_m - d_{m+1}) + (nk_{m+1} - d_{m+2} - nk_m) \\ &= nk_{m+1} - d_{m+1} - d_{m+2}. \end{aligned}$$

□

Example 3.3.9 ($S^{[3]}$)**.** *For the case $m = 2$ using the formulas found in [2] we have a description of $E_\infty = E_3(S^{[3]})$*

3	0			
2	k_2	$nk_2 + I_3$		
1	0	d_3	$\frac{d_4}{3}$	
0	1	n	0	0
	0	1	2	3

(3.6)

Example 3.3.10 ($S^{[m+1]}$)**.** *In general we have $E_\infty = E_3(S^{[m+1]})$ is*

3	0			
2	k_m	$nk_m + ?$		
1	0	d_{m+1}	?	
0	1	n	0	I_m
	0	1	2	3

(3.7)

Chapter 4

Irreducible polynomials and basic commutators

We saw that the minimal number of generators for the quotient of the lower p-central series of a free pro-p-group is given by the Witt numbers. In this chapter we call these generators basic commutators. The Witt numbers are also counting the number of irreducible polynomials over certain finite fields. In this chapter we show the explicit connection between basic commutators and irreducible polynomials of a fixed degree with coefficients in $\mathbb{F}_p$.

4.1 Basic commutators

Let S be a free group over the variables $x_1, \cdots, x_n$. For the following definitions we will follow [10] and [12]. By the commutator of x and y in the group S we note $[x, y] = x^{-1}y^{-1}xy$.

Definition 4.1.1 (Basic Commutators). *The set A of basic Commutators of the group S is defined inductively as follows*

(1) *Each basic commutator c has a weight $w(c)$ taking one of the values $1, 2, \cdots$*

(2) *The Basic commutators of weight 1 are $x_1, \cdots, x_n$. A basic commutator of weight > 1 is of the form $c = [c_1, c_2]$ where c_1, c_2 are previously defined basic commutators and $w(c) = w(c_1) + w(c_2)$.*

(3) *Basic commutators are ordered so as to satisfy the following:*

- *Basic commutators of the same weight are lexicographically, i.e.* $x_1 < x_2 < \cdots < x_n$ *and* $(c_1, c_2) < (c_1', c_2')$ *if and only if* $c_1 < c_1'$ *or* $c_1 = c_1'$ *and* $c_2 < c_2'$.
- *If* $w(c) < w(c')$ *then* $c < c'$.

(4)
- *If* $w(c) > 1$ *and* $c = [c_1, c_2]$ *then* $c_1 < c_2$.
- *If* $w(c) > 2$ *and* $c = [c_1, [c_2, c_3]]$ *then* $c_1 \geq c_2$.

Example 4.1.2. *Let* S *be a free group on the letters* x, y, z *then the basic commutators in* S *are*

- ***Weight = 1:*** $x < y < z$.
- ***Weight = 2:*** $[x, y] < [x, z] < [y, z]$
- ***Weight = 3:*** $[x, [x, y]] < [x, [x, z]] < [y, [x, y]] < [y, [x, z]] < [y, [y, z]] < [z, [x, y]] < [z, [x, z]] < [z, [y, z]]$.[1]

Definition 4.1.3. (1) *A word* $a_1 a_2 \cdots a_n$ *is circular if* a_1 *is regarded as following* a_n *where* $a_1 a_2 \cdots a_n, a_2 \cdots a_n a_1, \cdots, a_n a_1 \cdots a_{n-1}$ *are all regarded as the same word.*

(2) *A circular word* c *of length* n *may be given by repeating a segment of letters* n/d *times, where* $d|n$. *We say that* c *is of period* d *in this case.*

We will consider as the alphabet the set A of basic commutators, for example

$$x[x, [x, y]][y, z] \text{ and } [y, z]x[x, [x, z]]$$

are the same circular words in the three basic commutators $x, [y, z], [x, [x, z]]$.

---

1. Note that $[x, [y, z]]$ is not a basic commutator.

4.1.1 The bracketing process

Given a circular word w of the same length and period and a basic commutator c we define $Br(c,w)$ *the bracketing of* c *in the word* w as the following process

(1) If c is neither at the end nor at the beginning, i.e. $w = acb$ then

$$w \mapsto Br(c,w) = a[c,b]$$

(2) If c appears more than once consecutively, i.e. $w = acc\cdots cb$ then

$$w \mapsto Br(c,w) = a[c,[c,\cdots,b]\cdots]$$

(3) If c appears at the end of $w = ac$, then consider the word $w = ca$ and then apply 1.

(4) If c does not appear in w then there is nothing to do.

Note that the word $cc\cdots c$ is impossible because the period and the length are the same.

4.1.2 The process

Given a circular word w of the same length and period in the basic commutators of weight 1 we will show how to get a basic commutator applying the following rules:

(1) Find the minimal basic commutator m_c of the word w.

(2) Apply the bracketing process $Br(m_c,w)$ for m_c in w.

(3) Go back to 1 using the new word $Br(m_c,w)$ instead of w.

Proposition 4.1.4. *Given any circular word w in the alphabet A of basic commutators with the same length and period, the process ends with a word w' which is also a basic commutator. More over the number of circular words of length and period n is the same number as basic commutators of weight n.*

Proof. We will show by induction that if w is a circular word of basic commutators then after applying the bracketing process for a the minimal basic commutator c in w the result is also a circular word of basic commutators.

- Base Case: Let w be a circular word in basic commutators of weight one. Suppose x_i is its minimal basic commutator then apply $Br(x_i, w)$. The new word $Br(x_i, w)$ consist of basic commutators of weight one and commutators $[x_i, x_j]$ for $j > i$.

- Inductive case: Let w be a word in the basic commutators. Let c be its minimal basic commutator. Then if c_2 is a commutator of $Br(c, w)$ there are three options

  - c_2 is a word of w, i.e. the bracketing did not affect it.
  - $c_2 = [c, a]$ where $c < a$ and if $a = [r, s]$ then $r < c$.
  - $c_2 = [c, [c, \cdots, [c, a] \cdots]$.

  In all the cases the bracketing is giving a new word made only of basic commutators. To prove the second statement just note that "forgetting" the brackets or unbracketing is the inverse process.

□

4.2 Irreducible polynomials

Let p be a prime number and $q = p^l$ a power of p. Let $\mathbb{F}_q$ be the field with q elements and $\mathbb{F}_{q^l}$ its extension of degree l.

Definition 4.2.1. *A top element of the extension* $\mathbb{F}_{q^l}/\mathbb{F}_q$ *is an element in the* $\mathbb{F}_{q^l}$ *that does not belong to any intermediate field.*

Note that the number of irreducible monic polynomials with coefficients in $\mathbb{F}_q$ equals the number of top elements in the extension $\mathbb{F}_{q^l}/\mathbb{F}_q$ divided by l the degree of the extension. This is the key idea of the connection between the irreducible polynomials and the basic commutators.

The Galois group of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ is cyclic and is generated by the Frobenius map: $\alpha \mapsto \alpha^q$ for $\alpha \in \mathbb{F}_{q^l}$. A *normal basis* of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ is a linearly independent set of the form: $\{\alpha, \alpha^q, \cdots, \alpha^{q^{l-1}}\}$ for some $\alpha \in \mathbb{F}_{q^l}$. The Normal Basis theorem claim that this element α always exist.

Let us rename the elements of the base field by $\mathbb{F}_q = \{x_1, \cdots, x_n\}$. For a element $\beta \in \mathbb{F}_{q^l}$ we define the *wording process* of β by expressing β in a normal basis and then associate a word, i.e.

$$\beta = \sum_{i=1}^{l} x_{b_i} \alpha^{q^{i-1}} \mapsto x_{b_1} x_{b_2} \cdots x_{b_l}.$$

We are now ready for the main theorem.

4.3 Main theorem

With the notation from the section above we can state the following theorem.

Theorem 4.3.1. *The explicit bijection between the irreducible polynomials and basic commutators is given by the Wording and the bracketing process, i.e.*

$$\textit{Top Elements} \xrightarrow{\textit{Wording}} \textit{Circular Words} \xrightarrow{\textit{Bracketing}} \textit{Basic Commutators}$$

Proof. Let β be a top element in the extension $\mathbb{F}_{q^l}/\mathbb{F}_q$. If $\bar{\beta}$ is a conjugate of β observe that the wording process gives the same circular word for β and $\bar{\beta}$. Moreover this circular word has the same length and period, otherwise β would be in an intermediate field. This Wording process is then a bijection between circular words and Top elements module conjugates.

$$\beta \mapsto \sum_{i=1}^{l} x_{b_i} \alpha^{q^{i-1}} \xrightarrow{\text{Wording}} x_{b_1} x_{b_2} \cdots x_{b_l} \xrightarrow{\text{Bracketing}} \text{A Basic Commutator}$$

$\square$

4.4 Examples

The Finite Field $\mathbb{F}_8$

Consider the irreducible polynomial $p(z) = z^3 + z^2 + 1$ over the field $\mathbb{F}_2 = \{x, y\}$ with a root α. It is clear that $\{\alpha, \alpha^2, \alpha^4\}$ is a basis for $\mathbb{F}_8$ since $\alpha^4 = 1 + \alpha + \alpha^2$ As before the top elements of $\mathbb{F}_8$ over $\mathbb{F}_2$ are

$$\{\alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}.$$

The we will have $6/3 = 2$ Basic Commutators

(1) $\alpha = 1\alpha + 0\alpha^2 + 0\alpha^4 \mapsto xyy \mapsto [y, [x, y]]$

(2) $1 + \alpha = 0\alpha + 1\alpha^2 + 1\alpha 4 \mapsto yxx \mapsto [x, [x, y]]$.

The Finite Field $\mathbb{F}_{16}$

Let $p(z) = 1 + z + z^2 + z^3 + z^4$ over $\mathbb{F}_2 = \{x, y\}$, then $\mathbb{F}_{16}$ is the splitting field of $p(z)$. Let $\alpha \in \mathbb{F}_{16}$ be a root for $p(z)$. The set

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$$

is a basis for F_{16} over $\mathbb{F}_2$ with $\alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3$ and $\alpha^8 = \alpha^3$. In this case we only need to consider three top elements

(1) $\alpha = 1\alpha + 0\alpha^2 + 0\alpha^4 + 0\alpha^8 \mapsto xyyy \mapsto [y,[y,[x,y]]]$

(2) $1+\alpha = 0\alpha + 1\alpha^2 + 1\alpha^4 + 1\alpha^8 \mapsto xyyy \mapsto [x,[x,[x,y]]]$

(3) $\alpha+\alpha^2 = 1\alpha + 1\alpha^2 + 0\alpha^4 + 0\alpha^8 \mapsto xxyy \mapsto [y,[x,[x,y]]]$

The Finite Field $\mathbb{F}_{27}$

Let $p(z) = 1 + z + 2z^2 + z^3$ over $\mathbb{F}_3 = \{x, y, z\}$. $\mathbb{F}_{27}$ is the splitting field of $p(z)$. Let $\alpha \in \mathbb{F}_{27}$ be a root for $p(z)$. The set

$$\{\alpha, \alpha^3, \alpha^9\}$$

is a basis for F_{27} over $\mathbb{F}_3$

(1) $\alpha = 1\alpha + 0\alpha^3 + 0\alpha^9 \mapsto yxx \mapsto [x,[x,y]]$

(2) $1+\alpha = 0\alpha + 2\alpha^3 + 2\alpha^9 \mapsto xzz \mapsto [z,[x,z]]$

(3) $2+\alpha = 2\alpha + 1\alpha^3 + 1\alpha^9 \mapsto zyy \mapsto [y,[y,z]]$

(4) $2\alpha = 2\alpha + 0\alpha^3 + 0\alpha^9 \mapsto zxx \mapsto [x,[x,z]]$

(5) $1+2\alpha = 1\alpha + 2\alpha^3 + 2\alpha^9 \mapsto yzz \mapsto [z,[y,z]]$

(6) $2+2\alpha = 0\alpha + 1\alpha^3 + 1\alpha^9 \mapsto xyy \mapsto [y,[x,y]]$

(7) $\alpha^2 = 2\alpha + 0\alpha^3 + 1\alpha^9 \mapsto zxy \mapsto [z,[x,y]]$

(8) $2\alpha^2 = 1\alpha + 0\alpha^3 + 2\alpha^9 \mapsto yxz \mapsto [y,[x,z]]$.

Chapter 5

Fox calculus

In this chapter, we use Fox Calculus to give a new interpretation to the third cohomology group $H^3(G, \mathbb{F}_p)$. Fox Calculus is a construction in the theory of free groups developed in five papers in the *Annals of Mathematics* in 1953 by the American mathematician Ralph Fox. It has mainly applications to knot theory. Fox Calculus was originally developed by Fox in [11] to solve the problem of the topological classification of the 3-dimensional lens spaces which involves a generalization of Alexander's polynomial.

Let G be a finite p-group and p be a prime number. Let $1 \to R \to S \to G \to 1$ be a minimal presentation for G. We show that the module $H^1(R, \mathbb{F}_p)$ is the dual of the module generated by the image of R under the Fox derivatives where the action of G on this image is given by left multiplication.

Let G be a pro-p-group finitely generated with minimal presentation

$$1 \to R \to S \to G \to 1 \tag{5.1}$$

where S is a free pro-p-group. In section 3 we mentioned that

$$\begin{aligned} \dim H^1(G, \mathbb{F}_p) = \quad & \dim H^1(S, \mathbb{F}_p) = \quad && \text{Number of generators} \\ \dim H^2(G, \mathbb{F}_p) = \quad & \dim H^1(R, \mathbb{F}_p)^G = \quad && \text{Number of relations.} \end{aligned}$$

This follows from the 5-term exact sequence associated to 5.1. Now, from the LHS spectral sequence can easily deduce that

$$H^1(G, H^1(R)) \simeq H^3(G).^1$$

This guides our attention to understand the G-module $H^1(R)$. In order to do this we will introduce the Fox Calculus. First observe that

$$\left(\frac{R}{[R,R]R^p}\right)^* \simeq H^1(R)$$

are dual modules as $\mathbb{F}_p$-modules.

The Fox-Calculus concept was developed for the case of G a finite group and the ring of the integers $\mathbb{Z}$ in [17] and also for G a free pro-p-group and the ring of the p-adics integer $\mathbb{Z}_p$ in [16].

5.1 Fox differentials

Let G be a finite p-group finitely generated with minimal presentation as in 5.1.

Definition 5.1.1. *The augmentation ideal U is the kernel of the morphism of*

$$\begin{aligned} \varepsilon : \mathbb{F}_p[G] &\to \mathbb{F}_p \\ \sum n_g g &\mapsto \sum n_g. \end{aligned}$$

Proposition 5.1.2. *If G is finitely generated by the set $\{x_1 \cdots, x_d\}$ then U is generated by $\{x_1 - 1, \cdots, x_d - 1\}$ as a G-module.*

Proof. $\{x_i - 1 : i = 1, \cdots, d\}$ is a subset of U since $\varepsilon(x-1) = 1 - 1 = 0$. Let $u \in U$ such that $u = \sum n_g g$ with $\sum n_g g = 0$ then $u = \sum n_g(g-1)$, we just have to show

1. $H^n(G)$ means $H^n(G, \mathbb{F}_p)$ in this section.

by induction on the length of g that $g-1$ is in U. For the inductive step suppose $g = hx_1$ then $g-1 = (h-1)x + (x-1)$. $\square$

Let $1 \to R \to S \to G$ be a minimal presentation for G. Suppose that G is generated by the set $\{x_1, \cdots, x_d\}$ define the epimorphism β of G-modules by

$$\beta : \bigoplus^d \mathbb{F}_p[G] \;\to\; U \tag{5.2}$$

$$(\gamma_1, \cdots, \gamma_d) \;\to\; \sum_{i=1}^{d} \gamma_i(x_i - 1) \tag{5.3}$$

Let $M \subset \bigoplus^d \mathbb{F}_p[G]$ be kernel of β then there is an exact sequence of G-modules

$$1 \to M \to \bigoplus^d \mathbb{F}_p[G] \xrightarrow{\beta} \mathbb{F}_p[G] \to \mathbb{F}_p \to 0$$

Our next goal is to prove that

$$M \simeq \frac{R}{[R,R]R^p} \simeq (H^1(R))^*.$$

Definition 5.1.3. *Let S be a free group over the set $\{x_1, \cdots, x_d\}$.*[2] *For every x_i define the Fox differential of x_i*

$$\frac{\partial}{\partial x_i} : S \to \mathbb{F}_p[S]$$

by the rules

(1) $\frac{\partial x_j}{\partial x_i} = \delta_{ij}$.

(2) $\frac{\partial uv}{\partial x_i} = \frac{\partial u}{\partial x_i} + u\frac{\partial v}{\partial x_i}$

Proposition 5.1.4. *Let w be an element in S. Then $w - 1 = \sum_{i=1}^{d} \frac{\partial w}{\partial x_i}(x_i - 1)$.*

---

2. By abuse of notation we will see the x_i's as generator of S as well as of G.

Proof. By induction on the length of w. The Base case $w = x_i$ is obvious. Let w be $x_1 w_2$ then

$$\begin{aligned}\sum_{i=1}^{d} \frac{\partial w}{\partial x_i}(x_i - 1) &= \sum_{i=1}^{d} \left(\frac{\partial x_1}{\partial x_i} + x_1 \frac{\partial w_2}{\partial x_i} \right)(x_i - 1) = (x_1 - 1) + x_1(w_2 - 1) \\ &= x_1 w_2 - 1 = w - 1.\end{aligned}$$

□

In the presentation 5.1 observe that the homomorphism $S \to G$ induces

$$\phi : \mathbb{F}_p[S] \to \mathbb{F}_p[G]$$

a homomorphism of rings, which also induce

$$\Phi : \bigoplus^{d} \mathbb{F}_p[S] \to \bigoplus^{d} \mathbb{F}_p[G].$$

The Fox differentials also induce a map

$$\begin{aligned}\partial : S &\to \sum^{d} \mathbb{F}_p[S] \qquad (5.4)\\ w &\to \left(\frac{\partial w}{\partial x_1}, \cdots, \frac{\partial w}{\partial x_{x_d}} \right). \qquad (5.5)\end{aligned}$$

Proposition 5.1.5. *Consider the composition map*

$$S \xrightarrow{\partial} \bigoplus^{d} \mathbb{F}_p[S] \xrightarrow{\Phi} \bigoplus^{d} \mathbb{F}_p[G].$$

Let v be an element in S. Then $\Phi(\partial(v)) = 0$ if and only if $v \in [R, R]R^p$.

Proof. Suppose $v = [a, b]$, therefore

$$\begin{aligned}\frac{\partial v}{\partial x_i} &= \frac{\partial a^{-1}}{\partial x_i} + a^{-1}\frac{\partial b^{-1}}{\partial x_i} + a^{-1}b^{-1}\frac{\partial a}{\partial x_i} + a^{-1}b^{-1}a\frac{\partial b}{\partial x_i} \\ &= (a^{-1}b^{-1} - a)\frac{\partial a}{\partial x_i} + (a^{-1}b^{-1}a - a^{-1}b^{-1})\frac{\partial b}{\partial x_i}.\end{aligned}$$

Now if $v = a^p$ then

$$\frac{\partial v}{\partial x_i} = (1 + a + \cdots + a^{p-1})\frac{\partial a}{\partial x_i}.$$

If $a, b \in R$ then $\Phi(a) = \Phi(b) = 1$ and therefore $\partial(\Phi(v)) = 0$ for $v \in [R, R]R^p$. On the other hand. Let $v \in S$ such that $\partial(\Phi(v)) = 0$. We will prove by induction that $v \in [R, R]R^p$. Since each term on the left is a monomial in the variables $\{x_1^{\pm 1}, \cdots, x_d^{\pm 1}\}$ and each one of these belongs to the basis G of $\mathbb{F}[G]$ as a vector space over $\mathbb{F}_p$, the letters of v are partitioned into pairs with equal subscript i, opposite sign and their contributions to $\Phi(\frac{\partial v}{\partial x_i})$ cancelling out, i.e.

$$v = ax_ibx_i^{-1}c \quad \text{with} \quad \frac{\partial v}{\partial x_i} = (a - ax_ibx_i^{-1})\frac{\partial x_i}{\partial x_i} + \cdots$$

this implies that $b \in R$. Let $x_i^{-\varepsilon}$ be the first letter of v whose partner preceded it, so that if x_j^{δ} is the letter immediately preceding $x_i^{-\varepsilon}$, its partner must occur later. thus

$$v = ax_i^{\varepsilon}bx_j^{\delta}x_i^{-\varepsilon}cx_j^{-\delta}d$$

and as above bx_j^{δ} and $x^{-\varepsilon}c$ are in R. Modulo $[R, R]R^p$ we have

$$v = ax_i^{\varepsilon}(bx_j^{\delta})(x_i^{-\varepsilon}c)x_j^{-\delta}d \equiv ax_i^{\varepsilon}(x_i^{-\varepsilon}c)(bx_j^{\delta})x_j^{-\delta}d \equiv acbd = v'$$

Then the length of v' is less than the length of v

$$\frac{\partial v}{\partial x_i} = \frac{\partial v'}{\partial x_i}$$

the proof now follows by induction. □

Proposition 5.1.6. *Let* $\gamma = (\gamma_1, \cdots, \gamma_d) \in \bigoplus^d \mathbb{F}_p[S]$. *Consider the composition map*

$$\bigoplus^d \mathbb{F}_p[S] \xrightarrow{\Phi} \bigoplus^d \mathbb{F}_p[G] \xrightarrow{\beta} U$$

Then $\gamma \in \ker(\beta \circ \Phi)$ *if and only if there is an element* $r \in R$ *such that* $\Phi(\partial(r)) = \Phi(\gamma)$.

Proof. Let $r \in R$ such that $\Phi(\gamma) = \Phi(\partial(r))$ then by definition of β and proposition 5.14 is clear that

$$\begin{aligned} \beta(\Phi(\gamma)) = &\quad \beta(\Phi(\partial(r)) = \beta(\Phi\left(\tfrac{\partial r}{\partial x_1}, \cdots, \tfrac{\partial r}{\partial x_d}\right)) \\ = &\quad \textstyle\sum_{i=1}^d \Phi\left(\tfrac{\partial r}{\partial x_i}\right)(x_i - 1) = \Phi(r-1) = 0. \end{aligned}$$

On the other hand, let $\gamma \in \ker(\beta \circ \Phi)$ then $\sum_{i=1}^n \Phi(\gamma_i)(x_i - 1) = 0$. Define $s \in \mathbb{F}_p[S]$ by

$$s = \sum_{i=1}^n \gamma_i(x_i - 1).$$

Then $\Phi(s) = 0$ and s can be expressed as a difference of elements in $\mathbb{F}_p[G]$

$$s = \sum_{j=1}^m (u_j - w_j) = \sum_{j=1}^m (r_j - 1)w)j.$$

with $\Phi(u_j) = \Phi(w_j)$ and $r_j = u_j w_j^{-1}$ for $j = 1, \cdots, m$. Because U is freely generated as a G-module by the set $\{x_i - 1 : i = 1, \cdots, d\}$ and by proposition 5.1.4

$$\begin{aligned} \gamma_i &= \frac{\partial s}{\partial x_i} = \sum_{j=1}^m \left(\frac{\partial r_j}{\partial x_i} + (r_j - 1)\frac{\partial w_j}{\partial x_i}\right) \Rightarrow \\ \phi(\gamma_i) &= \sum_{j=1}^m \phi\left(\frac{\partial r_j}{\partial x_{x_i}}\right) \quad \text{With} \quad r = r_1 r_2 \cdots r_m \quad \text{then} \\ \Phi(\gamma) &= \Phi(\partial(r)). \end{aligned}$$

□

Theorem 5.1.7. *With the above notation we have the following isomorphism*

$$\begin{array}{rcl} \zeta : \dfrac{R}{[R,R]R^p} & \xrightarrow{\Phi\circ\partial} & M \\ \bar{r} & \mapsto & \Phi(\partial(r)). \end{array}$$

Proof. By proposition 5.1.6 $\zeta(r) \in M = \ker(\beta)$ and if $r \in [R,R,]R^p$ then $\zeta(r) = 0$ by proposition 5.1.5 then is well defined. Observe that

$$\zeta(r_1r_2) = \zeta(r_1) + \Phi(r_1)\zeta(r_2) = \zeta(r_1) + \zeta(r_2)$$

then the application is an injective homomorphism by proposition 5.1.5 and surjective by 5.1.6 rest to prove that k is a G-homomorphism. Let $w \in S$ such that $\phi(w) = g \in G$. $\zeta(g \cdot \overline{r}) = \zeta(\overline{wrw^{-1}}) = \Phi(\partial(w) + w\partial(r) - wrw^{-1}\partial(w)) = \Phi(w\partial(r)) = g\zeta(\overline{r})$ □

Corollary 5.1.8. *With hypothesis of the theorem above the action of G over M is given by left multiplication and*

$$\zeta([x,r]) = (1 - x^{-1})\zeta(r) \tag{5.6}$$

for $r \in R$ and $x \in S$.

Proof. It follows from the proof of the theorem. □

5.2 The G-module $H^1(R) \simeq M^*$

Let G be a pro-p-group finitely generated with minimal presentation

$$1 \to R \to S \to G \to 1.$$

Our main goal is the G-module $H^1(G, H^1(R))$. In this section we will describe the module M in detail this module. Let R be a subgroup of finite index b in a free group

S on d free generators. Then Schreier Theorem [12] 7.2.8. says that R is a free group on $1 + b(d - 1)$. From this theorem follows the next proposition.

Proposition 5.2.1. *The dimension of M as a vector space over $\mathbb{F}_p$ is $1 + |G|(n - 1)$.*

However the module M can be generated by less elements as a G-module. In fact if the normal subgroup R of S is the normal closure of the group generated by $r_1, \cdots, r_l$ then M as a G module is generated by the elements $\zeta(r_i)$ for $i = 1, \cdots, l$ this follows from corollary 5.1.8.

Example 5.2.2. *As in Section 3 consider the $p = 2$ and the 2-elementary abelian group $S^{[2]}$ over the two generators $\{x, y\}$ and minimal presentation*

$$S^{[2]} = \langle x, y | x^2 = [x, y] = y^2 = 1 \rangle.$$

Then M is generated by the elements $\zeta(x^2), \zeta([x, y]), \zeta(y^2)$ as a $S^{[2]}$-module but with dimension over $\mathbb{F}_2$ given by $1 + |S^{[2]}(2 - 1)| = 5$. To avoid confusion we will denote $\mathbb{F}_2[S^{[2]}] = \{0, 1, \sigma, \tau, \sigma\tau\}$ with $\sigma = \phi(x)$ and $\tau = \phi(y)$. It can be easily seen that the graph for the $S^{[2]}$-module M is

$$\begin{tikzcd}
& (1+\tau)\zeta(x^2) & & (1+\sigma)\zeta(y^2) & \\
\zeta(x^2) \arrow[ur, "1+\tau"] & & \zeta([x,y]) \arrow[ul, "1+\sigma"'] \arrow[ur, "1+\tau"] & & \zeta(y^2) \arrow[ul, "1+\sigma"']
\end{tikzcd} \tag{5.7}$$

Proposition 5.2.3. *The graph for the G-module $H^1(R) \simeq M^*$ is the upside down of the graph for $M \simeq R/[R, R]R^p$.*

Proof. Let $a, b \in M$, $\sigma \in G$ and suppose that $(1-\sigma)a = b$

$$\begin{tikzcd} \bullet\, b \\ \bullet\, a \arrow[u, "1+\sigma"] \end{tikzcd}$$

then $(1-\sigma)a = a - \sigma(a) \Rightarrow \sigma(a) = b - a$ and $\sigma(b) = b - c$ for some $c \in M$. In the dual G-module M^* we have

$$(1-\sigma)(b^*) = b^* - b^* \circ \sigma$$

$$(1-\sigma)(b^*)(a) = b^*(a) - b^*(\sigma(a)) = -b^*(a-b) = 1$$

$$(1-\sigma)(b^*)(b) = b^*(b) - b^*(\sigma(b)) = 1 - b^*(b-c) = 1$$

$$(1-\sigma)(b^*) = a^*.$$

$$\begin{tikzcd} \bullet\, a^* \\ \bullet\, b^* \arrow[u, "1+\sigma"] \end{tikzcd}$$

□

Definition 5.2.4. *Let G be a finite p-group and M a G-module. The Socle series of M is the series of submodules*

$$J_1 \subset J_2 \subset \cdots M$$

defined inductively by

- $J_1 = M^G$ *i.e. the fixed point of M by the action of G.*
- $J_{i+1} = \rho^{-1}(M/J_i)^G$ *where $\rho : M \to M/J_i$ is the natural projection.*

Then length of the series is the first value of i such that $J_i = M$.

Example 5.2.5. *In the example 5.7 the fixed module M^G has dimension two and is*

$$J_1 = \ker(1-\sigma)\bigcap \ker(1-\tau) = \langle (1-\tau)\zeta(x^2), (1-\sigma)\zeta(y^2)\rangle.$$

The length of the Socle series is two with $J_2 = M$.

Note that the first module in the Socle series are the "end points" of the graph for the module M, the second module J_2 are the "end points" of the graph of M without the points of J_1 and so on. However in the Socle series J_i^* for the dual module M^* of M the first module J_1^* correspond to the "first points" of the graph of M this are the generators of M as a G-module.

The original and beautiful proof for the following result can be found in [5], here we show a different proof using the power of Fox-Calculus.

Theorem 5.2.6. *Let S be a free pro-2-group on the d generators $\{x_1, \cdots, x_n\}$. Let G be the quotient group $S^{[2]} = S/S^{(2)}$ as in section 3 and the module M and homomorphism ζ as in theorem 5.1.7. Suppose that G is generated by $\sigma_1, \cdots, \sigma_l$. Then the set*

$$Z = \{(1-\sigma_{t_1})\cdots(1-\sigma_{t_r})d_{ij} : 1 \le i \le j \le n,\, i < t_1 < \cdots < t_r \le d\},$$

is a basis for M where $d_{ij} = \zeta([x_i, x_j])$ if $i \neq j$ and $d_{ii} = \zeta(x_i^2)$.

Proof. It is clear that the set Z span the whole module because the ring $\mathbb{F}_2[S^{[2]}]$ is commutative, is left to prove that is linearly independent. As in [5] the size of Z is

$$\sum_{i=1}^{d}(d-i+1)2^{d-i} = 1 + 2^d(d-1) = \dim(M).$$

$\square$

With the observation and the theorem above we have a basis in this particular case for each dual J_a^* in the socle series for $M^* \simeq H^1(R)$.

Corollary 5.2.7. *With hypothesis of the theorem above. For a fixed integer a the set*

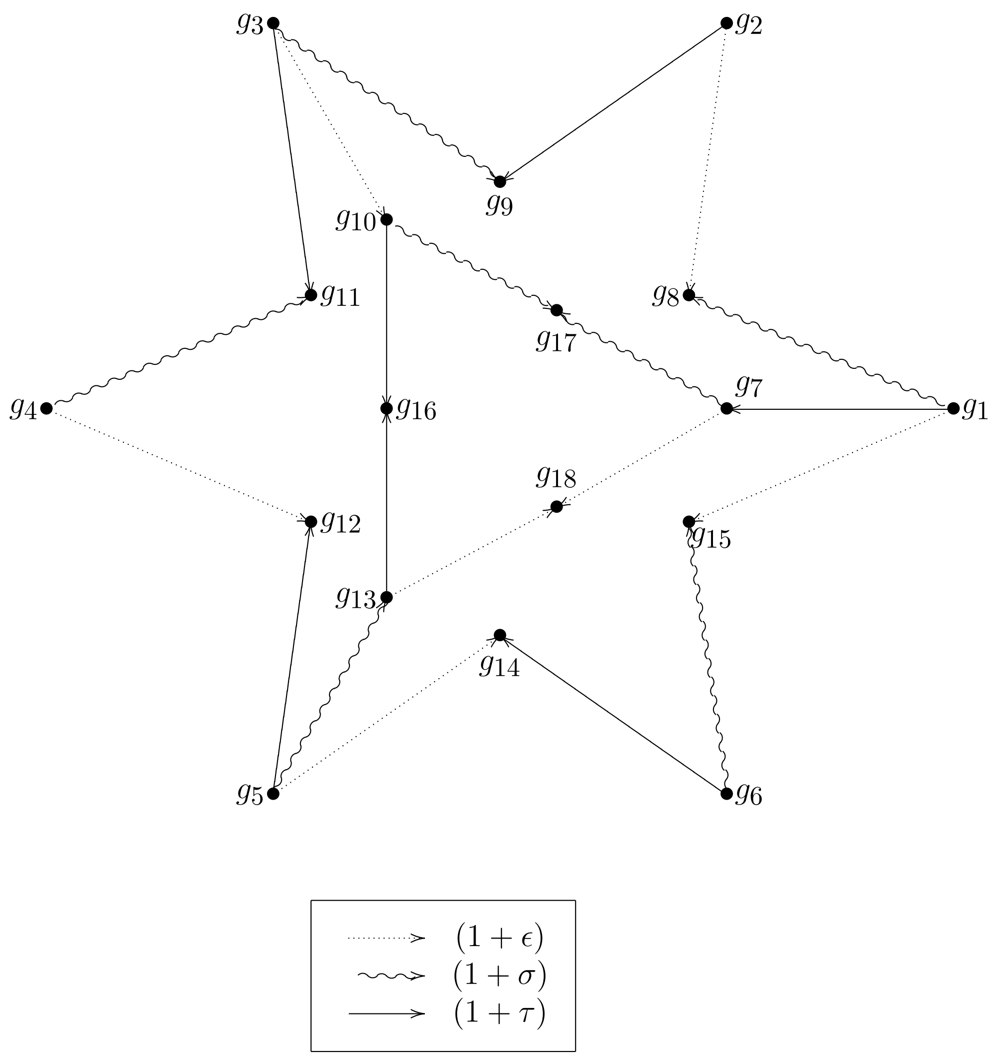
$$Z_a^* = \{(1-\sigma_{t_1})\cdots(1-\sigma_{t_a})d_{ij}^* : 1 \leq i \leq j \leq n,\, i < t_1 < \cdots < t_a \leq d\},$$

is a basis for J_a^* where d_{ij}^* is the dual of $\zeta([x_i, x_j])$ if $i \neq j$ and the dual of $\zeta(x_i^2)$ if $i = j$.

Example 5.2.8. *Consider the 2-elementary abelian group $S^{[2]}$ on three generators with minimal presentation*

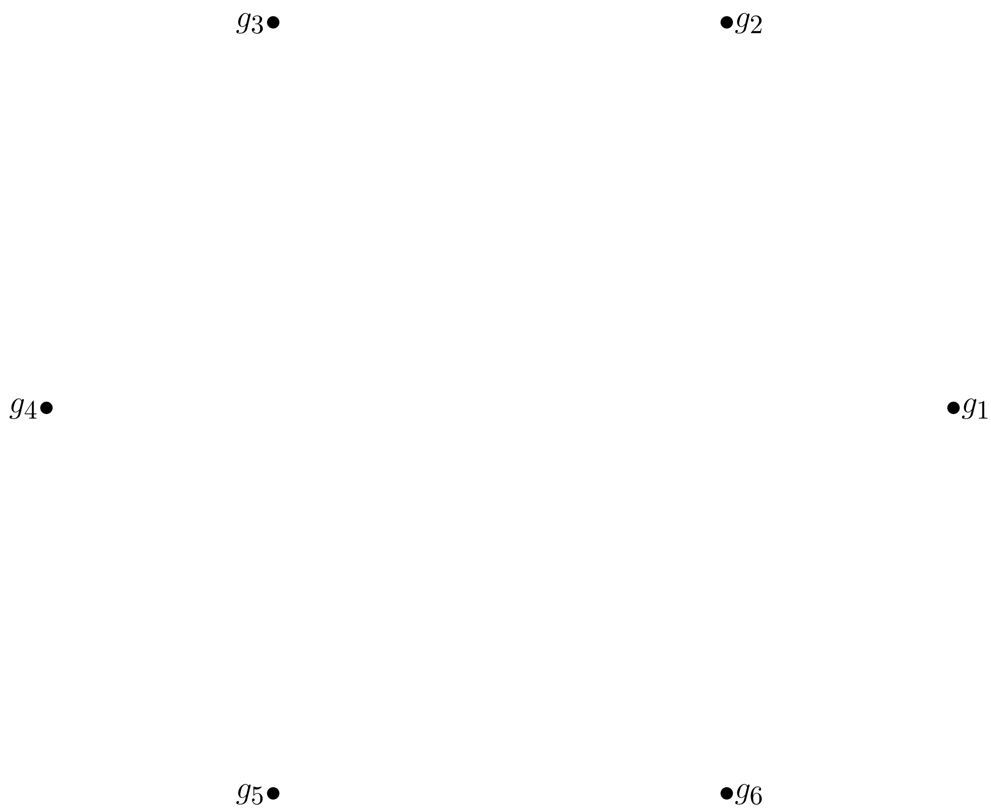
$$S^{[2]} = \langle x, y, z | x^2 = [x, y] = y^2 = [y, z] = z^2 = [x, z] = 1\rangle.$$

Then $M = \langle \zeta(x^2), \zeta([x, y]), \zeta(y^2), \zeta([y, z]), \zeta(z^2), \zeta([x, z])\rangle$ is generated as $S^{[2]}$-module *and graph with the action indicated*



The first module J_1 in the Socle series is generated by

$$
\begin{aligned}
g_1 &= (\sigma(1+\epsilon), 0, \epsilon(1+\sigma)) \\
g_2 &= ((1+\sigma), 0, 0) \\
g_3 &= (\sigma(1+\tau), \tau(1+\sigma), 0) \\
g_4 &= (0, (1+\tau), 0) \\
g_5 &= (0, \tau(1+\epsilon), \epsilon(1+\tau)) \\
g_6 &= (0, 0, (1+\epsilon)).
\end{aligned}
$$



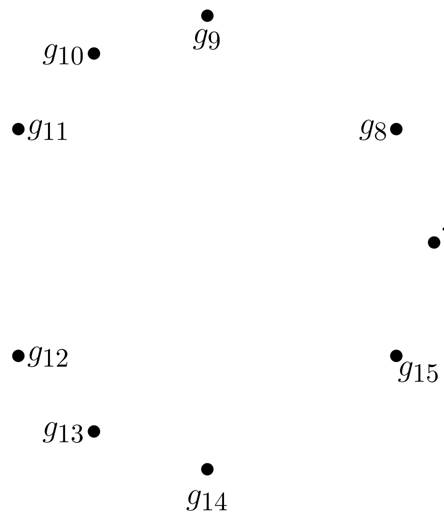
The Module J_2 is generated by

$$g_7 = (1+\tau)g_1 \qquad g_8 = (1+\sigma)g_1 \qquad g_9 = (1+\tau)g_2$$

$$g_{10} = (1+\epsilon)g_3 \qquad g_{11} = (1+\tau)g_3 \qquad g_{12} = (1+\epsilon)g_4$$

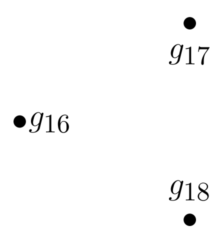
$$g_{13} = (1+\sigma)g_5 \qquad g_{14} = (1+\epsilon)g_5 \qquad g_{15} = (1+\sigma)g_6$$

But $\dim J_2 = 8$ *because* $g_7 + g_{11} + g_{15} = 0$. *This is the subgraph*



And finally the module J_3 *is generated by*

$$\begin{aligned} g_{16} &= (0, (1+\sigma)(1+\tau)(1+\epsilon), 0) = (1+\tau)(1+\epsilon)g_3 \\ g_{17} &= ((1+\sigma)(1+\tau)(1+\epsilon), 0, 0) = (1+\sigma)(1+\tau)g_1 \\ g_{18} &= (0, 0, (1+\sigma)(1+\tau)(1+\epsilon)) = (1+\epsilon)(1+\sigma)g_5 \end{aligned}$$



Theorem 5.2.9. *Let* S *be a free pro-p-group over* d *elements. Let* $S^{(m)}$ *be the m-Th group in the descending central central series of* S *and the quotient group* $S^{[m]}$ *as in section* 3. *Let*

$$H^1(S^{(m)})^{S^{[m]}} = J_1^* \subset J_2^* \subset \cdots J^* = H^1(S^{(m)})$$

be the socle series of the $S^{[m]}$*-module* $H^1(S^{(m)})$. *Then* $\dim J_1^* = k_m$ *and* $\dim J_2^* = k_{m+1}$.

Proof. Consider the short exact sequence $1 \to S^{(m)} \to S \to S^{[m]} \to 1$ with its associated five term exact sequence

$$1 \to H^1(S^{[m]}) \to H^1(S) \to H^1(S^{(m)})^{S^{[m]}} \to H^2(S^{[m]}) \to H^2(S).$$

Because S and $S^{(m)}$ are free groups it is clear that $H^1(S^{(m)})^{S^{[m]}} \simeq H^2(S^{[m]})$ this with theorem 3.2.1 proves the first statement. To see the second statement consider the exact sequence of $S^{[m]}$-modules

$$1 \to J_1^* \to J^* \to \frac{J^*}{J_1^*} \to 1$$

and the associated long exact sequence in cohomology

$$1 \to J_1^* \to J^* \to \left(\frac{J^*}{J_1^*}\right)^{S^{[m]}} \to H^1(S^{[m]}, J_1^*) \to H^1(S^{[m]}, J^*) \to H^1\left(S^{[m]}, \frac{J^*}{J_1^*}\right) \to \cdots$$

then by theorem 3.2.1

$$J_2^* \simeq \left(\frac{J^*}{J_1^*}\right)^{S^{[m]}} \simeq Ker : H^1\left(S^{[m]}, H^1\left(\frac{S^{(m)}}{S^{(m+1)}}\right)\right) \to H^1(S^{[m]}, H^1(S^{(m)}))$$

The last kernel by theorem 3.3.1 has dimension the Witt number d_{m+1} where from it follows the second statement. $\square$

Example 5.2.10. *As in section 3 consider the quotient group $S^{[3]}$ on two generators. Then the $S^{[3]}$-module $M^* = H^1(S^{(3)})$ has dimension 33 and socle series*

$$H^1(S^{(3)})^{S^{[3]}} = J_1^* \subset J_2^* \subset J_3^* \subset J_4^* \subset J_5^* \subset J_6^* \subset J_7^* = H^1(S^{(3)})$$

and respectively have dimensions $5 \leq 8 \leq 14 \leq 22 \leq 28 \leq 31 \leq 33$ and is generated by the dual of the k images of the elements of $S^{(3)}$

$x^4, y^4, [x,y]^2, [x,x,y], [y,x,y]$

$[x^4, y], [x^4, y^2], [x^4, [x,y]], [x^4, y^3];, [x^4, y[x,y]], [x^4, y^2[x,y]], [x^4, y^3[x,y]]$

$[y^4, x], [y^4, x^2], [y^4, [x, y]], [y^4, xy], [y^4, x^3], [y^4, x^2[x, y]], [y^4, xyx^2]$

$[[x, y]^2, x], [[x, y]^2, y], [[x, y]^2, x^2], [[x, y]^2, y^2], [[x, y]^2, [x, y]], [[x, y]^2, xy^2], [[x, y]^2, yx^2], [[x, y]^2, x^2y^2]$

$[[x, x, y], x], [[x, x, y], y], [[x, x, y], y^2], [[x, x, y], xy], [[x, x, y], y^2]$

$[[y, x, y], y]$.

5.3 The cohomology group $H^1(G, H^1(R))$

In order to compute the cohomology group $H^1(G, M^*)$ we will compute the cocycles and coboundaries. G will denote a finite p-group finitely generated over the set $\{x_1, \cdots, x_d\}$ and minimal presentation as in 5.1 and the normal group R as the normal closure of $\{r_1, \cdots, r_l\}$ in S.

Theorem 5.3.1. *The dimension of the coboundaries of G with coefficients in M^* is*

$$\dim H^1(R) - \dim H^2(G).$$

Proof. $B^1(G, M^*) = \{\psi_m : G \to M | \psi_m(g) = (1 + g) \cdot m, \text{ for } m \in M^*\}$, and $\psi_m \equiv \psi_{m'}$ only if $\psi_m - \psi_{m'} \in (M^*)^G$ then by theorem 3.2.1 the proof is complete. □

With the above proposition and the proposition 5.2.1 there is a beautiful equation

$$\dim B^1(G, M^*) = 1 + |G|(\dim H^1(G) - 1) - \dim H^2(G).$$

Theorem 5.3.2. *The $Z^1(G, M)$ is given by the kernel of the matrix*

$$D = \left(\frac{\partial r_i}{\partial x_j}\right)_{ij} : \bigoplus^{d} M^* \to \bigoplus^{l} \mathbb{F}_p[G]$$

where M is the G-module generated by $\{\zeta(r_i) : i = 1, \cdots, l\}$.

Proof. The key idea is that the elements of $Z^1(G, M^*) = \{\psi : G \to M^* | \psi(ab) = \psi(a) + a\psi(b)\}$ satisfy the Fox-Condition. For a given $\psi \in Z^1(G, M^*)$ denote $\psi_i :=$

$\psi(x_i)$. Observe that every ϕ can be extended to a function $\overline{\psi} : S \to M^*$

$$\begin{tikzcd} G \arrow[r, "\psi"] & M^* \\ S \arrow[u] \arrow[ur, dashed, "\overline{\psi}"] & \end{tikzcd} \tag{5.8}$$

making $\overline{\psi}(x_i) := \psi_i$. Every cocycle $\psi \in Z^1(G, M^*)$ is of course a cocycle in $Z^1(S, M^*)$. Let $\overline{\psi}$ be a cocycle in $Z^1(S, M^*)$ then it can be restricted to a cocycle $\psi \in Z^1(G, M^*)$ if and only if is trivial on the elements of R i.e.

$$Z^1(G, M^*) = \{\psi \in Z^1(S, M^*) | \psi(R) \equiv 0\}.$$

Let ψ as above and suppose that $R = \overline{\langle r_1, \cdots, r_l \rangle}$ is the normal closure of the group generated by the $r's$. With the notation of section 5.1 for $r \in S$ because the cocycles satisfy the Fox-Condition we have

$$\psi(r) = \left(\frac{\partial r}{\partial x_1}, \cdots, \frac{\partial r}{\partial x_d} \right) \cdot (\psi_1, \cdots, \psi_d) \in M^*$$

A cocycle $\psi \in Z^1(S, M^*)$ can be restricted to a element in $Z^1(G, M^*)$ if $\psi(r_i) = 0$ because it is a derivation and a it is determined by the images ψ_i. Then we are looking for the element $(\psi_1, \cdots, \psi_l)$ such that

$$\begin{array}{rcl} \bigoplus^{d} M^* & \to & \bigoplus^{l} \mathbb{F}_p[G] \\ (\psi_1, \cdots, \psi_l) & \mapsto & \left(\frac{\partial r_i}{\partial x_j} \right)_{ij} \cdot (\psi_1, \cdots, \psi_d) = 0 \end{array}$$

This is the kernel of the matrix of derivations for the relations of R. □

Example 5.3.3. *Consider the group $S^{[2]}$ with two generators x, y and presentation*

$$C_2 \times C_2 = S^{[2]} = \langle x, y | x^2 = y^2 = [x, y] \rangle.$$

To avoid confusion we will denote

$$\mathbb{F}_2[S^{[2]}] = \{0, 1, \sigma, \tau, \sigma + \tau, 1 + \sigma, 1 + \tau, 1 + \sigma + \tau\}.$$

M *is the submodule of* $\bigoplus^2 \mathbb{F}_2[S^{[2]}]$ *generated by the images of* $\zeta(x^2), \zeta(y^2)$ *and* $\zeta([x, y])$ *as a* $S^{[2]}$*-module. The dimension of* M *over* $\mathbb{F}_2$ *is* 5*. If* $g_1 = \zeta(x^2) = (1 + \sigma, 0), g_2 = \zeta([x, y]) = (\sigma(1 + \tau), \tau(1 + \sigma)), g_3 = \zeta(y^2) = (0, 1 + \tau)$ *and the other generators are* $g_4 = (1+\tau)g_1$ *and* $g_5 = (1+\sigma)g_3$ *we have the next explicit diagram for the* $S^{[2]}$*-module* M*.*

$$\begin{tikzcd}
& g_4 & & g_5 & \\
g_1 \arrow[ur, "1+\tau"] & & g_2 \arrow[ul, "1+\sigma"'] \arrow[ur, "1+\tau"] & & g_3 \arrow[ul, "1+\sigma"']
\end{tikzcd} \tag{5.9}$$

With dual module M^*

$$\begin{tikzcd}
g_1^* & & g_2^* & & g_3^* \\
& g_4^* \arrow[ul, "1+\tau"] \arrow[ur, "1+\sigma"'] & & g_5^* \arrow[ul, "1+\tau"] \arrow[ur, "1+\sigma"'] &
\end{tikzcd} \tag{5.10}$$

And Lowey's Series

$$J_0 = \langle g_1^*, g_2^*, g_3^* \rangle \subset J = M^*.$$

The dimension of the coboundaries $B^1(S^{[2]}, M^*)$ *equals two represented by*

$$\begin{aligned} \psi_{g_4^*}(x) &= g_1^* & \psi_{g_5^*}(x) &= g_2^* \\ \psi_{g_4^*}(y) &= g_2^* & \psi_{g_5^*}(y) &= g_3^* \end{aligned}$$

The cocycles are the kernel of the matrix

$$\begin{bmatrix} 1+\sigma & 0 \\ \sigma(1+\tau) & \tau(1+\sigma) \\ 0 & 1+\tau \end{bmatrix} : \bigoplus^2 (M^*) \to \bigoplus^3 \mathbb{F}_p[S^{[2]}].$$

then ψ_1 *and* ψ_2 *belongs to* $\ker(1+\sigma)$ *and* $\ker(1+\tau)$ *respectively. Then* $\psi_1, \psi_2 \in \langle g_1*, g_2*, g_3*\rangle$ *and dimension of* $Z^1(S^{[2]}, M^*)$ *is six.*

$$\dim H^3(S^{[2]}) = \dim H^1(S^{[2]}, M^*) = \dim Z^1(S^{[2]}, M^*) - \dim B^1(S^{[2]}, M^*) = 4.$$

Conclusion: In this thesis we obtained a complete information of the first two cohomology groups of certain important quotients of free pro-2-groups. We also obtained a partial information on the third cohomology of these groups. The key for this progress is the structure of certain modules. We plan to refine these techniques in order to obtain a full description of all three cohomology groups and their multiplicative properties. We further found a very interesting connection between higher commutators and elements in finite fields. We also consider various possible applications of these connections with in Galois theory and in coding theory.

Bibliography

[1] Adem, A. *Lectures On The Cohomology of Finite Groups*, Contemporary Mathematics 436 (2007), 317-334.

[2] Adem, A. Karagueuzian, D.B. and Mináč, J. *On The Cohomology of Galois Groups Determined by Witt Rings*, Advances in Mathematics 148, pp.105-160 (1999).

[3] Adem, A. and Pakianathan, J. *On the Cohomology Of Central Frattini Extension*, Journal of Pure and Applied Algebra 159, pp.1-14 (2001)

[4] Bogomolov, F. Tschinkel, Y. *Commuting Elements in Galois Groups of Function Fields* To appear.

[5] Chebolu, S. Mináč, J. *Auslander-Reiten sequences as appetizers for homotopists and arithmeticians*, Annales des sciences mathematiques du Quebec 32 (2008), no 2, 139-157.

[6] Chebolu, S. Efrat, I. Mináč, J. *Quotients of Absolute Galois Groups which determine the entire Galois Cohomology*, To appear.

[7] Dixon, J.D. Du Sautoy M.P.F. Mann, A. and Segal, D. *Analytic Pro-p Groups*, Cambridge studies in advanced mathematics. (1999).

[8] Douady, A. *Determination d'un groupe de Galois*, C.R. Acad. Sci. Paris, 258, 5305-8. 1964.

[9] Evens, L. *The Cohomology of Groups* Oxford Science Publications. 1991.

[10] Fenn, R. *Techniques of Geometric Topology* London Mathematical Society lecture note series, Volume 57. Cambrige University Press 1983.

[11] Fox, R. *Free Differential Calculus, I: Derivation in the Free Group Ring*, Annals of Mathematics 57 (3): 547560. 1953.

[12] Hall, M. Jr. *The Theory of Groups*, The Macmillan Company. (1959).

[13] Harbater, D. *Fundamental groups and embedding problems in characteristic* p, In Recent deelopments in the inverse Galois problem, pp 353-69, Contemp. Math, 186. American Mathematical Society, Providence, RI.(1995).

[14] Hochschild, G. Serre, J-P *Cohomology of Groups* Transactions of the American Mathematical Society Vol 74, No1 (Jan. 1953) pp. 110-134.

[15] Holt, D. Eick, B. and O'Brien E. *Handbook of Computational Group Theory*, Chapman & Hall/CRC Press. (2005)

[16] Ihara, Y. *On Galois Respresentations arising from towers of coverings of* $\mathbb{P}^1$ $\{0, 1, \infty\}$. Invent. Math 86 (1986, 427 - 459.)

[17] Johnson, D.L. *Presentation of Groups* Cambridge University Press 1990, 1997.

[18] Karagueuzian, K. Labute, J. Mináč, J.*The Bloch-Kato Conjecture and Galois Theory*, Ann. Sci. Math. Qubec (to appear)

[19] Kuhn, N.J. *Primitives and Central Detection Numbers in Groups Cohomology*, Adv. Math. 216 (2007), no. 1, 387–442. 20J06.

[20] Labute, J.P. *Classification of Demushkin Groups*, Canad. J. Math. 19 (1967), 106-132.

[21] Mináč, J. Spira, M. *Witt Rings and Galois Groups* The Annals of Mathematics. Second Series, Vol. 144, No. 1 (Jul., 1996), pp. 35-60

[22] Neukirch, J. Schmidt, A. Wingberg, K. *Cohomology of Number Fields* Springer (1991).

[23] Quillen, D. *The Mod 2 Cohomology Rings of Extra-special 2-groups and the Spinor Groups*, Math. Ann. 194, 197-212 (1971).

[24] Ribes, L. Zalesskii, P. *Profinite Groups*, Springer (1991).

[25] Serre, J.P. *Galois Cohomology*, Springer (1997).

[26] Shafarevich, I.R. *Factors of a descending central series.* Mathematical Notes. Vol. 45, No. 3, pp. 262-264, March, 1989.

[27] Shafarevich, I.R. *On p-extensions.* Mat. Sbornik, 20, 351-363: Englis transl. Amer. Math. Soc. Transl. Ser. (2), 4, 59-72. 1947.

[28] Snaith, V. *Topological Methods in Galois Representation Theory*, John Wiley & Sons, (1989).

[29] Wilson, J. *Profinite Groups*, Oxford (1998).

Chapter 6

Curriculum Vitae

CURRICULUM VITAE

for

GermanCombariza

PERSONAL DATA

Full Name: Germán Andrés Combariza Gonzalez

ACADEMIC BACKGROUND

Major in Mathematics with emphasis in Group Theory

Universidad de los Andes

Bogotá, Colombia

Master in Mathematics

Universidad de los Andes

Bogot, Colombia

CURRENT STUDIES

Ph.D in Mathematics

Fifth Year

University of Western Ontario

London, ON Canada

TEACHING EXPERIENCE

- Instructor: University of British Columbia, Vancouver Canada. Calculus III. Multivariable Calculus. Integral Calculus with Applications. Differencial Calculus for Social Science. 2007 - 2008.
- Instructor: Differential Calculus, Integral Calculus, Linear Algebra, Discrete Mathematics. 1999-2002, 2004, 2005.(One or two sections per semester) at La Universidad de los Andes.
- Instructor: Differential and Integral Calculus, Linear Algebra and applications (Linear Programming). 2004, 2005 at La Universidad Externado de Colombia.
- Instructor: Summer Course. Colegio San Carlos. June 2001.
- Instructor: Summer Course. A Logical Approach to Discrete Math. June 2002.
- Instructor: Colegio Santa Maria. 2002-2003.

COMPUTER EXPERIENCE

- C++, Assembler, Java, LaTeX, Office, GAP.

LANGUAGES

- Spanish(Native), English.

RESEARCH WORKS AND PUBLICATIONS

- *Extensiones de Grupos.* Undergraduate thesis in Mathematics, 2001.
- *The Hodge Conjeture in Torics Varieties.* Master thesis, 2004.
- *Descending Central Series of Free Pro-p-Groups.* Ph.D. Thesis.

TALKS

- *A Problem in Knot Theory*, Geometric and Topological Methods for Quantum Field Theory July 8-27 2003, Villa de Leyva Colombia.
- *An Introduction in Graph Theory*, The XIII Encuentro de Geometra y sus aplicaciones (XIII meeting of Geometry and applications), June 19-21 2003.
- *Topics In Commutative Algebra*, Commutative Algebra with a View Toward Algebraic Geometry. August - November 2004, Universidad de los Andes, Bogot Colombia.
- *Cohomology of Groups*, Learning Seminar in Topology. UBC Vancouver Canada. April 12, 19 2006.
- *The Mod 2 Cohomology Rings of Extra-special 2-groups*, Learning Seminar in Topology. UBC Vancouver Canada. November 6 2006.

CONFERENCES AND WORKSHOPS

- Participant at CIMPA's Summer School "Geometrical and Topological Methods for Quantum Field Theory", held at Villa de Leyva, Colombia, in July 1999.
- Participant at the II Encuentro Regional de Logica y Computacion (II Regional meeting in logic and computation), May 20-24 2002, Valle, Colombia.
- Participant (with full support) SOCIEDAD BRASILEA DE MATEMTICAS (SBM) SOCIEDAD MATEMTICA PERUANA (SMP) , June-19 July-20 2000, Lima, Peru.
- Participant at the XIII Encuentro de Geometra y sus aplicaciones (XIII meeting of Geometry and applications), June 20-22 2002.

- Participant at the I Encuentro de Aritmtica (I Arithmetic Meeting) 20-22 2002.
- Participant at CIMPA's Summer School "Geometrical and Topological Methods for Quantum Field Theory", held at Villa de Leyva, Colombia, in July 2003. (Full Support).
- Participant at II EMALCA Y XV EVM. Mrida, Venezuela . September 8 to 14 2002.
- Participant at III EMALCA 19 to 28 August 2003. Morelia, Michoacn Mxico. (Full support).
- Participant at II EMALCA Y XV EVM. Mrida, Venezuela . September 8 to 14 2002.
- Participant at III EMALCA 19 to 28 August 2003. Morelia, Michoacn Mexico. (Full support).
- Participant at the ABC Algebra Workshop. April 8-9, 2006. University of British Columbia. Vancouver, BC, Canada
- Participant at PIMS/UNAM Algebra Summer School. July 1-6, 2006. Banff International Research Station for Mathematical Innovation and Discovery. Banff, AB.
- Participant at the ABC Algebra Workshop. April 14-15 2007. University of Alberta. Edmonton, AB.
- Participant at the ABC Algebra Workshop. April 12-14 2008. Simon Fraser University. Vancouver, BC, Canada.

AREAS OF INTEREST

- Cohomology of Groups.

- Galois Cohomology.
- Profinite Groups.