6-28-2024 11:00 AM

Special quotients of absolute Galois Groups with Applications in Number Theory and Pythagorean fields

Oussama Rayen Hamza, *Western University*

Supervisor: Jan Minac, *The University of Western Ontario*
Co-Supervisor: Christian Maire, *Université de Franche-Comté, Institut FEMTO-ST, Besançon France*
A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

Abstract

This document introduces the work of Hamza and his collaborators during his PhD studies. Hamza works on profinite Galois Theory: more precisely, his work focuses on realisation of pro-p Galois groups over some fields with specific properties (filtrations, cohomology ...) for a fixed prime p. This thesis gives a particular attention to number fields and Pythagorean fields.

The first chapter studies connections between the work of Brumer on compact modules and the work of Lazard on filtrations. Using results of Koch and Shafarevich, the previous connections are applied to the theory of pro-p groups and fields extensions. This chapter sets the background to study the rest of the work of Hamza and his collaborators.

The second, third and fourth chapters are papers written by Hamza and his collaborators, in which they investigate extensions of number fields with restricted ramification and non trivial cohomology. The fifth chapter is a work in preparation between Hamza, Maire, Mináč and Tân where they introduce a class of pro-2 groups that they call Δ-Right Angled Artin Groups (Δ-RAAGs) and show that the ones occuring as absolute Galois groups are exactly the ones which are absolute Galois groups of Formally real Pythagorean fields of finite type.

The last chapter concludes with a complete answer to a question from Mináč-Rogelstad-Tân for which Hamza had already given a partial answer for mild groups.

Keywords: Action on pro-p groups, Zassenhaus and lower central filtrations, graded and filtered Lie algebras, Cohomology, Hilbert and Poincaré series, Mild groups, Right Angled Artin Groups and Algebras, Absolute Galois groups, Restricted ramification, Formally real Pythagorean fields, Koszulity

Summary for Lay Audience

Galois theory was originally introduced by Evariste Galois, a young French mathematician, in the 19-th century to characterise polynomial equations which are solvable by radicals, i.e. the solutions can be expressed by a formula involving only integers, n-th roots, additions and multiplications. For this purpose, Galois studied the group permutation of the solutions, which is called Galois group. He was one of the founder of modern Group theory.

Before Galois, it was already known that polynomial equations of degree less than 4 are all solvable by radicals. Abel, Galois and Ruffini were able to exhibit, for every integer n larger than 5, polynomials of degree n which are not solvable by radicals. As an application, some problems from Antiquity were solved: doubling the cube, trisecting the angle and characterising all polygons which are constructible with compasses and straightedges.

A more modern version of Galois' ideas focuses on studying all Galois groups of all possible equations together collecting them into one large infinite group called the "absolute Galois group". Due to its sheer size, this group is extremely difficult to understand and challenges many mathematicians even today. My work, together with my collaborators, aims to find new facts about this group.

Co-Authorship Statement

Chapters $2, 3, 4, 5$ and 6 of this Thesis are original work from Hamza and his collaborators Ján Mináč, Christian Maire and Nguyên Duy Tân (both independent and joint), during his PhD Thesis.

Chapter 2 is based on [45], which was written in collaboration with Christian Maire. The text was mostly written by Christian Maire with consultation with Hamza.

Chapter 3 is based on [44], where Hamza is the sole author.

Chapter 4 is based on [43], where Hamza is the sole author.

Chapter 5 is based on [46], which was done in collaboration with Ján Mináč, Christian Maire and Nguyên Duy Tân. This paper is mostly grounded on Hamza's master Thesis and Mináč' PhD Thesis, and the text was mostly written by Hamza, with consultation with co-authors.

Chapter 6 is an original work from Hamza where he gave a complete answer to [92, Question 2.13]. Hamza already partially answered to this question in [44].

Acknowledgments

My deepest gratitude goes to Christian Maire and Ján Mináč who both accepted to supervise my PhD thesis. I learnt a lot from both of them, they read carefully my work and gave several fundamental pieces of advice. I am also grateful to Leslie Mináčová for important technical help, and to Philippe Gille, Mathieu Florence and Laurent Berger for introducing me to Ján and Christian. I also appreciate the supervisory thesis committee members for their careful reading and following my work during my PhD thesis: Tatyana Barron and Chris Hall. I am also grateful to Mathieu Florence, Tatyan Barron, Anibal Medina-Mardones and Pauline Barmby for accepting to be examiners of my thesis.

Special thanks to Ján Mináč, Christian Maire, John Labute, Thomas Weigel, Andrei Jaïkin-Zapirain, Henrique Souza, Mathieu Florence, Donghyeok Lim, Michal Cizek, Michael Rogelstad and Chris Hall who allowed me to substantially improve the thesis manuscript.

During my PhD thesis, I had several interesting mathematical discussions and collaborations that played an influencal role in my mathematical work. Let me thank all of the people involved: Thomas Weigel, John Labute, Donghyeok Lim, Nguyên Duy Tân, Tung Nguyên, Andrei Jaikin-Zapirain, Henrique Souza, Antonella Perrucca, Elyes Boughattas, Baptiste Cerclé, Farshid Hajir, Ravi Ramakrishna, Simion Filip, Shubhankar Bhatt, Sayantan Roy Chowdhury, Martin Fatou, Rachad Bentbib, Mohamed Moaker, Juan Esteban Rodriguez Camargo, Michal Cizek, Jarl Flatten Gunnar Taxeras, Tao Gong, Michael Rogelstad, Ali Alkhairy, Lyle Muller, Prajwal Udanshive, Kumar Shukla, Steven Amelote, Larry So, Michael Francis, Vladimir Gorchakov. I am also thankful to Jacques Taillet, Pierre Lorenzon, Alberto Vezzani and Amaury Thuillier from whom I learnt a lot before my PhD studies.

I also had the chance to attend conferences and deliver several talks. I praise all of the organisors: Vivek Dewan, Elyes Boughattas, Claudio Quadrelli, Thomas Weigel, Christian Maire, Philippe Lebacque, Samuele Anni, Peter Stevenhagen, Philippe Elbaz-Vincent, Graham Ellis, Jennifer Park, Kevin Tucker, Félix Baril-Boudreaux, Leo Margolis, Gabor Wiese and Andrea Conti.

I am thankful to the math departement, my colleagues from UWO and my friends from Canada for accomodations to attend the previous talks and also for their interests in my thesis. Especially Manimugdha Saikia, Priya Bucha Jain, Alejandro Santacruz, Nathan Pagliaroli, Curtis Wilson, Babak Beheshti, Sepideh Bahrami, Zahra Shafiei, James Uren, Asghar Ghorbanpour, Albert Merza, Michael Payeur and Fowzeya Shararnek Elkassem.

I also praise my friends from France for their interest in my thesis: Hugo Guérin, Tarek Marcé, Lucille Marino, Thomas Rodelet and Jérémy Leroy. Let me also acknowledge

Benjamin Etchemendy, Clément Guillet, Thierry Tran, Sébastien Rizieri, David Lhomme, Sébastien Garzon, Michel Sautreuil, Maxhence Bouhier, Samuel Lepetre, Jean Marc Sam-Tow, Victor De Maghalles, Alexandre Brun, Stephane Picot, André Bouvil, Thierry, Nathalie and Lucas Dubois, Théo Le Meur, Victor et Marc Bonnel, An Toan Neyraud, Damian Nolan, Denis Grangier, Didier Poingt, Jacky Grivaux, Teddy Vintrou, Arzu Kalkan, Géraldine Soulat, Bachir Touati, Nuno De Barros, Joël and Agathe Couturier, Samy Mounder, Jeff Rey, Mélinda MacFarlane, Yannick Leroy, Patrick Pisani.

Let me finish to thank all of my family for their great support. I was deeply influenced by my grandfather Djendli Mohamed and my beloved mother Anissa Hamza for their strong dedication in their work and research. I also praised my father Mohamed Hamza, my aunt Samira Djendli, my brother Sofiane Hamza and my sister Chaïma Hamza for their great support in my daily life. Let me also acknowledge my grandmother Fatma Hamza, my aunts Zahia Salim, Amel Moussaoui, Mounia Zid, Malika Hamza, Sakina Mendjel, Fatiha Rachef, Lylia and Fatiha Djendli, Soraya, Hajira and Hajer Hamza, my uncles Abdessamed, Abderrahim Djendli, Chaabane, Faouzi, Messaoud, Reda, Riad Hamza, Abdelmajid, Abdelghani Djendli, Mohamed Moussaoui, Hassan Salim, Fakhar Zid and my cousins Kheir-eddine, Boubaker Mendjel and Mehdi Djendli.

Contents

Introduction

History and context

This document mostly deals with Galois theory, which allows us to reduce some problems from Field theory to Group theory. Galois originally introduced this theory in order to solve polynomial equations by radicals, but it gained more and more applications. Nowadays, people are interested in the following problem: given a field k, which groups are realisable as Galois groups over k? This question is the primary motivation for this thesis.

Fermat's Last Theorem

Non trivial integral solutions of the equation

$$x^n + y^n = z^n, \tag{FLTn}$$

with n a fixed integer larger than two, was one of the most important questions since the 17-th century (and since Antiquity for the case $n = 2$). The equation (FLT2) admits an infinite number of solutions, which are called Pythagorean triplets: for instance, if u and v are two fixed integers, then $(x := u^2 - v^2, y := 2uv, z := u^2 + v^2)$ satisfies (FLT2). This leads to the study of Pythagorean fields: the sum of two squares is a square. These fields were well investigated by Lam [67, 68], Mináč and Spira [87, 94, 95], Jacob [51], Marshall [82], Efrat-Haran [22], Griffin [36], Golmankani [32]... In particular, this thesis studies formally real Pythagorean fields k of finite type (RPF), i.e. (-1) is not a square and $k^\times/k^{2\times}$ is a finite group, where $k^\times$ (resp. $k^{2\times}$) is the group of invertible elements (resp. invertible squares) in k. Observe also that these fields have strong connections with quadratic forms and realisation of torsion-free Witt rings (see [26, 52, 51, 67]).

When n is strictly larger than two, it was conjectured by Fermat in the 17-th century that (FLTn) does not have non trivial solutions, and this was recently proved by Wiles and collaborators. The proof was long and difficult, we refer to [118] and [10] for a complete exposition. This result is well known as the Fermat last Theorem.

The work of Golod and Shafarevich

A first partial proof of Fermat's Last Theorem was given by Kummer in the 19-th century when n is a regular prime. Siegel conjectured in 1964 that $e^{-1/2}$ of prime numbers are regular,

but it is still unknown yet whether there is an infinite number of them [136]. This leads us to the imbedding problem: Is a number field k with class group h_k always embedded into a finite extension K with class group h_K trivial? It was conjectured that the imbedding problem always has a solution, but Golod and Shafarevich [33] gave as a counterexample the field $k := \mathbb{Q}(\sqrt{-2 \times 3 \times 5 \times 7 \times 11 \times 13})$.

The idea of Shafarevich was to study (pro)-p extensions, i.e. compositum of some Galois extensions with degree a power of p. More precisely, he studied presentations of Galois groups of p-extensions via generators and relations, and inferred a group theoretical criterion on group presentations, which allowed him to obtain information on the Galois group, and hence on the extension. Presentation of groups also played an important role in the development of general group Theory [79] and [78, Chapter 2]. With Golod in [33], they succeed in making this idea precise using filtrations/gradations and Lie algebra techniques. we refer the reader to [12] and [15, Chapter IX] for further details, and [59] for an exposition on p-extensions.

Gocha series and mild groups

The Golod-Shafarevich proof was based on the study of an invariant associated to a pro-p group: gocha series; which allows us to read the cardinality and the cohomology of the underlying pro-p group. Furthermore, from a pro-p group presentation, we infer (partial) information on the gocha series. Lazard [69, Théorème 3.11, Appendice A.3] was able to read possible Lie structures over $\mathbb{Q}_p$ on pro-p groups (also called analytic groups) from their gocha series's poles: this is "l'Alternative des Gocha". Let us also quote the recent work of Panov, Veryokin, Davis and collaborators [107, 132, 131, 16] who studied filtrations of Coxeter groups using Lazard's results [69] and inferred geometrical applications.

Labute and Mináč [62, 66] and [65] introduced a criterion on pro-p group presentations, that is called *mild*, to infer pro-p groups with prescribed gocha series. Forré [29] also proposed another approach to mild groups from ideas of Koch [60]. To proceed, they mostly combined ideas developped by Anick [3, 4, 5, 1] in Knot theory and Morishita [100, 99] who studied analogies between knots groups and Galois groups with restricted ramification. Let us also quote the recent work of Efrat [21] who generalised some parts of Morishita's work.

As an application, Labute obtained infinite extensions with Tame ramification (indeed of cohomological dimension 2). These ideas where also expanded by Hajir-Maire-Ramakrishna [41] with the "cutting tower strategy" which allows them to obtain (tame) towers of number fields with prescribed ramification and specific cohomological properties. Let us also quote Hamza-Maire [45], where they apply cutting tower strategy for infinite splitting. Mild groups are also an active topic of research in pro-p group Theory. For instance they played a key role in the recent work of Jaikin-Souza [53] on pro-p groups with Sylvester completed group algebra. Let us also quote the work of Mináč and his collaborators [98] who related Koszulity and mildness and the work of Hamza [44, 43] which is studied in the third and fourth chapters of this document.

The Fontaine-Mazur conjecture states that every analytic extension with finite tame ramification is finite. Hajir, Larsen, Maire and Ramakrishna showed in [38] that this con-

jecture does not hold when the set of prescribed tame ramification is infinite. Let us refer the reader to the work of Boston [9, 8] who gave a group theoretical interpretation of Fontaine-Mazur conjecture using Lazard's results [69]. Let us also quote Hajir-Larsen-Maire-Ramakrishna [38] who were interested in tame extensions, and Lim-Maire [74] who worked on analytic extensions.

Realisation of absolute Galois groups

Maximal p-extensions and their Galois groups allow us to collect all p-extensions. We study the converse problem: which pro-p groups are realisable as pro-p absolute Galois groups? Mináč and Tân [96, 97] recently introduced two conjectures which give us necessary conditions on these groups: the Massey vanishing and the Kernel Unipotent conjectures. The first conjecture was investigated by several mathematicians during the last decade, let us quote Merkurjev-Scavia [84, 85, 83], Snopce-Zalesski [122], Blumer-Quadrelli-Weigel [7], [110, 109], Efrat [23, 24].

The situation is of particular interest for formally real Pythagorean fields of finite type (RPF). Mináč [87] obtained a detailled classification of all pro-2 absolute Galois groups of formally real Pythagorean fields of finite type, as a minimal collection of pro-2 groups containing $\mathbb{Z}/2\mathbb{Z}$ and stable by coproduct and some "special" semi-direct products. Quadrelli proved the Massey vanishing conjecture for RPF, and in Chapter 5, we prove the Kernel Unipotent conjecture for these fields.

Realisation of specific quotients of the absolute Galois group (more precisely Galois group with prescribed ramification) is also an active problem, let us quote [105, 42, 25, 11] and others.

Summary

In this thesis, we pay particular attention to the following groups:

(i) The Galois group of the maximal extension, unramified outside a set of primes S which does not contain places above p (tame case), with underlying field rational numbers or quadratic extension with trivial p-class group,

(ii) Quotients of Galois groups over p-rational fields, i.e. quotients of artihmetic situations with free Galois groups,

(iii) Absolute Galois groups of formally real Pythagorean fields of finite type.

Results and outline of the Thesis

The absolute Galois group of a field k is mysterious in general but some information is known. For instance Neukirch and Uchida [129] showed that this group characterises number fields, but Lubotzky and Neftin [77] showed that p-Sylow subgroups are not sufficient. We study some specific (p-)quotients.

Chapter 1: Generalities

In the first chapter, we study generalities on profinite (and especially pro-p) groups; the work of Lazard and Brumer on compact and graded algebras, that we apply to pro-p groups; then we finish by studying Galois Theory to infer results about field extensions from pro-p groups.

If k is a number field, let S be a finite set of primes in k and denote by $\overline{k_S}$ the maximal extension of k unramified outside S. It is already known, see [58, Theorem 1.48] and [121, Theorem 2], that $\mathrm{Gal}(\overline{k_S}/k)$ is strongly complete, i.e. for every integer d there exists a finite number of algebraic extensions of degree d which are unramified outside S. Serre [119], Nikolov and Segal [104] investigate connections between strong completness and finitely generated profinite groups. However, it is still unknown whether the group $\mathrm{Gal}(\overline{k_S}/k)$ is finitely generated. We recall these results in Part 1.1.

A natural connection between groups and compact algebras is given by the completed group algebra. In Part 1.2, we focus on the study of these algebras. Graded algebras and their Hilbert series are heavily used in the proof of the Golod-Shafarevich Theorem and "l'Alternative des Gocha". In this part, we recall results from Brumer and Lazard on compact and graded algebras (especially strong freeness and Koszulity) that allow us to infer cohomological results. Compact and graded algebras are connected by the Grad functor. The typical exemple is given by Right Angled Artin Algebras, studied in this part.

Part 1.3 focuses on the completed group algebra of pro-p groups and their associated gradations. We give a particular attention to mild groups, introduced by Labute and Mináč [62] and [66] which illustrated these connections and have cohomological consequences.

We finish with Part 1.4 where we discuss Galois Theory, in order to relate previous results on group Theory with field extensions. Our main fields studied are local, global and RPF. We recall Koch's [59] results on p-extensions on local and number fields; then we finish by discussing standard results on Pythagorean fields [67] and the Milnor conjecture [86], which relates Witt rings, Cohomology and absolute Galois groups. Of course, the Milnor conjecture holds for any fields, but we prefer to discuss it only for RPF, as we infer in Chapter 5 a complete understanding of their absolute pro-2 groups which is also closely related to the number of orderings and cohomology.

Chapter 2: A Note on Asymptotically good extensions in which infinitely many primes split completely

This chapter covers the paper [45] written in collaboration with Christian Maire.

Let p be a prime and k be a number field. For $p = 2$, we assume that k is totally imaginary. In this chapter, we prove the existence of asymptotically good extensions L/K of cohomological dimension 2 in which infinitely many primes split completely. Our result is mostly based on mild groups introduced by Labute-Mináč [62, 66] and the "cutting tower strategy" from Hajir, Maire, and Ramakrishna [41].

Chapter 3: Zassenhaus and lower central filtrations of Pro-p groups considered as modules

This Chapter covers [44].

This paper is deeply inspired by the work of Filip [28] and it aims to study the action of groups on Zassenhaus and lower central filtrations of finitely generated pro-p groups. We shall focus on the semisimple case. Particular attention is given to mild groups; and for these groups, we answer positively to [92, Question 2.13].

Chapter 4: On extensions of number fields with given quadratic algebras and cohomology

This Chapter covers [43].

We introduce a criterion on the presentation of finitely presented pro-p groups which allows us to compute their cohomology groups and their gocha series. Consequently, we infer "new" quotients of mild groups of cohomological dimension strictly larger than two.

We interpret these groups as Galois groups over p-rational fields with prescribed ramification and splitting. These results are essentially grounded on Right Angled Artin Algebras properties.

Chapter 5: On Maximal extensions of Pythagorean fields and oriented Graph products

This Chapter covers [46] written in collaboration with Christian Maire, Ján Mináč and Nguyên Duy Tân.

We introduce Δ the group with two elements and a class of pro-2 groups that we call Δ-RAAG, which is a subclass of oriented pro-2 groups introduced by Blumer, Quadrelli and Weigel in [7]. Using results of Mináč' PhD Thesis [87] and Hamza's Master thesis, we show that pro-2 absolute Galois groups of formally real Pythagorean fields of finite type (RPF) are Δ-RAAGs.

Conversely, if a Δ-RAAG is realisable as an absolute pro-2 Galois group, we show that the underlying field is necessarily RPF. As an application, we exhibit Δ-RAAGs which are not pro-2 absolute Galois groups. We also infer that pro-2 absolute Galois groups of RPF satisfy the kernel Unipotent conjecture introduced by Mináč-Tân in [96].

Chapter 6: A complete answer to a question from Mináč-Rogelstad-Tân

This final chapter gives a complete proof to [92, Question 2.13] asked by Mináč-Rogelstad-Tân. A partial positive answer was already given by Hamza in [44], presented in Chapter 3.

General notations

• Let p be a prime number (in general odd), and G be a pro-p group (in general finitely presented). If G is finitely presented, we denote by $\{x_1;\dots;x_d\}$ (resp. $\{l_1;\dots;l_r\}$) a minimal set of generators (resp. relations) of G. We introduce $1\to R\to F\to G\to 1$, a minimal presentation of G.

• Define $[A;B]$ (resp. A^p) the closed subgroup of G generated by $[a;b]:=a^{-1}b^{-1}ab$ (resp. a^p), where A and B are subgroups of G, and $a\in A$, $b\in B$. Denotes by AB the closed subgroup of G generated by $\{ab;\quad a\in A, b\in B\}$.

• We define the i-th cohomology group of the profinite group G over $\mathbb{F}_p$ by:

$$H^i(G):=\varinjlim_U H^i(G/U,\mathbb{F}_p),\quad \text{where}\quad G:=\varprojlim_U G/U,$$

and U is taken in an open normal basis of G. The cohomological dimension of a pro-p group G is the least integer n such that $H^i(G)=0$ for all $i>n$.

Filtrations and gradations

• Let $\mathbb{A}$ be the ring $\mathbb{F}_p$ or $\mathbb{Z}_p$.

• Denote by $Al(\mathbb{A},G)$ the completed group algebra of G over $\mathbb{A}$ and observe that G embeds naturally into $Al(\mathbb{A},G)$. Define $Al_n(\mathbb{A},G)$ the n-th power of the augmentation ideal of $Al(\mathbb{A},G)$. We always assume that the $\mathbb{A}$-module $Al_n(\mathbb{A},G)/Al_{n+1}(\mathbb{A},G)$ is free. Notice that this condition is automatically checked when $\mathbb{A}:=\mathbb{F}_p$, contrary to the case $\mathbb{A}:=\mathbb{Z}_p$ (see for instance [63, Theorem]). Observe that $Al(\mathbb{A},G)$ endowed with the topology given by $\{Al_n(\mathbb{A},G)\}_{n\in\mathbb{N}}$ is a compact module.

• We fix $\{x_j\}_{1\leq j\leq d}$ a lift in F of a basis of $Al_1(\mathbb{A},G)/Al_2(\mathbb{A},G)$; by [120, Corollaire 3, Proposition 42, Chapitre 14], this basis does not depend on the choice of $\mathbb{A}$. The Magnus isomorphism, from [69, Chapitre II, Partie 3], gives us the following identification of $\mathbb{A}$-algebras between $Al(\mathbb{A},F)$ and the noncommuative series over X_j's with coefficients in $\mathbb{A}$:

$$\phi_{\mathbb{A}}\colon Al(\mathbb{A},F)\simeq \mathbb{A}\langle\langle X_j;1\leq j\leq d\rangle\rangle;\quad x_j\mapsto X_j+1 \tag{1}$$

• Define $E_e(\mathbb{A})$ (resp. $E(\mathbb{A})$), where $e:=(e_1;\dots;e_d)$ is a d-tuple of integers, as the algebra $\mathbb{A}\langle\langle X_j;1\leq j\leq d\rangle\rangle$ filtered by $\deg(X_j)=e_j$ (resp. $\deg(X_j)=1$) and write $\{E_{e,n}(\mathbb{A})\}_{n\in\mathbb{N}}$ (resp.$\{E_n(\mathbb{A})\}_{n\in\mathbb{N}}$, the n-th power of the augmentation ideal) for its filtration. One introduces $I(\mathbb{A},R)$ the ideal of $E_e(\mathbb{A})$ generated by $\{\phi_{\mathbb{A}}(r-1);r\in R\}$ endowed with the induced filtration $\{I_n(\mathbb{A},R):=I(\mathbb{A},R)\cap E_{e,n}(\mathbb{A})\}_{n\in\mathbb{N}}$, and $E_e(\mathbb{A},G)$ the quotient filtered algebra $E_e(\mathbb{A})/I(\mathbb{A},R)$, with induced filtration $\{E_n(\mathbb{A},G)\}_{n\in\mathbb{N}}$.

• Introduce the following filtration on G:

$$G_{e,n}(\mathbb{A}):=\{g\in G;\phi_{\mathbb{A}}(g)-1\in E_{e,n}(\mathbb{A},G)\}.$$

When $\mathbb{A}:=\mathbb{F}_p$ and e is trivial, this filtration denotes the Zassenhaus filtration of G (for references see [92]). Under some conditions on G (see for instance [64]), if $\mathbb{A}:=\mathbb{Z}_p$, the

filtration $G_n(\mathbb{Z}_p)$ corresponds to lower central series, defined by $\gamma_1(G) := \mathrm{G}$ and $\gamma_n(G) = [\gamma_{n-1}(G); G]$.

• Define

$$\mathscr{L}_e(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{L}_{e,n}(\mathbb{A}, G), \quad \text{where} \quad \mathscr{L}_{e,n}(\mathbb{A}, G) := G_{e,n}(\mathbb{A})/G_{e,n+1}(\mathbb{A}), \quad \text{and}$$
$$\mathscr{E}_e(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_{e,n}(\mathbb{A}, G), \quad \text{where} \quad \mathscr{E}_{e,n}(\mathbb{A}, G) := E_{e,n}(\mathbb{A}, G)/E_{e,n+1}(\mathbb{A}, G).$$

• Since G is finitely generated, one denominates for every integer n:

$$a_{e,n} := \mathrm{rank}_{\mathbb{A}}\mathscr{L}_{e,n}(\mathbb{A}, G), \quad \text{and} \quad c_{e,n} := \mathrm{rank}_{\mathbb{A}}\mathscr{E}_{e,n}(\mathbb{A}, G),$$
$$gocha_e(\mathbb{A}, t) := \sum_{n\in\mathbb{N}} c_{e,n}t^n.$$

If $P := \sum_{n\in\mathbb{N}} p_n t^n$ and $Q := \sum_{n\in\mathbb{N}} q_n t^n$ are two series with real coefficients, we say that: $P \leq Q \iff \forall n \in \mathbb{N}, \quad p_n \leq q_n$. We denote by μ the Möbius function.

Algebras

To simplify notations, when the underlying ring (resp. degree e is trivial) is clear from the context, we omit to write $\mathbb{A}$ (resp. e). We define $\mathscr{E} := \mathrm{Grad}(E)$; this the graded algebra $\mathbb{A}\langle X_1; \ldots, X_d\rangle$ of noncommutative polynomials on d variables over $\mathbb{A}$ where each X_i is endowed with degree e_i.

• An $\mathbb{F}_p$-basis on E and $\mathscr{E}$ is given by monomials on the set of variables $\mathbf{X} := \{X_1; \ldots; X_d\}$. An order on $\mathbf{X}$ (for instance $X_1 > X_2 > \cdots > X_d$) induces a lexicographic order on monomials on $\mathbf{X}$, that we denote by $>$. We say that a monomial X contains a monomial Y if there exist monomials M and N such that $X = MYN$.
Recall that we write commutators of X_i and X_j (in E or $\mathscr{E}$) as:

$$[X_i; X_j] := X_iX_j - X_jX_i.$$

• If z is an element in E, we denote by $\deg(z)$ (or n_z) the weight of z, i.e. the integer such that $z \in E_{\deg(z)} \setminus E_{\deg(z)+1}$. Then we define $\overline{z}$ the image of z in $E_{\deg(z)}/E_{\deg(z)+1}$, this is a homogeneous polynomial, and we denote its degree by $\deg(z)$. We call $\widehat{z}$ the leading monomial of z. For instance $\widehat{[X_i; X_j]} = X_iX_j$ if $X_i > X_j$.

• Consider a presentation of G with generators $\{x_1; \ldots; x_d\}$ and relations $\{l_i\}_{i\in\mathbf{I}}$ with $\mathbf{I}$ a countable set. We denote by $w_i := \phi_{\mathbb{F}_p}(l_i) - 1 \in E$. We say that G has a *mild* presentation if:

$$gocha(G, t) = \frac{1}{1 - dt + \sum_{i\in\mathbf{I}} t^{\deg(w_i)}}.$$

The group G has a quadratic presentation if $\mathbf{I}$ is finite and for every integer i, $\deg(w_i) = 2$.

• We say that the algebra $\mathscr{E}(G)$ is Koszul, if the trivial $\mathscr{E}(G)$-module $\mathbb{F}_p$ admits a linear resolution $(\mathscr{P}, \delta)$, i.e. $\mathscr{P}_i$ is a free-$\mathscr{E}(G)$-module generated by elements of degree i (see for instance [108, Chapter 2]).

Field Theory

• Let k be a field. We define G_k the maximal p-quotient of the absolute Galois group of k, we also call it the pro-p absolute Galois group of k.

• Furthermore, if k is a number field, we introduce $G_{\mathfrak{p}}$ the maximal p-quotient of the absolute Galois group of $k_{\mathfrak{p}}$, the completion of k at the prime p. We denote by S a finite set of tame primes of k, i.e for every $\mathfrak{p} \in S$, $N_{k/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$, and we introduce G_S the Galois group of the maximal p-extension unramified outside S.

• We denote by RPF the set of formally real Pythagorean fields k with characteristic different from two and such that the group $k^\times/k^{2\times}$ is finite, where $k^\times$ (resp. $k^{2\times}$) is the set of invertible elements (resp. invertible squares) of k. When k is RPF, we take $p = 2$.

Chapter 1

Generalities

The goal of this Chapter is to survey some results in profinite (and particularly pro-p) groups, filtered and graded Lie algebras, cohomology and Field theory in order to simplify the understanding of the rest of the document.

1.1 Notions on profinite groups

Galois theory gives a correspondence between profinite groups and some (infinite) extensions of a fixed field.

1.1.1 Generalities on profinite groups

This subpart is mostly inspired by [19, 138, 112].

Definition 1 (Profinite groups)**.** *A profinite group is a compact Haussdorf topological group whose open subgroups form a basis for the neighbourhoods of the identity.*

A pro-p group G is a profinite group, such that for every x in G and every open subgroup U of G, there exists an integer m such that for all integers $n \geq m$, we have $x^{p^n} \in U$.

Let us fix a base field k, and $\overline{k}$ a separable closure. Consider K a Galois (infinite) extension of k, and we write $K := \cup_{i \in I} K_i$, where K_i are finite Galois extension of k, and $K_i \subset K_{i+1}$.

Definition 2 (Krull Topology)**.** *The Krull topology on* $\mathrm{Gal}(K/k)$ *is given by the family* $\{\mathrm{Gal}(\overline{k}/K_i)\}$ *as a neighbourhood basis of* 1*.*

The study of profinite group is motivated by the Galois correspondence:

Theorem 1. *Every Galois group G (endowed with the Krull topology) is a profinite group. Furthermore, if L is a Galois extension of k with Galois group G, we have a bijection between fields extensions $k \subset K \subset L$ and closed subgroups H of $Gal(L/k)$, given by $K \mapsto Gal(L/K)$ and $H \mapsto L^H$, where K^H is the subfield of K fixed by H.*

Proof. See [112, Theorems 2.11.1 and 2.11.3]. □

Let us now study some topological properties of profinite groups.

Proposition 1. *If X is a subset of G, then the topological closure of X is $\bigcap_N XN$, where N is taken in a normal open basis of G.*

Proof. This is [19, Proposition 1.2]. □

We can also characterize profinite groups as "collections of finite groups". Let us be more precise:

Definition 3 (Filtered poset)**.** *Let Λ be a poset, endowed with relation $\leq$.*
We say that Λ is a filtered poset if for every element α and β in Λ, there exists an element ν in Λ such that $\nu \geq \alpha$ and $\nu \geq \beta$.

Definition 4 (Inverse limit of finite groups)**.** *Let $(G_\alpha)_{\alpha\in\Lambda}$, be a nonempty family of finite groups indexed by a filtered poset Λ.*
Let $f_{\alpha;\beta} : G_\beta \to G_\alpha$ be a collection of surjective groups morphisms, such that:

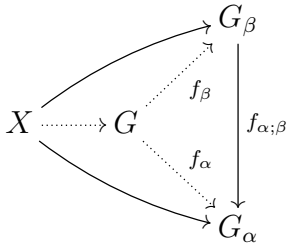
1. *for every α in Λ; $f_{\alpha;\alpha} = \mathrm{id}_{G_\alpha}$,*
2. *for all $\alpha \leq \beta \leq \gamma$; in Λ, we have $f_{\alpha;\gamma} = f_{\alpha;\beta} \circ f_{\beta;\gamma}$.*

We say that $(G_\alpha; f_{\alpha;\beta})_{\alpha\leq\beta\in\Lambda}$ is an inverse system.

Given an inverse system $(G_\alpha; f_{\alpha;\beta})_{\alpha\leq\beta\in\Lambda}$, we can define a group:

$$(G; f) = \{(g_\alpha)_{\alpha\in\Lambda}; f_{\alpha;\beta}(g_\beta) = g_\alpha \quad \forall \alpha \leq \beta\} \subset \prod_{\alpha\in\Lambda} G_\alpha.$$

The group $(G; f)$ (which we denote G by abuse of notations) satisfies the following universal property:



for all $\alpha \leq \beta$ in Λ, X finite groups, and f_α, f_β surjections.

We say that G is the inverse limit of the system: $(G_\alpha; f_{\alpha;\beta})_{(\alpha;\beta)\in\Lambda^2;\alpha\leq\beta}$, and we denote it by $G = \varprojlim_{\alpha\in\Lambda} G_\alpha$. The group G is also endowed with the profinite topology defined by kernels of the maps $f_\alpha \colon G \to G_\alpha$ as a neighbourhood basis of 1.

Proposition 2. *Consider a nonempty inverse system $(G_\alpha; f_{\alpha;\beta})$, then $\varprojlim_{\alpha\in\Lambda} G_\alpha$ is nonempty.*

Proof. See [19, Proposition 1.4] □

Proposition 3. *A group is profinite if and only if it is an inverse limit of finite groups. Moreover a group is a pro-p group if and only if it is an inverse limit of p-groups.*

Proof. See [19, Proposition 1.3] □

Example 1. *With Proposition 3, we can easily give examples of profinite groups and pro-p groups.*

- *Consider the set of p-adic integers* $\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$. *This is a pro-p group. For more general references on p-adic integers, we refer to the book of Katok [56].*
- *Consider the example* $\hat{\mathbb{Z}} := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$. *Observe by the Chinease reminder Theorem that*
$$\hat{\mathbb{Z}} := \prod_p \mathbb{Z}_p,$$
where p is taken in the collection of all prime numbers.

If G is a profinite group, then every open subgroup of G is of finite index. However, what can be said about finite index subgroups of G?

Definition 5 (Strongly complete)**.** *A profinite group is strongly complete if and only if every subgroup of finite index is open.*

Proposition 4. *A profinite group is strongly complete if and only if it does admit a countable number of subgroups of finite index.*

Proof. See [121, Theorem 2]. □

We say that a profinite group is finitely generated if it does admit a finite number of generators as a topological group. During the last decade, Nikolov and Segal showed the following result:

Theorem 2 (Nikolov-Segal)**.** *If G is a finitely generated profinite group, then G is strongly complete.*

Proof. See [104]. □

Example 2. *Let us consider*
$$\mathscr{A} := \prod_{n\geq 5} \mathscr{A}_n^{(n!)^n},$$
where $\mathscr{A}_n$ *is the alternating group over n elements. Then* $\mathscr{A}$ *is a strongly complete profinite group, but is not finitely generated (see [103, Part 6]).*

1.1.2 Notions on pro-p groups

From now, we only study pro-p groups.

Definition 6 (Pro-p completion)**.** *If G is a group, we define the pro-p completion of G by:*

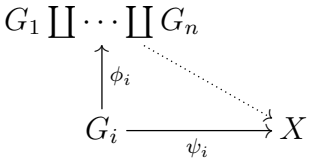
$$\widehat{G} := \varprojlim_{U \in \mathscr{U}} G/U,$$

where $\mathscr{U}$ is the collection of all subgroups of index a power of p.

Observe that $\widehat{G}$ is a pro-p group. This construction is very useful to construct coproducts, free pro-p groups, and free presentations. By universal property, we also have a natural map $G \to \widehat{G}$ with kernel given by $\bigcap_{U \in \mathscr{U}} U$.

Example 3. *Consider $G := \mathbb{Z}$, then $\widehat{G} = \mathbb{Z}_p$, the p-adic integers.*

Definition 7 (Free products)**.** *Let $\{G_1; \dots; G_n\}$ be a finite family of pro-p groups. The free products (or coproduct in the category of pro-p groups) of $\{G_1; \dots; G_n\}$, denoted by $G_1 \coprod \cdots \coprod G_n$, is the unique (up to isomorphisms) pro-p group, endowed with morphisms $\phi_i : G_i \to G_1 \coprod \cdots \coprod G_n$, satisfying the following universal property:*



where X is a pro-p group and $\psi_i : G_i \to X$ are fixed morphsims.

Proposition 5. *Free products exist in the category of pro-p groups.*

Proof. We just give their explicit constructions. For further details, we refer to [112, Proposition 9.1.2].
Let $\{G_i\}_{1 \leq i \leq n}$ be a finite family of pro-p groups. Call $G^{abs} = G_1 * \cdots * G_n$ the free product of $G_1; \dots; G_n$ in the category of groups, i.e. G^{abs} is given by words with letters in G_i. We define

$$G := \coprod_i G = \widehat{G^{abs}}.$$

□

Let us now study the smallest number of generators of the topological group G, that we denote by $d(G)$.

Proposition 6. *The pro-p group $G := \varprojlim_{\alpha \in \Lambda} G_\alpha$ is finitely generated if and only if the set $\{d(G_\alpha); \alpha \in \Lambda\}$ is bounded. Furtheremore there exits $\alpha_o \in \Lambda$ such that for all $\alpha \in \Lambda$ satisfying $\alpha \geq \alpha_0$, we have $d(G) = d(G_\alpha)$.*

Proof. See [112, Lemma 2.5.3]. □

Definition 8 (Frattini subgroups)**.** *Let G be a pro-p group.*
We define the Frattini subgroup of G by:

$$\mathrm{Frat}(G) = \bigcap_M M$$

where M is taken in the set of maximal open subgroups of G.

For pro-p groups, the Frattini subgroup is closely related to generators of G.

Theorem 3. *Let G be a pro-p group, and $\mathrm{Frat}(G)$ its Frattini subgroup.*

1. *If $G = \varprojlim_{\alpha\in\Lambda} G/N_\alpha$, then*

$$G/\mathrm{Frat}(G) = \varprojlim_{\alpha\in\Lambda} (G/N_\alpha)/(\mathrm{Frat}(G)/N_\alpha).$$

2. *We also have $\mathrm{Frat}(G) = G^p[G;G]$.*

3. *Furthermore, the pro-p group G is finitely generated if and only if $\mathrm{Frat}(G)$ is open. Particularly, the subgroup generated by the product G^p and $[G;G]$ is closed if and only if $d(G) < \infty$.*

4. *If $d(G) < \infty$, then*

$$G/\mathrm{Frat}(G) \simeq \mathbb{F}_p^{d(G)}.$$

Proof. The first point is given by [112, Corollary 2.8.3].
The second point is given by [19, Proposition 1.13].
The third point is given by [19, Proposition 1.14] and [19, Corollary 1.20].
The last point is given by [112, Lemmas 2.8.6 and 2.8.7]. □

Proposition 7. *Let G and H be two finitely generated pro-p groups, then $d(G\coprod H) = d(G) + d(H)$.*

Proof. See [112, Proposition 9.1.15]. □

The commutator subgroup $[G;G]$ is closely related to the Frattini sugroup of G and is very important in the study of finitely generated pro-p groups. Just to be complete, let us give general results on group commutators:

Proposition 8 (Commutator identities)**.** *Let x, y, z be elements in G, and take n an integer. We define $x^y := y^{-1}xy$. We have the following identities:*

1. $[x;y]^{-1} = [y;x]$,
2. $[xy;z] = [x;z]^y[y;z]$,
3. $[x;yz] = [x;z][x;y]^z$,

4. $[x^n; y] = [x; y]^{x^{n-1}} \dots [x; y]^x [x; y]$,

5. $[x; y^n] = [x; y][x; y]^y \dots [x; y]^{y^{n-1}}$,

6. $(xy)^n \equiv x^n y^n [y; x]^{\frac{n(n-1)}{2}} \mod [[G; G]; G]$,

7. *in particular,* $(xy)^n \equiv x^n y^n \mod [G; G]$.

Proof. These are just standard computations in group theory. □

Let us now define free pro-p-groups and presentations.

Definition 9. *Let* $\mathbf{X}$ *be a finite set,* F *a pro-p group, and* $i : \mathbf{X} \to F$ *a map. Then* $(F; i)$ *(that we will denote by* F *by abuse of notations) is a free pro-p group if and only if* F *satisfies the following universal property:*
for every pro-p group G*, and map* $\psi : \mathbf{X} \to G$*, there exists a unique map* $\overline{\psi}: F \to G$ *such that the following diagram commutes:*

$$\begin{array}{ccc} F & \overset{\overline{\psi}}{\dashrightarrow} & G \\ {\scriptstyle i}\uparrow & \nearrow_{\psi} & \\ \mathbf{X} & & \end{array}$$

Furthermore, for every finite set $\mathbf{X}$*, there exists a unique pro-p group* F *(up to isomorphisms) which is free over* $\mathbf{X}$*. In particular, if* $\mathbf{X}$ *is a finite set then* $d(F) = |\mathbf{X}|$.

Explicitely, we construct the free pro-p group F with d generators by: $F(d) = \coprod_{j=1}^{d} \mathbb{Z}_p$.

Definition 10 (Presentation of a pro-p group)**.** *Let* G *be a finitely generated pro-p group. Then by freeness, we define a (free) presentation of* G *by the following exact sequence:*

$$1 \to R \to Fd(G) \to G \to 1,$$

where d *is minimal.*

Let $\mathbf{I}$ *be a (countable) set. We say that* $\{l_i\}_{i \in \mathbf{I}} \subset F(d)$ *is a minimal subset of relations of* G *if the set* $\{l_i\}_{i \in \mathbf{I}}$ *is a minimal set of generators of the closed normal subgroup* R *in* F*. We define:* $r(G) := |\mathbf{I}|$*, if* $\{l_i\}_{i \in \mathbf{I}}$ *is a minimal set of relations defining* G.

The freeness of a finitely generated pro-p group G can also be seen by the number of generators of its open subgroups:

Theorem 4 (Generalised Schreier Formula)**.** *Let* G *be a finitely generated pro-p-group, then* G *is free if and only if for all open subgroups* H *of* G *we have:*

$$d(G) - 1 = [G : H](d(H) - 1).$$

Proof. This is the theorem 3.3.16 of [102]. □

Remark 1. *Labute and Dummit [20, Theorem 1] gave an analoguous result to Theorem 4 when G is a Demushkin group: the group G is Demushkin if and only if*

$$d(G) - 2 = [G : H](d(H) - 2).$$

These groups play a fundamental role in Group theory: they naturally appear in Number Theory and Geometry. For further references, let us for instance quote the book [123] from Souza-Zapata.

Let us conclude this subpart with Golod-Shafarevich Theorem:

Theorem 5. *Let G be a pro-p group with d generators and r relations. If $d^2 \geq 4r$, then G is infinite.*

Proof. This result is very famous, for a proof we can cite [19, Interlude D], [119, Appendix 2], [69, Appendice A.3] and [12, Parties 5 et 6]. We also propose an alternative proof in Subpart 1.3.2. □

1.1.3 Strong completness for pro-p groups

Strong completness for pro-p is well known:

Theorem 6. *Let G be a pro-p group. Then G is finitely generated if and only if G is strongly complete.*

Serre proved the direct way in the $60's$ (for instance see [19, Theorem 1.17]). In this part, we investigate the reverse way, which is also well known from specialists, but we did not find complete and direct references.

Introduce $\{x_i\}_{i\in\mathbf{I}}$ a minimal set of generators of G indexed by a set $\mathbf{I}$, and let $\mathrm{Frat}(G)$ be the Frattini subgroup of G, and $\psi : G \to G/\mathrm{Frat}(G)$ be the canonical surjection. Using [19, Proposition 1.9], we observe that :

$$G/\mathrm{Frat}(G) \simeq \prod_{i\in I} x_i^{\mathbb{F}_p},$$

as pro-p group (the second one with the product topology).

If G is infinitely generated, we construct a subgroup H of G which is dense (so not closed, hence not open). We explain the strategy of our construction. First, following [112, Example 4.2.12] we construct a subgroup of $G/\mathrm{Frat}(G)$, called H_P which is of finite index in $G/\mathrm{Frat}(G)$ and non open in $G/\mathrm{Frat}(G)$. Then, we consider the group $H := \psi^{-1}(H_P)$ which answers our problem. Ultrafilter theory is essential to construct the group H_P.

Definition 11. *Let P be a subset of the set of subsets of $\mathbf{I}$. We say that P is a ultrafilter if it satisfies the following propeties:*

1. *if A, B in P, then $A \cap B \in P$,*

2. *if $A \in P$ and B is a subset of $\mathbf{I}$ that contains A, then $B \in P$,*

3. *the empty set is not in P,*

4. *for every A subset of $\mathbf{I}$, either $A \in P$ or $\mathbf{I} \setminus A \in P$.*

For more references on ultrafilter theory, we refer to [49].

Construction of H_ϕ

This construction is done in [112, Example 4.12.2].
We consider $P_{\mathbf{I}}$ a non-principal ultrafilter, so it contains the Frechet filter of $\mathbf{I}$, i.e all subsets of $\mathbf{I}$ which contains all but finitely many elements in $\mathbf{I}$. The ultrafilter $P_{\mathbf{I}}$ exists by Zorn's Lemma. If $g \in G/\mathrm{Frat}(G)$, we write $g = (g_i)_{i\in\mathbf{I}} \in \prod_{i\in\mathbf{I}} x_i^{\mathbb{F}_p}$ and we define $\mathrm{Triv}(g) := \{i \in \mathbf{I}; g_i = 1\}$. Introduce:

$$H_P := \{h \in G; \mathrm{Triv}(h) \in P_{\mathbf{I}}\}.$$

First, we remark that H_P is dense in $G/\mathrm{Frat}(G)$, and if h_1 and h_2 are in H_P, then $\mathrm{Triv}(h_1) = \mathrm{Triv}(h_1^{-1})$ and $\mathrm{Triv}(h_1) \cap \mathrm{Triv}(h_2) \subset \mathrm{Triv}(h_1 h_2)$, so by filter and ultrafilter properties $\mathrm{Triv}(h_1 h_2) \in P_{\mathbf{I}}$. So H_P is a group. Moreover, if $g \in G$, and $h \in H_P$, then $\mathrm{Triv}(h) \subset \mathrm{Triv}(ghg^{-1})$, so H_P is a normal subgroup of $G/\mathrm{Frat}(G)$. Then H_P is a dense proper subgroup of $G/\mathrm{Frat}(G)$.

Now, we show that H_P is of finite index in $G/\mathrm{Frat}(G)$. Define $c_k = (x_i^k)_{i\in\mathbf{I}} \in G/\mathrm{Frat}(G)$. For every $g := (g_i) \in G$ and $k \in \mathbb{F}_p$, we define

$$\mathbf{I}_k := \{i \in \mathbf{I}; g_i x_i^{-k} = 1\}.$$

Then $\mathbf{I} = \bigcup_{k\in\mathbb{F}_p} \mathbf{I}_k$. So by ultrafilter property, there exists $k \in \mathbb{F}_p$ such that $\mathbf{I}_k \in P_{\mathbf{I}}$. So $g c_k^{-1} \in H_P$. This implies that H_P is of index equal or less than p. However H_P is proper in $G/\mathrm{Frat}(G)$ and dense, this implies that H_P is not open in $G/\mathrm{Frat}(G)$. Since G is a pro-p group, then H_P is of index p (see for instance [19, Lemma 1.18]).

Construction of H

Let $\psi\colon G \to G/\mathrm{Frat}(G)$. Take $H := \psi^{-1}(H_P)$, this is a normal subgroup of G. Take $t_1; \ldots; t_p$ a system of generators of $(G/\mathrm{Frat}(G))/H_P$. Then $t_1; \ldots; t_p$ are also generators of G/H. Since ψ is surjective, then H is proper in G, and by a Frattini argument H is dense in G. This implies that H is non open in G and proper.

1.2 Compact and Locally finite graded Algebras

Let us give some general algebraic results before applying them to pro-p groups. This Part is mostly inspired from [69, 14, 71]. Let us also quote [72, Chapter 1].

1.2.1 Generalities

We begin by defining the categories of Compact Algebras and Graded locally finite Connected Algebras (GCA).

Definition 12 (Filtered Compact Algebras)**.** *The set A is an object in the category of compact algebra over $\mathbb{A}$ if and only if:*

1. *A is an $\mathbb{A}$-algebra,*
2. *A is a complete and Haussdorf topological space,*
3. *there exists a countable family of closed two sided ideals $\{A_n\}_{n\in\mathbb{N}}$, basis of 0 such that for every n, A_n/A_{n+1} is a free $\mathbb{A}$-module with finite rank.*

The family $\{A_n\}_{n\in\mathbb{N}}$ is called a filtration of A (name given by Lazard, in [69]). Since A is Haussdorf, we have $\bigcap_n A_n = \{0\}$.
An arrow in the category of compact algebras is a morphism of $\mathbb{A}$-algebras agreeing with the topology. An arrow in the category of filtered compact algebras is a morphism of $\mathbb{A}$-algebras agreeing with filtrations.

The category of compact Algebras was defined by Brumer, in [14]. These two categories have the same objects but not the same morphisms. If z is an element in the compact filtered algebra A, we define the weight of z, that we denote by n_z, by the integer n such that $z \in A_n \setminus A_{n+1}$.

Example 4 (Noncommutative series)**.** *Consider the algebra $\mathbb{A}\langle\langle X_1; \dots; X_d\rangle\rangle$. We can endow each X_i with a weight e_i. This allows us to define a filtration on $\mathbb{A}\langle\langle X_i\rangle\rangle$, that we call (X, e)-filtration. Take $x \in A\langle\langle X_i\rangle\rangle$, then we write $x := \sum_\alpha a_\alpha X_\alpha$. We define the weight of x in $E_e(\mathbb{A})$ by: $n_x := \min_{a_\alpha \neq 0}\{e_{\alpha_1} + \cdots + e_{\alpha_n}\}$. Consequently we introduce $E_e(\mathbb{A})$, the algebra $\mathbb{A}\langle\langle X_i\rangle\rangle$, endowed with the filtration:*

$$E_{e,n}(\mathbb{A}) := \{x \in A; n_x \geq n\}.$$

For general references on (X, e)-filtrations, let us quote [27, 69, 29].
Assume that for all i, we have $e_i := 1$, then we define $E(\mathbb{A}) := \mathbb{A}\langle\langle X_1; \dots; X_d\rangle\rangle$, the free algebra of noncommutative series over $\mathbb{A}$, filtered by $E_n(\mathbb{A})$, the n-th power of the augmentation ideal $E_1(\mathbb{A})$, which is the closed two-sided ideal of $E(\mathbb{A})$ generated by $\{X_1; \dots; X_d\}$.
For every choice of e, we have an isomorphism of compact algebras $E_e(\mathbb{A}) \simeq E(\mathbb{A})$, but this is not an isomorphism of filtered compact algebras.

Let us now introduce the category of graded algebras.

Definition 13 (CGA)**.** *Let $\mathscr{A}$ be an $\mathbb{A}$-algebra. We say that $\mathscr{A}$ is:*

1. *graded if there exists a countable family of free $\mathbb{A}$-modules $\{\mathscr{A}_n\}_{n\in\mathbb{N}}$ such that $\mathscr{A} := \bigoplus_{n\in\mathbb{N}} \mathscr{A}_n$,*

2. *connected if* $\mathscr{A}_0 := \mathbb{A}$,

3. *locally finite if for every integer* n, *the space* $\mathscr{A}_n$ *is a free finitely generated* $\mathbb{A}$*-module.*

An arrow in the category of locally finite, connected graded algebras is a morphism of algebra agreeing with gradation.

The category of connected, locally finite graded algebras is denoted by CGA. It was studied by Anick (see for instance [3]) and Lemaire [71].
Every element z in $\mathscr{A}$ can be written as a sum $z := \sum_{n\in\mathbb{N}} z_n$ where for every integer n, z_n is in $\mathscr{A}_n$. We define by $\deg(z)$ the least integer n such that $z_n \neq 0$.

Example 5 (Filtrations on $\mathbb{A}$)**.** *We can always define a filtration on the ring* $\mathbb{A}$*: the trivial one, i.e.* $\mathbb{A}_0 := \mathbb{A}$ *and* $\mathbb{A}_i := 0$ *for* i *larger than one.*

On $\mathbb{Z}_p$*, we also have another filtration by* n*-th power of the augmentation ideal* $p\mathbb{Z}_p$*.*

Example 6 (Noncommutative polynomials)**.** *Denote by* $\mathscr{E}_e(\mathbb{A})$ *the algebra* $\mathbb{A}\langle X_1; \ldots; X_d\rangle$*, where each* X_i *is endowed with degree* e_i*, graded by homogenous elements (sum of monomials with same degree) of degree* n*. This is an object in CGA.*

If we put $e_i := 1$*, we write* $\mathscr{E}(\mathbb{A})$ *rather than* $\mathscr{E}_e(\mathbb{A})$*.*

Example 7. *Let us consider an example of filtrations on* $\mathbb{A}\langle\langle X_1; \ldots; X_d\rangle\rangle$ *in an equivariant context.*

Assume Δ *is a cyclic group of order a prime* q *dividing* $p-1$*. Consider* V *a* $\mathbb{A}[\Delta]$*-module which is free on* $\mathbb{A}$ *and of dimension* d*. By Maschke's Theorem, we can define a* $\mathbb{A}[\Delta]$*-basis, of* V*,* $\{X_j^\chi\}$ *satisfying* $\delta(X_j^\chi) := \chi(\delta)X_j^\chi$*, where* χ *is taken in the set of irreducible characters of* Δ *over* $\mathbb{A}$*, that we denote* $\mathrm{Irr}(\Delta)$*.*
Choose χ_0 *an nontrivial element in* $\mathrm{Irr}(\Delta)$*, then we have a bijection:*

$$\psi_{\chi_0} \colon \mathrm{Irr}(\Delta) \to \{1; \ldots; q\}; \quad \chi_0^i \mapsto i.$$

Define $E_{\chi_0}(\mathbb{A})$ *the filtered algebra* $\mathbb{A}\langle\langle X_j^\chi; \chi \in \mathrm{Irr}(\Delta)\rangle\rangle$*, where each* X_j^χ *has weight* $\psi_{\chi_0}(\chi)$*. Denote by* $\mathscr{E}_{\chi_0} := \mathrm{Grad}(E_{\chi_0}(\mathbb{A})$*. These algebras were studied by Hamza in [44]. In particular, he was able to give some results on equivariant components of some Lie algebras related to a finitely generated pro-p group* G*.*

Similarly, we define compact modules and graded modules.

Definition 14. *Let* A *be a* $\mathbb{A}$*-(filtered) compact algebra with filtration* $\{A_n\}_{n\in\mathbb{N}}$*. We say that a* A*-module* M *is (filtered) compact if:*

(*i*) M *is a topological, separated and complete space,*

(*ii*) M *admits a family of submodules* $\{M_n\}_{n\in\mathbb{N}}$ *closed basis of zero such that* M/M_n *has finite length.*

(*iii*) *we have* $A_nM_m \subset M_{n+m}$*.*

Morphisms of (filtered) compact-modules respect (filtrations) the topology.

Definition 15. *Let $\mathscr{A} := \bigoplus_{n\in\mathbb{N}} \mathscr{A}_n$ be a $\mathbb{A}$-CGA. We say that a $\mathscr{A}$-module $\mathscr{M}$ is graded*

(i) if there exists a countable family of free finitely generated $\mathscr{A}$-modules $\{\mathscr{M}_n\}_{n\in\mathbb{N}}$ such that $\mathscr{M} := \bigoplus_{n\in\mathbb{N}} \mathscr{M}_n$,

(ii) we have the relation $\mathscr{A}_n\mathscr{M}_m \subset \mathscr{M}_{m+n}$.

Morphisms respect gradations.

Definition 16 (Hilbert Series)**.** *If $\mathscr{M}$ is a $\mathscr{A}$-CGA module, we denote the Hilbert Series of $\mathscr{M}$ by:*

$$\mathscr{M}(t) := \sum_n \mathrm{rank}_{\mathbb{A}}\mathscr{M}_n t^n.$$

Proposition 9. *Assume that we have an exact sequence of $\mathscr{A}$-CGA modules:*

$$0 \to \mathscr{K} \to \mathscr{M} \to \mathscr{N} \to 0.$$

Then we have the following equality of Hilbert series:

$$\mathscr{M}(t) = \mathscr{N}(t) + \mathscr{K}(t).$$

Proof. From the exact sequence, we infer for every integer n an exact sequence of free $\mathbb{A}$-modules:

$$0 \to \mathscr{K}_n \to \mathscr{M}_n \to \mathscr{N}_n \to 0.$$

Then we infer $\mathrm{rank}_{\mathbb{A}}\mathscr{M}_n = \mathrm{rank}_{\mathbb{A}}\mathscr{N}_n + \mathrm{rank}_{\mathbb{A}}\mathscr{K}_n$. □

The product $\prod$ (resp. the coproduct $\bigoplus$) is well defined in the category of A-(filtered) compact modules (resp. $\mathscr{A}$-CGA) modules.

Let M (resp. $\mathscr{M}$) be a A (filtered)-compact (resp. $\mathscr{A}$-CGA) module. We say that M (resp. $\mathscr{M}$) is free if there exists a family $\{m_i\}_{i\in\mathbf{I}}$ in M (resp. $\{\mu_i\}_{i\in\mathbf{I}}$ in $\mathscr{M}$) such that $M \simeq \prod_i m_i A$ (resp. $\mathscr{M} \simeq \bigoplus_i \mu_i\mathscr{A}$). The filtration on M (resp. the gradation on $\mathscr{M}$) is given by the weights of the m_i's (resp. the degrees of the μ_i's). Free-modules satisfy a universal property and can be read from their Hilbert series.

Proposition 10. *Let $\mathscr{M}$ be a $\mathscr{A}$-CGA module generated by a family $\{\mu_i\}_{i\in\mathbf{I}}$. Then $\mathscr{M}$ is free on $\{\mu_i\}_{i\in\mathbf{I}}$ if and only if*

$$\mathscr{M}(t) = \sum_i t^{\deg(\mu_i)}\mathscr{A}(t).$$

Proof. The first implication is clear from $\mathscr{M} \simeq \bigoplus_i \mu_i\mathscr{A}$. Conversely, since $\{\mu_i\}$ generates $\mathscr{M}$, then by the universal property there exist a $\mathscr{A}$-CGA module $\mathscr{K}$ and an exact sequence of $\mathscr{A}$-CGA modules:

$$0 \to \mathscr{K} \to \mathscr{M}' := \bigoplus_i \mu_i\mathscr{A} \to \mathscr{M} \to 0.$$

Consequently by Proposition 9 and the first implication, we have

$$\mathscr{M}'(t) := \sum_i t^{\deg(\mu_i)} \mathscr{A}(t) = \mathscr{M}(t) + \mathscr{K}(t).$$

By hypothesis $\mathscr{M}(t) = \mathscr{M}'(t)$, so we infer $\mathscr{K}(t) = 0$ which implies $\mathscr{K} = 0$, so $\mathscr{M} \simeq \mathscr{M}'$ is free. □

Example 8. *We have the isomorphisms:*

$$E_{e,1}(\mathbb{A}) \simeq X_1 E_e \times \cdots \times X_d E_e, \quad \textit{and} \quad \mathscr{E}_{e,\geq 1}(\mathbb{A}) \simeq X_1 \mathscr{E}_e \oplus \cdots \oplus X_d \mathscr{E}_e,$$

where $\mathscr{E}_{e,\geq 1}(\mathbb{A}) := \bigoplus_{i\geq 1} \mathscr{E}_{e,i}(\mathbb{A})$ is the kernel of the augmentation map $\mathscr{E}_e(\mathbb{A}) \to \mathbb{A}$; which maps X_i to 1.

Consequently $E_{e,1}(\mathbb{A})$ and $\mathscr{E}_{e,\geq 1}(\mathbb{A})$ are free $E_e(\mathbb{A})$-compact module and $\mathscr{E}_e(\mathbb{A})$-CGA module, and the filtration (resp. gradation) is given by the weight (resp. degree) of X_i which is e_i. Observe also that we have the following Hilbert series:

$$\mathscr{E}_e(t) = \frac{1}{1 - \sum_i t^{e_i}}, \quad \textit{and} \quad \mathscr{E}_{e\geq 1}(t) = \frac{\sum_i t^{e_i}}{1 - \sum_i t^{e_i}}.$$

1.2.2 Grad functor and Hilbert Series

Let us now study links between filtered compact algebras and CGA. More precisely, we define a functor, called Grad, from the category of filtered A-compact modules to $\mathscr{A}$-CGA modules. For more details, we refer to the first parts of [69].

Let A be a filtered compact algebra endowed with a filtration $\{A_n\}_{n\in\mathbb{N}}$. We define $\mathscr{A}_n := \mathrm{Grad}_n(A) := A_n/A_{n+1}$, this is a free $\mathbb{A}$-module. Then, we introduce $\mathscr{A} := \mathrm{Grad}(A) := \bigoplus_{n\in\mathbb{N}} \mathscr{A}_n$. Therefore $\mathscr{A}$ is a free $\mathbb{A}$-module naturally endowed with an algebra structure: this is an object in CGA, endowed with gradation $\{\mathscr{A}_n\}_{n\in\mathbb{N}}$.

Furthermore, if we have a map $f\colon A \to B$ of (filtered) compact modules, then we have $f(A_n) \subset B_n$, and so we can define maps $f_n\colon A_n/A_{n+1} \to B_n/B_{n+1}$. Then we define $\mathrm{Grad}(f) := \bigoplus_n f_n\colon \mathrm{Grad}(A) \to \mathrm{Grad}(B)$.

If x is a non trivial element in A, we define n_x the weight of x, i.e. the integer n such that x is in A_n but not in A_{n+1}. Therefore, we write $\overline{x}$ the image of x in $A_{n_x}/A_{n_x+1} \subset \mathrm{Grad}(A)$.

Example 9. *We have $\mathscr{E}_e(\mathbb{A}) = \mathrm{Grad}(E_e(\mathbb{A})) := \bigoplus_{n\in\mathbb{N}} E_{e,n}(\mathbb{A})/E_{e,n+1}(\mathbb{A})$.*

Let s be an element in $E_e(\mathbb{A})$, then s is a series and we can write $s := \sum_i s_i$ where s_i is a homogeneous polynomial of degree i. Observe that n_s is the least integer such that $s_i \neq 0$, and $\overline{s} := s_{n_s}$.

Similarly, if M is a A-filtered compact module, we define $\mathscr{M} := \mathrm{Grad}(M) := \bigoplus_n M_n/M_{n+1}$ and $M(t) := \mathscr{M}(t)$. This is a $\mathscr{A}$-CGA module. If $f\colon M \to N$ is a morphism in the category of (filtered) A-compact modules, then we define as previously a morphism of $\mathscr{A}$-CGA modules $\mathrm{Grad}(f)\colon \mathrm{Grad}(M) \to \mathrm{Grad}(N)$.

Proposition 11 (Grad of free compact-modules)**.** *We have the isomorphism:*

$$\mathrm{Grad}(\prod_i m_i A) \simeq \bigoplus_i \mu_i \mathscr{A},$$

where $\mu_i := \overline{m_i}$.

Conversely, if $\mathscr{M}$ *is a free* $\mathscr{A}$*-CGA module, then there exists a unique filtered* A*-compact free module* M *such that* $\mathscr{M} \simeq \mathrm{Grad}(M)$.

Proof. See [69, Chapitre I, Formule (2.3.12)]. □

Assume that M is a filtered A-compact module. If K is a A-compact module which embeds in M then we can endow K with the induced filtration on M by $K_n := M_n \cap K$. It is also sufficient to assume K closed in M, to obtain a filtered A-compact module structure. If we have a surjection of A-compact modules $f\colon M \to N$, then we can endow N with the quotient filtration: this is the lowest filtration which makes f an epimorphism of filtered A-modules, i.e. for every x in N, we have:

$$n_x := \sup_{y \in M; f(y)=x} n_y.$$

It is also sufficient to assume N closed for the topology induced by the quotient filtration, to obtain a filtered A-compact module structure.

Proposition 12. *Assume that* K *is closed in* M*, and define* $N := M/K$*. Then we have the following exact sequence of* A*-compact modules:*

$$0 \to K \to M \to N \to 0.$$

Consequently, if M *is a filtered* A*-compact module, we infer the following exact sequence of* $\mathscr{A}$*-CGA modules:*

$$0 \to \mathscr{K} := \mathrm{Grad}(K) \to \mathscr{M} := \mathrm{Grad}(M) \to \mathscr{N} := \mathrm{Grad}(N) \to 0.$$

Proof. [69, Chapitre I, Formule (2.3.8.2)]. □

Corollary 1. *We have* $\mathscr{M}(t) := \mathscr{K}(t) + \mathscr{N}(t)$.

1.2.3 Quotients of noncommutative series and polynomials

The main reference for this subpart is [69, Chapitre I, Partie 2].

Let us define I a closed two-sided ideal of $E_e(\mathbb{A})$ generated by a family $\{w_i\}_{i \in \mathbf{I}}$. We define the induced filtration by $E_e(\mathbb{A})$ on I by $I_n := E_{e,n}(\mathbb{A}) \cap I$. Consequently, I endowed with the filtration $\{I_n\}_{n \in \mathbb{N}}$ is a compact algebra.

Let us introduce $E_e(w) := E_e/I$ the quotient of E_e by I, which is a compact $\mathbb{A}$-algebra generated by the images of $\{X_1; \ldots; X_d\}$. We have a natural surjection $f\colon E_e \to E_e(w)$. We define the quotient filtration on $E_e(w)$ induced by E_e as the lower bound on filtrations on

$E_e(w)$, which makes f an epimorphism of filtred $\mathbb{A}$-compact algebras, i.e. if x is an element in $E_e(w)$, we define:

$$n_x := \sup_{y \in E_e; f(y)=x} n_y.$$

We denote the previous filtration by $\{E_{e,n}(w)\}_{n\in\mathbb{N}}$.

Finally, we introduce $\mathscr{I} := \mathrm{Grad}(I)$ and $\mathscr{E}_e(w) := \mathrm{Grad}(E_e(w))$.

Theorem 7. *We have the following exact sequences:*

- *In the category of $\mathbb{A}$-filtered compact algebras:*

$$0 \to I \to E_e(\mathbb{A}) \to E_e(w) \to 0,$$

- *In the category $\mathscr{A}$-CGA:*

$$0 \to \mathscr{I} \to \mathscr{E}_e(\mathbb{A}) \to \mathscr{E}_e(w) \to 0.$$

Proof. This is exactly [69, Formule (2.3.8.2)]. □

Let us define $\rho_i := \overline{w_i}$ the image of w_i in $\mathscr{E}_{e,n_{w_i}}$, $\mathscr{I}(\rho)$ the ideal of $\mathscr{E}_e$ generated by ρ and $\mathscr{E}_e(\rho) := \mathscr{E}_e/\mathscr{I}(\rho)$. Observe that $\mathscr{I}(\rho)$ is also a $\mathbb{A}$-CGA algebra. Computing $\mathscr{I}$ (and $\mathscr{E}_e(w)$) is in general pretty hard, but we have the following result:

Proposition 13. *We have an inclusion $\mathscr{I}(\rho) \subset \mathscr{I}$.*

Proof. Observe that ρ_i is an element in $I \cap E_{e,n_{w_i}}/I \cap E_{e,n_{w_i}+1} \simeq J_{n_{w_i}}/E_{e,n_{w_i}+1}$, where $J_{n_{w_i}}$ is the ideal generated by $I \cap E_{e,n_{w_i}}$ and $E_{e,n_{w_i}+1}$. Consequently, ρ_i is in $\mathscr{I}$. We conclude since $\mathscr{I}$ is an ideal. □

Let us now call $\mathscr{E}(\rho) := \mathscr{E}/\mathscr{I}(\rho)$. We have the following result on Hilbert series.

Corollary 2. *We have:*

$$\mathscr{E}_e(w,t) \leq \mathscr{E}_e(\rho,t),$$

with equality if and only if $\mathscr{I}(\rho) = \mathscr{I}$.

Proof. From the last proposition, we have a surjection of graded vector spaces $\mathscr{E}_e(\rho) \to \mathscr{E}_e(w)$, which gives us the desired inequality. Furthermore the surjection is an isomorphism if and only if we have equality of Hilbert series. □

Let us now study some quotients of $\mathscr{E}_e$, and for the rest of the subpart, we consider the case $\mathbb{A} := \mathbb{F}_p$.

A basis of the $\mathbb{F}_p$-graded vector space $\mathscr{E}_e$ is given by monomials: $X^\alpha := X_{i_{\alpha_1}}^{\alpha_1} \dots X_{i_{\alpha r}}^{\alpha_r}$, where α is an r-uplet and i_{α_k} an element in $\{1;\dots;d\}$. Consequently, every element $x \in \mathscr{E}_e$ can be written $x := \sum_\alpha a_\alpha X^\alpha$, with $a_\alpha \in \mathbb{F}_p$.

Let us introduce an order on monomials $>$ (for instance the order induced by $X_d > X_{d-1} > \dots > X_1$), and denote by $\deg(X^\alpha)$ the degree of X^α, i.e. $\alpha_1 + \dots + \alpha_r$. We say that $X^\alpha < X^\beta$, if $\deg(X^\alpha) > \deg(X^\beta)$ and if we have equality, we use the lexicographic order. If $\rho_i \in \mathscr{E}_e$ is of the form $\rho_i := \sum_\alpha a_\alpha X^\alpha$, we introduce $\deg(\rho_i) := \min_{a_\alpha}\{\deg(X^\alpha)\}$. Define $\widehat{\rho_i} := \max_\alpha\{X^\alpha\}$.

Remark 2. *Let us give in this remark few words on Gröbner bases, and how to use them to compute Hilbert series. For more details, we refer to [130, Chapters 2 and 3].*

A subset G of $\mathscr{I}$ is a Gröbner basis of $\mathscr{I}$ if the ideal generated by the leading monomials in G is equal to $\widehat{\mathscr{I}}$, the ideal generated by the leading monomials of elements in $\mathscr{I}$. We say that a monomial is normal if it does not contain a submonomial in $\widehat{\mathscr{I}}$, and we denote by $\mathscr{N}$ the linear hull of all normal words. From [130, Theorem Part 2.3], we have the decomposition $\mathscr{E}_e = \mathscr{N} \bigoplus \mathscr{I}$. In particular, we obtain an isomorphism of graded spaces $\mathscr{E}_e(w) \simeq \mathscr{N}$

From [3] we have the following result:

Lemma 1. *We have the following inequality of Hilbert series:*

$$\mathscr{E}(\rho, t) \geq \mathscr{E}(\widehat{\rho}, t).$$

Proof. This is [3, Theorem 1.4]. □

So now, we are interested in the computation of monomial algebras. In [4], Anick introduced n-chains. Assume that the family $\widehat{\rho}$ is an antichain of monomials, i.e. not stable by submonomials. We inductively define n-chains of $\widehat{\rho}$ by 1-chain $\widehat{\rho}^{(1)} := \widehat{\rho}$ and we say that a monomial $u := x_{i_1} \dots x_{i_t}$ is an n-chain if there exist integers a_j and b_j with $1 \leq j \leq n$ such that:

- $1 = a_1 < a_2 \leq b_1 < a_3 \leq b_2 < \cdots < a_n \leq b_{n-1} < b_n = t$
- $x_{i_{a_j}} \dots x_{i_{b_j}} \in \widehat{\rho}$,
- $x_{i_1} \dots x_{i_s}$ is not an m-chain for $s < b_m, 1 \leq m \leq n$.

We denote by $\widehat{\rho}^{(n)}$ the set of n-chains of $\widehat{\rho}$. Observe that $\widehat{\rho}^{(k)}\mathbb{F}_p \bigotimes \mathscr{E}_e(\widehat{\rho})$ is a free graded $\mathscr{E}_e(\widehat{\rho})$-module where elements in $\widehat{\rho}^{(k)}$ are endowed with degree defined in their embeddings in $\mathscr{E}_e$.

Theorem 8 (Anick resolution)**.** *We have the following exact sequence of $\mathscr{E}_e(\widehat{\rho})$-CGA modules:*

$$\cdots \to \widehat{\rho}^{(n)}\mathbb{F}_p \bigotimes \mathscr{E}_e(\widehat{\rho}) \to \cdots \to \widehat{\rho}^{(1)}\mathbb{F}_p \bigotimes \mathscr{E}_e(\widehat{\rho}) \to \bigoplus_i X_i \mathscr{E}_e(\widehat{\rho}) \to \mathscr{E}_e(\widehat{\rho}) \to \mathbb{F}_p \to 0,$$

where of course $\deg(X_i) = e_i$.

Proof. This is [4, Theorem 1.4]. □

Corollary 3. *We have the equality:*

$$\mathscr{E}_e(\widehat{\rho}, t) = \frac{1}{1 - \sum_i t^{e_i} + \sum_{k \geq 1} (-1)^{k+1} \widehat{\rho}^{(k)}(t)}.$$

Proof. We apply Theorem 8 and then we use Corollary 1. □

Let us now discuss the special case of combinatorially free families. We say that a monomial X^α is a submonomial of the monomial $X^{\alpha'}$, if there exists two monomials X^β and $X^{\beta'}$ such that $X^{\alpha'} := X^\beta X^\alpha X^{\beta'}$. Therefore, we write $X^\alpha \subset X^{\alpha'}$.

Definition 17. *Let $\mathscr{F} := \{X^{\alpha(i)}\}_{i\in\mathbf{I}}$ be a family of monomials. We say that $\mathscr{F}$ is combinatorially free, if:*

1. *for every $i \neq j$, $X^{\alpha(i)}$ is not a submonomial of $X^{\alpha(j)}$,*
2. *for every i, j, there do not exist nontrivial monomials X^β and X^γ such that $X^\beta X^{\alpha(i)} = X^{\alpha(j)}X^\gamma$.*

Corollary 4. *If the family $\widehat{\rho}$ is combinatorially free, then*

$$\mathscr{E}(\widehat{\rho}, t) = \frac{1}{1 - dt + \sum_i t^{\deg(\rho_i)}}.$$

Proof. We observe that $\widehat{\rho}^{(2)} = \{0\}$. Then we conclude using Corollary 1. □

Remark 3. *When $\widehat{\rho}$ is combinatorially free, we can also observe that $\widehat{\rho}$ is a Gröbner basis of $\mathscr{I}(\rho)$, and normal words are exactly words which do not contain $\widehat{\rho}$ as submonomials.*

Combinatorially free families also satisfy the following nice property:

Theorem 9. *Let w be a family in E_e and write $\rho := \overline{w}$. We assume that the family $\widehat{\rho}$ is combinatorially free, then we have*

$$\mathscr{I} = \mathscr{I}(\rho).$$

As a consequence, we infer:

$$\mathscr{E}(w, t) = \mathscr{E}(\rho, t) = \mathscr{E}(\widehat{\rho}, t) = \frac{1}{1 - dt + \sum_i t^{\deg(\rho_i)}}.$$

Proof. This is done in the proof of [29, Theorem 3.7], see also [60] and [43, Theorem B]. □

We conclude this part with an example.

Example 10 (Right Angled Artin Algebras)**.** *Let $\Gamma := (\mathbf{X}; \mathbf{E})$ be an undirected graph on d vertices $\{X_1; \ldots; X_d\}$. We define $w_{ij} := [X_i; X_j]$ when $\{X_i; X_j\}$ is in $\mathbf{E}$. Observe that we also have $\rho_{ij} := \overline{w_{ij}} = [X_i; X_j]$.*

Then upto the fixed order on monomials, either $\widehat{\rho_{ij}} = X_iX_j$ or $\widehat{\rho_{ij}} = X_jX_i$. Furthermore, the family $\widehat{\rho_{ij}}$ is combinatorially free (up to some order) exactly when Γ is a bipartite graph.

We define Δ (resp. $I(\Gamma)$, $\mathscr{I}(\Gamma)$) the two-sided ideal generated by w_{ij} (resp. ρ_{ij}). It is not hard to see that $\Delta = I(\Gamma)$ and $\mathrm{Grad}(\Delta) = \mathrm{Grad}(I(\Gamma)) = \mathscr{I}(\Gamma)$ (see [43, Proposition 1.7]). We also introduce

$$E(\Gamma) := E(w) := E/I(\Gamma).$$

When Γ is bipartite and has r edges, we infer:

$$\mathscr{E}(\Gamma, t) = \frac{1}{1 - dt + rt^2}.$$

In Example 11, we infer a formula for every graph using Koszulity.

1.3 Group filtrations and cohomology

In this part, we study some filtrations of pro-p groups (mostly the Zassenhaus and the lower central series) and relate them to Lie algebras. We infer several consequences on pro-p groups.

1.3.1 Some Definitions

First, we introduce some definitions.

Definition 18 ((Completed) group algebra)**.** *Take G a finitely generated pro-p group. Define the group algebra of G over $\mathbb{A}$ by:*

$$\mathbb{A}[G] = \{\sum_{g\in G} a_g g; (a_g)_{g\in G} \text{ almost zero everywhere in } \mathbb{A}\}.$$

Take $N \subset N'$ two open subgroups of G, then we have a surjection $G/N' \to G/N$ and so we obtain the following surjection: $\mathbb{A}[G/N'] \to \mathbb{A}[G/N]$: this is an inverse system.
Define the completed group algebra of G over $\mathbb{A}$ by:

$$Al(\mathbb{A}, G) := \varprojlim_N \mathbb{A}[G/N], \quad \text{where } N \text{ is open and normal.}$$

The algebra $Al(\mathbb{A}, G)$ admits an augmentation map $Al(\mathbb{A}, G) \to \mathbb{A}$. We denote its kernel $Al_1(\mathbb{A}, G)$. The topology given by $\{Al_n(\mathbb{A}, G)\}$, the n-th power of $Al_1(\mathbb{A}, G)$ makes $Al(\mathbb{A}, G)$ a $\mathbb{A}$-compact algebra. Furthermore, we have a map

$$G \to Al(\mathbb{A}, G); \quad g \mapsto \prod_N gN, \quad \text{where } N \text{ is taken in an open normal basis of } G.$$

Thus $\mathbb{A}[G]$ is dense into $Al(\mathbb{A}, G)$.

Let us now endow $Al(\mathbb{A}, G)$ with filtrations. For this purpose, consider a minimal presentation of G:

$$1 \to R \to F \to G \to 1,$$

defined by generators $\{x_1; \dots; x_d\}$ and relations $\{l_i\}_{i\in \mathbf{I}}$. Magnus isomorphism [69, Chapitre II, Partie 3] gives us:

$$\phi_{\mathbb{A}} \colon Al(\mathbb{A}, F) \to \mathbb{A}\langle\langle X_1; \dots; X_d\rangle\rangle; \quad x_i \mapsto X_i + 1.$$

Then we infer an isomorphism between $Al(\mathbb{A}, F)$ and $E_e(\mathbb{A})$. We denote by $I(\mathbb{A}, R)$ the closed two-sided ideal of $E_e(\mathbb{A})$ generated by $\{w_i := \phi_{\mathbb{A}}(l_i - 1)\}$.

Consequently, we can define an (X, e)-filtration on $Al(\mathbb{A}, F)$ and $I(\mathbb{A}, R)$ by the Magnus isomorphism between $Al(\mathbb{A}, F)$ and $E_e(\mathbb{A})$. The filtration on $I(\mathbb{A}, R)$ is given by the induced filtration from $E_e(\mathbb{A})$ (given by $\{I(\mathrm{R}) \cap E_n(\mathbb{A})\}_{n\in\mathbb{N}}$). Then, we introduce $E_e(\mathbb{A}, G) := E_e(\mathbb{A})/I(\mathbb{A}, R)$: this is a $\mathbb{A}$-filtered compact algebra endowed with quotient filtration (see

[69, Chapitre I, Resultat 2.1.7]). Magnus isomorphism gives us the following isomorphism of compact algebras:

$$E_e(\mathbb{A}, G) \simeq Al(\mathbb{A}, G).$$

Introduce the following (X, e)-filtration on G:

$$G_{e,n}(\mathbb{A}) := \{g \in G; \phi_{\mathbb{A}}(g) - 1 \in E_{e,n}(\mathbb{A}, G)\}.$$

When $\mathbb{A} := \mathbb{F}_p$ and $e = 1$, this filtration denotes the Zassenhaus filtration of G (for references see [92]). Under some conditions on G (see for instance [64]), if $\mathbb{A} := \mathbb{Z}_p$ and $e = 1$, the filtration $G_n(\mathbb{Z}_p)$ corresponds to lower central series, defined by $\gamma_1(G) := G$ and $\gamma_n(G) = [\gamma_{n-1}(G); G]$.

We are interested in the following sets:

$$\mathscr{L}_e(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{L}_{e,n}(\mathbb{A}, G), \quad \text{where} \quad \mathscr{L}_{e,n}(\mathbb{A}, G) := G_{e,n}(\mathbb{A})/G_{e,n+1}(\mathbb{A}), \quad \text{and}$$
$$\mathscr{E}_e(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_{e,n}(\mathbb{A}, G), \quad \text{where} \quad \mathscr{E}_{e,n}(\mathbb{A}, G) := E_{e,n}(\mathbb{A}, G)/E_{e,n+1}(\mathbb{A}, G).$$

We always assume that $\mathscr{L}_e(\mathbb{A}, G)$ is **torsion-free** over $\mathbb{A}$. Notice that this condition is automatically checked when $\mathbb{A} := \mathbb{F}_p$, contrary to the case $\mathbb{A} := \mathbb{Z}_p$ (see for instance [63, Theorem]). Since G is finitely generated, one denominates for every integer n:

$$a_{e,n} := \mathrm{rank}_{\mathbb{A}} \mathscr{L}_{e,n}(\mathbb{A}, G), \quad \text{and} \quad c_{e,n} := \mathrm{rank}_{\mathbb{A}} \mathscr{E}_{e,n}(\mathbb{A}, G),$$
$$gocha_e(\mathbb{A}, t) := \sum_{n\in\mathbb{N}} c_{e,n} t^n.$$

Finally, we define $n_{e,i}$ the weight of w_i in $E_e(\mathbb{A})$ and ρ_i the image of w_i in $E_{e,n_{e,i}}(\mathbb{A})/E_{e,n_{e,i}+1}(\mathbb{A})$.

Let us introduce a criterion on presentations of pro-p groups which allows us to compute the gocha series.

Definition 19. *We say that the presentation of G is mild, if the family $w := \{\phi_{\mathbb{F}_p}(l_i - 1)\}_i$ is combinatorially free in $E_e(\mathbb{F}_p)$, for some (X, e)-filtration.*

1.3.2 (Co)homology of pro-p groups and algebras

In this subpart, we mostly follow [112, Chapter 6], [59] and [31, Chapter 3] for cohomological results.

We observe that $\mathbb{A}$ is a compact $Al(\mathbb{A}, G)$-module with trivial action (so also a filtered compact $E_e(\mathbb{A}, G)$-module). Let us consider a free resolution of $Al(\mathbb{A}, G)$-compact modules of $\mathbb{A}$ that we denote by:

$$\cdots \to P_n \to \cdots \to P_1 \to P_0 \to \mathbb{A} \to 0.$$

Let us consider B a discrete $Al(\mathbb{A}, G)$-module, then we have a complex:

$$0 \to \mathrm{Hom}_{Al(\mathbb{A},G)}(\mathbb{A}, B) \to \mathrm{Hom}_{Al(\mathbb{A},G)}(P_0, B) \to \cdots \to \mathrm{Hom}_{Al(\mathbb{A},G)}(P_n, B) \to \ldots.$$

Similarly, if we consider C a compact $Al(\mathbb{A},G)$-module, then we have a complex:

$$\cdots \to P_n \otimes_{Al(\mathbb{A},G)} C \to \cdots \to P_1 \otimes_{Al(\mathbb{A},G)} C \to P_0 \otimes_{Al(\mathbb{A},G)} C \to \mathbb{A} \otimes_{Al(\mathbb{A},G)} C \to 0.$$

Then we define $H^\bullet(G,B)$ the homology of the first complex, and $H_\bullet(G,B)$ the homology of the second complex. To simplify notations, we write for every integer n:

$$H^n(G) := H^n(G,\mathbb{A}), \quad \text{and} \quad H_n(G) := H_n(G,\mathbb{A}).$$

Observe that $H^n(G;\bullet)$ (resp. $H_n(G;\bullet)$) is a functor from the category of $Al(\mathbb{A},G)$-compact modules to the category of $Al(\mathbb{A},G)$-discrete modules (resp. $Al(\mathbb{A},G)$-compact modules). Furthermore, for every exact sequence $0 \to A \to B \to C \to 0$ of $Al(\mathbb{A},G)$-compact modules, we have connecting morphisms $\{\delta^n\}_{n\in\mathbb{N}}$ (resp. $\{\delta_n\}_{n\in\mathbb{N}}$) and long exact sequences:

$$\cdots \to H^n(G,A) \to H^n(G,B) \to H^n(G,C) \to^{\delta^n} H^{n+1}(G,A) \to \dots$$
$$\cdots \to H_n(G,A) \to H_n(G,B) \to H_n(G,C) \to^{\delta_n} H_{n-1}(G,A) \to \dots$$

Moreover, these functors do not depend on the resolution of $\mathbb{A}$.

We define the cohomological dimension of G as the minimal integer n (eventually infinite) such that for all $m > n$, $H^m(G) = 0$.

Remark 4. • *In general we work with projective rather than free modules. However, since here G is a finitely generated pro-p group, then by [102, Corollary 5.20] these notions coincide.*

• *For other references on (profinite) group cohomology, we also quote [119] and the Thesis of Rogelstad [114, Chapter 2].*

We can use cohomology to compute $d(G)$ and $r(G)$.

Theorem 10. *Let G be a finitely generated pro-p group. Then we have*

1. $d(G) = \dim_{\mathbb{F}_p} G/\mathrm{Frat}(G) = G/G^p[G;G] = dim_{\mathbb{F}_p} H^1(G)$.
2. $r(G) = \dim_{\mathbb{F}_p} R/R^p[R;F] = \dim_{\mathbb{F}_p} H^2(G)$.

Proof. For the first point, see [59, Theorem 6.1].
For the second point, see [59, Theorem 6.13]. □

Consequently, we can define $H(G) := \bigoplus_n H^n(G)$: this is a graded $\mathbb{A}$-vector space which is endowed by a structure of graded algebra, where the product is given by the cup-product. (see for instance the construction [31, Part 3.4]).

Remark 5. *Similarly, we can construct (co)homology theory for compact and CGA algebras. For instance, we notice that $H(G) \simeq H(Al(G))$. Furthermore, in some cases, we compare $H(G)$ with $H(\mathscr{E}(G))$ (which are not always isomorphic, we refer to [73] for more details).*

Proposition 14. *We have the following assertions:*

(*i*) *If H is a closed subgroup of G, then* $\mathrm{cd}(H) \leq \mathrm{cd}(G)$.

(*ii*) *The group G is free if and only if* $\mathrm{cd}(G) = 1$.

(*iii*) *If G has torsion then its cohomological dimension is infinite.*

Proof. For (i), we refer to [59, Theorem 5.3].

For (ii), we refer to [102, Proposition 3.5.17].

For (iii), there exists an element x in G of order p^k. Then the closed subgroup H generated by x is finite cyclic (indeed isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$). From [31, Exemple 3.2.9], the group H has infinite cohomological dimension. So by (i), the group G has also infinite cohomological dimension. □

Consequently, if a group has finite cohomological dimension, then it is torsion-free, so infinite.

1.3.3 Mild presentation, Koszulity and Right Angled Artin Groups

We finish this part by concrete examples of groups with cohomological dimensions larger than or equal two. We refer to [108] for results on Koszulity, but also [75, 106]. In this subpart, we always take $\mathbb{A} := \mathbb{F}_p$.

We remind that $\mathscr{I}(\rho)$ is the ideal generated by $\rho := \overline{w} := \overline{\phi_{\mathbb{F}_p}(l_\bullet - 1)}$ in $\mathscr{E}_e$, and $\mathscr{I}(\mathbb{F}_p; R) = \mathrm{Grad}(I(\mathbb{F}_p, R)$ where $I(\mathbb{F}_p, R)$ is the ideal generated by w in E_e.

Definition 20. *We say that a pro-p group G has a mild presentation, if the family $\widehat{\rho}$ is combinatorially free in $\mathscr{E}_e(\mathbb{F}_p)$.*

We begin by studying the cohomology of mild groups.

Theorem 11. *If G has a mild presentation, then we have the following exact sequence of filtered $E_e(\mathbb{F}_p, G)$-modules:*

$$0 \to \prod_j w_j E_e(\mathbb{F}_p, G) \to \prod_i X_i E_e(\mathbb{F}_p, G) \to E_e(\mathbb{F}_p, G) \to \mathbb{F}_p \to 0.$$

Proof. First of all, from the proof of [29, Theorem 3.7], we have the following equality:

$$\mathscr{I}(\rho) = \mathscr{I}(\mathbb{F}_p, R).$$

Furthermore since ρ is strongly free, we infer the filtered isomorphism (see [29])

$$\mathscr{I}(\mathbb{F}_p, R)/\mathscr{E}_{e,\geq 1}(G)\mathscr{I}(\mathbb{F}_p, R) \simeq \bigoplus_j \rho_j \mathscr{E}_e(\mathbb{F}_p, G),$$

where $\mathscr{E}_{e,\geq 1}(\mathbb{F}_p, G)$ is the augmentation ideal of $\mathscr{E}_e(\mathbb{F}_p, G)$.

This gives us the resolution of $\mathscr{E}_e(\mathbb{F}_p, G)$-modules:

$$0 \to \bigoplus_j \rho_j \mathscr{E}_e(\mathbb{F}_p, G) \to \bigoplus_i X_i \mathscr{E}_e(\mathbb{F}_p, G) \to \mathscr{E}_e(\mathbb{F}_p, G) \to \mathbb{F}_p \to 0.$$

From Serre's Lemma [69, Chapitre 5, Lemme (2.1.1)], we can lift the previous resolution to infer:

$$0 \to \prod_j w_j E_e(\mathbb{F}_p, G) \to \prod_i X_i E_e(\mathbb{F}_p, G) \to E_e(\mathbb{F}_p, G) \to \mathbb{F}_p \to 0.$$

□

Corollary 5. *If G has a mild presentation, then :*

- *the presentation is minimale,*
- *G has cohomological dimension 2,*
- *the gocha series is given by:*

$$gocha_e(\mathbb{F}_p, t) = \frac{1}{1 - \sum_i t^{e_i} + \sum_i t^{\deg_e(\rho_i)}},$$

Proof. This is a direct Corollary from Theorem 11, we also refer to [29, Corollary 5.3]. □

Let us now introduce Koszulity and for the rest of the subpart, we assume $e = 1$. Let us denote by $\mathscr{N} := \mathscr{E}/\mathscr{I}$, this is a $\mathbb{F}_p$-CGA. We say that $\mathscr{N}$ is Koszul if:

(*i*) the ideal $\mathscr{I}$ admits quadratic generators,

(*ii*) the trivial $\mathscr{N}$-CGA module admits a linear finite resolution, i.e. there exists an integer n and free $\mathscr{N}$-CGA modules $\mathscr{P}_i := \bigoplus_j \mu_{i,j}\mathscr{N}$ where $\deg(\mu_i) := i$ such that we have an exact sequence of $\mathscr{N}$-CGA modules:

$$0 \to \mathscr{P}_n \to \mathscr{P}_{n-1} \to \cdots \to \mathscr{N} \to \mathbb{F}_p \to 0.$$

Let us denote by ρ the set of quadratic relations which defines $\mathscr{N}$ (so in $\mathscr{E}_2$). Let us denote by V^* the dual of a vector space V. Observe that $\mathscr{E}_2^* \simeq \mathscr{E}_1^* \otimes \mathscr{E}_1^*$, and we have a canonical pairing $\mathscr{E}_2 \times \mathscr{E}_2^* \to \mathbb{F}_p$. We define by $\rho^!$ a set of generators of the orthogonal complement of $\rho\mathbb{F}_p$. And we define $\mathscr{I}^!$ the two-sided ideal generetad by $\rho^!$ and $\mathscr{N}^! := \mathscr{E}/\mathscr{I}^!$.

Proposition 15. *If $\mathscr{N}$ is Koszul, then we have the following isomorphism of graded algebras:*

$$\mathscr{N}^! \simeq H(\mathscr{N}).$$

Furthermore, we have:

$$\mathscr{N}(t)\mathscr{N}^!(-t) = 1.$$

Moreover, if $\mathscr{N}^!$ is Koszul, then $\mathscr{N}$ is also and we have $(\mathscr{N}^!)^! \simeq \mathscr{N}$.

Proof. See [108, Chapter 2, Part 1]. □

From [43, Proposition], we have the following result, we also refer to Leoni-Weigel [73]:

Proposition 16. *If the algebra $\mathscr{E}(G)$ is Koszul, then we have*

$$H(G) \simeq \mathscr{E}(G)^!.$$

The difficulty here is to compute $\mathscr{E}(G)$. Let us give some examples.

Example 11. • *If G admits a mild and Koszul presentation then Minàč-Pasini-Quadrelli-Tân [98] showed that $\mathscr{E}(G)$ is Koszul.*

• *Let Γ be an undirected graph, and define $G(\Gamma)$ with relations $l_{uv} := [x_u; x_v]$ where $\{u; v\}$ is an edge of Γ. We define $\mathscr{E}(\Gamma) := \mathscr{E}/\mathscr{I}(\Gamma)$ where $\mathscr{I}(\Gamma)$ is the two-sided ideal of $\mathscr{E}$ generated by $[X_u; X_v]$ where $\{u; v\}$ is an edge of Γ. Observe that $\mathscr{E}(\Gamma)^! \simeq \mathscr{A}(\Gamma)$, where $\mathscr{A}(\Gamma)$ is presented by the following relations:*

- X_iX_j *when* $\{i, j\} \notin \mathbf{E}$,
- X_u^2 *for* $u \in [\![1; d]\!]$,
- $X_uX_v + X_vX_u$ *for* u, v *in* $[\![1; d]\!]$.

From [30], the algebra $\mathscr{A}(\Gamma)$ is Koszul, thus $\mathscr{E}(\Gamma)$ is also. Furthermore, we showed in [43] that $\mathscr{E}(G(\Gamma)) \simeq \mathscr{E}(\Gamma)$.

Let us denote by $\Gamma(t) := \sum_n c_n(\Gamma)t^n$, where $c_n(\Gamma)$ is the clique number of Γ, i.e. the number of complete subgraphs of Γ with exactly n vertices. Then we infer

$$\mathscr{A}(\Gamma, t) = \Gamma(t), \quad \text{and} \quad \mathscr{E}(\Gamma, t) = gocha(G(\Gamma), t) = \frac{1}{\Gamma(-t)}.$$

Finally, the cohomological dimension of $G(\Gamma)$ is given by the clique number of Γ, i.e. the number of vertices of the maximal complete subgraph of Γ.

1.4 Galois Theory

In this part, we are interested by Galois groups over fields of characteristic zero. We will give some results on local, global and formally real Pythagorean fields k. The goal of this part, is to study some quotients of the group $\mathrm{Gal}(\hat{k}/k)$, where $\hat{k}$ is the maximal p-extension of k: this is the compositum of all finite p-extensions of k (i.e finite Galois extension of order a power of p). Let us first show that $\hat{k}$ is stable by p-extensions.

Proof. Let L be a p-extension of $\hat{k}$. If L' is a conjugate of L over k, then L' is also a p-extension of $\hat{k}$. Take N the normal closure of L/k, this is the compositum of L and its conjugate over k. Then the Galois group of N over k is a fibered product of p-groups. Which implies that N is a p-extension of k, so $\hat{k} \subset L \subset N \subset \hat{k}$. □

1.4.1 Local fields

This subpart mostly follow [59, Chapters 8 and 10]. Let k be a local field of characteristic zero, O_k its ring of valuation, $\mathfrak{p}_k$ its maximal ideal, π_k a uniformizer, $\kappa(k)$ its residual field, q_k the characteristic of the residue field, $N(\mathfrak{p}_k)$ the number of elements of $\kappa(k)$. Here we study the group $G := \mathrm{Gal}(\hat{k}/k)$.

Case where q_k is a power of p

Assume q_k is a power of p, then we have the following result (for more details, we refer to [139, §2] and [37]):

Theorem 12. *The pro-p group G has $[k : \mathbb{Q}_p] + 1 + \delta$ generators. If k does not contain the p-th root of unity, then G is free, else G is a Demushkin group.*

Case q_k is not a power of p

Assume that q_k is not a power of p. We define:

$$k(n) := \{x \in k^\times; x \equiv 1 \pmod{\pi_k^n}\}.$$

Lemma 2. *We have:*

$$k^\times = \pi_k^{\mathbb{Z}} \times \kappa(k)^\times \times k(1),$$

with

$$k(1) \simeq \mu_{q^\infty}(k) \times \mathbb{Z}_{q_k}^{[k;\mathbb{Q}_{q_k}]},$$

where $\mu_{q^\infty}(k)$ designates the roots of unity in k of order coprime to q_k.

Proof. See [101, Proposition (2.5.7)]. □

Let K be a Galois finite extension of k, with degree d, ramification index e, and inertia degree f. Define $T_K := k(\mu_{N(\mathfrak{p}_K)-1})$, the maximal unramified extension contained in K. We say $\delta_p(K) = 0$ if K does not contain p-th roots of unity, else $\delta_p(K) = 1$.

Corollary 6. *Assume q_k and p are coprime. Then, the following assertions are equivalent:*

1. $\delta_p(K) = 1$
2. $\mu_p(K)$ *is a subgroup of* $\kappa(K)^\times$,
3. p *divides* $N(\mathfrak{p}_K) - 1 := N(\mathfrak{p}_k)^f - 1$
4. $N(\mathfrak{p}_K) \equiv N(\mathfrak{p}_k)^f \equiv 1 \pmod{p}$.

Let us now study K/k, a tamely ramified extension: which means the ramification index e is coprime with q_k. Since K/T_K is totally ramified, then $\pi_K^e \in T_K^\times$, and:

$$\pi_K^e := \pi_k \times \zeta \times \epsilon,$$

with $\zeta \in \kappa(T_K)$, and $\epsilon \in T_K(1)$. However $\kappa(T_K) \times T_K(1)$ is a $\mathbb{Z}_{q_k}$-module, and $gcd(e, q_k) = 1$. Therefore $1/e \in \mathbb{Z}_{q_k}$, and:

$$(\frac{\pi_K}{\epsilon^{1/e}})^e = \pi_k \zeta.$$

So $\pi_k\zeta$ is an e-th power in K, which implies:

$$K := T_K((\zeta\pi_k)^{1/e}).$$

Moreover, K/T_K is Galois if and only if K contains e-th roots of unity.
In particular, assume K/k is a p-extension, with p coprime to q_k. Then $e = 1$ or a power of p, so K/k is tamely ramified. If k does not contain roots of unity, then K does not (equivalence), and so $e = 1$. We obtain:

Corollary 7. *Let p be coprime to q_k, then:*
$N(\mathfrak{p}_k) \not\equiv 1 \pmod{p}$ if and only if every p-extension of k is unramified.

Let us denote by

$$G_k := \mathrm{Gal}(\hat{k}/k), \text{ and } \mathscr{T}_k := \mathrm{Gal}(\hat{k}/T_{\hat{k}})$$

these are pro-p-groups, and we have:

$$G_k/\mathscr{T}_k \simeq \mathbb{Z}_p.$$

Local class field theory identifies the uniformizer π_k with a generator of $G_k/\mathscr{T}_k$ (Frobenius), and a system ϵ_j of principal units with generators of $\mathscr{T}_k$ (Inertia group).

Proposition 17. *If $\delta_p(k) = 0$, then $\hat{k}$ is the maximal p-unramified extension of k and*

$$G_k \simeq \mathbb{Z}_p.$$

We can take the Frobenius as a generator of G_k.

Proof. If $\delta_p(k) = 0$, then every p-extension is unramified. □

Proposition 18. *If $\delta_p(k) = 1$, then the group G_k has two generators σ and τ, and one relation:*

$$[\sigma; \tau] = \tau^{N(\mathfrak{p}_k)-1}.$$

We can write:

$$G_k \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p \simeq \mathscr{T}_k \rtimes G_k/\mathscr{T}_k,$$

here σ acts over τ by conjugacy given before.

Proof. Assume $\delta_p(k) = 1$, then p divides $N(\mathfrak{p}_k) - 1$. Consequently

$$N(\mathfrak{p}_k) \equiv 1 \pmod{p} \implies N(\mathfrak{p}_k)^{p^{n-1}} \equiv 1 \pmod{p^n}.$$

Therefore the family $\{\zeta_{p^n}\}_n$ generates subgroups of $\kappa(T_k)$.
One concludes that

$$T_k = \bigcup_{n\in\mathbb{N}} k(\zeta_{p^n}).$$

Define

$$K_n := k(\zeta_{p^n}; \pi_k^{1/p^n}), \text{ then, } \hat{k} := \bigcup_n K_n.$$

Considering Lemma 2, let us introduce:

$$\begin{aligned} \sigma_n(\zeta_{p^n}) &:= \zeta_{p^n}^{N(\mathfrak{p}_k)}, \qquad \text{and} \quad \sigma_n(\pi_k^{1/p^n}) &:= \pi_k^{1/p^n} \\ \tau_n(\zeta_{p^n}) &:= \zeta_{p^n}, \qquad \text{and} \quad \tau_n(\pi_k^{1/p^n}) &:= \zeta_{p^n}\pi_k^{1/p^n}. \end{aligned}$$

So, we conclude writing $\tau := \prod_n \tau_n$ and $\sigma := \prod_n \sigma_n$. □

1.4.2 Global Field

Here we consider k a number field. We give here some tools to compare the global case with the local one. Several pieces of information on the second case are known, see [59, Chapter 10]. We mostly follow for this subpart [59, Chapters 8 and 11], [139, § 3] and [37]. Let us consider $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_d\}$ a set of d different primes, and we define by k_S the maximal p-extension of k unramified outside S.

Wild case

Assume that S contains all primes above p.

Theorem 13. *Assume either $p \neq 2$ or k totally imaginary, then $\mathrm{cd}(G_S) \leq 2$.*

Proof. [37, Proposition 7]. □

Definition 21. *We say that k is p-rational if G_S is free.*

Example 12. *Let us give some examples:*

- *Take $k := \mathbb{Q}(\zeta_p)$, when p is an irregular prime.*
- *A conjecture of Gras [34] states that if k is a fixed number field, then it is p-rational for p large enough.*

Tame case

Let us here consider $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_d\}$ a set of d different tame primes, i.e. p divides $N_{k/\mathbb{Q}}(\mathfrak{p}_i) - 1$. Define k_S the p-maximal extension of k unramified outside S, and $G_S := \mathrm{Gal}(k_S/k)$. Observe that the group G_p injects into $G_k := \mathrm{Gal}(\hat{k}/k)$ and G_k surjects onto G_S. Consider the map $\phi_{\mathfrak{p}}$ given by:

$$\phi_{\mathfrak{p}} \colon G_{\mathfrak{p}} \to G_k \to G_S.$$

Then, we obtain a map:

$$\phi_S^* \colon H^2(G_S; \mathbb{F}_p) \to \bigoplus_{\mathfrak{p} \in S} H^2(G_{\mathfrak{p}}; \mathbb{F}_p).$$

The goal of this part is to obtain some conditions ensuring that ϕ_S^* is injective. For this purpose, let us introduce:

$$\mathrm{V}_S = \{x \in k^\times, x \in k_{\mathfrak{p}}^p \quad \forall \mathfrak{p} \in S\}.$$

Observe that $k^{\times p}$ is included in V_S, and the group $V_S/k^{\times p}$ is finite. Introduce $B_S := (V_S/k^{\times p})^*$, the dual of $V_S/k^{\times p}$.

Theorem 14. *We have the following injection:*

$$\ker(\phi_S^*) \to B_S.$$

Proof. See proof [59, Theorem 11.3]. □

Assume $k := \mathbb{Q}$, or k is a quadratic imaginary extension of $\mathbb{Q}$ (if $p = 3$, assume $k \neq \mathbb{Q}(j)$, where j is a root of $X^2 + X + 1$). Then $B_S = 0$.
Therefore (see for instance [115, Theorem 2.6]), the pro-p group G_S can be described by $x_1, \cdots, x_d$ generators and $l_1, \cdots, l_d$ relations verifying:

$$l_i = \prod_{j \neq i} [x_i, x_j]^{a_j(i)} \mod F_3(\mathbb{F}_p), \tag{1.1}$$

where $a_j(i) \in \mathbb{Z}/p\mathbb{Z}$.

Furthermore, by Class Field theory, the element x_i can be chosen as a generator of the inertia group of $\mathfrak{p}_i$. The element $a_j(i)$ is zero if and only the prime $\mathfrak{p}_i$ splits in $\mathrm{k}^p_{\{\mathfrak{p}_j\}}/\mathrm{k}$, where $k^p_{\{\mathfrak{p}\}}$ is the (unique) cyclic degree p-extension of k unramified outside $\mathfrak{p}$. This is equivalent to

$$p_i^{(p_j-1)/p} \equiv 1 \pmod{p_j},$$

where p_i is a prime in $\mathbb{Q}$ below $\mathfrak{p}_i$.

Finally, by Class Field theory, the group G_S is also FAB (finite abelianisation property), i.e. every open subgroup has finite abelianisation. For references on FAB groups, we refer to [62, 81]. For further references on Class Field Theory, we refer to [59, Part 8], [116, Chapter 2] and [101, Chapters IV-VI].

Example 13. *We give some examples.*

• *Take $p = 3$, and $S_0 = \{7, 13\}$, $T = \emptyset$. Put $S = \{p_1, p_2, p_3, p_4, p_5\}$ with $p_1 = 31, p_2 = 19, p_3 = 13, p_4 = 337, p_5 = 7$. The highest terms of the relations (1.1), viewed in $\mathscr{E}(\mathbb{A}) := \mathbb{A}\langle X_1; \ldots; X_5\rangle$, are $\widehat{\rho_1} = X_5X_1$, $\widehat{\rho_2} = X_5X_2$, $\widehat{\rho_3} = X_4X_3$, $\widehat{\rho_4} = X_4X_2$, $\widehat{\rho_5} = X_5X_3$. Since the $\widehat{\rho_i}$'s are combinatorially free, then G_S is of cohomological dimension 2 by Theorem 5.*

• *Take $p = 3$, and consider $k := \mathbb{Q}(\sqrt{-163})$. Then we define $\Delta := \mathrm{Gal}(k/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, and fix χ_0 the nontrivial irreducible character of Δ over $\mathbb{F}_p$. Consider the following set of primes in $\mathbb{Q}$: $\{p_1 := 31, p_2 := 19, p_3 := 13, p_4 := 337, p_5 := 7, p_6 := 43\}$. The class group of k is trivial, the primes p_1, p_2, p_3, p_4, p_5 are inert in k, and the prime p_6 totally splits in k. Define S the primes above the previous set in k, and k_S the maximal p-extension unramified outside S. Then Δ acts on $G := \mathrm{Gal}(k_S/k)$, which is FAB by Class Field theory. Following Koch's presentation, the group G admits 7 generators and 7 relations which satisfies: $\hat{\rho}_1 = X_5X_1, \hat{\rho}_2 = X_5X_2, \hat{\rho}_3 = X_4X_3, \hat{\rho}_4 = X_4X_2, \hat{\rho}_5 = X_5X_3, \hat{\rho}_6 := X_6X_3, \hat{\rho}_7 = X_7X_3$.*
Therefore the pro-p group G is mild, so we obtain

$$gocha(\mathbb{F}_p, t) := \frac{1}{1 - 7t + 7t^2}.$$

1.4.3 Formally real Pythagorean fields of finite type

The main reference is [68] and [67, Chapter VIII].

A field k is formally real if -1 is not a sum of squares. Furthermore, it is Pythagorean if the sum of two squares is a square. Finally k is RPF if k is a formally real, Pythagorean field and $|k^\times/k^{2\times}|$ is finite. We denote by G_k the pro-2 absolute Galois group of k. Observe that G_k is a finitely presented pro-2 group and we have an isomorphism of $\mathbb{F}_2$-vector spaces $G_k/G_{k,2} \simeq k^\times/k^{2\times}$. So G_k is finitely generated and we denote by $d := \dim_{\mathbb{F}_2} H^1(G_k)$.

Definition 22. *An ordering on k is a set P which satisfies the following properties:*

(*i*) $P + P \subset P$,

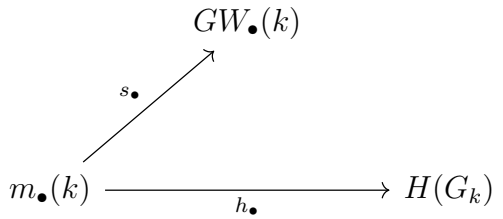
(*ii*) $P.P \subset P$,

(*iii*) $k = P \cup (-P)$.

The number of orderings of k, that we call $o(k)$ is bounded by d and 2^{d-1}. This is a well studied invariant, and we refer to [13] and [89]. There exist always fields k which reach the previous bounds for every d: we say that k is SAP if $o(k) = d$ and k is superpythagorean if $o(k) = 2^{d-1}$. An ordering P also defines a unique morphism $\sigma_P \colon k^\times/k^{2\times} \to \mathbb{F}_2$. We denote by X_k the set of orderings of k endowed with the topology induced by the product topology on $\mathbb{F}_2^{k^\times/k^{2\times}}$. Indeed Marshall [82] showed that the tuple $(X_k; k^\times/k^{2\times})$ classifies RPF fields.Ináč and Spira [95, 94] also showed that indeed the quotient $G_k/G_{k,3}(\mathbb{F}_2)$ classifies RPF.

We finish by a discussion on the Milnor conjecture which was proved by Jacob for RPF fields [52] (it is also true for general fields, for further details, we refer to [111, 86, 133, 17], etc). This conjecture gives isomorphisms of commutative $\mathbb{F}_2$-CGA algebras, that we describe

in more details below, between the graded Witt ring $GW_\bullet(k)$, the mod 2 Milnor K-theory of $m_\bullet(k)$ and the cohomology algebra $H(G)$:



Let us first begin to describe these graded algebras. Recall that $H(G_k)$ is the cohomology algebra of the pro-2 absolute Galois group of k, that we denote by G_k, with coefficient in $\mathbb{F}_2$, where the product is given by the cup-product.

We define by $M_1(k)$ the group $\{[a]; a \in k^*\}$ with additive notation, i.e. $[ab] := [a] + [b]$; and $M_\bullet(k)$ by the quotient of the tensor algebra $\bigoplus_n M_1(k)^{\otimes n}$ by the ideal generated by the relations $[a] \otimes [1-a]$ with $[a]$ and $[1-a]$ in $M_1(k)$. Finally, we introduce

$$m_\bullet(k) := M_\bullet(k)/2M_\bullet(K).$$

This gives us for instance $m_0(k) := \mathbb{F}_2$ and $m_1(k) := k^*/k^{2*}$.

We define the Witt group of k as the Grothendieck group of the monoid on equivalence classes of quadratic forms over k by hyperbolic forms with sum given by direct orthogonal sum. Then we denote by $W(k)$ the Witt ring of k, which is the Witt group of k endowed with product given by the tensor product. Since isotropic forms have even dimension, then we have a well defined and nontrivial map $\overline{\dim}\colon W(k) \to \mathbb{F}_2$, which maps a quadratic form to its dimension modulo 2. We define $Ik := \ker(\overline{\dim})$ and

$$GW_\bullet(k) := \bigoplus_n Ik^n/Ik^{n+1}.$$

Witt rings play a fundamental role in the study of quadratic forms and Formally real Pythagorean fields are exactly the fields with torsion-free Witt rings (see [67, Theorem 4.1, Chapter VIII]).

Let us now describe the morphism $s_\bullet$ and $h_\bullet$. For every integer n, we define $s_n\colon m_n(k) \to GW_n(k)$ by

$$s_n([a_1] \otimes \cdots \otimes [a_n]) := \otimes_{1 \leq i \leq n} < 1; -a_i > .$$

Furthermore, we already have an isomorphism $h_1\colon k^*/k^{2*} \to H^1(G)$, that we extend to a morphism

$$h_\bullet\colon m_\bullet(k) \to H(G).$$

Example 14. *Let us finish this part with some examples of Pythagorean fields:*

- *The field $\mathbb{R}$ is RPF with absolute Galois group $G := \mathbb{Z}/2\mathbb{Z}$. The field of constructible numbers is also Pythagorean and formally real (but not of finite type). Both of these fields only have a unique ordering.*

- *For every integer d, we define $k := \mathbb{R}((x_2))\dots((x_d))$ the iterated Laurent series on $x_2, \dots, x_d$. Then k is a superpythagorean field satisfying $|k^\times : k^{2\times}| = 2^d$ and $o(k) = 2^{d-1}$. For further references, we refer to [68], [26] and [32, Example* 2.19*].*

- *For every integer d, we construct an algebraic extension k of $\mathbb{Q}$ which is SAP and satisfies $o(k) = d$ and $|k^\times : k^{2\times}| = 2^d$. Let us consider the polynomial $P := 5(X - 1)\dots(X - d) + 1$, then P has exactly d real roots and is irreducible (see an extension of Polya's criterion [128]). Consider $E := \mathbb{Q}/P$, then from [67, Corollary* 2.20*], the field E has exactly d orderings $P_1, \dots, P_d$. Take R_i the Euclidean closure of (E, P_i), and define $k := \cap_{i=1}^d R_i$. Then k is SAP and satisfies the desired conditions. We also refer to Lam [68, Chapter* 17*].*

Chapter 2

A Note on Asymptotically good extensions in which infinitely many primes split completely

Let K be a number field, and let L/K be an infinite unramified extension. Denote by $\mathscr{S}_{L/K}$ the set of prime ideals of K that split completely in L/K. In [50] Ihara proved that $\sum_{\mathfrak{p}\in\mathscr{S}_{L/K}} \frac{\log \mathrm{N}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})} < \infty$, where $\mathrm{N}(\mathfrak{p}) := |\mathscr{O}_K/\mathfrak{p}|$; and this result raised the following interesting question: are there L/K for which $\mathscr{S}_{L/K}$ is infinite? This question was answered in the positive by Hajir, Maire, and Ramakrishna in [41]. Infinite unramified extensions L/K are special cases of infinite extensions for which the root discriminants $\mathrm{rd}_F := |\mathrm{Disc}_F|^{1/[F:\mathbb{Q}]}$ are bounded, where the field F ranges over the finite-dimensional subextensions of L/K, and Disc_F is the discriminant of F. Such extensions are called *asymptotically good*, and it is now well-known that in such extensions the inequality of Ihara involving $\mathscr{S}_{L/K}$ still holds (see for example [127], [70]).

Pro-p extensions of number fields with restricted ramification allow us to exhibit asymptotically good extensions. Let p be a prime number, and let S be a finite set of prime ideals of K coprime to p (more precisely each $\mathfrak{p} \in S$ is such that $\mathrm{N}(\mathfrak{p}) \equiv 1 (\mathrm{mod}\ p)$); the set S is called *tame*. Let K_S be the maximal pro-p extension of K unramified outside S, put $G_S := \mathrm{Gal}(K_S/K)$. In K_S/K the root discriminants are bounded by some constant depending on the discriminant of K and the norm of the places of S (see for example [40, Lemma 5]). Moreover thanks to the Golod-Shafarevich criterion, it is well-known that K_S/K is infinite when $|S|$ is large in comparison to the degree of K over $\mathbb{Q}$ (see for example [102, Chapter X, §10, Theorem 10.10.1]), and therefore asymptotically good. For instance, if $p > 2$, $\mathbb{Q}_S/\mathbb{Q}$ is infinite when $|S| \geq 4$. In [41] the authors showed that when S is large, there exists infinite subextension L/K of K_S/K for which the set $\mathscr{S}_{L/K}$ is infinite, without providing any information on $\mathrm{Gal}(L/K)$. Here we prove:

Theorem A. *Let p be a prime number, and let K be a number field. For $p = 2$ assume K totally imaginary. Let T and S_0 be two disjoint finite sets of prime ideals of K, where S_0 is*

tame. Then for infinitely many finite sets S of tame prime ideals of K containing S_0, there exists an infinite pro-p extension L/K in K_S/K such that

(i) the set $\mathscr{S}_{L/K}$ is infinite and contains T;

(ii) the pro-p group $G := \mathrm{Gal}(L/K)$ is of cohomological dimension 2;

(iii) the minimal number of relations of G is infinite, i.e. $|H^2(G, \mathbb{F}_p)| = \infty$;

(iv) for each $\mathfrak{p} \in S$, the local extension $L_\mathfrak{p}/K_\mathfrak{p}$ is maximal, i.e. isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$;

(v) we have the equality $gocha(G,t) = \big(1 - dt + rt^2 + t^3 \sum_{n\geq 0} t^n\big)^{-1}$, where d is the minimal number of generators of G_S, and where r is explicit, depending on K, S, T.

Remark 1. *We will see that the pro-p group G of Theorem A is mild in the terminology of Anick [2]. See also Labute [62] for arithmetic contexts.*

Remark 2. *Let L/K be an asymptotically good extension.*
Set $\mathscr{T}_{L/K} := \{\mathfrak{p} \subset \mathscr{O}_K, f(\mathfrak{p}) < \infty\}$, where $f(\mathfrak{p})$ is the residue extension degree of $\mathfrak{p}$ in L/K. Then one actually has $\sum_{\mathfrak{p}\in\mathscr{T}_{L/K}} \frac{\log \mathrm{N}(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})} < \infty$ (see [50], [127], etc.). But observe that $\mathscr{S}_{L/K} = \mathscr{T}_{L/K}$ in the context of Theorem A. To be complete, also note that for $X \geq 2$ one has (assuming the GRH):

$$|\{\mathfrak{p} \in \mathscr{S}_{L/K},\ \mathrm{N}(\mathfrak{p}) \leq X\}| \leq cX^{1/2}\big([K:\mathbb{Q}]\log X + b\big),$$

where c is an absolute constant, and where b is an upper bound for the sequence of the root discriminants in L/K; in particular one can take $b = \log|Disc_K|$ when L/K is unramified (see [41]).

The proof follows the strategy developed by Labute [62] (see also [66], [117], [29] etc.) for studying the cohomological dimension of a pro-p group G, through the notion of strongly free sets introduced by Anick [3]. By following the approach of Forré [29], we adapt this idea to the setting where the minimal number of relations of G is infinite. This key idea is associated to a result of Schmidt [117] that shows that the pro-p group G_S is of cohomological dimension 2 for some well-chosen S; the proof of Schmidt involves the cup-product $H^1(G_S, \mathbb{F}_p) \cup H^1(G_S, \mathbb{F}_p)$. Here we use the translation of this cup-product to the polynomial algebras, due to Forré [29]. In particular, this allows us to choose infinitely many Frobenius elements in G_S such that the family of the highest terms of these plus the highest terms of the relations of G_S, is combinatorially free (see §2.1.1 and Definition 23). We conclude by cutting the tower K_S/K by all these Frobenius elements: this is the strategy of [41].

This note contains two sections. In §1 we recall the results we need regarding pro-p groups, graded algebras, and arithmetic of pro-p extensions with restricted ramification. In §2 we start with an example involving $K = \mathbb{Q}$, and prove the main result.

Notations.
Let p be a prime number.
• If V is a $\mathbb{F}_p$-vector space we denote by $\dim V$ its dimension over $\mathbb{F}_p$.
• For a pro-p group G, we denote by $H^i(\mathrm{G})$ the cohomology group $H^i(\mathrm{G}, \mathbb{F}_p)$. The p-rank of G, which is equal to $\dim H^1(\mathrm{G})$, is noted $d(G)$.

2.1 The results we need

2.1.1 On pro-p groups

For this section we refer to [14], [59, Chapters 5, 6 and 7], and [29]. Take a prime number p.

Let G be a pro-p group of finite p-rank d, and let $1 \to R \to F \to G \to 1$ be a minimal presentation of G by a free pro-p group F. We denote by $\{x_1; \ldots; x_d\}$ a minimal set of generators of G, and $\{l_i; i \in \mathbf{I}\}$ a minimal set of presentation of G. We observe that $R/R^p[R,R]$ is a $Al(\mathbb{F}_p, G)$-compact module, which is generated by the $w_i := \phi(l_i - 1)$'s, where ϕ denotes the Magnus isomorphism (1) and $Al(\mathbb{F}_p, G)$ is the completed group algebra of G over $\mathbb{F}_p$. The cohomological dimension $\mathrm{cd}(G)$ of G is the smallest integer n (possibly $n = \infty$) such that $H^i(\mathrm{G}) = 0$ for every $i \geq n+1$.

Theorem. *One has* $\mathrm{cd}(G) \leq 2$ *if and only if* $R/R^p[R,R] \simeq \prod_{\mathbf{I}} w_i Al(\mathbb{F}_p, G)$. *Moreover* $\dim H^2(G) = |\mathbf{I}|$.

Proof. See [14, Corollary 5.3] or [59, Chapter 7, §7.3, Theorem 7.7]. □

We are going to translate conditions of Theorem 2.1.1 into the algebra $\mathscr{E} := \langle X_1, \cdots, X_d \rangle$.

Filtred and graded algebras

The results of this section can be found in [3].

• Let E be the algebra of series in noncommuting variables $X_1, \cdots, X_d$ with coefficients in $\mathbb{F}_p$. We consider now non-commutative multi-indices $\alpha = (\alpha_1, \cdots, \alpha_n)$, with $\alpha_i \in \{1, \cdots, d\}$, and we denote by X_α the monomial element of the form $X_\alpha := X_{\alpha_1} \cdots X_{\alpha_n}$. We endow each X_i with degree 1; and we denote by $\deg(X_\alpha)$ the degree of X_α which is $|\alpha|$.

For $Z = \sum_\alpha a_\alpha X_\alpha$, the quantity $\deg(Z) := \min_{a_\alpha \neq 0}\{\deg(X_\alpha)\}$ is the valuation of Z, with the convention that $\deg(0) = \infty$.

For $n \geq 0$, put $E_n := \{Z \in E, \deg(Z) \geq n\}$. Observe that E_1 is the augmentation ideal of E: this is the two-sided ideal of E topologically generated by the X_i's. The algebra E is filtered by the E_n's and its graded algebra $\mathrm{Grad}(E)$ is then:

$$\mathrm{Grad}(E) := \bigoplus_{n \in \mathbb{Z}_{\geq 0}} E_n/E_{n+1} \simeq \mathscr{E}.$$

In other words, $\mathrm{Grad}(E)$ is isomorphic to $\mathscr{E}$, the non-commutative polynomial algebra $\mathbb{F}_p\langle X_1, \ldots, X_d\rangle$, where each X_i is endowed with formal degree 1. Let $\mathscr{E}_{\geq n} := \{z \in \mathscr{E}, \deg(z) \geq n\}$ be the filtration of $\mathscr{E}$; observe that $\mathscr{E}_{\geq 1}$ is the augmentation ideal of $\mathscr{E}$.

• Let $X_\alpha, X_{\alpha'}$ be two monomials (viewed in E or in $\mathscr{E}$). The element X_α is said to be a *submonomial* of $X_{\alpha'}$, if $X_{\alpha'} = X_\beta X_\alpha X_{\beta'}$, with $X_\beta, X_{\beta'}$ two monomials of $\mathscr{E}$.

Definition 23. *A family $\mathscr{F} = \{X_{\alpha^{(i)}}\}_{i\in\mathbf{I}}$ of monomials of $\mathscr{E}$ is combinatorially free if for all i, j:*

(i) $X_{\alpha^{(i)}}$ is not a strict submonomial of $X_{\alpha^{(j)}}$,

(ii) if $X_{\alpha^{(i)}} = X_\alpha X_\beta$ and $X_{\alpha^{(j)}} = X_{\alpha'} X_{\beta'}$, then $X_\alpha \neq X_{\beta'}$, with X_α, X_β, $X_{\alpha'}$, $X_{\beta'}$ nontrivial monomials, i.e. different from 1.

The monomials may be endowed with a total order $<$ as follows. First let us consider the natural ordering $<'$ defined by: $X_1 <' X_2 <' \cdots <' X_d$.

Definition 24. *Let X_α and X_β be two monomials. We say that $X_\alpha > X_\beta$, if $\deg(X_\alpha) < \deg(X_\beta)$. If X_α and X_β have the same valuation, we use the lexicographic order induced by $<'$.*

Now, let $Z = \sum_\alpha a_\alpha X_\alpha$ be a nonzero element of E, with $a_\alpha \in \mathbb{F}_p$. Then $\widehat{Z} := \max\{X_\alpha,\ a_\alpha \neq 0\}$ is the *highest term* respecting the order $<$. Observe that $\widehat{Z} \in \mathscr{E}$.

• Let $\widehat{\mathscr{I}} = \mathscr{E}\mathscr{F}\mathscr{E}$ be the two-sided $\mathscr{E}$-ideal generated by $\mathscr{F} := \{Z_i\}_{i\in\mathbf{I}}$, where $\mathscr{F}$ is a locally finite graded subset of $\mathscr{E}_{\geq 1}$; in particular $\mathbf{I}$ is countable. Let $\widehat{\mathscr{E}} := \mathscr{E}/\widehat{\mathscr{I}}$ be the quotient endowed with the quotient filtration; we denote by $\widehat{\mathscr{E}}(t) := \sum_{n\in\mathbb{Z}_{\geq 0}} \dim \widehat{\mathscr{E}}_n \cdot t^n$ the Hilbert series of $\widehat{\mathscr{E}}$. Observe that the family $\mathscr{F}$ generates the $\widehat{\mathscr{E}}$-CGA module $\widehat{\mathscr{I}}/\widehat{\mathscr{I}}\mathscr{E}_{\geq 1}$.

Theorem (Anick)**.** *If the family $\{\widehat{Z}\}_{i\in\mathbf{I}}$ is combinatorially free, then*

(i) $\widehat{\mathscr{I}}/\widehat{\mathscr{I}}\mathscr{E}_{\geq 1}$ is a free $\widehat{\mathscr{E}}$-CGA module over the Z_i's, and

(ii) $\widehat{\mathscr{E}}(t) = \big(1 - dt + \sum_{i\in I} t^{n_i}\big)^{-1}$, where $n_i := \deg(Z_i)$.

Proof. See [3, Theorems 2.6 and 3.2]. □

If $\widehat{\mathscr{I}}/\widehat{\mathscr{I}}\mathscr{E}_{\geq 1}$ is a free $\widehat{\mathscr{E}}$-module over the Z_i's, we say that the family $\mathscr{F} = \{Z_i\}_{i\in\mathbf{I}}$ is *strongly free* (see [3]).

Example 15. *Take $d = 5$. Let $a_n \geq 1$ be an increasing sequence, and consider the family $\mathscr{F} = \{X_5X_3, X_4X_2, X_4X_3, X_5X_2, X_5X_1, X_5X_4^{a_n}X_1, n \geq 1\}$. Put $\widehat{\mathscr{E}} := \mathscr{E}/\mathscr{E}\mathscr{F}\mathscr{E}$. Then $\mathscr{F}$ is combinatorially free, and $\widehat{\mathscr{E}}(t) = \big(1 - 5t + t^2 \sum_{n\geq 1} t^{a_n}\big)^{-1}$.*

Pro-p groups of cohomological dimension ≤ 2 and polynomial algebras

Let F be a free pro-p group on d generators $x_1, \cdots, x_d$. Let $Al(\mathbb{F}_p, F)$ be the complete group algebra of F over $\mathbb{F}_p$. Recall that $Al(\mathbb{F}_p, F)$ is isomorphic to the Magnus algebra E; this isomorphism φ is given by $x_i \mapsto X_i + 1$ (see for example [59, Chapter 7, §7.6, Theorem 7.16]). Let us endow E with the filtration and the ordering of §2.1.1. Observe that $E_1 \simeq I_F := \mathrm{Ker}(Al(\mathbb{F}_p; F) \to \mathbb{F}_p)$; that is, E_1 is isomorphic to the augmentation ideal of $Al(\mathbb{F}_p; F)$.

Take $x \in F$, nontrivial. Then the degree $\deg(x)$ of x is defined as $\deg(x) := \deg(\phi(x-1))$. We denote by $\widehat{x} \in \mathscr{E}$ the highest monomial of $\phi(x-1) \in E$; we say that $\widehat{x}$ is the highest term (or monomial) of x.

Example 16. *Take $d \geq 3$ with the lexicographic ordering $X_1 < X_2 < X_3 < \cdots < X_d$.*

(i) The highest term of $[x_1, [x_2^{p^n}, x_3]]$ is $X_3 X_2^{p^n} X_1$, $n \geq 1$.

(ii) Given $x, y \in \mathrm{F}$, let us write $f_x(y) = [x, y] \in \mathrm{F}$. Then the highest term of $f_{x_1} \circ f_{x_2}^{\circ n}(x_3)$ is $X_3 X_2^n X_1$, $n \geq 1$.

Let G be a pro-p group of p-rank d, and let $1 \to R \to F \to G \to 1$ be a minimal presentation of G by F; this induces a morphism of compact algebras $\theta : Al(\mathbb{F}_p; F) \to Al(\mathbb{F}_p; G)$, which respects the filtration given by n-th power of augmentation ideals. For $i \in \mathbf{I}$, put $w_i := \varphi(l_i - 1) \in E_1$; $n_i = \deg(w_i)$. Let $I(R) \subset E_1$ be the closed two-sided ideal of E_1 topologically generated by the w_i's, $i \in \mathbf{I}$; one has $\mathrm{Ker}(\theta) \simeq I(\mathrm{R})$ (see for example [59, Chapter 7, §7.6, Theorem 7.17]). Then Magnus isomorphism induces an isomorphisms $\phi\colon Al(\mathbb{F}_p; G) \to E(G) := E/I(R)$. Observe that $E(G)$ is endowed with the quotient filtration of E defined as follows for the valuation $\deg_G$: for $z \in E(G)$, let us define

$$\deg_G(z) := \max\{\deg(\varphi(z')), z' \in Al(\mathbb{F}_p; F), \varphi(\theta(z')) = z\}.$$

Put $E_n(G) := \{z \in E(G), \deg_G(z) \geq n\}$, the filtration of $E(G)$. Then $\mathrm{Grad}(E(G)) := \bigoplus_n E_n(G)/E_{n+1}(G)$ is the graded algebra $\mathscr{E}(G)$ respecting the quotient filtration with $\mathscr{E}(G,t) := gocha(G,t) := \sum_{n \geq 0} \dim E_n(G)/E_{n+1}(G) \cdot t^n$ as Hilbert series.

For $n \geq 1$, put $F_n := \{x \in F, \phi(x-1) \in E_n\}$, and $G_n := F_n R/R$. The sequences (F_n) and (G_n) are the Zassenhaus filtrations of F and G. The filtration $(E_n(G))$ also corresponds to the filtration coming from the augmentation ideal of $Al(\mathbb{F}_p, G)$ (see [69, Appendice A.3, Théorème 3.5]).

Theorem. *Let $\mathscr{F} = \{l_i\}_{i \in \mathbf{I}}$ be a family of elements of R which generates R as closed normal subgroup of F. If $\{\widehat{l_i}\}_{i \in \mathbf{I}}$ is combinatorially free, then*

(i) $R/R^p[R,R] \simeq \prod_{i \in \mathbf{I}} l_i E(G)$, $\mathrm{cd(G)} \leq 2$, and $\dim H^2(\mathrm{G}) = |\mathbf{I}|$;

(ii) $gocha(G,t) = \left(1 - dt + \sum_{i \in I} t^{n_i}\right)^{-1}$, where $d = d_p\mathrm{G}$, and $n_i := \deg(l_i)$.

Proof. When the set of indices $\mathbf{I}$ is finite, this version can be found in [29]. We show here that the result also holds when $\mathbf{I}$ is infinite. First, observe that as $\{\widehat{l_i}\}_{i\in\mathbf{I}}$ is combinatorially free then $\mathbf{I}$ is countable infinite, and $\mathscr{F}$ is a convergent family.

Let us recall now that one has the topological G-isomorphism $R/R^p[R,R] \simeq I(R)/I(R)E_1$ (see for example [29, Proposition 4.3]). We want some informations on the G-module $R/R^p[R,R]$, and then on $I(R)/I(R)E_1$.

For $i \in \mathbf{I}$, let $\rho_i \in \mathscr{E}$ be the initial form of $w_i := \phi(l_i - 1) \in E_1$ defined as follows: let us write $w_i = \rho_{i,n_i} + \rho_{i,n_i+1} + \cdots$, where $n_i = \deg(w_i)$ and where $\rho_{i,j}$ are homogeneous polynomials of degree j (possibly $\rho_{i,j} = 0$); then put $\rho_i := \rho_{i,n_i}$. Observe that $\widehat{\rho_i} = \widehat{w_i} = \widehat{l_i}$.

Let $\mathscr{I}(\rho)$ be the closed two-sided ideal of $\mathscr{E}$ generated by the family $\{\rho_i\}_{i\in\mathbf{I}}$. Since the family $\{\widehat{l_i}\}_{i\in\mathbf{I}}$ is combinatorially free then by Anick's Theorem the family $\{\rho_i\}_{i\in\mathbf{I}}$ is strongly free. Put $\mathscr{E}(\rho) := \mathscr{E}/\mathscr{I}(\rho)$.

Proposition 19. *One has $\mathscr{I}(\rho) = \mathrm{Grad}(I(R)) \subset \mathscr{E}$. In particular, one gets $\mathscr{E}(G) \simeq \mathscr{E}(\rho)$, and the following isomorphisms of $\mathscr{E}(\rho)$-CGA modules:*

$$\mathrm{Grad}(I(R)/I(R)E_1) \simeq \mathscr{I}(\rho)/\mathscr{I}(\rho)\mathscr{E}_{\geq 1} \simeq \bigoplus_{i\in\mathbf{I}} \mathscr{E}(\rho)\rho_i \simeq \bigoplus_{i\in\mathbf{I}} \mathscr{E}(\rho)[n_i],$$

where $\mathscr{E}(\rho)[n_i]$ means $\mathscr{E}(\rho)$ as $\mathscr{E}$-module with an n_i-shift filtration.

Proof. This is only a slight generalization of the case $\mathbf{I}$ finite; see proof of [29, Theorem 3.7]. We also refer to the Theorem 11 and its proof. □

Then by Theorem 2.1.1 and Proposition 19 we first get

$$gocha(G,t) = \mathscr{E}(\rho,t) = \big(1 - dt + \sum_{i\in\mathbf{I}} t^{n_i}\big)^{-1}.$$

Consider now the continuous morphism

$$\Psi : \prod_{i\in\mathbf{I}} E(G) \to I(R)/I(R)E_1 \simeq R/R^p[R,R],$$

which sends (a_i) to $\sum_i a_i w_i \pmod{I(R)\mathscr{E}_1}$. Since $n_i \to \infty$ with i, the morphism Ψ is well-defined. Remember that $E(G) \simeq E/I(R)$.

Lemma 3. *The map Ψ is surjective.*

Proof. Put $W := \{\sum_{i\in\mathbf{I}} a_i w_i, a_i \in E\} \subset I(R)$. Then

$$I(R) = WE = W\mathbb{F}_p + WE_1 = W + WE_1.$$

We conclude by noticing that $WE_1 \subset I(R)E_1$. □

Set $\mathrm{N} := \mathrm{Ker}(\Psi)$. Therefore one gets a sequence of filtered G-modules:

$$1 \to \mathrm{N} \to \prod_{i\in\mathbf{I}} E(G)[n_i] \stackrel{\Psi}{\to} I(R)/I(R)E_1 \to 1.$$

This one induces the following sequence of graded $\mathscr{E}$-modules:

$$0 \to \mathrm{Grad}(\mathrm{N}) \to \mathrm{Grad}(\prod_{i\in\mathbf{I}} E(G)[n_i]) \to \mathrm{Grad}(I(R)/I(R)E_1) \to 0.$$

For the surjectivity, use the fact that $\mathbf{I}$ is countable. Now since $n_i \to \infty$ with i, then

$$\mathrm{Grad}\big(\prod_{i\in\mathbf{I}} E(G)[n_i]\big) \simeq \bigoplus_{i\in\mathbf{I}} \mathscr{E}(G)[n_i].$$

By Proposition 19, we finally get that Ψ induces an isomorphism between $\mathrm{Grad}\big(\prod_{i\in I} E(G)[n_i]\big)$ and $\mathrm{Grad}\big(I(R)/I(R)E_1\big)$, which implies $\mathrm{Grad}(\mathrm{N}) = 0$, then $\mathrm{N} = 0$. Hence, as G-modules, $\prod_{i\in I} E(G) \simeq I(R)/I(R)E_1 \simeq R/R^p[R,R]$. One concludes by applying Theorem 2.1.1. □

Remark 6. *The conclusions of Theorem 5 also hold if $\{\widehat{l_i}\}_{i\in\mathbf{I}}$ is strongly free.*

Cup-products and cohomological dimension

Here we assume $p > 2$.

Let G be a pro-p group of p-rank d which is not free pro-p. Recall that the cup product maps $H^1(G) \otimes H^1(G)$ to $H^2(G)$. Labute in [62] gave a criterion involving cup-products so that $\mathrm{cd}(G) = 2$. This point of view has been developed by Forré in [29].

Theorem (Forré)**.** *Let $p > 2$ be a prime number. Let G be a finitely presented pro-p group which is not free pro-p. Suppose that $H^1(G) = U \oplus V$ with U and V such that $U \cup U = 0$ and $U \cup V = H^2(\mathrm{G})$. Then $\mathrm{cd}(G) = 2$, and G can be described by d generators and r relations $l_1, \cdots, l_r$ such that the highest term of each l_i is of the form $X_{t(i)}X_{s(i)}$ for some $s(i), t(i)$ such that $s(i) \leq \dim V < t(i)$, and $(s(i), t(i)) \neq (s(j), t(j))$ for $i \neq j$.*

Proof. See the proof of [29, Theorem 6.4, Corollary 6.6] with the choice of the ordering $X_1 < X_2 < \cdots < X_d$. □

Let us make the following observation: given $n \geq 1$, according to Example 16 one can find some $x \in F$ for which the highest term is of the form $X_k X_j^n X_i$, for $i < j < k$.

Corollary 8. *Under the assumptions of Theorem 2.1.1, suppose $c := \dim V \geq 2$. For some fixed $1 < i_0 \leq c < j_0 \leq d$, and $n \geq 1$, let $x_n \in F$ with highest term $X_{j_0}X_{i_0}^n X_1$. Suppose moreover that $r < (d-c)(c-1)$. Then there exists (i_0, j_0) such that the family $\{\widehat{l_1}, \cdots, \widehat{l_r}, \widehat{x_n}, n \geq 1\}$ is combinatorially free. In particular, for such (i_0, j_0) one has:*

(i) *the cohomological dimension of the quotient* $Q := F/\langle l_1, \cdots, l_r, x_n, n \in \mathbb{Z}_{>0}\rangle^{\mathrm{Nor}}$ *of* G *is smaller than* 2*;*

(ii) $\dim H^2(\Gamma) = \infty$*;*

(iii) $gocha(Q,t) = \big(1 - dt + rt^2 + t^3 \sum_{n\geq 0} t^n\big)^{-1}$.

Proof. According to Theorem 2.1.1, for $i = 1, \cdots, r$, the highest term of l_i is of the form $X_{t(i)}X_{s(i)}$ for some $s(i) \leq c < t(i)$, and the family $\widehat{\mathscr{I}} := \{X_{t(1)}X_{s(1)}, \cdots, X_{t(r)}X_{s(r)}\}$ is combinatorially free. Now, since $r < (d-c)(c-1)$ and $c \geq 2$, we can find (i_0, j_0) such that $X_{j_0}X_{i_0}$ is not in $\widehat{\mathscr{I}}$; therefore $\widehat{\mathscr{I}} \cup \{X_{j_0}X_{i_0}^n X_1, n \in \mathbb{Z}_{>0}\}$ is combinatorially free. And we can apply Theorem 5. □

Remark 7. *In fact* $r \leq (d-c)c-2$ *is enough. Indeed, with such a condition one has* $X_{j_0}X_{i_0} \notin \widehat{\mathscr{I}}$ *for some* $(i_0, j_0) \neq (1, r)$, $i_0 \leq c < j_0 \leq r$. *Hence if* $i_0 \neq 1$, *the family* $\widehat{\mathscr{I}} \cup \{X_{j_0}X_{i_0}^n X_1, n \in \mathbb{Z}_{>0}\}$ *is combinatorially free. Otherwise* $j_0 \neq r$, *and take* $\widehat{\mathscr{I}} \cup \{X_r X_{j_0}^n X_{i_0}, n \in \mathbb{Z}_{>0}\}$.

2.1.2 Arithmetic background

Let p be a prime number, and let K be a number field. For $p = 2$, assume K totally imaginary. Let S and T be two disjoint finite sets of K. We assume moreover S tame. We denote by $\mathrm{Cl}_K^T(p)$ the p-Sylow of the T-class group of K. Let K_S^T/K be the maximal pro-p extension of K unramified outside S where each $\mathfrak{p} \in T$ splits completely; put $G_S^T := \mathrm{Gal}(K_S^T/K)$. Let us recall Shafarevich's formula (see for example [35, Chapter I, §4, Theorem 4.6]):

$$d_p G_S^T = |S| - (r_1 + r_2) + 1 - |T| - \delta_{K,p} + \dim \mathrm{V}_S^T/(K^\times)^p,$$

where

$$\mathrm{V}_S^T = \{x \in K^\times,\ x \in (K_\mathfrak{p}^\times)^p U_\mathfrak{p}\ \forall x \notin S \cup T,\ x \in (K_\mathfrak{p}^\times)^p\ \forall \mathfrak{p} \in S\},$$

and where $\delta_{K,p} = 1$ if K contains μ_p (the p-roots of 1), 0 otherwise. Here as usual, $K_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$, and $U_\mathfrak{p}$ is the group of local units of $K_\mathfrak{p}$. Observe that if there is no p-extension of $K(\mu_p)$ unramified outside T and p in which each prime of S splits completely, then $\mathrm{V}_S^T/(K^\times)^p$ is trivial: this is a Chebotarev condition type.

Schmidt in [117] showed that G_S^T may be *mild* following the terminology of Labute [62]. More precisely, he proved:

Theorem (Schmidt)**.** *Let* K *be a number field and let* p *be a prime number. For* $p = 2$ *suppose* K *totally imaginary. Let* S_0 *and* T *be two disjoint finite sets of prime ideals of* K *with* S_0 *tame. Assume* T *sufficiently large so that* $\mathrm{Cl}_K^T(p)$ *is trivial; when* $\mu_p \subset K$, *assume moreover that* T *contains all prime ideals above* p. *Then there exist infinitely many finite tame sets* S *containing* S_0 *such that* $H^1(\mathrm{G}_S^T) = U \oplus V$, *where the subspaces* U *and* V *satisfy: (i)* $U \cup U = 0$*; (ii)* $U \cup V = H^2(G_S^T)$. *Moreover, one has* $\dim H^2(G_S^T) = \dim H^1(G_S^T) + r_1 + r_2 + |T| - 1$.

Theorem 2.1.2 is not in this form in [117]: the result presented here can be found in the proof of Theorem 6.1 of [117].

At this level, following [117] let us compute the value of $c = \dim V$.

When $\mu_p \subset K$, we expand S_0 so that for every $\mathfrak{p} \in S_0$, $d_p \mathrm{G}^T_{S_0\setminus\{\mathfrak{p}\}} = |S_0| - r_1 - r_2 - |T|$, which is equivalent by Shafarevich's formula to the triviality of $\mathrm{V}^T_{S_0\setminus\{\mathfrak{p}\}}/(K^\times)^p$.

When $\mu_p \subset K$, we expand S_0 so that the set of the Frobenius elements at $\mathfrak{p}$ in G_T^{el} when $\mathfrak{p}$ ranges over S_0, corresponds to the set of the nontrivial elements of G_T^{el}; here $G_T^{el} = \mathrm{Gal}(K_T^{el}/K)$, where K_T^{el} is the maximal elementary abelian p-extension of K inside K_T. One also has $\mathrm{V}^T_{S_0\setminus\{\mathfrak{p}\}}/(K^\times)^p = \{1\}$.

The set S of Theorem 2.1.2 contains S_0, and is of size $2|S_0|$; the prime ideals $\mathfrak{p} \in S - S_0$ are choosen with respect to some local conditions, according to Chebotarev density theorem. Moreover $U = H^1(G^T_{S_0}, \mathbb{F}_p)$, and the subspace V is such that $\dim V = c = |S_0|$. See [117, Theorem 6.1] for more details.

Lemma 4. *Under the previous assumptions, each prime $\mathfrak{p} \in S$ is ramified in the maximal elementary abelian p-extension $K_S^{T,el}/K$ inside K_S^T.*

Proof. Observe first that if $S'' \subset S'$, then $\mathrm{V}^T_{S'}/(K^\times)^p \hookrightarrow \mathrm{V}^T_{S''}/(K^\times)^p$. Hence afforded by the choice of S_0, one has: for every $\mathfrak{p} \in S$, $\mathrm{V}^T_{S\setminus\{\mathfrak{p}\}}/(K^\times)^p$ is trivial. Then by Shafarevich's formula, one gets $d_p G^T_S = 1 + d_p G^T_{S\setminus\{\mathfrak{p}\}}$, showing that $\mathfrak{p}$ is ramified in $K_S^{T,el}/K$. □

Put $\alpha_{K,T} = 3 + 2\sqrt{2 + r_1 + r_2 + |T|}$. By obvious arguments one finds:

Lemma 5. *If $d_p G^T_S > \alpha_{K,T}$, then $d_p G^T_S + r_1 + r_2 + |T| - 1 < (d-c)(c-1)$ for every $c \in [2, d]$.*

Let us finish this part with an obvious observation.

Remark 8. *If G^T_S is not trivial and such that $\mathrm{cd}(G^T_S) \leq 2$, then $\mathrm{cd}(G^T_S) = 2$.*

2.2 Example and proof

2.2.1 Example

• Take $p > 2$, and $K = \mathbb{Q}$. In this case the relations of the pro-p groups G_S are all local: this is the description due to Koch [59, Chapter 11, §11.4, Example 11.11]. Let ℓ be a prime number such that $p|\ell - 1$. Denote by $\mathbb{Q}_\ell$ the (unique) cyclic extension of $\mathbb{Q}$ of degree p unramified outside ℓ.

Let $S = \{\ell_1, \cdots, \ell_d\}$ be a set of d different primes such that $\ell_i \equiv 1 \pmod p$. The pro-p group G_S can be described by generators $x_1, \cdots, x_d$, and relations $l_1, \cdots, l_d$ such that

$$l_i \equiv \prod_{j \neq i} [x_i, x_j]^{a_j(i)} \pmod{F_3}, \tag{2.1}$$

where $a_j(i) \in \mathbb{Z}/p\mathbb{Z}$, and where each x_i is a generator of the inertia group of ℓ_i. The element $a_j(i)$ is zero if and only if the prime ℓ_i splits in $\mathbb{Q}_{\ell_j}/\mathbb{Q}$, which is equivalent to $\ell_i^{(\ell_j-1)/p} \equiv 1 \pmod{\ell_j}$.

• Take $p = 3$, $S_0 = \{7, 13\}$, and $T = \emptyset$. Put $S = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5\}$ with $\ell_1 = 31, \ell_2 = 19, \ell_3 = 13, \ell_4 = 337, \ell_5 = 7$. Then the highest terms of the relations (1.1), viewed in $\mathbb{F}_p\langle X_1, \cdots, X_5\rangle$, are: $\widehat{l_1} = X_1X_3$, $\widehat{l_2} = X_2X_4$, $\widehat{l_3} = X_2X_3$, $\widehat{l_4} = X_1X_4$, $\widehat{l_5} = X_1X_5$. Since the $\widehat{l_i}$'s are combinatorially free, G_S is of cohomological dimension 2 by Theorem 5.

Now for each $n > 0$, let us choose a prime number ℓ_n of $\mathbb{Z}$ such that the highest term of a lift x_n in F of its Frobenius element $\sigma_n \in G_S$, is of the form $X_5X_4^nX_1$ (which is possible by Example 16, see next section). Next consider the maximal Galois subextension $L/\mathbb{Q}$ of $\mathbb{Q}_S/\mathbb{Q}$ fixed by all the conjuguates of the σ_n's (this is the "cutting towers" strategy of [41]). Put $G := \mathrm{Gal}(L/\mathbb{Q})$. Then the pro-3 group G can be described by generators $x_1, \cdots, x_5$, and relations $\{l_1, \cdots, l_5, x_n, n \in \mathbb{Z}_{>0}\}$ (which is not *a priori* a minimal set). By construction, the ℓ_n's split totally in $L/\mathbb{Q}$. Observe now that

$$\{\widehat{l_1}, \cdots, \widehat{l_5}, \widehat{x_n}, n > 0\} = \{X_5X_1, X_5X_2, X_4X_3, X_4X_2, X_5X_3, X_5X_4^nX_1, n > 0\}$$

which is combinatorially free. By Theorem 5 the pro-3-group G is of cohomological dimension 2, $H^2(G)$ is infinite, and

$$P_G(t) = \big(1 - 5t + 5t^2 + t^3(1 + t + t^2 + \cdots)\big)^{-1}.$$

2.2.2 Proof of the main result

• Take $p > 2$. Let S_0 and T be two finite disjoint sets of prime ideals of K, where S_0 is tame. Take T sufficiently large so that $\mathrm{Cl}_K^T(p)$ is trivial. When K contains μ_p, assume moreover that T contains all p-adic prime ideals.

First take S containing S_0 as in Theorem 2.1.2, and sufficiently large so that $d := d_p\mathrm{G}_S^T > \alpha_{K,T}$. Put $G = G_S^T$. Here $\dim H^2(G) = d + r_1 + r_2 - 1 + |T|$; set $r := \dim H^2(G)$.

Let us start with a minimal presentation of G:

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1.$$

By Theorem 2.1.2 and Theorem 2.1.1, the subgroup R can be generated as normal subgroup by some relations $l_1, \cdots, l_r$ such that the highest terms $\widehat{l_k}$ are of the form X_iX_j for some $i \leq c < j$, where $c = \dim V$. Observe that since G is FAb then $c \in [2, d-2]$.

Given $n \geq 1$, the quotient G/G_{n+1} is finite. Put $K_{(n+1)} := (K_S^T)^{G_{n+1}}$. For $n \geq 1$, take $x_n \in F_{n+2}\backslash F_{n+3}$. By Chebotarev density theorem there exists some prime ideal $\mathfrak{p}_n \subset \mathscr{O}_K$ such that $\sigma_{\mathfrak{p}_n}$ is conjuguate to x_n in $\mathrm{Gal}(K_{(n+3)}/K)$; here $\sigma_{\mathfrak{p}_n} \in G$ denotes the Frobenius element of $\mathfrak{p}_n$. Now take $z_n \in F$ such that $\phi(z_n) = \sigma_{\mathfrak{p}_n}$. Then $z_n \equiv \sigma_{\mathfrak{p}_n} \pmod{RF_{n+3}}$. In other words, there exists $y_n \in F_{n+3}$, $\alpha_n \in F$, and $r_n \in R$ such that $\alpha_n z_n \alpha_n^{-1} = x_n y_n r_n$.

Set $\Sigma := T \cup \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots\}$, and consider K_S^Σ the maximal pro-p extension of K unramified oustide S and where each primes $\mathfrak{p}$ of Σ splits completely. Put $G_S^\Sigma := \mathrm{Gal}(K_S^\Sigma/K)$. Then

$$G_S^\Sigma \simeq G/\langle \sigma_{\mathfrak{p}_n}, n \geq 1\rangle^{\mathrm{Nor}}.$$

Here $\langle \sigma_{\mathfrak{p}_n}, n \geq 1 \rangle^{\mathrm{Nor}}$ is the normal closure of $\langle \sigma_{\mathfrak{p}_n}, n \geq 1 \rangle$ in G. Therefore K_S^{Σ}/K satisfies (i) of Theorem A. But observe now that

$$\begin{aligned} G/\langle \sigma_{\mathfrak{p}_n}, n \geq 1 \rangle^{\mathrm{Nor}} &\simeq F/\langle l_1, \cdots, l_r, z_n, n \geq 1 \rangle^{\mathrm{Nor}} \\ &= F/\langle l_1, \cdots, l_r, x_n y_n, n \geq 1 \rangle^{\mathrm{Nor}}. \end{aligned}$$

For $n \geq 1$, the highest term of $x_n y_n$ is equal to the highest term of x_n; therefore it is enough to choose the x_n's as in Corollary 8 which is possible: indeed since $d > \alpha_{K,T}$, by Lemma 5, one has $r < (c-1)(d-c)$ for every $c \in [1, d-1]$. Afforded by Corollary 8, one gets (ii), (iii), and (v) of Theorem A.

Let us proof (iv). By Lemma 4 each prime ideal $\mathfrak{p} \in S$ is ramified in $K_S^{T,el}/K$, showing that $\tau_{\mathfrak{p}} \in G$ is not in $RF^p[F,F]$, where $\tau_{\mathfrak{p}} \in$ G is a generator of the inertia group at $\mathfrak{p}$. Therefore $d_p G_S^{\Sigma} = d_p G$, and then every prime $\mathfrak{p} \in S$ is ramified in K_S^{Σ}/K. But since G is torsion-free (because $\mathrm{cd}(G) = 2$), then $\langle \tau_{\mathfrak{p}} \rangle \simeq \mathbb{Z}_p$, and the local extension $(K_S^{\Sigma})_{\mathfrak{p}}/K_{\mathfrak{p}}$ must be maximal.

• Assume $p = 2$, and suppose K totally imaginary. Then Theorem 2.1.2 holds, but Theorem 2.1.1 does not. As explained by Forré in [29, Proof Theorem 6.4], one has to take two orderings to show that the highest terms of the relations $l_1, \cdots, l_r$ are strongly free. Now in this context the strategy of the approximation of the x_n's by some Frobenius elements as in Corollary 8 also applies. Along the same lines as in the proof of Theorem 6.4 in [29], and by choosing the x_n's as for $p \neq 2$, we observe that the initial forms of the new relations $\{l_1, \cdots, l_r, x_n, n \geq 1\}$ are still strongly free. We conclude by invoking Remark 6. □

Chapter 3

Zassenhaus and Lower central filtrations of pro-p groups considered as modules

Context

Let G be a finitely generated pro-p group, and denote by $\mathbb{A}$ the ring $\mathbb{Z}_p$ or $\mathbb{F}_p$. From $\mathbb{A}$, we recover some filtrations on G. Introduce $Al(\mathbb{A},G) := \varprojlim \mathbb{A}[G/U]$, where U is an open normal subgroup of G, the completed group algebra of G over $\mathbb{A}$. Since $\mathbb{A}[G/U]$ is an augmented algebra over $\mathbb{A}$, then $Al(\mathbb{A},G)$ is also. Consequently, we denote by $Al_n(\mathbb{A},G)$ the n-th power of the augmentation ideal of $Al(\mathbb{A},G)$. Define:

$$G_n(\mathbb{A}) := \{g \in G; g-1 \in Al_n(\mathbb{A},G)\},$$

this is a filtration of G.

Observe that $\{G_n(\mathbb{F}_p)\}_{n\in\mathbb{N}}$ denotes the Zassenhaus filtration of G (see for instance [92]), and is an open characteristic basis of G. Similarly, under certain conditions (see [64]), the filtration $\{G_n(\mathbb{Z}_p)\}_{n\in\mathbb{N}}$ is equal to the lower central series of G, i.e. $G_1(\mathbb{Z}_p) = G$ and $G_{n+1}(\mathbb{Z}_p) = [G_n(\mathbb{Z}_p); G]$. When the context is clear, we omit to write $\mathbb{A}$ for filtrations (and future associated invariants). Our goal is to study the following Lie algebras:

$$\mathscr{L}(\mathbb{A},G) := \bigoplus_{n\in\mathbb{N}} \mathscr{L}_n(\mathbb{A},G), \quad \text{where} \quad \mathscr{L}_n(\mathbb{A},G) := G_n(\mathbb{A})/G_{n+1}(\mathbb{A}), \quad \text{and}$$
$$\mathscr{E}(\mathbb{A},G) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_n(\mathbb{A},G), \quad \text{where} \quad \mathscr{E}_n(\mathbb{A},G) := Al_n(\mathbb{A},G)/Al_{n+1}(\mathbb{A},G).$$

We always assume that $\mathscr{L}(\mathbb{A},G)$ is **torsion-free** over $\mathbb{A}$. Notice that this condition is automatically satisfied when $\mathbb{A} := \mathbb{F}_p$, contrary to the case $\mathbb{A} := \mathbb{Z}_p$ (see for instance [63, Theorem] and [61, Théorème 2]). Since G is finitely generated, one defines for every integer n:

$$a_n(\mathbb{A}) := \mathrm{rank}_{\mathbb{A}}\mathscr{L}_n(\mathbb{A},G), \quad \text{and} \quad c_n(\mathbb{A}) := \mathrm{rank}_{\mathbb{A}}\mathscr{E}_n(\mathbb{A},G),$$
$$gocha(\mathbb{A},t) := \sum_{n\in\mathbb{N}} c_n t^n.$$

The series $gocha(\mathbb{F}_p, t)$ was first introduced by Golod and Shafarevich in [33]. It allowed them to obtain information on class field towers over some fields (see for instance [15, Chapter IX]). Later in 1965, Lazard studied analytic pro-p groups in [69], i.e. Lie groups over $\mathbb{Q}_p$ (see [69, Définition 3.1.2]). Labute [62], also used the series $gocha(\mathbb{Z}_p, t)$ in order to study mild groups and their related properties.

Jennings, Lazard and Labute gave an explicit relation between $gocha$ and $(a_n)_{n\in\mathbb{N}}$ ([69, Proposition 3.10, Appendice A], and [92, Lemma 2.10]):

$$\begin{aligned} gocha(\mathbb{A}, t) &= \prod_{n\in\mathbb{N}} P(\mathbb{A}, t^n)^{a_n(\mathbb{A})}, \\ \text{where} \quad P(\mathbb{F}_p, t) &:= \left(\frac{1-t^p}{1-t}\right), \quad \text{and} \qquad P(\mathbb{Z}_p, t) := \left(\frac{1}{1-t}\right). \end{aligned} \tag{3.1}$$

From Formula (3.1), Lazard deduced an alternative for the growth of $(c_n(\mathbb{F}_p))_{n\in\mathbb{N}}$ (for general references, see [19, Part 12.3]), this is [69, Théorème 3.11, Appendice A.3]:

Theorem (Alternative des Gocha)**.** *We have the following alternative:*

- *Either G is an analytic pro-p group, so there exists an integer n such that $a_n(\mathbb{F}_p) = 0$ and the sequence $(c_n(\mathbb{F}_p))_{n\in\mathbb{N}}$ has polynomial growth with n.*
- *Or G is not an analytic pro-p group, then for every $n \in \mathbb{N}$, $a_n(\mathbb{F}_p) \neq 0$, and the sequence $(c_n(\mathbb{F}_p))_{n\in\mathbb{N}}$ does admit an exponential growth with n (i.e. grows faster than any polynomial in n).*

In 2016,Ináč, Rogelstad and Tân [92] improved Formula (3.1): they gave an explicit relation between the sequences $(a_n)_{n\in\mathbb{N}}$ and $(c_n)_{n\in\mathbb{N}}$. The main idea was to introduce the coefficients $b_n \in \mathbb{Q}$, namely defined by:

$$\log(gocha(\mathbb{A}, t)) := \sum_{n\in\mathbb{N}} b_n(\mathbb{A}) t^n.$$

They obtained the following formula ([92, Theorem 2.9 and Lemma 2.10]): if we write $n = mp^k$, with m coprime to p, then

$$\begin{aligned} a_n(\mathbb{F}_p) &= w_m(\mathbb{F}_p) + w_{mp}(\mathbb{F}_p) + \cdots + w_{mp^k}(\mathbb{F}_p), \quad a_n(\mathbb{Z}_p) = w_n(\mathbb{Z}_p); \\ \text{where } w_n(\mathbb{A}) &:= \frac{1}{n}\sum_{m|n} \mu(n/m) m b_m(\mathbb{A}) \quad \text{and} \quad \mu \text{ is the Möbius function.} \end{aligned} \tag{3.2}$$

Notice that the number $w_n(\mathbb{F}_p)$ (resp. $c_n(\mathbb{Z}_p), a_n(\mathbb{Z}_p)$) is denoted by $w_n(G)$ (resp. $d_n(G), e_n(G)$) in [92, Part 2]. Furthermore,Ináč, Rogelstad and Tân asked the following question, [92, Question 2.13]:

Do we have $c_n(\mathbb{F}_p) := c_n(\mathbb{Z}_p)$?

Theorem 19 answers this question positively when G is finitely presented and mild with respect to some specific filtrations (see Definition 27). To proceed, we compute $(c_n(\mathbb{A}))_{n\in\mathbb{N}}$ by the Lyndon resolution (see [14, Corollay 5.3]), and as a consequence, we infer an explicit formula for $a_n(\mathbb{A})$ using Formula (3.2). Weigel ([137, Theorem D]) also gave a different formula from (3.2), involving $a_n(\mathbb{Z}_p)$ and roots of $1/gocha(\mathbb{Z}_p, t)$.

Statement of main results

The goal of this chapter is to extend equations (3.1), (3.2) and Gocha's alternative in an equivariant context. We use here the terminology equivariant to stress the action of groups.

Let q be a prime dividing $p-1$, and assume that $Aut(G)$ contains a cyclic subgroup Δ of order q. We denote by $\mathrm{Irr}(\Delta)$ the group of $\mathbb{A}$-irreducible characters χ of Δ, with trivial character $\mathbb{1}$: this is a group of order q which does not depend on the choice of $\mathbb{A}$ (for general references on $\mathbb{A}$-characters, see [120, Chapitre 14]). If M is a $\mathbb{A}[\Delta]$-module, one defines the eigenspaces of M by:

$$M[\chi] := \{x \in M; \quad \forall \delta \in \Delta, \quad \delta(x) = \chi(\delta)x\}.$$

Notice that $\mathscr{L}_n(\mathbb{A}, G)$ and $\mathscr{E}_n(\mathbb{A}, G)$ are free, finitely generated over $\mathbb{A}$ and are $\mathbb{A}[\Delta]$-modules. We study the following quantities:

$$a_n^\chi(\mathbb{A}) := \mathrm{rank}_{\mathbb{A}} \mathscr{L}_n(\mathbb{A}, G)[\chi], \quad \text{and} \quad c_n^\chi(\mathbb{A}) := \mathrm{rank}_{\mathbb{A}} \mathscr{E}_n(\mathbb{A}, G)[\chi].$$

From Maschke's Theorem and [120, Partie 14.4], we obtain the following equality:

$$a_n(\mathbb{A}) = \sum_{\chi \in \mathrm{Irr}(\Delta)} a_n^\chi(\mathbb{A}), \quad \text{and} \quad c_n(\mathbb{A}) = \sum_{\chi \in \mathrm{Irr}(\Delta)} c_n^\chi(\mathbb{A}).$$

This chapter has three parts.

Part 3.1 is mostly inspired by arguments given in [92]. Denote by $R[\Delta]$ the finite representation ring of Δ over $\mathbb{A}$. Observe that $R[\Delta]$ is a ring isomorphic to $\mathbb{Z}[\mathrm{Irr}(\Delta)]$, consequently $R[\Delta] \bigotimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra isomorphic to $\mathbb{Q}[\mathrm{Irr}(\Delta)]$. Instead of considering series with coefficients in $\mathbb{Q}$, as Filip [28] and Stix [124] did, we study series with coefficients in $R[\Delta] \bigotimes_{\mathbb{Z}} \mathbb{Q}$. Let us introduce:

$$gocha^*(\mathbb{A}, t) := \sum_{n \in \mathbb{N}} \left(\sum_{\chi \in \mathrm{Irr}(\Delta)} c_n^\chi(\mathbb{A}) \chi \right) t^n.$$

We infer an equivariant version of the equality (3.1):

Theorem B. *The following equality holds for series with coefficients in $R[\Delta]$:*

$$gocha^*(\mathbb{A}, t) = \prod_{n \in \mathbb{N}} \prod_{\chi \in \mathrm{Irr}(\Delta)} P_\chi(\mathbb{A}, t^n)^{a_n^\chi(\mathbb{A})},$$

$$\textit{where} \quad P_\chi(\mathbb{F}_p, t) := \frac{1 - \chi.t^p}{1 - \chi.t}, \quad \textit{and} \quad P_\chi(\mathbb{Z}_p, t) := \frac{1}{1 - \chi.t}$$

As done in Part 2 [92], one introduces the logarithm of series with coefficients in $R[\Delta]$, defined by rationals $b_n^\chi(\mathbb{A}) \in \mathbb{Q}$:

$$log(gocha^*(\mathbb{A}, t)) := \sum_{n \in \mathbb{N}} \left(\sum_{\chi \in \mathrm{Irr}(\Delta)} b_n^\chi(\mathbb{A}) \chi \right) t^n.$$

Then, we obtain an equivariant version of Formula (3.2).

Write $n := mp^k$, with $(m,p)=1$, and assume $(n,q)=1$. Then:

$$a_n^\chi(\mathbb{F}_p) = w_m^\chi(\mathbb{F}_p) + w_{mp}^\chi(\mathbb{F}_p) + \cdots + w_{mp^k}^\chi(\mathbb{F}_p), \quad \text{and} \quad a_n^\chi(\mathbb{Z}_p) = w_n^\chi(\mathbb{Z}_p),$$
$$\text{where} \quad w_n^\chi(\mathbb{A}) := \frac{1}{n}\sum_{m|n} \mu(n/m) m b_m^{\chi^{m/n}}(\mathbb{A}) \in \mathbb{Q}. \tag{3.3}$$

Some results on the coefficients $a_n^\chi(\mathbb{Z}_p)$ were given by Filip [28] and Stix [124] for groups defined by one quadratic relation.

In Part 3.2, we study cardinalities of eigenspaces of $\mathscr{L}(\mathbb{A},G)$. When $\mathscr{L}(\mathbb{A},G)$ is infinite dimensional (as a free module over $\mathbb{A}$), we observe using the pigeonhole principle that $\mathscr{L}(\mathbb{A},G)$ admits at least one infinite dimensional eigenspace.

Main Question: Which eigenspaces of $\mathscr{L}(\mathbb{A},G)$ are infinite dimensional?

For this purpose, we introduce χ_0-filtration on $Al(\mathbb{A},G)$, which depends on a fixed non-trivial irreducible character χ_0. It is denoted by $(E_{\chi_0,n}(\mathbb{A},G))_n$, and described in Subpart 3.2.1. Furthermore, we assume that $E_{\chi_0,n}(\mathbb{A},G)/E_{\chi_0,n+1}(\mathbb{A},G)$ is **torsion-free** over $\mathbb{A}$. This condition is automatically satisfied when $\mathbb{A}=\mathbb{F}_p$; and for $\mathbb{A}=\mathbb{Z}_p$, it is true whenever G is free or in the situation of [61, Théorème 2]. This allows us to define $gocha_{\chi_0}(\mathbb{A},t)$ by:

$$gocha_{\chi_0}(\mathbb{A},t) := \sum_{n\in\mathbb{N}} c_{\chi_0,n}(\mathbb{A}) t^n,$$
$$\text{where} \quad c_{\chi_0,n}(\mathbb{A}) := \operatorname{rank}_{\mathbb{A}}(E_{\chi_0,n}(\mathbb{A},G)/E_{\chi_0,n+1}(\mathbb{A},G)).$$

Part 3.3 illustrates our theoretical results for finitely presented pro-p groups G, with mild presentations.

Proposition 23 allows us to compute the *gocha* series of G, and shows that the inverse of the gocha series is a polynomial. Then Theorem 19 answers (and generalizes) [92, Question 2.13], showing that $gocha(\mathbb{A},t)$, $gocha^*(\mathbb{A},t)$ and $gocha_{\chi_0}(\mathbb{A},t)$ do not depend on the choice of the ring $\mathbb{A}$. Finally, considering [137, Theorem D] in our context, one recovers a_n^χ from roots of the polynomial $1/gocha^*$ (see Proposition 24).

Let us now introduce our last result. Since (Proposition 23) $\chi_{eul,\chi_0}(t) := 1/gocha_{\chi_0}(t)$ is a polynomial, we write the degree of χ_{eul,χ_0} as $\deg_{\chi_0}(G)$. Denote the χ_0-eigenvalues of G by $\lambda_{\chi_0,i}$, and let $L_{\chi_0}(G)$ be the χ_0-entropy of G defined by:

$$\chi_{eul,\chi_0}(t) := \prod_{i=1}^{\deg_{\chi_0}(G)} (1-\lambda_{\chi_0,i}t), \quad L_{\chi_0}(G) := \max_{1\le i\le \deg_{\chi_0}(G)} |\lambda_{\chi_0,i}|.$$

Theorem C. *Assume for some χ_0 that $L_{\chi_0}(G)$ is reached for a unique eigenvalue $\lambda_{\chi_0,i}$ such that:*

(i) $\lambda_{\chi_0,i}$ is real,

(ii) $L_{\chi_0}(G) = \lambda_{\chi_0,i} > 1$.

Then every eigenspace of $\mathscr{L}(\mathbb{A}, G)$ *is infinite dimensional.*

We also prove in Theorem 22, that every finitely generated noncommutative free pro-p group G satisfies the hypotheses of Theorem C. Let us finish this introduction with explicit examples:

Example 1 (Cohomological dimension 2)**.** *Let us take* $p = 103$, $q = 17$. *Observe that* $\overline{8} \in \mathbb{F}_{103}$ *is a primitive* 17*-th root of unity.*
*Consider the pro-*103 *group* G, *generated by three generators* x, y, z *and one relation* $u = [x; y]$. *By [63, Theorem], the* $\mathbb{Z}_p$*-module* $\mathscr{L}(\mathbb{Z}_p, G)$ *is torsion-free. If we apply [29, Corollary* 5.3*] and Proposition 23, we remark that* $\mathrm{cd}(G) = 2$ *and:*

$$gocha(\mathbb{A}, t) := 1/(1 - 3t + t^2).$$

Introduce an automorphism δ *on* G, *by* $\delta(x) := x^8$, $\delta(y) := y^{8^2}$ *and* $\delta(z) := z^{8^3}$*; Proposition 25 justifies that this action is well defined. Consequently* $\Delta := \langle \delta \rangle$ *is a subgroup of order* 17 *of* $Aut(G)$. *Fix the character* $\chi_0 \colon \Delta \to \mathbb{F}_{103}^{\times}; \delta \mapsto \overline{8}$.

Applying Formula (3.3)*, let us compute some coefficients* a_n^{χ} *and* c_n^{χ}.
Observe first that:

$$gocha^*(\mathbb{A}, t) := \frac{1}{1 - (\chi_0 + {\chi_0}^2 + {\chi_0}^3).t + {\chi_0}^3.t^2}, \quad \textit{and}$$

$$\log(gocha^*(\mathbb{A}, t)) = (\chi_0 + {\chi_0}^2 + {\chi_0}^3).t + ({\chi_0}^6/2 + {\chi_0}^5 + \frac{3\chi_0^4}{2} + \frac{\chi_0^2}{2}).t^2 + (\frac{\chi_0^9}{3} + {\chi_0}^8 + 2{\chi_0}^7 + \frac{4\chi_0^6}{3} + \chi_0^5 + \frac{\chi_0^3}{3}).t^3 + \dots.$$

From Formula (3.2)*, we infer:* $a_2 = 2$ *and* $a_3 = 5$. *Furthermore Formula* (3.3) *gives us:*

$$a_2^{\chi_0^i} = \frac{2b_2^{\chi_0^i} - b_1^{\chi_0^{9i}}}{2}, \quad \textit{and} \quad a_3^{\chi_0^i} = \frac{3b_3^{\chi_0^i} - b_1^{\chi_0^{6i}}}{3}.$$

Consequently, we obtain:

- $a_2^{\chi_0^4} = a_2^{\chi_0^5} = 1$, *else* $a_2^{\chi_0^i} = 0$ *when* $i \neq 5$.
- $a_3^{\chi_0^8} = a_3^{\chi_0^6} = a_3^{\chi_0^5} = 1$, *and* $a_3^{\chi_0^7} = 2$. *Else if* $i \notin \{5; 6; 7; 8\}$, $a_3^{\chi_0^i} = 0$.

Here, by [64, Theorem 1 *and Part* 3*], the algebra* $\mathscr{L}_{\chi_0}(G, \mathbb{Z}_p)$ *is torsion-free over* $\mathbb{Z}_p$. *We have:*

$$gocha_{\chi_0}(\mathbb{A}, t) := \frac{1}{1 - t - t^2},$$

and the maximal χ_0*-eigenvalue of* G *is real and strictly greater than* 1.
Therefore by Theorem C, all eigenspaces of $\mathscr{L}(\mathbb{A}, G)$ *are infinite dimensional.*

Example 2 (FAB example)**.** *Following arguments given by [35], we enrich the example given in [45, Part* 2.1*], and obtain an example where G is FAB, i.e. every open subgroup has finite abelianization (for more details, see Example 21, and for references on FAB groups, see [62] and [81]).*

Take $p = 3$, and consider $K := \mathbb{Q}(\sqrt{-163})$. Then we define $\Delta := \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, and fix χ_0 the non-trivial irreducible character of Δ over $\mathbb{F}_p$. Consider the following set of places in $\mathbb{Q}$: $\{7, 19, 13, 31, 337, 43\}$. The class group of K is trivial, the primes $7, 19, 13, 31, 337$ are inert in K, and the prime 43 totally splits in K.

Define S the primes above the previous set in K, and K_S the maximal p-extension unramified outside S. Then Δ acts on $G := \mathrm{Gal}(K_S/K)$, which is FAB by Class Field Theory.

We can show that the pro-p group G is mild, and Proposition 26 gives:

$$gocha^*(\mathbb{F}_p, t) := \frac{1}{1 - (6 + \chi_0)t + (6 + \chi_0)t^2}, \quad \text{and} \quad gocha_{\chi_0}(\mathbb{F}_p, t) := \frac{1}{1 - t - 5t^2 + 6t^4}.$$

Therefore by Theorem C, all eigenspaces of $\mathscr{L}(\mathbb{F}_p, G)$ are infinite dimensional.

Notations

We follow the notations and definitions of [3] and [69, Appendice A].

Let p be an odd prime, and G a finitely generated pro-p group with minimal presentation $1 \to R \to F \to G \to 1$, and denote by $\mathbb{A}$ one of the rings $\mathbb{F}_p$ or $\mathbb{Z}_p$. Assume that $Aut(G)$ contains a cyclic subgroup Δ of order q, a prime factor of $p - 1$. By [39, Lemma 2.15], we observe that Δ lifts to a subgroup of $Aut(F)$.

When the context is clear, we omit the $\mathbb{A}$ when denoting filtrations (and associated invariants). Additionally, we always suppose that $\mathscr{L}(\mathbb{A}, G)$ is **torsion-free over** $\mathbb{A}$.

Denote by $Al(\mathbb{A}, G)$ the completed group algebra of G over $\mathbb{A}$ and observe that G embeds naturally into $Al(\mathbb{A}, G)$.

For $\chi \in \mathrm{Irr}(\Delta)$, we fix $\{x_j^\chi\}_{1 \le j \le d^\chi}$ a lift in F of a basis of $\mathscr{L}_1(\mathbb{A}, G)[\chi]$, where $d^\chi := \mathrm{rank}_{\mathbb{A}} \mathscr{L}_1(\mathbb{A}, G)[\chi]$; by [120, Corollaire 3, Proposition 42, Chapitre 14], this basis does not depend on the choice of $\mathbb{A}$. The Magnus isomorphism, from [69, Chapitre II, Partie 3], gives us the following identification of $\mathbb{A}$-algebras between $Al(\mathbb{A}, F)$ and the noncommuative series over X_j^χ's with coefficients in $\mathbb{A}$:

$$\phi_{\mathbb{A}} \colon Al(\mathbb{A}, F) \simeq \mathbb{A}\langle\langle X_j^\chi; \chi \in \mathrm{Irr}(\Delta), 1 \le j \le d^\chi \rangle\rangle; \quad x_j^\chi \mapsto X_j^\chi + 1 \tag{3.4}$$

Define $E(\mathbb{A})$ as the algebra $\mathbb{A}\langle\langle X_j^\chi; \chi \in \mathrm{Irr}(\Delta), 1 \le j \le d^\chi \rangle\rangle$ filtered by $\deg(X_j^\chi) = 1$ and write $\{E_n(\mathbb{A})\}_{n \in \mathbb{N}}$ for its filtration. One introduces $I(\mathbb{A}, R)$ the ideal of $E(\mathbb{A})$ generated by $\{\phi_{\mathbb{A}}(r - 1); r \in R\}$ endowed with the induced filtration $\{I_n(\mathbb{A}, R) := I(\mathbb{A}, R) \cap E_n(\mathbb{A})\}_{n \in \mathbb{N}}$, and $E(\mathbb{A}, G)$ the quotient filtered algebra $E(\mathbb{A})/I(\mathbb{A}, R)$, with induced filtration $\{E_n(\mathbb{A}, G)\}_{n \in \mathbb{N}}$.

We call $M := \bigoplus_{n \in \mathbb{N}} M_n$ a graded locally finite ($\mathbb{A}[\Delta]$-)module, if M_n is a finite dimensional ($\mathbb{A}[\Delta]$)-module for every integer n; and denote its Hilbert series by:

$$M(t) := \sum_{n \in \mathbb{N}} (\mathrm{rank}_{\mathbb{A}} M_n) t^n.$$

We make the following convention; we say that M is an $\mathbb{A}$-Lie algebra if M is a graded locally finite Lie algebra over $\mathbb{A}$, and when $\mathbb{A} := \mathbb{F}_p$ we assume in addition that M is a restricted p-Lie algebra. Recall the following graded locally finite $\mathbb{A}[\Delta]$-module and $\mathbb{A}$-Lie algebra, defined at the beginning:

$$\mathscr{E}(\mathbb{A}) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_n(\mathbb{A}), \quad \text{where} \quad \mathscr{E}_n(\mathbb{A}) := E_n(\mathbb{A})/E_{n+1}(\mathbb{A}),$$
$$\mathscr{L}(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{L}_n(\mathbb{A}, G), \quad \text{and} \quad \mathscr{E}(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_n(\mathbb{A}, G).$$

If $P := \sum_{n\in\mathbb{N}} p_n t^n$ and $Q := \sum_{n\in\mathbb{N}} q_n t^n$ are two series with real coefficients, we say that : $P \leq Q \iff \forall n \in \mathbb{N}, \quad p_n \leq q_n$. We denote by μ the Möbius function.

3.1 An equivariant version of Mináč-Rogelstad-Tân's results

Recall:

$$gocha^*(\mathbb{A}, t) := \sum_{n\in\mathbb{N}} \left(\sum_{\chi\in \mathrm{Irr}(\Delta)} c_n^\chi \chi \right) t^n \in R[\Delta][[t]],$$

where $R[\Delta]$ denotes the finite representation ring of Δ (over $\mathbb{A}$).

3.1.1 Equivariant Hilbert series

The aim of this subpart is to prove the following formula:

$$\begin{gathered} gocha^*(\mathbb{A}, t) = \prod_{n\in\mathbb{N}} \prod_{\chi\in\mathrm{Irr}(\Delta)} P_\chi(\mathbb{A}, t^n)^{a_n^\chi}, \\ \text{where} \quad P_\chi(\mathbb{F}_p, t) := \frac{1-\chi.t^p}{1-\chi.t}, \quad \text{and} \quad P_\chi(\mathbb{Z}_p, t) := \frac{1}{1-\chi.t}. \end{gathered} \tag{3.5}$$

This is Theorem B defined in our introduction.

Definition 25. *Let $M := \bigoplus_{n\in\mathbb{N}} M_n$ be an $\mathbb{A}$-Lie algebra, graded locally finite $\mathbb{A}[\Delta]$-module, with basis $\{x_{n,1}; \ldots; x_{n,m_n}\}_{n\in\mathbb{N}}$, where $m_n := \mathrm{rank}_{\mathbb{A}} M_n$. We define:*

- *the graded locally finite module with basis given by words on $\{x_{n,j}\}_{n\in\mathbb{N}; j\in[\![1;m_n]\!]}$ by:*

$$\tilde{U}(M) := \bigoplus_{n\in\mathbb{N}} \tilde{U}(M)_n,$$

moreover, when $\mathbb{A} := \mathbb{F}_p$, we also assume that the p-restricted operation is compatible with the multiplicative structure of $\tilde{U}(M)$;

- *the equivariant Hilbert series of M with coefficient in $R[\Delta]$ by:*

$$M^*(t) := \sum_{n\in\mathbb{N}} \left(\sum_{\chi\in \mathrm{Irr}(\Delta)} m_n^\chi \chi \right) t^n$$
$$\text{where} \quad m_n^\chi := \mathrm{rank}_{\mathbb{A}} M_n[\chi] \quad \text{for every integer } n.$$

Remark 9. *Since the action of Δ over a graded locally finite module is semi-simple, it always preserves the grading. Consequently, if M is a graded locally finite $\mathbb{A}[\Delta]$-module, then the graded locally finite module $\tilde{U}(M)$ is also endowed with a natural structure of graded locally finite $\mathbb{A}[\Delta]$-module.*

We give a well-known result on Lie algebras, telling us that $\tilde{U}$ is a universal enveloping algebra of M.

Theorem 15 (Poincaré-Birkhoff-Witt)**.** *Let M be a graded locally finite $\mathbb{A}[\Delta]$-module and $\mathbb{A}$-Lie algebra. Then $\tilde{U}(M)$ is a graded locally finite $\mathbb{A}[\Delta]$-module, universal $\mathbb{A}$-Lie algebra of M.*

Proof. When $\mathbb{A} := \mathbb{Z}_p$, see for instance [62, Theorem 2.1].
When $\mathbb{A} := \mathbb{F}_p$, see for instance [19, Proposition 12.4]. □

Corollary 9. *The set $\mathscr{E}(\mathbb{A}, G)$ is a graded locally finite, $\mathbb{A}$-universal Lie algebra of $\mathscr{L}(\mathbb{A}, G)$. Consequently $\mathscr{E}(\mathbb{A}, G)$ is torsion-free.*

Proof. Let us first prove that $\mathscr{E}(\mathbb{A}, G)$ is a graded locally finite, $\mathbb{A}$-universal Lie algebra of $\mathscr{L}(\mathbb{A}, G)$. By Theorem 15, we only need to show that $\tilde{U}(\mathscr{L}(\mathbb{A}, G)) \simeq \mathscr{E}(\mathbb{A}, G)$.

For $\mathbb{A} := \mathbb{F}_p$, see [69, Appendice A, Théorème 2.6].

For $\mathbb{A} := \mathbb{Z}_p$, the proof of [48, Theorem 1.3] carries to the case $E(\mathbb{Z}_p, G)$ with minor alterations. We consider $\mathbb{Z}_p$ and $\mathbb{Q}_p$ rather than $\mathbb{Z}$ and $\mathbb{Q}$. Furthermore, we conclude using the fact that G is finitely generated, so $\mathrm{Grad}(E(\mathbb{Z}_p, G)) = \mathscr{E}(\mathbb{Z}_p, G)$ is isomorphic to $\mathrm{Grad}(\mathbb{Z}_p[G])$, where $\mathbb{Z}_p[G]$ is filtered by power of the augmentation ideal over $\mathbb{Z}_p$. □

Remark 10. *Notice that $\mathscr{E}(\mathbb{A}, G)$ is also isomorphic to $\tilde{U}(\mathscr{L}(\mathbb{A}, G))$ as an $\mathbb{A}[\Delta]$-module. Therefore, we have:*

$$\tilde{U}(\mathscr{L}(\mathbb{A}, G))^*(t) := gocha^*(\mathbb{A}, t).$$

Before proving Formula 3.5, we need the following result:

Lemma 6. *Let M be a graded locally finite $\mathbb{A}[\Delta]$-module and $\mathbb{A}$-Lie algebra, then:*

$$\tilde{U}(M)^*(t) = \prod_{n\in\mathbb{N}} \prod_{\chi\in \mathrm{Irr}(\Delta)} P_\chi(\mathbb{A}, t^n)^{m_n^\chi},$$
$$\text{where} \quad P_\chi(\mathbb{F}_p, t) := \frac{1-\chi.t^p}{1-\chi.t}, \quad \text{and} \quad P_\chi(\mathbb{Z}_p, t) := \frac{1}{1-\chi.t}.$$

Proof. Let us first prove the case $\mathbb{A} := \mathbb{F}_p$.

We are inspired by the proof of [19, Corollary 12.13]. Observe that if M and N are graded locally finite $\mathbb{F}_p[\Delta]$-modules, then $M \bigotimes_{\mathbb{F}_p} N$ is also a graded locally finite $\mathbb{F}_p[\Delta]$-module; moreover $(M \bigotimes_{\mathbb{F}_p} N)^*(t) := M^*(t)N^*(t)$, and $\tilde{U}(M \bigoplus N) = \tilde{U}(M) \bigotimes_{\mathbb{F}_p} \tilde{U}(N)$. So assume that :

$$M^*(t) := \sum_n m_n \chi_0 . t^n, \quad \text{for some fixed and non-trivial } \chi_0 \in \mathrm{Irr}(\Delta).$$

Consider $X_n := \{x_{n,1}, \ldots, x_{n,m_n}\}$, an $\mathbb{F}_p[\Delta]$-basis of M_n, where each $x_{n,j}$ is of degree n. Then a graded locally finite $\mathbb{F}_p[\Delta]$-basis of M is given by the (disjoint) union of all X_n's. Denote by

$$\tilde{U}(M)^*(t) := \sum_{r \in \mathbb{N}} \left(\sum_{\chi \in \mathrm{Irr}(\Delta)} u_r^\chi \chi \right) t^r, \text{ where } u_r^\chi := \dim_{\mathbb{F}_p} \tilde{U}(M)_r[\chi].$$

We need to compute $u_r^{\chi_0^i}$, where $i \in \mathbb{Z}/q\mathbb{Z}$: this is the number of products of the form

$$\prod_{n=1}^{r} \prod_{j=1}^{m_n} (x_{n,j}\chi_0)^{m_{n,j}}, \quad \text{where} \quad 0 \leq m_{n,j} \leq p-1,$$

such that

$$\sum_{n=1}^{r} \sum_{j=1}^{m_n} n m_{n,j} = r \quad \text{and} \quad \sum_{n=1}^{r} \sum_{j=1}^{m_n} m_{n,j} \equiv i \pmod{q}.$$

Notice that the coefficient before t^r of the polynomial

$$\prod_{n=1}^{r} [1 + \chi_0 t^n + \cdots + \chi_0^{p-1} t^{(p-1)n}]^{m_n}$$

is

$$\sum_{n=1}^{r} \left(\sum_{j=1}^{m_n} {\chi_0}^{m_{n,j}} \right) t^r, \quad \text{where} \quad 0 \leq m_{n,j} \leq p-1, \quad \text{and} \quad \sum_{n=1}^{r} \sum_{j=1}^{m_n} n m_{n,j} = r.$$

Consequently the coefficient before $\chi_0^i t^r$ is exactly $u_r^{\chi_0^i}$.

Let us now prove the case $\mathbb{A} := \mathbb{Z}_p$.
By the Poincaré-Birkhoff-Witt Theorem, the set $\tilde{U}(M)$ is the symmetric Lie algebra over M. Similarly to the previous case, we just need to study the case where there exists a unique χ_0 such that $M^*(t) := \sum_n m_n \chi_0 . t^n$. We get:

$$\tilde{U}(M)^*(t) = \prod_n \left(\frac{1}{1 - \chi_0 . t} \right)^{m_n^\chi}.$$

One deduces the general case. □

Proof of Formula (3.5). We apply Lemma 6 and Corollary 9 to obtain:

$$gocha^*(\mathbb{A},t)=\prod_{n\in\mathbb{N}}\prod_{\chi\in\mathrm{Irr}(\Delta)}P_\chi(\mathbb{A},t^n)^{a_n^\chi},$$

$$\text{where}\quad P_\chi(\mathbb{F}_p,t):=\frac{1-\chi.t^p}{1-\chi.t},\quad\text{and}\quad P_\chi(\mathbb{Z}_p,t):=\frac{1}{1-\chi.t}$$

□

3.1.2 Proof of Formula (3.3)

The aim of this part is to prove the following Proposition:

Proposition 20. *Write $n=mp^k$ with $(m,p)=1$ and $(n,q)=1$, then:*

$$a_n^\chi(\mathbb{F}_p)=w_m^\chi(\mathbb{F}_p)+w_{mp}^\chi(\mathbb{F}_p)+\cdots+w_{mp^k}^\chi(\mathbb{F}_p),\quad \textit{and}\quad a_n^\chi(\mathbb{Z}_p)=w_n^\chi(\mathbb{Z}_p);$$

$$\textit{where}\quad w_n^\chi:=\frac{1}{n}\sum_{m|n}\mu(n/m)mb_m^{\chi^{m/n}}\in\mathbb{Q}.$$

This is Formula (3.3) given in our introduction.

The strategy of the proof is to transform the product formula given by (3.5), into a sum in $(R[\Delta]\otimes_{\mathbb{Z}}\mathbb{Q})[[t]]$.

Definition 26 (log function)**.** *If $P\in 1+tR[\Delta][[t]]$, we define:*

$$\log(P)(t):=-\sum_n\frac{(1-P(t))^n}{n}\in(R[\Delta]\otimes_{\mathbb{Z}}\mathbb{Q})[[t]].$$

Remark 11. *Note that the* log *function enjoys the following properties:*

(i) If P and Q are in $1+tR[\Delta][[t]]$, then:

$$\log(PQ)=\log(P)+\log(Q),\qquad \textit{and}$$

$$\log(1/P)=-\log(P).$$

(ii) If u is in $tR[\Delta][[t]]$, then

$$\log\left(\frac{1}{1-u}\right)=\sum_{\nu=1}^{\infty}\frac{u^\nu}{\nu}.$$

Define the sequence $(b_n^\chi(\mathbb{A}))_{n\in\mathbb{N}}\in\mathbb{Q}^{\mathbb{N}}$ by:

$$\log(gocha^*(\mathbb{A},t))=\sum_{n\geq 1}\left(\sum_{\chi\in\mathrm{Irr}(\Delta)}b_n^\chi(\mathbb{A})\chi\right)t^n.$$

Proposition 21. *If $(n,q)=1$, we infer:*

$$b_n^{\chi^n}(\mathbb{F}_p) := \frac{1}{n}\left(\sum_{m|n} m a_m^{\chi^m}(\mathbb{F}_p) - \sum_{rp|n} rp a_r^{\chi^r}(\mathbb{F}_p)\right), \quad \textit{and} \quad b_n^{\chi^n}(\mathbb{Z}_p) := \frac{1}{n}\sum_{m|n} m a_m^{\chi^m}(\mathbb{Z}_p).$$

Proof. Let us just prove the case $\mathbb{A} := \mathbb{F}_p$ (the case $\mathbb{A} := \mathbb{Z}_p$ is similar).

First, Formula (3.5) gives us:

$$gocha^*(\mathbb{F}_p, t) = \prod_{n\in\mathbb{N}} \prod_{\chi\in \mathrm{Irr}(\Delta)} \left(\frac{1-\chi.t^{np}}{1-\chi.t^n}\right)^{a_n^\chi}.$$

Let us take the logarithm to obtain:

$$\log(gocha^*(\mathbb{F}_p,t)) = \sum_n \sum_{\chi\in\mathrm{Irr}(\Delta)} a_n^\chi \left[\log(1-(\chi.t^n)^p) - \log(1-\chi.t^n)\right],$$

so that

$$\sum_{n\in\mathbb{N}} \left(\sum_{\chi\in\mathrm{Irr}(\Delta)} b_n^\chi \chi\right) t^n = \sum_{w=1}^{\infty} \sum_{\chi\in\mathrm{Irr}(\Delta)} a_w^\chi \left(\sum_{\nu=1}^{\infty} \frac{(\chi.t^w)^\nu}{\nu} - \sum_{r=1}^{\infty} \frac{(\chi.t^w)^{rp}}{r}\right),$$

from which we conclude

$$\sum_{n=1}^{\infty} n\left(\sum_{\chi\in\mathrm{Irr}(\Delta)} b_n^\chi \chi\right) t^n = \sum_{n=1}^{\infty}\left(\sum_{\chi\in\mathrm{Irr}(\Delta)} \left(\sum_{m|n} m a_m^\chi \chi^{n/m} - \sum_{rp|n} rp a_r^\chi \chi^{n/r}\right)\right) t^n.$$

Then we infer:

$$n b_n^{\chi^n} = \sum_{m|n} m a_m^{\chi^m} - \sum_{rp|n} rp a_r^{\chi^r}.$$

□

Proof of Proposition 20. Again, we just prove the case $\mathbb{A} := \mathbb{F}_p$.
We are inspired by the proof of [92, Theorem 2.9].
First, we assume $(n,p)=1$, then by Proposition 21, we obtain:

$$n b_n^{\chi^n} = \sum_{m|n} m a_m^{\chi^m}.$$

So, using the Möbius inversion Formula, we obtain:

$$a_n^{\chi^n} = w_n^{\chi^n}, \quad \text{thus} \quad a_n^\chi = w_n^\chi.$$

Now, let us assume p divides n. We show by induction on n that:

$$a_n^{\chi^n} = a_{n/p}^{\chi^{n/p}} + w_n^{\chi^n} \qquad (*)$$

- If $n = p$, then by Proposition 21, we have: $pb_p^{\chi^p} = pa_p^{\chi^p} + a_1^{\chi} - pa_1^{\chi}$. So,

$$pw_p^{\chi^p} = pb_p^{\chi^p} - b_1^{\chi} = pa_p^{\chi^p} - pa_1^{\chi}.$$

  Therefore, $a_p^{\chi^p} = a_1^{\chi} + w_p^{\chi^p}$.

- Let us fix n, an integer such that $p|n$, and assume equation $(*)$ is true for all m such that $m \neq n$ and $p|m|n$. Then, following Proposition 21, we have:

$$\begin{aligned} nb_n^{\chi^n} &= \sum_{m|n} ma_m^{\chi^m} - \sum_{rp|n} rpa_r^{\chi^r} \\ &= \sum_{m|n;(m,p)=1} ma_m^{\chi^m} + \sum_{p|m|n} m\left(a_m^{\chi^m} - a_{m/p}^{\chi^{m/p}}\right) \\ &= \sum_{m|n;(m,p)=1} mw_m^{\chi^m} + \sum_{p|m|n;m\neq n} mw_m^{\chi^m} + n\left(a_n^{\chi^n} - a_{n/p}^{\chi^{n/p}}\right) \\ &= \sum_{m|n;m\neq n} mw_m^{\chi^m} + n\left(a_n^{\chi^n} - a_{n/p}^{\chi^{n/p}}\right). \end{aligned}$$

  Moreover, by the Möbius inversion formula, we have:

$$nb_n^{\chi^n} = \sum_{m|n} mw_m^{\chi^m}.$$

  Therefore, we obtain:

$$nw_n^{\chi^n} = n\left(a_n^{\chi^n} - a_{n/p}^{\chi^{n/p}}\right).$$

□

Remark 12. *Formula* (3.3) *was already given for groups defined by one quadratic relation by Filip [28, Formula* (4.7)*] (for* $\mathbb{C}$*-representations in a geometrical context) and by Stix [124, Formula* (14.16)*] (in a Galois-theoretical context). Additionally, they computed explicitely the coefficients* $b_n^{\chi}(\mathbb{Z}_p)$*. We discuss this analogy in Theorem 24.*

Remark 13. *Let us reformulate [92, Question* 2.13*], asked byInáč-Rogelstad-Tân, in our equivariant context:*

> Do we have for every integer n and every irreducible character χ, the equality $c_n^{\chi}(\mathbb{Z}_p) = c_n^{\chi}(\mathbb{F}_p)$?

Later in this chapter, we give a positive answer to this question, when G *is finitely presented and* $\mathrm{cd}(G) \leq 2$ *(see Theorem 19).*

3.2 Infinite dimensional eigenspaces of $\mathscr{L}(\mathbb{A}, G)$

The goal of this part is to study infinite dimensional eigenspaces (as a free $\mathbb{A}$-module) of

$$\mathscr{L}(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{L}_n(\mathbb{A}, G), \quad \text{where} \quad \mathscr{L}_n(\mathbb{A}, G) := G_n(\mathbb{A})/G_{n+1}(\mathbb{A}).$$

For this purpose, we introduce χ_0-filtrations.

3.2.1 Definition of χ_0-filtrations

From now on, we make no distinction between $\mathbb{Z}/q\mathbb{Z}$ and the set $[\![1; q]\!]$. Observe the following isomorphism of groups, which depends on the choice of a fixed non-trivial irreducible character χ_0:

$$\psi_{\chi_0} \colon (\mathrm{Irr}(\Delta); \otimes) \to (\mathbb{Z}/q\mathbb{Z}; +); \quad \chi_0^i \mapsto i.$$

Recall that $\phi_{\mathbb{A}}$ denotes the Magnus' isomorphism introduced in (1). We define $E_{\chi_0}(\mathbb{A})$ as the $\mathbb{A}$-algebra $\mathbb{A}\langle\langle X_j^\chi; \chi \in \mathrm{Irr}(\Delta), 1 \le j \le d^\chi\rangle\rangle$ filtered by $\deg(X_j^\chi) = \psi_{\chi_0}(\chi)$, and $\{E_{\chi_0,n}(\mathbb{A})\}_{n\in\mathbb{N}}$ as its filtration: called the χ_0-filtration of $Al(\mathbb{A}, F)$. We introduce

$$\mathscr{E}_{\chi_0}(\mathbb{A}) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_{\chi_0,n}(\mathbb{A}), \quad \text{where} \quad \mathscr{E}_{\chi_0,n}(\mathbb{A}) := E_{\chi_0,n}(\mathbb{A})/E_{\chi_0,n+1}(\mathbb{A}).$$

Write $I_{\chi_0}(\mathbb{A}, R)$ for the two-sided ideal generated by $\{\phi_{\mathbb{A}}(r-1); r \in R\} \subset E_{\chi_0}(\mathbb{A})$, endowed with filtration $\{I_{\chi_0,n}(\mathbb{A}, R) := I_{\chi_0}(\mathbb{A}, R) \cap E_{\chi_0,n}(\mathbb{A})\}_{n\in\mathbb{N}}$; and $E_{\chi_0}(\mathbb{A}, G)$ the quotient filtered algebra $E_{\chi_0}(\mathbb{A})/I_{\chi_0}(\mathbb{A}, R)$.
Define the following $\mathbb{A}$-module:

$$\mathscr{E}_{\chi_0}(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_{\chi_0,n}(\mathbb{A}, G), \quad \text{where} \quad \mathscr{E}_{\chi_0,n}(\mathbb{A}, G) := E_{\chi_0,n}(\mathbb{A}, G)/E_{\chi_0,n+1}(\mathbb{A}, G).$$

Introduce:

$$G_{\chi_0,n}(\mathbb{A}) := \{g \in G; \phi_{\mathbb{A}}(g-1) \in E_{\chi_0,n}(\mathbb{A}, G)\}, \quad \text{and}$$
$$\mathscr{L}_{\chi_0}(\mathbb{A}, G) := \bigoplus_{n\in\mathbb{N}} \mathscr{L}_{\chi_0,n}(\mathbb{A}, G), \quad \text{where} \quad \mathscr{L}_{\chi_0,n}(\mathbb{A}, G) := G_{\chi_0,n}(\mathbb{A})/G_{\chi_0,n+1}(\mathbb{A}).$$

We always assume that the $\mathbb{A}$-Lie algebra $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$ is **torsion-free** over $\mathbb{A}$.

Lemma 7. *The set $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$ is a graded locally finite, $\mathbb{A}$-universal Lie algebra of $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$. Consequently, the graded $\mathbb{A}$-Lie algebra $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$ is torsion-free.*

Proof. This is similar to the proof of Corollary 9. □

Since G is finitely generated, we define:

$$gocha_{\chi_0}(\mathbb{A}, t) := \sum_n c_{\chi_0,n}(\mathbb{A}) t^n, \quad \text{where} \quad c_{\chi_0,n}(\mathbb{A}) := \mathrm{rank}_{\mathbb{A}} \mathscr{E}_{\chi_0,n}(\mathbb{A}, G),$$
$$\text{and} \quad a_{\chi_0,n}(\mathbb{A}) := \mathrm{rank}_{\mathbb{A}}(G_{\chi_0,n}(\mathbb{A})/G_{\chi_0,n+1}(\mathbb{A})).$$

3.2.2 Properties of χ_0-filtrations

This subpart aims to develop various properties of χ_0-filtations.

Lemma 8. *The modules $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$ and $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$ are graded locally finite $\mathbb{A}[\Delta]$-modules. More precisely, we have:*

$$\begin{aligned}\mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A}, G)[\chi] =& c_{\chi_0,n}(\mathbb{A})\delta_n^{\psi_{\chi_0}(\chi)},\\ \mathrm{rank}_{\mathbb{A}}\mathscr{L}_{\chi_0,n}(\mathbb{A}, G)[\chi] =& a_{\chi_0,n}(\mathbb{A})\delta_n^{\psi_{\chi_0}(\chi)},\end{aligned}$$

where $\delta_n^{\psi_{\chi_0}(\chi)} = 1$ *if* $n \equiv \psi_{\chi_0}(\chi) \pmod q$, *otherwise* $\delta_n^{\psi_{\chi_0}(\chi)} = 0$.

Proof. Let us denote by $\mathscr{I}_{\chi_0,n}(\mathbb{A}, R) := I_{\chi_0,n}(\mathbb{A}, R)/I_{\chi_0,n+1}(\mathbb{A}, R)$. Remind by [39, Lemma 2.15], that $\Delta \subset Aut(F)$ and $\Delta(R) = R$. So $\mathscr{E}_{\chi_0}(\mathbb{A})$ is a graded locally finite $\mathbb{A}[\Delta]$-module, and $\mathscr{I}_{\chi_0,n}(\mathbb{A}, R)$ is stable by Δ. By [69, Chapitre I, Résultat 2.3.8.2], we have the following exact sequence:

$$0 \to \mathscr{I}_{\chi_0,n}(\mathbb{A}, R) \to \mathscr{E}_{\chi_0,n}(\mathbb{A}) \to \mathscr{E}_{\chi_0,n}(\mathbb{A}, G) \to 0.$$

Then $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$ and $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$ are graded locally finite $\mathbb{A}[\Delta]$-modules. Let us now study more precisely the $\mathbb{A}[\Delta]$-module structure of $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$ and $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$.

For the structure of $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$: take $u \in \mathscr{E}_{\chi_0,n}(\mathbb{A})$ and write $u := X_{j_1}^{\chi_0^{i_1}} \dots X_{j_u}^{\chi_0^{i_u}}$, with $i_1 + \dots + i_u = n$. Therefore, for every $\delta \in \Delta$, $\delta(u) = \chi_0^n(\delta)u$. Then, we infer for every χ:

$$\mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A})[\chi] = \mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A})\delta_n^{\psi_{\chi_0}(\chi)}. \qquad (**)$$

Since $\mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A})[\chi] \geq \mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A}, G)[\chi]$, we conclude by Equation $(**)$ that:

$$\mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A}, G)[\chi] = c_{\chi_0,n}\delta_n^{\psi_{\chi_0}(\chi)}.$$

For the structure of $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$: note by Lemma 7 that $\mathscr{E}_{\chi_0}(\mathbb{A}, G)$ is a graded locally finite $\mathbb{A}[\Delta]$-module, universal $\mathbb{A}$-Lie algebra of $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$. Hence for every χ, and every n:

$$\mathrm{rank}_{\mathbb{A}}\mathscr{E}_{\chi_0,n}(\mathbb{A}, G)[\chi] \geq \mathrm{rank}_{\mathbb{A}}\mathscr{L}_{\chi_0,n}(\mathbb{A}, G)[\chi].$$

This allows us to conclude for every χ:

$$\mathrm{rank}_{\mathbb{A}}\mathscr{L}_{\chi_0,n}(\mathbb{A}, G)[\chi] = a_{\chi_0,n}\delta_n^{\psi_{\chi_0}(\chi)}.$$

□

Now, let us compare $(c_{\chi_0,n})_{n\in\mathbb{N}}$, $(a_{\chi_0,n})_{n\in\mathbb{N}}$, $(c_n^{\chi})_{n\in\mathbb{N}}$ and $(a_n^{\chi})_{n\in\mathbb{N}}$.

Proposition 22. *The following inequalities hold:*

$$c_{\chi_0,qn+i} \leq \sum_{j=n}^{qn+i} c_j^{\chi_0^i}, \quad a_{\chi_0,qn+i} \leq \sum_{j=n}^{qn+i} a_j^{\chi_0^i}, \tag{3.6}$$

$$c_n^\chi \leq \sum_{k=\lceil \frac{n-\psi_{\chi_0}(\chi)}{q} \rceil}^{\lfloor n-\psi_{\chi_0}(\chi)/q \rfloor} c_{\chi_0,qk+\psi_{\chi_0}(\chi)}, \quad a_n^\chi \leq \sum_{k=\lceil \frac{n-\psi_{\chi_0}(\chi)}{q} \rceil}^{\lfloor n-\psi_{\chi_0}(\chi)/q \rfloor} a_{\chi_0,qk+\psi_{\chi_0}(\chi)}. \tag{3.7}$$

Proof. Observe first that the $\mathbb{A}$-Lie algebras $\mathscr{L}_{\chi_0}(\mathbb{A},G)$, $\mathscr{L}(\mathbb{A},G)$, $\mathscr{E}_{\chi_0}(\mathbb{A},G)$ and $\mathscr{E}(\mathbb{A},G)$ are generated by $\{X_j^\chi\}$. We only check inequalities involving c_n (proof of inequalities involving a_n are simlar).

Let us prove inequalities (3.6).
Take u in $\mathscr{E}_{\chi_0,qn+i}(\mathbb{A},G)$. Since u is a sum of monomials u_l in $\mathscr{E}_{\chi_0,qn+i}(\mathbb{A},G)$, we can assume that u is a monomial. So, let us write $u = X_{j_1}^{\chi_0^{i_1}} \dots X_{j_{r_u}}^{\chi_0^{i_{r_u}}}$, where $i_1 + \dots + i_{r_u} = qn+i$. Consequently for every $\delta \in \Delta$,

$$\begin{aligned} \delta(u) &= {\chi_0}^{i_1}(\delta) X_{j_1}^{\chi_0^{i_1}} \dots {\chi_0}^{i_{r_u}}(\delta) X_{j_{r_u}}^{\chi_0^{i_{r_u}}} \quad \text{thus} \\ \delta(u) &= {\chi_0}^{i_1+\dots+i_{r_u}}(\delta) X_{j_1}^{\chi_0^{i_1}} \dots X_{j_{r_u}}^{\chi_0^{i_{r_u}}} = \chi_0^i(\delta) u. \end{aligned}$$

Therefore $u \in \mathscr{E}_{r_u}(\mathbb{A},G)[\chi_0^i]$. To conclude, we need to estimate r_u.

- If $i_l = 1$ for all l, then $r_u = qn+i$.
- If $i_l = q$ for all l, then $qr_u = qn+i$. Therefore, $r_u \geq n$.

In any case:

$$n \leq r_u \leq qn+i.$$

Let us now prove inequalities (3.7).
Take $u \in \mathscr{E}_n(\mathbb{A},G)[\chi]$. Since u is a sum of monomials, we can again assume that u is a monomial. Then by Lemma (8), we write $u = X_{j_1}^{\chi_0^{i_1}} \dots X_{j_n}^{\chi_0^{i_n}}$, with $i_1 + \dots + i_n = kq + \psi_{\chi_0}(\chi)$ for some k. Let us see which values can take k:

- if each $i_l = 1$, one obtains $kq + \psi_{\chi_0}(\chi) = n$, and so $k \geq \lceil \frac{n-\psi_{\chi_0}(\chi)}{q} \rceil$,
- if each $i_l = q$, one obtains $qn = kq + \psi_{\chi_0}(\chi)$, and so $k \leq \lfloor \frac{qn-\psi_{\chi_0}(\chi)}{q} \rfloor$.

In any case:

$$\lceil \frac{n-\psi_{\chi_0}(\chi)}{q} \rceil \leq k \leq \lfloor n - \psi_{\chi_0}(\chi)/q \rfloor.$$

□

Remark 14. *Proposition 22 was also given and proved by Anick: Proof of [5, Theorem 3].*

3.2.3 Some results on the series $\log(gocha_{\chi_0}(\mathbb{A},t))$

In this subpart, we obtain information on $(a_{\chi_0,n}(\mathbb{A}))_{n\in\mathbb{N}}$. For this purpose, we study the sequence $(b_{\chi_0,n}(\mathbb{A}))_{n\in\mathbb{N}}$ namely defined by:

$$\log(gocha_{\chi_0}(\mathbb{A},t)) := \sum_{n\in\mathbb{N}} b_{\chi_0,n}t^n.$$

Theorem 16. *The following equality holds in $\mathbb{N}[[t]]$:*

$$gocha_{\chi_0}(\mathbb{A},t) = \prod_n P(\mathbb{A},t^n)^{a_{\chi_0,n}},$$
$$\text{where} \quad P(\mathbb{F}_p,t) := \frac{1-t^p}{1-t}, \quad \text{and} \quad P(\mathbb{Z}_p,t) := \frac{1}{1-t}.$$

Proof. By Lemma 7, $\mathscr{E}_{\chi_0}(\mathbb{A},G)$ is a graded locally finite, $\mathbb{A}$-universal Lie algebra of $\mathscr{L}_{\chi_0}(\mathbb{A},G)$. [113, Corollary 2.2] allows us to conclude the case $\mathbb{A} := \mathbb{F}_p$, and [62, Proposition 2.5] allows us to conclude the case $\mathbb{A} := \mathbb{Z}_p$. □

Corollary 10. *Let us write $n = mp^k$, with $(m,p) = 1$, then:*

$$a_{\chi_0,n}(\mathbb{F}_p) = \sum_{r=1}^{k} w_{\chi_0,mp^r}(\mathbb{F}_p), \quad \text{and} \quad a_{\chi_0,n}(\mathbb{Z}_p) = w_{\chi_0,n}(\mathbb{Z}_p);$$
$$\text{where} \quad w_{\chi_0,n} := \frac{1}{n}\sum_{m|n} \mu(n/m) b_{\chi_0,m}.$$

Proof. This proof is similar to the proof of [92, Theorem 2.9]. □

Corollary 11. *The following assertions hold:*

(i) If χ is a non-trivial irreducible character, and there exists an infinite family of primes $q_i \equiv \psi_{\chi_0}(\chi) \pmod q$ such that

$$b_{\chi_0,q_i} > b_{\chi_0,1},$$

then $\mathscr{L}(\mathbb{A},G)[\chi]$ is infinite dimensional.

(ii) If there exists an infinite family of primes $(l_m)_m$ such that:

$$b_{\chi_0,ql_m} \geq q b_{\chi_0,q} + l_m b_{\chi_0,l_m},$$

then $\mathscr{L}(\mathbb{A},G)[\mathbb{1}]$ is infinite dimensional.

Proof. This is a consequence of Corollary 10. □

Theorem 17. *Assume there exist $\alpha > 1$ and a constant $C \neq 0$ such that $b_{\chi_0,n} \underset{n\to\infty}{\sim} C\alpha^n/n$. Then every eigenspace of $\mathscr{L}(\mathbb{A},G)$ is infinite dimensional.*

Proof. By Corollary 11, we have:

$$a_{\chi_0,q_i} = b_{\chi_0,q_i} - b_{\chi_0,1}/q_i, \quad \text{and}$$
$$a_{\chi_0,ql_m} = b_{\chi_0,ql_m} - qb_{\chi_0,q} - l_m b_{\chi_0,l_m}.$$

Since, $b_{\chi_0,n} \underset{n\to\infty}{\sim} C\alpha^n/n$, we can find families of primes $\{q_i\}_i$ and $\{l_m\}_m$ where q_i and l_m are sufficiently big, such that: $a_{\chi_0,q_i} > 0$, and $a_{\chi_0,ql_m} > 0$. Therefore by inequalities (3.6), we extract an infinite subsequence of $(a_n^\chi)_n$ which is strictly positive. □

3.3 Examples

Recall that $1 \to R \to F \to G \to 1$ denotes a minimal presentation of G, and by [39, Lemma 2.15], the group Δ lifts to a subgroup of $Aut(F)$. Keep in mind that $\mathscr{L}(\mathbb{A}, G)$ and $\mathscr{L}_{\chi_0}(\mathbb{A}, G)$ are assumed to be torsion-free over $\mathbb{A}$. Additionally here, G is assumed finitely presented and mild.

Consider the following $\mathbb{A}[\Delta]$-modules:

$$R(\mathbb{F}_p) := R/R^p[R;F], \quad \text{and} \quad R(\mathbb{Z}_p) := R/[R;F].$$

Choose χ_0 a non-trivial element of $\mathrm{Irr}(\Delta)$. For every $\chi \in \mathrm{Irr}(\Delta)$, we fix $\{l_j^\chi\}_{1\le j\le r^\chi}$, where $r^\chi := \mathrm{rank}_{\mathbb{A}} R(\mathbb{A})$, a lifting in F of a basis of $R(\mathbb{A})[\chi]$. By [120, Corollaire 3, Proposition 42, Chapitre 14], these liftings do not depend on $\mathbb{A}$.

Recall that we defined, using the Magnus isomorphism $\phi_{\mathbb{A}}$ given by (1), the filtered algebras $E(\mathbb{A}, G)$ (in Notations) and $E_{\chi_0}(\mathbb{A}, G)$ (in Subpart 3.2.1).
Name n_j^χ (resp. $n_{\chi_0,j}^\chi$) the least integer n such that $\phi_{\mathbb{A}}(l_j^\chi - 1)$ is in $E_n(\mathbb{A}) \setminus E_{n+1}(\mathbb{A})$ (resp. $E_{\chi_0,n}(\mathbb{A}) \setminus E_{\chi_0,n+1}(\mathbb{A})$): this is the degree of l_j^χ in $E(\mathbb{A})$ (resp. $E_{\chi_0}(\mathbb{A})$). We show in Lemma 9 that these degrees do not depend on $\mathbb{A}$. Set the series:

$$\chi_{eul}(\mathbb{A}, t) := 1 - dt + \sum_{\chi;1\le j\le r^\chi} t^{n_j^\chi},$$
$$\chi^*_{eul}(\mathbb{A}, t) := 1 - \sum_{\chi} d^\chi \chi.t + \sum_{\chi;1\le j\le r^\chi} \chi.t^{n_j^\chi},$$
$$\chi_{eul,\chi_0}(\mathbb{A}, t) := 1 - \sum_{\chi} d^\chi t^{\psi_{\chi_0}(\chi)} + \sum_{\chi;1\le j\le r^\chi} t^{n_{\chi_0,j}^\chi}.$$

Definition 27 (χ_0-mild)**.** *We say that a group G is χ_0-mild if:*

- *the previous presentation introduced above is mild for both the χ_0-filtration and the Zassenhaus filtration,*
- *the module $\mathscr{I}(\mathbb{Z}_p, R)/\mathscr{E}_{\ge 1}(\mathbb{Z}_p, F)\mathscr{I}(\mathbb{Z}_p, R)$ is a free $\mathscr{E}(\mathbb{Z}_p, G)$-module, with $\mathscr{E}_{\ge 1}(\mathbb{Z}_p, G)$ the augmentation ideal of $\mathscr{E}(\mathbb{Z}_p, G)$,*

- *the module* $\mathscr{I}_{\chi_0}(\mathbb{Z}_p,R)/\mathscr{E}_{\chi_0,\geq 1}(\mathbb{Z}_p,F)\mathscr{I}_{\chi_0}(\mathbb{Z}_p,R)$ *is a free* $\mathscr{E}_{\chi_0}(\mathbb{Z}_p,G)$*-module, with* $\mathscr{E}_{\chi_0,\geq 1}(\mathbb{Z}_p,G)$ *the augmentation ideal of* $\mathscr{E}_{\chi_0}(\mathbb{Z}_p,G)$*,*
- *we have* $\mathscr{I}(\mathbb{Z}_p,R)=\mathscr{I}(\mathbb{Z}_p,\rho)$ *and* $\mathscr{I}_{\chi_0}(\mathbb{Z}_p,R)=\mathscr{I}_{\chi_0}(\mathbb{Z}_p,\rho)$*, where* ρ_j *is the image of* $\phi_{\mathbb{A}}(l_j-1)$ *in* $E_{n_j}(\mathbb{A})/E_{n_j+1}(\mathbb{A})$*.*

3.3.1 Generalities

We give some generalities on groups with a χ_0-mild presentation.

Computation of some *gocha* series

Let us first recall the Lyndon's resolution, which allows us to compute *gocha* series as inverses of polynomials of the form χ_{eul}. A general reference is the article of Brumer [14].

Theorem 18. *We have the following exact sequence of filtered* $E(\mathbb{A},G)$*-modules:*

$$0\to\prod_{\chi;1\leq j\leq r^\chi}(\phi_{\mathbb{A}}(l_j^\chi-1))E(\mathbb{A},G)\to\prod_{\chi;1\leq j\leq d^\chi}(\phi_{\mathbb{A}}(x_j^\chi-1))E(\mathbb{A},G)\to E(\mathbb{A},G)\to\mathbb{A}\to 0.$$

We have the following exact sequence of filtered $E_{\chi_0}(\mathbb{A},G)$*-modules:*

$$0\to\prod_{\chi;1\leq j\leq r^\chi}(\phi_{\mathbb{A}}(l_j^\chi-1))E_{\chi_0}(\mathbb{A},G)\to\bigoplus_{\chi;1\leq j\leq d^\chi}(\phi_{\mathbb{A}}(x_j^\chi-1))E_{\chi_0}(\mathbb{A},G)\to E_{\chi_0}(\mathbb{A},G)\to\mathbb{A}\to 0.$$

Proof. To simplify notations, we write $X_i^\chi:=\phi_{\mathbb{A}}(x_j^\chi-1)$ and $w_j^\chi:=\phi_{\mathbb{A}}(l_j^\chi-1)$. One denotes by ρ_j^χ (resp. $\rho_{\chi_0,j}^\chi$) the image of $\phi_{\mathbb{A}}(l_j^\chi-1)$ in $\mathscr{E}_{n_j^\chi}(\mathbb{A})$ (resp. $\mathscr{E}_{n_{\chi_0,j}^\chi}(\mathbb{A})$).

We have the resolutions of $\mathscr{E}(\mathbb{A},G)$-modules and $\mathscr{E}_{\chi_0}(\mathbb{A},G)$-modules:

$$0\to\bigoplus_{j,\chi}\rho_j^\chi\mathscr{E}(\mathbb{A},G)\to\bigoplus_{i,\chi}X_i^\chi\mathscr{E}(\mathbb{A},G)\to\mathscr{E}(\mathbb{A},G)\to\mathbb{A}\to 0,$$

and

$$0\to\bigoplus_{\chi,j}\rho_{\chi_0,j}\mathscr{E}_{\chi_0}(\mathbb{A},G)\to\bigoplus_{\chi,i}X_i^\chi\mathscr{E}_{\chi_0}(\mathbb{A},G)\to\mathscr{E}_{\chi_0}(\mathbb{A},G)\to\mathbb{A}\to 0.$$

From Serre's Lemma [69, Chapitre 5, Lemme (2.1.1)], we can lift the previous resolutions to infer:

$$0\to\prod_{\chi,j}w_j^\chi E(\mathbb{F}_p,G)\to\prod_{\chi,i}X_i^\chi E(\mathbb{F}_p,G)\to E(\mathbb{F}_p,G)\to\mathbb{F}_p\to 0,$$

and

$$0\to\prod_{\chi,j}w_j^\chi E_{\chi_0}(\mathbb{A},G)\to\prod_{\chi,i}X_i^\chi E_{\chi_0}(\mathbb{A},G)\to E_{\chi_0}(\mathbb{A},G)\to\mathbb{A}\to 0.$$

□

Let us now compute *gocha* series:

Proposition 23. *Assume that G is χ_0-mild, then:*

(i) $gocha(\mathbb{A},t)=\frac{1}{\chi_{eul}(\mathbb{A},t)}$

(ii) $gocha^*(\mathbb{A},t)=\frac{1}{\chi^*_{eul}(\mathbb{A},t)}$

(iii) $gocha_{\chi_0}(\mathbb{A},t)=\frac{1}{\chi_{eul,\chi_0}(\mathbb{A},t)}$.

Proof. One denotes by ρ_j^χ (resp. $\rho_{\chi_0,j}^\chi$) the image of $\phi_{\mathbb{A}}(l_j^\chi-1)$ in $\mathscr{E}_{n_j^\chi}(\mathbb{A})$ (resp. $\mathscr{E}_{n_{\chi_0,j}^\chi}(\mathbb{A})$).

By Theorem 18, we have the following exact sequences of graded locally finite modules:

$$0 \to \bigoplus_{\chi;j} \rho_j^\chi \mathscr{E}(\mathbb{A},G) \to \bigoplus_{\chi;j} X_j^\chi \mathscr{E}(\mathbb{A},G) \to \mathscr{E}(\mathbb{A},G) \to \mathbb{A} \to 0, \quad (\star)$$

$$0 \to \bigoplus_{\chi;j} \rho_{\chi_0,j}^\chi \mathscr{E}_{\chi_0}(\mathbb{A},G) \to \bigoplus_{\chi;j} X_j^\chi \mathscr{E}_{\chi_0}(\mathbb{A},G) \to \mathscr{E}_{\chi_0}(\mathbb{A},G) \to \mathbb{A} \to 0. \quad (\star\star)$$

From Theorem 18 and sequence $(\star)$, we infer:

$$gocha(\mathbb{A},t)=\frac{1}{\chi_{eul}(\mathbb{A},t)}.$$

Moreover Theorem 18 and sequence $(\star\star)$ give us:

$$gocha_{\chi_0}(\mathbb{A},t)=\frac{1}{\chi_{eul,\chi_0}(\mathbb{A},t)}.$$

From the choice of the families $\{x_j^\chi\}$ and $\{\rho_j^\chi\}$, we infer that the sequence $(\star)$ is exact in the category of graded locally finite $\mathbb{A}[\Delta]$-modules. This allows us to conclude:

$$gocha^*(\mathbb{A},t)=\frac{1}{\chi^*_{eul}(\mathbb{A},t)}.$$

□

Answer to [92, Question 2.13**]**

Extending and reformulating [92, Question 2.13] in our equivariant context, when G is χ_0-mild, we show in this Subsubpart that:

> *The series $gocha(\mathbb{A},t)$, $gocha^*(\mathbb{A},t)$ and $gocha_{\chi_0}(\mathbb{A},t)$ do not depend on the ring $\mathbb{A}$?*

Lemma 9. *Assume that $\mathscr{L}(\mathbb{Z}_p, G)$ is torsion-free. Then, for every j and every χ, the integers $n_j^\chi(\mathbb{A})$ do not depend on $\mathbb{A}$. Similarly, if $\mathscr{L}_{\chi_0}(\mathbb{Z}_p, G)$ is torsion-free, then the integers $n_{\chi_0,j}^\chi(\mathbb{A})$ do not depend on $\mathbb{A}$*

Proof. Let us prove that n_j^χ does not depend on $\mathbb{A}$. Recall that $n_j^\chi(\mathbb{F}_p)$ (resp. $n_j^\chi(\mathbb{Z}_p)$) is the degree of l_j^χ in $E(\mathbb{F}_p)$ (resp. $E(\mathbb{Z}_p)$), and $\rho_j^\chi(\mathbb{F}_p)$ (resp. $\rho_j^\chi(\mathbb{Z}_p)$) denotes the image of $\phi_{\mathbb{F}_p}(l_j^\chi - 1)$ in $\mathscr{E}_{n_j^\chi}(\mathbb{F}_p)$ (resp. $\phi_{\mathbb{Z}_p}(l_j^\chi - 1)$ in $\mathscr{E}_{n_j^\chi}(\mathbb{Z}_p)$). Notice that we have a filtered surjection:

$$E(\mathbb{Z}_p) \overset{(\mathrm{mod}\ p)}{\to} E(\mathbb{F}_p), \quad \text{with kernel} \quad pE(\mathbb{Z}_p).$$

Since the choice of the family $\{l_j^\chi\}_{j,\chi}$ does not depend on $\mathbb{A}$, we infer that $\phi_{\mathbb{Z}_p}(l_j^\chi - 1) \equiv \phi_{\mathbb{F}_p}(l_j^\chi - 1) \pmod p$. Therefore, $n_j^\chi(\mathbb{Z}_p) \leq n_j^\chi(\mathbb{F}_p)$.

To show that $n_j^\chi(\mathbb{Z}_p) = n_j^\chi(\mathbb{F}_p)$, it is sufficient to show that for every integer j, and character χ, we have $\rho_j^\chi(\mathbb{Z}_p)$ not in $p\mathscr{E}(\mathbb{Z}_p)$.

From [29, Proposition 4.3], we infer the following isomorphism of $E(\mathbb{Z}_p, G)$-modules:

$$K(\mathbb{Z}_p) := R/[R;R] \simeq I(\mathbb{Z}_p, R)/E_1(\mathbb{Z}_p)I(\mathbb{Z}_p, R).$$

Since, G is of cohomological dimension 2, by [59, Theorem 7.7], we have

$$K(\mathbb{Z}_p) \simeq \prod_{j,\chi} \phi_{\mathbb{Z}_p}(l_j^\chi - 1)E(\mathbb{Z}_p, G).$$

Introduce

$$\mathscr{I}_n(\mathbb{Z}_p, R) := I_n(\mathbb{Z}_p, R)/I_{n+1}(\mathbb{Z}_p, R), \quad \text{and} \quad \mathscr{I}(\mathbb{Z}_p, R) := \bigoplus_{n\in\mathbb{N}} \mathscr{I}_n(\mathbb{Z}_p, R).$$

Since G is χ_0-mild, we infer

$$\mathrm{Grad}(K(\mathbb{Z}_p)) \simeq \bigoplus_{j,\chi} \rho_j^\chi(\mathbb{Z}_p)\mathscr{E}(\mathbb{Z}_p, G) \simeq \mathscr{I}(\mathbb{Z}_p, R)/\mathscr{E}_1(\mathbb{Z}_p)\mathscr{I}(\mathbb{Z}_p, R).$$

Assume now, by contradiction, that there exists one integer j_0 and one character χ_0 such that $\rho_{j_0}^{\chi_0}(\mathbb{Z}_p)$ is in $p\mathscr{E}(\mathbb{Z}_p)$, then there exists $u \in \mathscr{E}(\mathbb{Z}_p)$ such that $\rho_{j_0}^{\chi_0} := pu$. Moreover, since $\mathscr{E}(\mathbb{Z}_p, G)$ is torsion-free, we deduce that u is in $\mathscr{I}(\mathbb{Z}_p, R)$. Therefore, there exist elements g_j^χ in $\mathscr{E}(\mathbb{Z}_p, G)$ such that $u \equiv \sum_{j,\chi} g_j^\chi \rho_j^\chi \pmod{\mathscr{E}_1(\mathbb{Z}_p)\mathscr{I}(\mathbb{Z}_p, R)}$. Consequently:

$$\rho_{j_0}^{\chi_0} := pu \equiv \sum_{j,\chi} pg_j^\chi \rho_j^\chi \pmod{\mathscr{E}_1(\mathbb{Z}_p)\mathscr{I}(\mathbb{Z}_p, R)}.$$

Since the family ρ_j^χ is a basis of the free $\mathscr{E}(\mathbb{Z}_p, G)$-module $\mathscr{I}(\mathbb{Z}_p, R)/\mathscr{E}_1(\mathbb{Z}_p)\mathscr{I}(\mathbb{Z}_p, R)$, we infer $pg_{j_0}^{\chi_0} = 1$. This is impossible since p is not invertible in $\mathscr{E}(\mathbb{Z}_p, G)$.

□

Theorem 19. *Assume that $\mathscr{L}(\mathbb{Z}_p, G)$ is torsion-free, then :*

$$gocha(\mathbb{Z}_p, t) = gocha(\mathbb{F}_p, t), \quad and \quad gocha^*(\mathbb{Z}_p, t) = gocha^*(\mathbb{F}_p, t).$$

Furthermore, if $\mathscr{L}_{\chi_0}(\mathbb{Z}_p, G)$ is torsion-free, then

$$gocha_{\chi_0}(\mathbb{Z}_p, t) = gocha_{\chi_0}(\mathbb{F}_p, t).$$

Proof. We apply Proposition 23 and Lemma 9. □

Remark 15. *Let us remove the hypothesis that $Aut(G)$ contains a subgroup Δ of order q. If we assume that*

- *the group G has a mild presentation for the Zassenhaus filtration,*
- *the module $\mathscr{I}(\mathbb{Z}_p, R)/\mathscr{E}_{\geq 1}(\mathbb{Z}_p, F)\mathscr{I}(\mathbb{Z}_p, R)$ is a free $\mathscr{E}(\mathbb{Z}_p, G)$-module, with $\mathscr{E}_{\geq 1}(\mathbb{Z}_p, G)$ the augmentation ideal of $\mathscr{E}(\mathbb{Z}_p, G)$,*
- *$\mathscr{I}(\mathbb{Z}_p, R) = \mathscr{I}(\mathbb{Z}_p, \rho)$.*

Then we have a postive answer to [92, Question 2.13], i.e.

$$gocha(\mathbb{Z}_p, t) = gocha(\mathbb{F}_p, t).$$

Mild groups were originally introduced by [62] when p is odd, and by [66] when $p = 2$.

Gocha's series and eigenvalues

Thanks to Proposition 23, we can compute *gocha* series. Then applying Formulae (3.2) and (3.3), we obtain an explicit equation relating coefficients a_n and a_n^χ. However, the computation of b_n has complexity n (more precisely it depends on $\{c_m\}_{m \leq n}$).

If we consider roots of χ_{eul}, we infer a formula for b_n which depends on the arithmetic complexity of n. The following results are mostly adapted in our context from ideas of Labute ([63, Formula (1)]) and Weigel ([137, Theorem D]).

Let $\deg(G)$ be the degree of χ_{eul}, and λ_i the eigenvalues of G, written as:

$$\chi_{eul}(t) := \prod_{i=1}^{\deg(G)} (1 - \lambda_i t).$$

One denotes by M_n the necklace polynomial of degree n:

$$M_n(t) := \sum_{m|n} \mu(n/m) \frac{t^m}{n}.$$

Let us state [137, Theorem D]:

Theorem 20. *Assume $(n,q)=1$ and write $n=mp^k$, with $(m,p)=1$. Then we infer:*

$$a_n(\mathbb{Z}_p)=\sum_{i=1}^{n} M_n(\lambda_i), \quad a_n(\mathbb{F}_p)=\sum_{i=1}^{n}\sum_{j=0}^{k} M_{mp^j}(\lambda_i).$$

Proof. Weigel showed in the proof of [137, Theorem 3.4], that:

$$\sum_{i=1}^{n} M_n(\lambda_i)=w_n.$$

Then we conclude using Theorem 19 and Formula (3.2). □

Let us adapt this result in an equivariant context. By a choice of a primitive q-th root of unity, we have $\mathbb{F}_q\subset\mathbb{F}_p^{\times}\subset\overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$. Consider δ a non-trivial element in Δ, and evaluate χ^*_{eul} in δ by:

$$\chi^*_{eul}(\delta)(t):=1-\sum_{\chi} c_1^{\chi}\chi(\delta)t+\sum_{\chi;1\leq j\leq r^{\chi}}\chi(\delta)t^{n_j^{\chi}}\in\mathbb{F}_p[t]\subset\overline{\mathbb{F}_p}[t].$$

Define $\{\lambda_{\delta,j}\}_{1\leq j\leq \deg(G)}\subset\overline{\mathbb{F}_p}$ the eigenvalues of $\chi^*_{eul}(\delta)(t)$. We introduce $\mathscr{F}(\Delta,\overline{\mathbb{F}_p})$ the $\overline{\mathbb{F}_p}$-algebra of functions from Δ to $\overline{\mathbb{F}_p}$ and:

$$\eta_j\colon\Delta\to\overline{\mathbb{F}_p};\quad \delta\mapsto\lambda_{\delta,j}.$$

Therefore, we infer:

$$\chi^*_{eul}(t):=\prod_{j=1}^{\deg(G)}(1-\eta_j t)\in\mathscr{F}(\Delta,\overline{\mathbb{F}_p})[t].$$

Consequenlty, if we apply the log function to the previous equality, we obtain:

$$b^*_m:=\sum_{\chi\in\mathrm{Irr}(\Delta)} b_m^{\chi}\chi=\frac{\eta_1^m+\cdots+\eta_{\deg(G)}^m}{m}.$$

Let us define for every $\eta\in\mathscr{F}(\Delta,\overline{\mathbb{F}_p})$:

$$M_n^*(\eta):=\sum_{m|n}\frac{1}{n}\mu(n/m)\eta^{m,(n/m)},\quad \text{where}\quad \eta^{m,(u)}(\delta)=\eta(\delta^u)^m.$$

Proposition 24. *Let us assume q divides $p-1$ and $(n,q)=1$. Write $n=mp^k$, with $(m,p)=1$, then:*

$$a_n(\mathbb{Z}_p)^*:=\sum_{\chi} a_n^{\chi}(\mathbb{Z}_p)\chi=\sum_{j=1}^{\deg(G)} M_n^*(\eta_j),\quad \textit{and}$$

$$a_n(\mathbb{F}_p)^*:=\sum_{\chi} a_n^{\chi}(\mathbb{F}_p)\chi=\sum_{j=1}^{\deg(G)}\sum_{i=0}^{k} M^*_{mp^i}(\eta_j),$$

the equality is in the $\overline{\mathbb{F}_p}$-algebra $\mathscr{F}(\Delta,\overline{\mathbb{F}_p})$.

Proof. Let us remind that $b_n^* := \sum_\chi b_n^\chi \chi$. After making the following change of variable: $\gamma = \chi^{n/m}$, we observe that for every δ in Δ, we have

$$b_m^{*1,(n/m)}(\delta) := b_m^*(\delta^{n/m}) = \sum_\chi b_m^\chi \chi(\delta^{n/m}) = \sum_{\chi \in \mathrm{Irr}(\Delta)} b_m^\chi \chi(\delta)^{n/m} = \sum_{\gamma \in \mathrm{Irr}(\Delta)} b_m^{\gamma^{m/n}} \gamma(\delta).$$

Consequently, $b_m^{*1,(n/m)} = \sum_\chi b_m^{\chi^{m/n}} \chi$. Since $m b_m^* = \eta_1^m + \cdots + \eta_{\deg(G)}^m$, we obtain:

$$m b_m^{*1,(m/n)} = \left(\eta_1^m + \cdots + \eta_{\deg(G)}^m\right)^{(n/m)} = \eta_1^{m,(n/m)} + \cdots + \eta_{\deg(G)}^{m,(n/m)}.$$

Using Formula (3.3), the conclusion follows. □

Remark 16. *Filip ([28, Formula* (4.8)*]) and Stix ([124, Formula* (14.16)*]) also obtained Proposition 24 for some groups defined by one quadratic relation. They computed explicitely the functions η_j.*

Example 17. *Let us illustrate Proposition 24, with Example 1.*

When splitting χ_{eul}^* into eigenvalues, we obtain:

$$\chi_{eul}^*(t) = (1-\eta_1 t)(1-\eta_2 t) = 1 - (\chi_0 + \chi_0^2 + \chi_0^3)t + \chi_0^3 t^3,$$

Moreover, $\eta_1\eta_2 = \chi_0^3$ and $\eta_1 + \eta_2 = \chi_0 + \chi_0^2 + \chi_0^3$ (as functions). Therefore, if we apply Proposition 24, we get:

$$a_2^* := \sum_\chi a_2^\chi = \frac{\eta_1^2 + \eta_2^2 - \eta_1^{(2)} - \eta_2^{(2)}}{2} = \frac{(\eta_1+\eta_2)^2 - 2\eta_1\eta_2 - (\eta_1+\eta_2)^{(2)}}{2}$$
$$= \frac{\chi_0^2 + \chi_0^4 + \chi_0^6 + 2\chi_0^3 + 2\chi_0^4 + 2\chi_0^5 - 2\chi_0^3 - \chi_0^2 - \chi_0^4 - \chi_0^6}{2} = \chi_0^4 + \chi_0^5.$$

Let us now compute a_3^χ. For this purpose, we first observe that

$$\eta_1^3 + \eta_2^3 = (\chi_0 + \chi_0^2 + \chi_0^3)^3 - 3(\chi_0 + \chi_0^2 + \chi_0^3)\chi_0^3$$
$$= \chi_0^9 + 3\chi_0^8 + 6\chi_0^7 + 4\chi_0^6 + 3\chi_0^5 + \chi_0^3.$$

Therefore, we have:

$$a_3^* := \sum_\chi a_3^\chi = \frac{\eta_1^3 + \eta_2^3 - \eta_1^{(3)} - \eta_2^{(3)}}{3} = \frac{\eta_1^3 + \eta_2^3 - (\eta_1+\eta_2)^{(3)}}{3} = \chi_0^5 + \chi_0^6 + 2\chi_0^7 + \chi_0^8.$$

Let us conclude this subpart by proving Theorem C given in our introduction.

Theorem 21. *Assume that $\mathscr{L}(\mathbb{A}, G)$ is infinite dimensional and for some χ_0 that $L_{\chi_0}(G)$ is reached for a unique eigenvalue λ_{χ_0} such that:*

(i) λ_{χ_0} is real,

(ii) $L_{\chi_0}(G) = \lambda_{\chi_0} > 1$.

Then every eigenspace of $\mathscr{L}(\mathbb{A}, G)$ is infinite dimensional.

Proof. We study the asymptotic behaviour of $(b_{\chi_0,n})_{n\in\mathbb{N}}$. By Proposition 23, we have:

$$gocha_{\chi_0}(t) := \frac{1}{\chi_{eul,\chi_0}(t)}.$$

Let us denote by $\{\lambda_1; \ldots; \lambda_u\}$ the real χ_0-eigenvalues of G and $\{\beta_1 e^{i\pm\theta_1}; \ldots; \beta_v e^{i\pm\theta_v}\}$ the polar forms of non real χ_0-eigenvalues of G. Without loss of generality, assume that $\lambda_{\chi_0} := \lambda_1$. Let us write

$$\chi_{eul,\chi_0}(t) := \prod_{i=1}^{u}(1-\lambda_i t)\prod_{j=1}^{v}(1-\beta_j e^{i\theta_j}t)(1-\beta_j e^{-i\theta_j}t).$$

Then, we obtain:

$$\log(\chi_{eul,\chi_0}(t)) = \sum_{n\in\mathbb{N}} \frac{\sum_{i=1}^{u}\lambda_i^n + \sum_{j=1}^{v}\beta_j^n(e^{in\theta_j}+e^{-in\theta_j})}{n}t^n.$$

Thus $b_{\chi_0,n} \underset{n\to\infty}{\sim} C\lambda_1^n/n$, for some $C > 0$. We conclude by Theorem 17. □

3.3.2 Group Theoretical examples

Free pro-p groups

In this subpart, assume that G is a free finitely generated pro-p group. Observe that $\mathscr{L}(\mathbb{Z}_p, G)$ and $\mathscr{L}_{\chi_0}(\mathbb{Z}_p, G)$ are torsion-free.

Theorem 22. *Assume that G is a noncommutative free pro-p group, then every eigenspace of $\mathscr{L}(\mathbb{A}, G)$ is infinite dimensional.*

Proof. Let us fix a non-trivial character $\chi_0 \in \mathrm{Irr}(\Delta)$, such that $d^{\chi_0} \leq d^{\chi}$ for every non-trivial χ. Then we have $\chi_{eul,\chi_0}(t) := 1 - \sum_{i=1}^{q} d^{\chi_0^i}t^i$. Set s a minimal positive real root of χ_{eul,χ_0}. We will show that s is the unique root of minimal absolute value of χ_{eul,χ_0}.

We have:

$$0 = 1 - \sum_{i=1}^{q} d^{\chi_0^i}s^i \leq 1 - d^{\chi_0}s\sum_{i=0}^{q-2}s^i - d^{\mathbb{1}}s^q \leq 1 - d^{\chi_0}s - d^{\mathbb{1}}s^q.$$

Then $d^{\chi_0}s + d^{\mathbb{1}}s^q \leq 1$. Thus $s \leq \min\{1/d^{\chi_0}; (1/d^{\mathbb{1}})^{1/q}\}$, so $0 < s < 1$.

If we denote by z a complex root (not in $]0;1[$) of χ_{eul,χ_0}, then we notice by the triangle inequality, that $\chi_{eul,\chi_0}(|z|) < \chi_{eul,\chi_0}(z) = 0$. Therefore $|z| > s$.

Consequently, χ_{eul,χ_0} admits a unique root s of minimal absolute value which is in $]0;1[$. Therefore, by Theorem C, we conclude. □

Let us give some examples.

Example 18. *Consider $\Delta := \mathbb{Z}/2\mathbb{Z}$, and fix χ_0 the non-trivial irreducible character of Δ over $\mathbb{A}$. Assume that G is a free pro-p group with two generators $\{x, y\}$, and Δ acts on G by: $\delta(x) = x$, $\delta(y) = y^{-1}$. Then following our notations, we have: $x = x^{\mathbb{1}}$, and $y = x^{\chi_0}$. Observe that $Al(\mathbb{A}, G)$ is a free algebra on two variables over $\mathbb{A}$.*
Let us first compute some coefficients a_n^{χ}, with Formula (3.3). We have:

$$gocha^*(\mathbb{A}, t) := \frac{1}{1-(1+\chi_0).t}, \quad \text{and} \quad \log(gocha^*(\mathbb{A}, t)) := \sum_n \frac{(1+\chi_0)^n}{n} t^n.$$

So

$$c_{2n}^{\mathbb{1}} = c_{2n}^{\chi_0} = 2^{2n-1}, \quad c_{2n+1}^{\chi_0} = c_{2n+1}^{\mathbb{1}} = 2^{2n},$$
$$b_{2n+1}^{\chi_0} = b_{2n+1}^{\chi_0} = \frac{2^{2n}}{2n+1}, \quad \text{and} \quad b_{2n}^{\mathbb{1}} = b_{2n}^{\chi_0} = \frac{2^{2n-1}}{2n}.$$

Assume for instance $p \neq 3$, then one obtains:

$$a_3^{\chi_0} = \frac{2^2-1}{3} = 1, \quad \text{and} \quad a_3^{\mathbb{1}} = 1.$$

Observe by Theorem 22, that every eigenspace of $\mathscr{L}(\mathbb{A}, G)$ is infinite.

Example 19. *Again, take $\Delta := \mathbb{Z}/2\mathbb{Z}$ and χ_0 the unique non-trivial $\mathbb{A}$-irreducible character of Δ. Assume G is free generated by $\{x_1^{\chi_0}; \ldots; x_d^{\chi_0}\}$.*

First, we compute some coefficients of $(c_n^{\chi})_n$ and $(a_n^{\chi})_n$. Observe:

$$gocha^*(\mathbb{A}, t) := \frac{1}{1-d\chi_0 t}, \quad \text{and} \quad gocha_{\chi_0}(\mathbb{A}, t) := \frac{1}{1-dt}.$$

Then $c_{2n}^{\mathbb{1}} = d^{2n}$, $c_{2n}^{\chi_0} = 0$, $c_{2n+1}^{\chi_0} = d^{2n+1}$, and $c_{2n+1}^{\mathbb{1}} = 0$.
Moreover,

$$\log(gocha^*(\mathbb{A}, t)) := \sum_n \frac{(d\chi_0)^n}{n} t^n, \quad \log(gocha_{\chi_0}(\mathbb{A}, t)) := \sum_{n\in\mathbb{N}} \frac{d^n}{n} t^n.$$

So, $b_{2n+1}^{\chi_0} := d^{2n+1}/(2n+1)$, $b_{2n}^{\chi_0} = 0$, $b_{2n}^{\mathbb{1}} = d^{2n}/(2n)$, and $b_{2n+1}^{\mathbb{1}} = 0$.
For instance, if we apply Formula (3.3), one obtains when $p \neq 3$:

$$a_3^{\chi_0} = \frac{d^3-d}{3}, \text{ and } a_3^{\mathbb{1}} = 0.$$

If we apply Proposition 24, we obtain:

$$a_2^{\chi_0} = 0, \quad \text{and} \quad a_2^{\mathbb{1}} = \frac{d^2-d}{2}.$$

Observe that $c_{\chi_0,n} = d^n$ and $b_{\chi_0,n} := d^n/n$. Theorem 22, allows us to check that every eigenspace of $\mathscr{L}(\mathbb{A}, G)$ is indeed infinite dimensional.

Non-free case

Let us now construct some non-free examples that illustrate Theorem C. For this purpose, consider Δ a subgroup of $Aut(F)$. We construct here a finitely presented pro-p quotient G of F, such that Δ induces a subgroup of $Aut(G)$.

We remind that F is the free pro-p group generated by $\{x_j^\chi\}_{\chi\in \mathrm{Irr}(\Delta);1\leq j\leq d^\chi}$ and define $\mathscr{F}$ the free abstract group generated by the family $\{x_j^\chi\}_{\chi;j}$. Assume also that the action of Δ is diagonal over $\{x_j^\chi\}$, i.e. for all δ in Δ, $\delta(x_j^\chi) = (x_j^\chi)^{\chi(\delta)}$.

Definition 28 (Comm-family)**.** *The family $(l_j)_{j\in[\![1;r]\!]} \subset \mathscr{F}$ is said to be a comm-family if:*

$$l_j := \prod_{l=1}^{\eta_j} u_{j,\gamma_l}^{\alpha_{j,\gamma_l}} \in F,$$

where γ_l and α_{j,γ_l} are integers, and u_{j,γ_l} is a γ_l-th commutator on $\{x_j^\chi\}_{\chi;j}$, i.e. $u_{j,\gamma_l} := [x_1;\dots;x_{\gamma_l}]$ where $x_i \in \{x_j^\chi\}_{\chi;j}$.

Proposition 25. *Let $(l_j)_{j\in[\![1;r]\!]}$ be a comm-family, and denote by R its normal (topological) closure in F. Then for all δ in Δ, $\delta(R) = R$ thus Δ induces a subgroup of $Aut(F/R)$.*

Proof. First of all, if u and v are elements in F, we write $u^v := v^{-1}uv$.
Assume $[x;y] \in R$, where x and y are elements in $\{x_j^\chi\}_{\chi;j}$. Observe the following identity:

$$1 = [x;yy^{-1}] = [x;y^{-1}][x;y]^{y^{-1}}.$$

Therefore $[x;y^{-1}]$ is in R. Remark also for all integers a:

$$[x;y^a] = [x;y^{a-1}][x;y]^{y^{a-1}}.$$

Thus by induction, we see that for all $a \in \mathbb{Z}$, the commutator $[x;y^a]$ is in R.
Finally, for all integers b, we also have:

$$[x^b;y] = [x;y]^{x^{b-1}}[x^{b-1};y].$$

We conclude as before that $[x^b;y] \in R$, for all integers b.
Then $\delta(R) = R$, for every $\delta \in \Delta$. □

Example 20. *Here assume q is an odd prime that divides $p-1$. Take F a free pro-p group with three generators: $\{x_1^{\chi_0}, x_1^{\chi_0^2}, x_1^{\chi_0^3}\}$. Assume also that Δ acts diagonally on the previous set.*

Consider R the closed normal subgroup of F generated by commutators $l_1 := [x_1^{\chi_0}; x_1^{\chi_0^2}]$ and $l_2 := [x_1^{\chi_0}; x_1^{\chi_0^3}]$. By Proposition 25, the group Δ induces a subgroup of $Aut(G)$. Observe that G is χ_0-mild (see for instance [29]), so we have:

$$gocha_{\chi_0}(\mathbb{F}_p, t) = \frac{1}{\chi_{eul,\chi_0}(\mathbb{F}_p, t)} = \frac{1}{1-t-t^2+t^4}.$$

Thus by Theorem C, we conclude that every eigenspace of $\mathscr{L}(\mathbb{F}_p, G)$ is infinite dimensional.

3.3.3 FAB quadratic mild examples

Let K be a quadratic imaginary extension over $\mathbb{Q}$, with class number coprime to p. Denote by $S := \{\mathfrak{p}_1; \dots; \mathfrak{p}_d\}$ a finite set of tame places of K, i.e. for $\mathfrak{p} \in S$, $N_{K/\mathbb{Q}}(\mathfrak{p}) \equiv 1 \pmod{p}$, and assume that S is stable by Δ. We define K_S the p-maximal unramified extension of K outside S. Set $G := \mathrm{Gal}(K_S/K)$ and $\Delta := \mathrm{Gal}(K/\mathbb{Q})$. Again, fix χ_0 the non-trivial character of Δ over $\mathbb{F}_p$. The group Δ acts on G, and thanks to Class Field Theory, the group G has the FAB property: every open subgroup has finite abelianization.

Write $U_\mathfrak{p}$ for the unit group of the completion of K at the place $\mathfrak{p} \in S$. We define the element $X_\mathfrak{p} \in \mathscr{E}_1(\mathbb{F}_p, G)$ as the image, given by Class Field Theory, of a generator of $U_\mathfrak{p}/U_\mathfrak{p}^p$. Then (see for instance [115, Theorem 2.6]), the set $\{X_\mathfrak{p}\}_{\mathfrak{p}\in S}$ is a basis of $\mathscr{E}_1(\mathbb{F}_p, G)$.

Denote by $x_\mathfrak{p}$ an element in G that lifts $X_\mathfrak{p}$. We introduce F, the free pro-p group generated by $x_\mathfrak{p}$. Koch [59, Chapter 11] gave a presentation of G, with generators $\{x_\mathfrak{p}\}_{p\in S}$ and relations $\{l_\mathfrak{p}\}_{\mathfrak{p}\in S}$ verifying:

$$l_{\mathfrak{p}_i} \equiv \prod_{j\neq i} [x_{\mathfrak{p}_i}, x_{\mathfrak{p}_j}]^{a_j(i)} \pmod{F_3(\mathbb{F}_p)}, \quad \text{where} \quad a_j(i) \in \mathbb{Z}/p\mathbb{Z}.$$

The element $a_j(i)$ is zero if and only if the prime $\mathfrak{p}_i$ splits in $k^p_{\{\mathfrak{p}_j\}}/k$, where $k^p_{\{\mathfrak{p}\}}$ is the (unique) cyclic extension of degree p of k unramified outside $\mathfrak{p}$. This is equivalent to

$$p_i^{(p_j-1)/p} \equiv 1 \pmod{p_j},$$

where p_i is a prime in $\mathbb{Q}$ below $\mathfrak{p}_i$.

From now, we assume that this presentation is **mild and quadratic** (the relations are all of weight 2), which means that we have the following isomorphisms of $\mathbb{F}_p[\Delta]$-modules:

$$\mathscr{E}_1(\mathbb{F}_p) = \bigoplus_{i=1}^{d} X_{\mathfrak{p}_i}\mathbb{F}_p, \quad \text{and} \quad R(\mathbb{F}_p) \simeq \bigoplus_{i=1}^{d} \left(\sum_{j\neq i} a_j(i)[X_{\mathfrak{p}_j}; X_{\mathfrak{p}_i}] \right) \mathbb{F}_p.$$

Denote by i (resp. s), the number of inert or totally ramified (resp. totally split) primes below S in $\mathbb{Q}$, then $d = r = |S| := i + 2s$. Recall that for every χ:

$$d^\chi := \dim_{\mathbb{F}_p} \mathscr{E}_1(\mathbb{F}_p)[\chi], \quad \text{and} \quad r^\chi := \dim_{\mathbb{F}_p} R(\mathbb{F}_p)[\chi].$$

By [35, Theorem 1] and Class Field Theory, we obtain:

$$d^{\mathbb{1}} = i + s \quad (\text{resp. } r^{\mathbb{1}} = i + s) \quad \text{and} \quad d^{\chi_0} = s \quad (\text{resp. } r^{\chi_0} = s).$$

Proposition 26. *We have the following equalities of series:*

$$gocha^*(\mathbb{F}_p, t) := \frac{1}{1 - (i + s + s\chi_0)t + (i + s + s\chi_0)t^2},$$
$$gocha_{\chi_0}(\mathbb{F}_p, t) := \frac{1}{1 - st - it^2 + (s + i)t^4}.$$

Consequently, the action of Δ on G is not trivial if and only if at least one place above S in $\mathbb{Q}$ totally splits in K.

Proof. Here, the relations have all weight 2, so:

$$\chi^*_{eul}(t) := 1 - (d^{\mathbb{1}} + d^{\chi_0}\chi_0)t + (r^{\mathbb{1}} + r^{\chi_0}\chi_0)t^2 = 1 - (i + s + s\chi_0)t + (i + s + s\chi_0)t^2.$$

Since the presentation is mild, we conclude using Proposition 23. □

Remark 17. *Before giving examples, let us add some complements.*

- *The $\mathbb{F}_p[\Delta]$-module structure of $\mathscr{E}_1(\mathbb{F}_p)$ (or $R(\mathbb{F}_p)$) gives us the integers i and s.*
- *If every place $\mathfrak{p}$ above S is inert or totally ramified in K, then $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ and $G := \mathrm{Gal}(K_S/K)$ admit the same number of generators. Then Gras [35, Theorem 1], showed that $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ and G are isomorphic, so the action of Δ over G is trivial.*
- *Assume now that all places in $\mathbb{Q}$ below a set of primes S are totally split in K. If $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ is mild, Rougnant in [115, Théorème 0.3] gave a criterion to also obtain $\mathrm{Gal}(K_S/K)$ mild.*

Example 21. *We give explicit arithmetic examples where G is mild and defined by quadratic relations:*

1. *We study the following example given by [134, Example 3.2]: let $p = 3$, $K := \mathbb{Q}(i)$, and consider the set of primes: $S := \{q_1 := 229, q_2 := 241\}$. These primes totally split in K. and the places above S (in K) are given by:*

   $$S := \{\mathfrak{p}_1 := (2 + 15i), \overline{\mathfrak{p}_1} := (2 - 15i), \mathfrak{p}_2 := (4 + 15i), \overline{\mathfrak{p}_2} := (4 - 15i)\}.$$

   The group $G := \mathrm{Gal}(K_S/K)$ is mild quadratic. Then by Proposition 26:

   $$gocha^*(\mathbb{F}_p, t) = \frac{1}{1 - (2 + 2\chi_0)t + (2 + 2\chi_0)t^2}, \quad \text{and} \quad gocha_{\chi_0}(\mathbb{F}_p, t) = \frac{1}{1 - 2t + 2t^4}.$$

   However, the polynomial $1 - 2t + 2t^4$ admits only non real roots, so we can not apply Theorem C.

   Observe by [59, Example 11.15], that the group $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ is finite.

2. *[115, Part 6]: Take $p = 3$, $K := \mathbb{Q}(\sqrt{-5})$, and $S := \{61; 223; 229; 481\}$. The Class group of K is $\mathbb{Z}/2\mathbb{Z}$, the primes in S are totally split in K, and the groups $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ and $G := \mathrm{Gal}(K_S/K)$ are both mild quadratic. Therefore, by Proposition 26, we obtain:*

   $$gocha^*(\mathbb{F}_p, t) = \frac{1}{1 - (4 + 4\chi_0)t + 4\chi_0 t^2} \quad \text{and} \quad gocha_{\chi_0}(\mathbb{F}_p, t) = \frac{1}{1 - 4t + 4t^4}.$$

   By Theorem C, the graded spaces $\mathscr{L}(\mathbb{F}_p, G)[\chi_0]$ and $\mathscr{L}(\mathbb{F}_p, G)[\mathbb{1}]$ are both infinite dimensional.

3. *We enrich the example given in [45, Part 2.1]: Consider* $p = 3$, $K := \mathbb{Q}(\sqrt{-163})$, *and* $T := \{31, 19, 13, 337, 7\}$. *The class group of* K *is trivial,* $\mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$ *is mild, and the primes in* T *are inert in* K. *Therefore by [35, Theorem 1], the group* $\mathrm{Gal}(K_T/K)$ *is mild (in fact, it has the same linking coefficients as* $\mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$*).*

   Observe that 43 *is totally split in* K*, so we take* $\{\mathfrak{p}_6, \overline{\mathfrak{p}_6}\}$ *to be the primes in* K *above* 43. *Consider now* $S := T \cup \{\mathfrak{p}_6; \overline{\mathfrak{p}_6}\}$. *By [134, Corollary 4.3], the group* $G := \mathrm{Gal}(K_S/K)$ *is mild quadratic. Proposition 26 gives us*

$$gocha^*(\mathbb{F}_p, t) := \frac{1}{1-(6+\chi_0)t+(6+\chi_0)t^2}, \quad \textit{and} \quad gocha_{\chi_0}(\mathbb{F}_p, t) := \frac{1}{1-t-5t^2+6t^4}.$$

   Therefore, by Theorem C, the graded spaces $\mathscr{L}(\mathbb{F}_p, G)[\mathbb{1}]$ *and* $\mathscr{L}(\mathbb{F}_p, G)[\chi_0]$ *are infinite dimensional.*

Remark on lower p-central series and mild groups

Assume here that G is a finitely presented pro-p group, and q divides $p-1$. We define the lower p-central series of G by:

$$G_{\{1\}} := G, \quad \text{and} \quad G_{\{n+1\}} := G^p_{\{n\}}[G_{\{n\}}; G].$$

Remark that $\bigoplus_{n\in\mathbb{N}}(G_{\{n\}}/G_{\{n+1\}})$ is an $\mathbb{F}_p[t][\Delta]$-module, where $\mathbb{F}_p[t]$ is the ring of polynomials over $\mathbb{F}_p$.

Furthermore, if we assume G mild (see [62, Definition 1.1]), Labute showed in [62, Part 4], that the lower p-central series come from the filtered algebra defined by $Al(\mathbb{Z}_p, G)$ endowed with the filtration induced by $\{Al_{\{n\}}(G) := \ker(Al(\mathbb{Z}_p, G) \to \mathbb{F}_p)^n\}_{n\in\mathbb{N}}$. Additionally, the set $\bigoplus_{n\in\mathbb{N}}(G_{\{n\}}/G_{\{n+1\}})$ is a free $\mathbb{F}_p[t]$-module. Since G is finitely generated, we introduce:

$$a^\chi_{\{n\}} := \mathrm{rank}_{\mathbb{F}_p}(G_{\{n\}}/G_{\{n+1\}})[\chi], \quad \text{and} \quad c^\chi_{\{n\}} := \mathrm{rank}_{\mathbb{F}_p}(Al_{\{n\}}(G)/Al_{\{n+1\}}(G))[\chi].$$

If we replace $a_n(\mathbb{Z}_p)$ (resp. $c_n(\mathbb{Z}_p)$) by $a_{\{n\}}$ (resp. $c_{\{n\}}$), then the results of this chapter can be adapted for lower p-central series. Moreover, extending [62, Corollary 2.7] in an equivariant context, we can deduce a relation between the coefficients c^χ_n and $a^\chi_{\{n\}}$.

Chapter 4

On extensions of number fields with given quadratic algebras and cohomology

Presentations of (pro-p) groups via generators and relations have played an important role in the development of group theory (see [78, Chapter 2] and [79]), and more generally in the current theory of profinite groups and especially pro-p groups. These methods, combined with cohomological results, are also used to detect Galois groups of p-extensions, see for instance Koch [59],Ináč-Rogelstad-Tân [97] and [93], and Efrat-Quadrelli [24].

Shafarevich's great idea and insight was to present important Galois pro-p groups via generators and relations, and to search for a numerical criterium, depending on the presentation, for proving that some of these groups are infinite. In the work with Golod [33], he succeeded to make this idea precise, using associated filtrations and graded algebras techniques. Their numerical criterium was later refined to a famous Golod-Shafarevich criterium: if a pro-p group admits d generators and r relations satisfying $d^2 \geq 4r$, then it is infinite (see [15, Chapter IX]).

Around the same time, Lazard also inferred "l'Alternative des Gocha" (from the names of Golod and Shafarevich, see [69, Appendice A.3, Théorème 3.11]) which characterizes the topological structure of a pro-p group from the gradation of its group algebra. In the early 21^{st} century, Labute-Ináč [62] and [66], and Forré [29] used Anick's techniques [3] to define mild groups and infer FAB groups, i.e. groups such that every open subgroup has finite abelianization, of cohomological dimension 2.

In this chapter, we construct quotients of mild groups of larger cohomological dimension by using and enriching previous techniques: presentations of pro-p groups, projective resolutions, graded algebras, graph theory and Gröbner basis. From the "cutting tower" strategy introduced by Hajir-Maire-Ramakrishna [41], we conclude this chapter with arithmetical examples (see Theorem D below).

Arithmetic context

Let p be a prime number and K be a p-rational number field. The latter means that the Galois group G_K, of the maximal pro-p extension of K unramified outside p, is isomorphic

to a finitely generated free pro-p group. By a conjecture of Gras [34, Conjecture 8.11], if K is a fixed number field, then it is p-rational for every prime p large enough.

Introduce T a finite set of finite primes of K. Denote by G_K^T the Galois group of the maximal pro-p extension of K unramified outside p and totally splitting in T. We infer a free presentation $G_K^T = G_K/R$, with R a normal closed subgroup of G_K presented by relations $\{l_i\}_{i\in|T|}$. From the "cutting tower" strategy (see [45, Part 2] or [41]) based on the Chebotarev density Theorem, one can choose a set of primes T in K such that G_K^T has a *mild* presentation (see [29, Part 1]), so cohomological dimension 2. Mild groups play an important role in the understanding of Galois extensions with prescribed ramification and splitting (see [62], [66] and [117]).

Using the theory of Right Angled Artin Groups (RAAGs, see for instance [6], [135] and [76, Part 2]), we can construct quotients of G_K with prescribed cohomology. Let us fix $\{x_1, \dots, x_d\}$ a minimal set of generators of G_K and an undirected graph Γ with set of vertices $[\![1; d]\!]$. We define $G(\Gamma)$ as a quotient of G_K by commutators $[x_i; x_j]$ whenever $\{i, j\}$ is an edge of Γ. The dimension of the n-th cohomology group of $G(\Gamma)$ is given by $c_n(\Gamma)$, the number of n-cliques of Γ: i.e. complete subgraphs of Γ with n vertices.

In this work, we investigate quotients of mild groups with large finite cohomological dimension, using ideas introduced by RAAGs. Let G be a quotient of G_K and set $h^n(G)$ to be the dimension of $H^n(G; \mathbb{F}_p)$. We prove the following result:

Theorem D. *Let $\Gamma := \Gamma_{\mathbf{A}} \sqcup \Gamma_{\mathbf{B}}$ be a graph where $\Gamma_{\mathbf{A}}$ is bipartite. Then, there exist a totally imaginary field K and a set T of primes in K such that G_K^T is presented by relations $l_{\mathbf{A}} := \{l_{ij}; (i, j) \in \mathbf{A}\}$ which, modulo the third Zassenhaus filtration of G_K, satisfy the equality $l_{ij} \equiv [x_i; x_j]$. In particular G_K^T is mild.*

Furthermore, there exists a quotient G of G_K^T, such that for $n \geq 2$, $h^n(G) = c_n(\Gamma)$. Consequently the cohomological dimension of G is equal to $\max(2; n_{\Gamma_{\mathbf{B}}})$, with $n_{\Gamma_{\mathbf{B}}}$ the clique number of $\Gamma_{\mathbf{B}}$.

The construction of G_K^T is currently well-known, we use the "cutting tower strategy" introduced by Hajir-Maire-Ramakrishna (see references [41] and [45, Part 2]). The crucial part of Theorem D is the existence (and the construction) of the quotient G.

Cohomological results

We first introduce our main objects of study.

Let us denote by G a finitely presented pro-p group with presentation $G = F/R$, where F is a free pro-p group with generators $\{x_1, \dots, x_d\}$, and R is a normal closed subgroup of F generated by a finite family $\{l_1, \dots, l_r\}$. We define $E(G)$ as the completed group algebra of G over $\mathbb{F}_p$. This is an augmented algebra, and we denote by $E_n(G)$ the n-th power of the augmentation ideal of $E(G)$. Introduce

$$\mathscr{E}_n(G) := E_n(G)/E_{n+1}(G), \qquad \text{and} \qquad \mathscr{E}(G) := \bigoplus_{n\in\mathbb{N}} \mathscr{E}_n(G).$$

The graded algebra $\mathscr{E}(G)$ plays a fundamental role in this chapter, and more generally in the understanding of filtrations (see [69, Chapitre II and Appendice A.3], [62], [92] and [43]), topology (see [69, Alternative des Gocha, Théorème 3.11, Appendice A.3]) and cohomology (see [62], [66], [91], [98]) of G. Note that $H^n(G;\mathbb{F}_p)$ is a discrete $\mathbb{F}_p$-vector space, and denote by $H^\bullet(G)$ the graded algebra $\bigoplus_n H^n(G;\mathbb{F}_p)$ with product given by cup-product. We emphazise links between $E(G)$, $\mathscr{E}(G)$ and $H^\bullet(G)$.

In [14], Brumer defined the functor Ext for compact modules, and showed that ([14, Lemma 4.2] and [59, Part 3.9]) we have an isomorphism of graded algebra $H^\bullet(G) \simeq \mathrm{Ext}^\bullet_{E(G)}(\mathbb{F}_p;\mathbb{F}_p)$, where the product is given by the cup-product. Furthermore, using May spectral sequence (see [73, Theorem 5.1.12]), we obtain an identification of $H^\bullet(G)$ and $\mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p;\mathbb{F}_p)$ when $\mathscr{E}(G)$ is Koszul, i.e. the trivial $\mathscr{E}(G)$-module $\mathbb{F}_p$ admits a free-$\mathscr{E}(G)$ resolution $(\mathscr{P}_\bullet;\delta_\bullet)$, where $\mathscr{P}_i$ is generated by elements of degree i (we refer to [108, Chapter 2] for further references on Koszul algebra):

Proposition 27. *If $\mathscr{E}(G)$ is a Koszul algebra, then we have the following isomorphism of graded algebras:*

$$H^\bullet(G) \simeq \mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p;\mathbb{F}_p),$$

where the product is given by the cup-product. The algebra $H^\bullet(G)$ is the quadratic dual of $\mathscr{E}(G)$.

Ináč-Pasini-Quadrelli-Tân already observed, in [98, Proof of Theorem 4.6], that if G admits a mild presentation with quadratic relation, i.e. $l \subset F_2\backslash F_3$, then $\mathscr{E}(G)$ is Koszul. They also observed that if G is mild and $H^\bullet(G)$ is quadratic, then $H^\bullet(G)$ is the quadratic dual of $\mathscr{E}(G)$. As a direct consequence of Proposition 27, we complete [98, Theorem 1.3]: if the group G admits a mild presentation with quadratic relations, then $H^\bullet(G)$ is the quadratic dual of the Koszul algebra $\mathscr{E}(G)$. For more details on quadratic duals, we refer to [108, Part 1.2].

Computation of graded algebras

Currently, the algebra $\mathscr{E}(G)$ is only known when G is free, or mild, or in a few other specific cases (see [62], [66] and [92]). We give a criterion on the presentation of G which allows us to compute $\mathscr{E}(G)$. As a consequence, we obtain the cohomology groups of a pro-p group G (which will be here a quotient of a mild group) directly from its presentation. We are mostly inspired by the theory of RAAGs (see for instance [6] and [135]) and the work of Koch [60] and Forré [29, Theorem 3.7]. Let us now explain the strategy we adopt in this chapter to construct situations where $\mathscr{E}(G)$ is Koszul.

The Magnus isomorphism from [69, Chapitre II, Partie 3] gives us a surjection, that we denote by ϕ, between $E(G)$ (resp. $\mathscr{E}(G)$) and the $\mathbb{F}_p$-algebra of noncommutative series (resp. polynomials) over a set of variables $\mathbf{X} := \{X_1,\dots,X_d\}$, that we denote by E (resp. $\mathscr{E}$). In particular $\mathscr{E}(G)$ is a quotient of $\mathscr{E}$, and we denote by $\mathscr{I}$ its kernel. It is in general difficult to explicitly compute the ideal $\mathscr{I}$.

From the Magnus isomorphism, we write $w_i := \phi(l_i - 1)$ as a sum of homogeneous polynomials in E. A priori, every homogeneous polynomial in w_i plays a role in the computation of the ideal $\mathscr{I}$. Labute [62] and Forré [29], following ideas of Anick [3], gave a criterion (mild presentation) on the presentation of G such that the ideal $\mathscr{I}$ is generated only by the dominant term of w_i. However, this criterion restricts the cohomological dimension of G to less than or equal to two. In this chapter, we give another criterion, ensuring that $\mathscr{I}$ is also generated by dominant terms of w_i and in addition to the mild case, we infer situations where the cohomological dimension is strictly larger than two.

Let $\Gamma := (\mathbf{N}, \mathbf{E})$ be a graph with set of vertices $\mathbf{N} := [\![1; d]\!]$ and set of edges $\mathbf{E}$. We introduce a set $l_{\mathbf{E}} := \{l_{ij}\}_{\{i,j\}\in\mathbf{E}}$ of relations in F, and we state the following condition on the graph Γ and the family $l_{\mathbf{E}}$:

$$\begin{cases} \bullet \text{The graph } \Gamma \text{ can be written as a disjoint union of two components} \\ \quad \text{that we call } \Gamma_{\mathbf{A}} \text{ and } \Gamma_{\mathbf{B}}, \text{ with sets of edges } \mathbf{A} \text{ and } \mathbf{B}. \\ \bullet \text{The graph } \Gamma_{\mathbf{A}} \text{ is bipartite, and} \\ \quad w_{ij} := \phi(l_{ij} - 1) \equiv [X_i; X_j] \pmod{E_3}, \text{ for } \{i,j\} \in \mathbf{A}. \\ \bullet \text{We have } l_{uv} := [x_u; x_v], \text{ for } \{u,v\} \in \mathbf{B}. \end{cases} \tag{4.1}$$

Let us call $\mathscr{I}(\Gamma)$ the ideal in $\mathscr{E}$ generated by the family $\{[X_i; X_j]\}_{\{i,j\}\in\mathbf{E}}$, the dominant terms of $l_{\mathbf{E}}$ when it satisfies the Condition (4.1), and call $\mathscr{E}(\Gamma)$ the graded algebra $\mathscr{E}(\Gamma) := \mathscr{E}/\mathscr{I}(\Gamma)$. We use ideas from Forré [29], Wade [135], Labute-Mináč [62] and [66], Mináč-Pasini-Quadrelli-Tân [91] and [98], Anick [4] and Ufnarovskij [130] to show that if G admits a presentation satisfying the Condition (4.1), we have $\mathscr{I} = \mathscr{I}(\Gamma)$. Then we infer:

Theorem E. *Assume that G is a finitely generated pro-p group presented by relations $l_{\mathbf{E}}$ satisfying the Condition* (4.1)*, then $\mathscr{E}(G) = \mathscr{E}(\Gamma)$.*

When $\mathscr{E}(G) \simeq \mathscr{E}(\Gamma)$, we say that $\mathscr{E}(G)$ is a Right Angled Artin Algebra (RAAAs). RAAAs play a fundamental role in geometric group theory (see for instance [6]). In particular, since $\mathscr{E}(\Gamma)$ is Koszul (see [6, Part 4])

$$\mathrm{Ext}^{\bullet}_{\mathscr{E}(\Gamma)}(\mathbb{F}_p; \mathbb{F}_p) \simeq \mathscr{A}(\Gamma),$$

where $\mathscr{A}(\Gamma) := \mathscr{E}/\mathscr{I}^!(\Gamma)$, with $\mathscr{I}^!(\Gamma)$ the two sided ideal of $\mathscr{E}$ generated by the family

- X_iX_j when $\{i,j\} \notin \mathbf{E}$,
- X_u^2 for $u \in [\![1; d]\!]$,
- $X_uX_v + X_vX_u$ for u, v in $[\![1; d]\!]$.

Observe that $\dim_{\mathbb{F}_p} \mathscr{A}_n(\Gamma) = c_n(\Gamma)$, where $c_n(\Gamma)$ is the number of n-cliques of Γ, i.e. complete subgraphs of Γ with n vertices. Since $\mathscr{E}(\Gamma)$ is a Koszul algebra, we can apply Proposition 27 and we infer that

$$H^{\bullet}(G) \simeq \mathscr{A}(\Gamma), \quad \text{and} \quad h^n(G) := \dim_{\mathbb{F}_p} H^n(G) = c_n(\Gamma).$$

Outline

We begin with Part 4.1, where we give some backgrounds on Right Angled Artin Algebras (that we denote RAAA). Then we prove Theorem E in Part 4.2. We finish by Part 4.3, where we first prove Proposition 27, then we compute the algebras $\mathscr{E}(G)$ and $H^\bullet(G)$ when G is free, mild quadratic and pro-p RAAG. We conclude Part 4.3 with the proof of Theorem D, which follows from Theorem E and Proposition 27.

Notation

We introduce here some general notations:

• We recall that G is a finitely presented pro-p groups with generators $\{x_1;\dots;x_d\}$ and relations $\{l_1;\dots;l_r\}$.

• If x,y are elements in G (or in F), we denote by $[x,y]:=x^{-1}y^{-1}xy$.

• We define $H^n(G;\mathbb{F}_p)$ the n-th (continuous) cohomology group of the trivial (continuous) G-module $\mathbb{F}_p$. The cohomological dimension of G is the integer n (which can be infinite) such that for every $m>n$ we have $H^m(G;\mathbb{F}_p)=0$.

• The Magnus isomorphism from [69, Chapitre II, Partie 3] gives us the following identification of $\mathbb{F}_p$-algebras between $E(F)$ and the noncommutative series over $\mathbb{F}_p$ on $\{X_1;\dots;X_d\}$ that we call E:

$$\phi\colon E(F)\simeq E;\quad x_j\mapsto X_j+1. \tag{4.2}$$

The algebra E is filtered by $\{E_n\}_{n\in\mathbb{N}}$, the n-th power of the augmentation ideal, and we denote by $F_n:=\{f\in F;\phi(f-1)\in E_n\}$ the Zassenhaus filtration of F.

• Denote by I the closed two-sided ideal in E generated by $w_i:=\phi(l_i-1)$, this is an algebra with a filtration given by $\{I_n:=I\cap E_n\}_{n\in\mathbb{N}}$. From the Magnus isomorphism (1), we identify the filtered algebra $E(G)$ with the quotient algebra E/I: this is a filtered algebra and we denote its filtration by $\{E_n(G)\}_{n\in\mathbb{N}}$. Let us define:

$$\mathscr{E}_n(G):=E_n(G)/E_{n+1}(G),\quad\text{and}\quad\mathscr{E}(G):=\bigoplus_n\mathscr{E}_n(G).$$

• We introduce the functor Grad (see for instance [69, Chapitre I]) from the category of compact $\mathbb{F}_p$-vector spaces (or compact $E(G)$-modules) to graded $\mathbb{F}_p$-vector spaces (or graded $\mathscr{E}(G)$-modules). This is an exact functor. For instance, if we denote by $\mathscr{E}$ the noncommutative polynomials over $\mathbb{F}_p$ on $\{X_1;\dots;X_d\}$, and $\mathscr{E}_n:=E_n/E_{n+1}$, we have

$$\mathrm{Grad}(E):=\bigoplus_{n\in\mathbb{N}}\mathscr{E}_n=\mathscr{E}.$$

• Let us define $\mathscr{I}:=\mathrm{Grad}(I)=\bigoplus_n I_n/I_{n+1}$. Observe by [69, (2.3.8.2), Chapitre I] that the functor Grad is exact, so from the Magnus isomorphism, we can identify $\mathscr{E}(G)$ with the graded algebra $\mathrm{Grad}(E(G))\simeq\mathscr{E}/\mathscr{I}$, and we denote its gradation by $\{\mathscr{E}_n(G)\}_{n\in\mathbb{N}}$. We define the gocha series of G by:

$$gocha(G,t):=\sum_{n=0}^{\infty}c_nt^n,\quad\text{where}\qquad c_n:=\dim_{\mathbb{F}_p}\mathscr{E}_n(G)$$

• An $\mathbb{F}_p$-basis on E and $\mathscr{E}$ is given by monomials on the set of variables $\mathbf{X} := \{X_1; \dots; X_d\}$. The order $X_1 > X_2 > \cdots > X_d$ induces a lexicographic order on monomials on $\mathbf{X}$, that we denote by $>$. We say that a monomial X contains a monomial Y if there exist monomials M and N such that $X = MYN$.
Recall that we write commutators of X_i and X_j (in E or $\mathscr{E}$) as:

$$[X_i; X_j] := X_iX_j - X_jX_i \text{ for } \{i, j\} \in \mathbf{E}.$$

• If z is an element in E, we denote by $\deg(z)$ the integer such that $z \in E_{\deg(z)} \setminus E_{\deg(z)+1}$. Then we define $\overline{z}$ the image of z in $E_{\deg(z)}/E_{\deg(z)+1}$, this is a homogeneous polynomial, and we denote its degree by $\deg(z)$. We call $\widehat{z}$ the leading monomial of z. For instance $\widehat{[X_i; X_j]} = X_iX_j$.

• We say that G has a *mild* presentation if:

$$gocha(G, t) = \frac{1}{1 - dt + \sum_{i=1}^{r} t^{\deg(w_i)}}.$$

The group G has a quadratic presentation if for every integer i, $\deg(w_i) = 2$.

• We say that the algebra $\mathscr{E}(G)$ is Koszul, if the trivial $\mathscr{E}(G)$-module $\mathbb{F}_p$ admits a linear resolution $(\mathscr{P}, \delta)$, i.e. $\mathscr{P}_i$ is a free-$\mathscr{E}(G)$-module generated by elements of degree i (see for instance [108, Chapter 2]).

4.1 Preliminaries on Right Angled Artin Algebras (RAAA)

Recall that we denote by $\Gamma := (\mathbf{N}, \mathbf{E})$ an undirected graph, where $\mathbf{N} := [\![1; \dots d]\!]$. For every integer n, we denote by $c_n(\Gamma)$ the number of n-cliques of Γ. Let $\mathscr{I}(\Gamma)$ (resp. $I(\Gamma)$) be the closed two sided ideal of $\mathscr{E}$ (resp. E) generated by the family $\{[X_i; X_j]\}_{\{i,j\} \in \mathbf{E}}$ and $\mathscr{E}(\Gamma) := \mathscr{E}/\mathscr{I}(\Gamma)$ (resp. $E(\Gamma) := E/I(\Gamma)$).

We take the following orientation on Γ, that we call *standard*: if $(i, j) \in \mathbf{E}$ then $i < j$. For more references on RAAAs, let us quote [6].

4.1.1 Introductory results on graphs

Let us begin with few results on graphs. I am thankful to Chris Hall for the following Lemma. We refer to [18, Chapters 1 and 5] for a general introduction on graph theory.

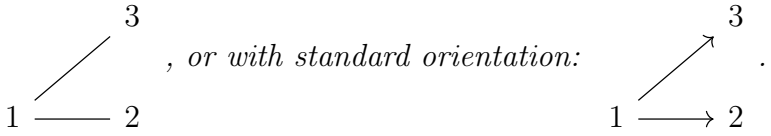
Lemma 10. *The undirected graph Γ is bipartite if and only if there exists an orientation on Γ such that the tail of an edge of Γ is not the head of another one.*

Proof. The undirected graph Γ is bipartite if and only if it is 2-colored (let us call these colors black and white). For instance, we can direct edges from white vertices to black vertices.
Conversely, we can give a 2-coloring on a graph Γ where the tail of an edge is not the head of another one. We endow heads of edges with white color and tails of edges with black color. □

Remark 18 (Bipartite graphs, orientation and combinatorially free families)**.** *Up to relabelling vertices, we assume that bipartite graphs satisfy the property given in Lemma 10 for the standard orientation. Equivalently, if* Γ *is bipartite, then the family* $\{X_iX_j\}_{(i,j)\in\mathbf{E}}$ *is combinatorially free in* E *(recall that we took the order on monomials induced by* $X_1 > X_2 > \cdots > X_d$*), i.e. for every different cuples* (i_1, j_1) *and* (i_2, j_2) *in* $\mathbf{E}$*, we have* $j_1 \neq i_2$*.*

From now, we denote by $\{i, j\}$ edges from the undirected graph Γ and (i, j) edges of the graph Γ endowed with its standard orientation. Of course, we only discuss cliques of the undirected graph Γ. Let us give an example:

Example 22. *Consider* Γ *the graph with three vertices* $\{1; 2; 3\}$ *and two edges* $\{\{1, 2\}; \{1, 3\}\}$*. The graph* Γ *is bipartite and we have the following representation:*



4.1.2 Gradation and RAAAs

Let us begin with some introductory results on the functor Grad (for more references, see [69, Chapitre I]). We first show that the functor Grad sends homogeneous ideals (i.e. ideals generated by homogeneous polynomials) in E to homogenous ideals in $\mathscr{E}$.

Observe that $E(\Gamma)$ is an augmented algebra, so filtered by powers of the augmentation ideal.

Lemma 11 (Gradation of $E(\Gamma)$)**.** *We have* $\mathrm{Grad}(E(\Gamma)) = \mathscr{E}(\Gamma)$*.*

Proof. We just need to show that $\mathrm{Grad}(I(\Gamma)) = \mathscr{I}(\Gamma)$. We always have $\mathscr{I}(\Gamma) \hookrightarrow \mathrm{Grad}(I(\Gamma))$. Let us show the reverse inclusion.

Take $z \in I(\Gamma)$, and write $z := \sum_{ijul} a_{ijul}[X_i; X_j]b_{iju}$, where $a, b \in E$. Let us express z as a (possibly infinite) sum of homogeneous polynomials:

$$a_{ijul} := \sum_{g\in\mathbb{N}} {}_g a_{ijul}, \quad \text{and} \quad b_{iju} := \sum_{h\in\mathbb{N}} {}_h b_{iju},$$

where ${}_g a_{ijul}$ and ${}_h b_{iju}$ are homogeneous polynomials of degree g and h. Therefore, we have the following (possibly infinite) sum of homogeneous polynomials:

$$z = \sum_{n\in\mathbb{N}} \sum_{ijul} \sum_{g+h+2=n} ({}_g a_{ijul})[X_i; X_j]({}_h b_{iju}).$$

So, if $\deg(z) = n$, we infer:

$$\overline{z} = \sum_{ijul} \sum_{g+h+2=n} ({}_g a_{ijul})[X_i; X_j]({}_h b_{iju}) \in \mathscr{I}(\Gamma).$$

Therefore $\mathrm{Grad}(I(\Gamma)) = \mathscr{I}(\Gamma)$ is a homogeneous ideal. □

Remark 19. *Lemma 11 is still true if we take I a two-sided ideal in E generated by homogeneous elements w_u (which can be seen both in E and $\mathscr{E}$). More precisely,* $\mathrm{Grad}(I)$ *will also be generated by w_u as a two-sided ideal in $\mathscr{E}$.*

Recall, from the Condition (4.1), that we defined $w_{uv} := \phi([x_u; x_v]-1)$ in E. We compute here the homogeneous polynomials occurring in the expression of w_{uv}.

Lemma 12. *We have the following equality:*

$$w_{uv} = \left(\sum_{n\in\mathbb{N}}(-1)^n \sum_{k=0}^{n} P_{n,k}(X_u; X_v)\right)[X_u; X_v], \quad \textit{where} \quad P_{n,k}(X_u; X_v) = X_u^k X_v^{n-k}.$$

Proof. For every integer n, we introduce the homogeneous polynomial of degree n: $P_n(X_u; X_v) := (-1)^n \sum_{k=0}^{n} P_{n,k}(X_u; X_v) \in E_n$. Let us observe that P_n satisfies the following equalities:

$$\begin{aligned} P_n(X_u; X_v) &= X_u^n + P_{n-1}(X_u; X_v)X_v = X_v^n + P_{n-1}(X_u; X_v)X_u \\ &= X_u^n + X_v^n + P_{n-2}(X_u; X_v)X_uX_v. \end{aligned} \tag{$*$}$$

Now, let us compute w_{uv}. For this purpose, we introduce the series $Z := \sum_{n=1}^{\infty}(-1)^n P_n(X_u; X_v)$, and we infer:

$$\begin{aligned} w_{uv} &= (1+X_u)^{-1}(1+X_v)^{-1}(1+X_u)(1+X_v) - 1 \\ &= (1+Z)(1+X_u+X_v+X_uX_v) - 1. \\ &= X_u + X_v + X_uX_v + Z + Z(X_u+X_v) + ZX_uX_v. \end{aligned} \tag{$**$}$$

Let us denote by $w_{uv,n}$ the term (homogeneous polynomial) of degree n in w_{uv}, i.e. $w_{uv} := \sum_{n=1}^{\infty} w_{uv,n}$. Observe that:

$$w_{uv,1} = 0, \quad \text{and} \quad w_{uv,2} = [X_u; X_v].$$

For $n \geq 3$, we obtain from $(**)$:

$$w_{uv,n} = (-1)^n \left[P_n(X_u; X_v) - P_{n-1}(X_u; X_v)(X_u+X_v) + P_{n-2}(X_u; X_v)X_uX_v\right].$$

We conclude by applying relations given in $(*)$. □

Proposition 28. *Denote by Δ the ideal in E generated by $\{w_{uv} := \phi([x_u; x_v]-1); (u,v) \in \mathbf{E}\}$. Then $\Delta = I(\Gamma)$ and* $\mathrm{Grad}(\Delta) = \mathscr{I}(\Gamma)$.

Proof. From Lemma 12, we notice that $\Delta \subset I(\Gamma)$. Furthermore, $\mathscr{I}(\Gamma) \subset \mathrm{Grad}(\Delta)$ and from Lemma 11 we infer that $\mathrm{Grad}(\Delta) = \mathscr{I}(\Gamma)$. Consequently, $\mathrm{Grad}(\Delta) = \mathrm{Grad}(I(\Gamma)) = \mathscr{I}(\Gamma)$. By [69, Corollaire (2.3.15), Chapitre I] we conclude that $\Delta = I(\Gamma)$. □

4.2 Proof of Theorem E

The goal of this part is to compute $\mathscr{E}(G)$, when G is presented by a family of relations $l_{\mathbf{E}}$ coming from a graph Γ, endowed with standard orientation (see Remark 10), satisfying the Condition (4.1).

Theorem 23. *Assume that G admits a presentation with relation $l_{\mathbf{A}\cup\mathbf{B}}$ satisfying* (4.1)*. Then $\mathscr{E}(G) = \mathscr{E}(\Gamma)$.*

We show that $\mathscr{I} = \mathscr{I}(\Gamma)$. We split the proof into several steps. Using the proof of [29, Theorem 3.7] we give Equalities (B1) and (B2) in subpart 4.2.1. This allows us to express elements in I modulo E_{n+1} for every integer n. The rest of the proof is done by contradiction.

In subpart 4.2.2, we infer Equalities (B3) and (B4) from monomial analysis (Gröbner basis, see [130]) and the fact that $\widehat{w_{\mathbf{A}}} := \{X_iX_j\}_{(i,j)\in\mathbf{A}}$ is combinatorially free. In subpart 4.2.3, we show Equality (B5) from $l_{uv} := [x_u; x_v]$, Lemma 12 and Gröbner basis arguments. We finish the proof with subpart 4.2.4, where we conclude that the contributions given by the homogeneous polynomials in the expressions of w_{ij} and w_{uv}, for the computation of $\mathscr{I}$, only come from the dominant terms. So we conclude $\mathscr{I} = \mathscr{I}(\Gamma)$.

Recall that $\widehat{w_{\mathbf{A}}} := \{X_iX_j\}_{(i,j)\in\mathbf{A}}$ and $\widehat{w_{\mathbf{B}}} := \{X_uX_v\}_{(u,v)\in\mathbf{B}}$. We introduce $\mathscr{I}_{\mathbf{A}}$ and $\mathscr{I}_{\mathbf{B}}$ the ideals in $\mathscr{E}$ generated by $\overline{w_{\mathbf{A}}} := \{[X_i; X_j]\}_{(i,j)\in\mathbf{A}}$ and $\overline{w_{\mathbf{B}}} := \{[X_u; X_v]\}_{(u,v)\in\mathbf{B}}$. We denote by $\widehat{\mathscr{I}(\Gamma)}$ (resp. $\widehat{\mathscr{I}_{\mathbf{A}}}$, $\widehat{\mathscr{I}_{\mathbf{B}}}$) the leading terms of a fixed Gröbner basis of $\mathscr{I}(\Gamma)$ (resp. $\mathscr{I}_{\mathbf{A}}$, $\mathscr{I}_{\mathbf{B}}$), i.e. $\widehat{\mathscr{I}(\Gamma)}$ is a set of generators of the ideal generated by the leading monomials of elements of $\mathscr{I}(\Gamma)$. By Remark 18, we can take $\widehat{\mathscr{I}_{\mathbf{A}}} := \widehat{w_{\mathbf{A}}}$, furthermore since $\mathscr{I}_{\mathbf{A}} + \mathscr{I}_{\mathbf{B}} = \mathscr{I}(\Gamma)$, we choose $\widehat{\mathscr{I}(\Gamma)}$, $\widehat{\mathscr{I}_{\mathbf{A}}}$ and $\widehat{\mathscr{I}_{\mathbf{B}}}$ such that:

$$\widehat{w_{\mathbf{A}}} \cup \widehat{w_{\mathbf{B}}} \subset \widehat{\mathscr{I}_{\mathbf{A}}} \cup \widehat{\mathscr{I}_{\mathbf{B}}} \subset \widehat{\mathscr{I}(\Gamma)}, \quad \text{and} \quad \widehat{\mathscr{I}_{\mathbf{A}}} := \{X_iX_j\}_{(i,j)\in\mathbf{A}}, \quad \widehat{w_{\mathbf{B}}} \subset \widehat{\mathscr{I}_{\mathbf{B}}}. \tag{B0}$$

4.2.1 Decomposition

If A is a subset of E, we recall that we have

$$\mathrm{Grad}(A) := \bigoplus_n [(A \cap E_n + E_{n+1})/E_{n+1}].$$

Furthermore, $\mathrm{Grad}(A)$ is a subset of $\mathscr{E}$.

Observe that $\mathscr{I}(\Gamma) \subset \mathscr{I}$. By [130, Theorems, Parts 2.3 and 2.4], the ideal $\mathscr{I}(\Gamma)$ admits a complementary subspace $\mathscr{C}_\Gamma$ with a monomial basis given by monomials not containing $\widehat{\mathscr{I}(\Gamma)}$. By Equation (B0), these monomials do not contain $\widehat{w_{\mathbf{A}}} \cup \widehat{w_{\mathbf{B}}}$.

Furthermore, we denote the gradation on $\mathscr{C}_\Gamma$ by $\mathscr{C}_\Gamma := \bigoplus_n \mathscr{C}_{\Gamma,n}$. Let us define by $\mathscr{C}_n$ a complementary subspace of $\mathscr{I}_n \cap \mathscr{C}_{\Gamma,n}$ in $\mathscr{C}_{\Gamma,n}$, i.e. $\mathscr{C}_{\Gamma,n} = \mathscr{C}_n \bigoplus (\mathscr{I}_n \cap \mathscr{C}_{\Gamma,n})$.
Introduce $\mathscr{C} := \bigoplus_n \mathscr{C}_n$, this is a complementary subspace of $\mathscr{I}$ in $\mathscr{E}$, and every element $c \in \mathscr{C}_n$ can be uniquely written as $c = \sum_i c_i$, where c_i is a monomial of degree n in $\mathscr{C}_{\Gamma,n}$. Denote by $C := \prod_n \mathscr{C}_n$ and $C_\Gamma := \prod_n \mathscr{C}_{\Gamma,n}$, these are filtered subsets of E. By [69, Chapitre I, (2.3.7)], we have $\mathrm{Grad}(C) = \mathscr{C}$.

In the beginning of the proof (first two pages) of [29, Theorem 3.7], Forré showed that C is a complementary subspace of I in E, and for every integer n, we have the following decomposition:

$$I = CWE + I^{n+1}, \tag{B1}$$

where W is the $\mathbb{F}_p$-vector space generated by $w_{ij} := \phi(l_{ij} - 1)$, for (i, j) in $\mathbf{A} \cup \mathbf{B}$.

Our goal is to show that $\mathscr{I} = \mathscr{I}(\Gamma)$. Take $f \in I$ of degree n, we need to prove that $\overline{f}$ (which describes a general element in $\mathscr{I}$) is in $\mathscr{I}(\Gamma)$. Using Equality (B1), we can write:

$$f := \sum_{(i,j)\in\mathbf{A}} \sum_{k=1}^{n_{ij}} \sum_{l=1}^{n_{ijk}} s_{ijkl} + \sum_{(u,v)\in\mathbf{B}} \sum_{o=1}^{n_{uv}} \sum_{q=1}^{n_{uvo}} s_{uvoq} + r_{n+1}, \quad \text{where}$$

$$s_{ijkl} = c_{ijkl} w_{ij} X_{ijk}, \quad s_{uvoq} = c_{uvoq} w_{uv} X_{uvo}, \quad \text{and} \quad r_{n+1} \in I^{n+1};$$

for $c_\bullet$ in C and $X_\bullet$ a monomial in E.

Therefore,

$$f \equiv \sum_{\deg\leq n} s_{ijkl} + \sum_{\deg\leq n} s_{uvoq} \pmod{E_{n+1}}. \tag{B2}$$

Then, without loss of generalities, we can write as a sum of monomials of degree less or equal than n in C_Γ: $c_{ijkl} := \sum_{g=1}^{n_{ijkl}} c_{ijklg}$, and $c_{uvoq} := \sum_{h=1}^{n_{uvoq}} c_{uvoqh}$.
From now, we simplify the notations on indices by denoting c_{ijkl} and c_{uvoq} as monomials in C_Γ. Recall by Lemma 12 that we have the following sum of homogeneous polynomials:

$$w_{uv} := \sum_{r=2}^{\infty} \sum_{z=0}^{r} w_{uvrz}, \quad \text{with } w_{uvrz} := P_{r-2,z}(X_u; X_v)[X_u; X_v],$$

where w_{uvrz} is of degree r.

A natural candidate for $\overline{f}$ would be $\sum_{\deg\leq n} c_{ijkl}[X_i; X_j]X_{ijk} + \sum_{\deg\leq n} c_{uvoq}[X_u; X_v]X_{uvo}$. However, the terms in the previous sums can be of degree strictly less than n. We then work on degree arguments. Especially, we shall study particular leading monomials and so we shall choose special indices, that we will denote by bold letters.

4.2.2 Monomial analysis

Similarly to the proof of [29, Theorem 3.7], we introduce $m_{\mathbf{A}} := \inf_{ijkl,(i,j)\in\mathbf{A}}(\deg(s_{ijkl}))$. The goal of the rest of the proof is to show that $m_{\mathbf{A}} = n$, then we conclude that this equality allows us to show that $\overline{f}$ is in $\mathscr{I}(\Gamma)$. We argue by contradiction to show that $m_{\mathbf{A}} = n$. Assume that $m_{\mathbf{A}} < n$, then from Equality (B2), we infer:

$$\sum_{\deg=m_{\mathbf{A}}} c_{ijkl}[X_i; X_j]X_{ijk} + \sum_{\deg=m_{\mathbf{A}}} c_{uvoq} w_{uvrz} X_{uvo} = 0.$$

Furthermore, by definition of $m_{\mathbf{A}}$, we can assume for every (i, j) in $\mathbf{A}$ and k that $\sum_l c_{ijkl} \neq 0$. Define $\mu_{\mathbf{A}}$ and $\mu_{\mathbf{B}}$ by

$$\mu_{\mathbf{A}} := \sum_{\deg=m_{\mathbf{A}}} c_{ijkl}[X_i; X_j]X_{ijk}, \quad \text{and} \quad \mu_{\mathbf{B}} := \sum_{\deg=m_{\mathbf{A}}} c_{uvoq} w_{uvrz} X_{uvo}.$$

Before studying the polynomials $\mu_{\mathbf{A}}$ and $\mu_{\mathbf{B}}$, we bring back some results on strongly and combinatorially free families from [29]. Recall that $\mathscr{I}_{\mathbf{A}}$ is the ideal of $\mathscr{E}$ generated by $\overline{w_{\mathbf{A}}} := \{[X_i; X_j]\}_{(i,j)\in\mathbf{A}}$, and denote by $\mathscr{J}_{\mathbf{A}}$ the ideal of $\mathscr{E}$ generated by $\widehat{w_{\mathbf{A}}}$. Since $\widehat{w_{\mathbf{A}}}$ is combinatorially free, we infer that $\widehat{w_{\mathbf{A}}}$ is a Gröbner basis of $\mathscr{I}_{\mathbf{A}}$, and by [29, Theorem 2.6] the family $\overline{w_{\mathbf{A}}}$ is strongly free, i.e. if we denote by $\mathscr{E}_{\geq 1}$ the augmentation ideal of $\mathscr{E}$, the $\mathscr{E}/\mathscr{I}_{\mathbf{A}}$-module $\mathscr{I}_{\mathbf{A}}/\mathscr{I}_{\mathbf{A}}\mathscr{E}_{\geq 1}$ is free over $\overline{w_{\mathbf{A}}}$. Moreover, by [29, Theorem 2.3], the family $\widehat{w_{\mathbf{A}}}$ is a basis of the free $\mathscr{E}/\mathscr{J}_{\mathbf{A}}$-module $\mathscr{J}_{\mathbf{A}}/\mathscr{J}_{\mathbf{A}}\mathscr{E}_{\geq 1}$.

Let us define $\mathscr{C}_{\mathbf{A}}$ the subspace of $\mathscr{E}$ generated by all monomials not containing $\widehat{w_{\mathbf{A}}}$. By [130, Theorems Parts 2.3 and 2.4], we notice that the $\mathbb{F}_p$-vector space $\mathscr{C}_{\mathbf{A}}$ is both a complementary subspace of $\mathscr{I}_{\mathbf{A}}$ and $\mathscr{J}_{\mathbf{A}}$. From that fact, we can apply the strategy used in [29, Theorem 3.7, beginning of the page 181].

If $\mu_{\mathbf{B}} = 0$, then $\mu_{\mathbf{A}} = 0$. The proof of [29, Theorem 3.7, beginning page 181] shows that this case is impossible, since $\{[X_i; X_j]\}_{(i,j)\in\mathbf{A}}$ is strongly free and c_{ijkl} does not contain monomials in $\widehat{w_{\mathbf{A}}}$ so is in $\mathscr{C}_{\mathbf{A}}$. Consequently, $\mu_{\mathbf{B}}$ and $\mu_{\mathbf{A}}$ are both different from zero. This implies that

$$\widehat{\mu_{\mathbf{A}}} = \widehat{\mu_{\mathbf{B}}} \neq 0 \tag{B3}$$

We study now the structure of the monomials $\widehat{\mu_{\mathbf{A}}}$ and $\widehat{\mu_{\mathbf{B}}}$.
From Remark 10, the family $\widehat{\mathscr{I}_{\mathbf{A}}}$ is combinatorially free, then it is strongly free (see [29, Theorem 2.3]). Using a similar argument as [29, Beginning of page 181], we infer that $\widehat{\mu_{\mathbf{A}}} = c_{\mathbf{ijkl}}X_{\mathbf{i}}X_{\mathbf{j}}X_{\mathbf{ijk}}$ for some fixed coefficients $(\mathbf{i},\mathbf{j}) \in \mathbf{A}$ and $\mathbf{k},\mathbf{l}$. Indeed if the previous equality does not hold, there exists a relation of the form:

$$\sum_{ijkl} c_{ijkl}X_iX_jX_{ijk} = 0.$$

Since $\{X_1; \ldots; X_d\}$ is a $\mathscr{E}$-linearly independant family, we can assume that at least one monomial $X_{\mathbf{ijk}}$ has valuation zero (so is in $\mathbb{F}_p$), then we obtain a relation:

$$\sum c_{ijkl}X_iX_jX_{ijk} \equiv 0 \pmod{\mathscr{J}_{\mathbf{A}}\mathscr{E}_{\geq 1}}.$$

Since $\widehat{w}_{\mathbf{A}}$ is strongly free, we infer that $\sum_l c_{\mathbf{ijk}l}$ is in $\mathscr{C}_{\mathbf{A}} \cap \mathscr{J}_{\mathbf{A}} = \{0\}$. This is a contradiction. Consequently, we can write:

$$\widehat{\mu_{\mathbf{A}}} := M_{\mathbf{A}}X_{\mathbf{i}}X_{\mathbf{j}}X_{\mathbf{A}} \tag{B4}$$

where $M_{\mathbf{A}} := c_{\mathbf{ijkl}}$ and $X_{\mathbf{A}} := X_{\mathbf{ijk}}$. Observe that $M_{\mathbf{A}}$ is a monomial in $\mathscr{C}_\Gamma$, so from (B0), the monomial $M_{\mathbf{A}}$ does not contain monomials in $\widehat{w_{\mathbf{A}}} \cup \widehat{w_{\mathbf{B}}}$.

Recall, from hypothesis, that $m_{\mathbf{A}} < n := \deg(f)$. Let us show that $\widehat{\mu_{\mathbf{B}}}$ has the following form:

$$\widehat{\mu_{\mathbf{B}}} := M_{\mathbf{B}}X_{\mathbf{u}}X_{\mathbf{v}}X_{\mathbf{B}} \tag{B5}$$

for some fixed $(\mathbf{u},\mathbf{v})$ in $\mathbf{B}$, some monomial $X_{\mathbf{B}}$ and some monomial $M_{\mathbf{B}}$ not containing submonomials in $\widehat{w_{\mathbf{A}}} \cup \widehat{w_{\mathbf{B}}}$. From Lemma 12, $\widehat{\mu_{\mathbf{B}}}$ has one of the following forms, for some fixed index $(\mathbf{u},\mathbf{v}) \in \mathbf{B}$:

$$(a)\quad \widehat{\mu_{\mathbf{B}}} = c_{\mathbf{uvoq}}P_{\mathbf{r}-2,\mathbf{z}}(X_{\mathbf{u}},X_{\mathbf{v}})X_{\mathbf{u}}X_{\mathbf{v}}X_{\mathbf{uvoq}},\quad \text{or}\quad (b)\quad \widehat{\mu_{\mathbf{B}}} = c_{\mathbf{uvoq}}P_{\mathbf{r}-2,\mathbf{z}}(X_{\mathbf{u}},X_{\mathbf{v}})X_{\mathbf{v}}X_{\mathbf{u}}X_{\mathbf{uvo}}.$$

The monomial $P_{\mathbf{r}-2,\mathbf{z}}(X_{\mathbf{u}}, X_{\mathbf{v}})$ contains a monomial of the form $X_u X_v$ with $(u,v) \in \mathbf{B}$ if and only if $0 < \mathbf{z} < \mathbf{r} - 2$. Observe that $\widehat{\mu_{\mathbf{B}}}$ has one of the following from:

(i) the case (a),

(ii) the case (b) with $0 < \mathbf{z} \leq \mathbf{r} - 2$,

(iii) the case (b) with $0 = \mathbf{z}$, but $c_{\mathbf{uvoq}} := XX_u$ where X is a monomial and $(u, \mathbf{v}) \in \mathbf{B}$,

(iv) the case (b) with $0 = \mathbf{z}$, and $c_{\mathbf{uvoq}}$ does not finish by X_u such that $(u, \mathbf{v}) \in \mathbf{B}$.

For the case $(i) - (iii)$, we always infer a monomial $M_{\mathbf{B}}$ not containg a submonomial in $\widehat{w_{\mathbf{A}}} \cup \widehat{w_{\mathbf{B}}}$ such that $\widehat{\mu}_{\mathbf{B}} = M_{\mathbf{B}} X_u X_v X_{\mathbf{B}}$, so a positive solution to Equation (B5). In the next subpart, we show that the case (iv) is impossible, which allows us to infer (B5).

4.2.3 Structure of $\widehat{\mu_{\mathbf{B}}}$.

To conclude, under the hypothesis $m_{\mathbf{A}} < n$, we show that the case (iv) is impossible. By contradiction, we assume that

$$\widehat{\mu_{\mathbf{B}}} = c_{\mathbf{uvoq}} X_{\mathbf{v}}^{\mathbf{r}-2} X_{\mathbf{v}} X_{\mathbf{u}} X_{\mathbf{uvo}}, \quad \text{for some integer } \mathbf{r}, \text{ and}$$
$$c := c_{\mathbf{uvoq}} X_{\mathbf{v}}^{\mathbf{r}-2} \text{ does not contain a monomial in } \widehat{w_{\mathbf{A}}} \cup \widehat{w_{\mathbf{B}}}.$$

By Equalities (B4) and (B3), we infer:

$$\widehat{\mu_{\mathbf{B}}} = c X_{\mathbf{v}} X_{\mathbf{u}} X_{\mathbf{uvo}} = c_{\mathbf{ijkl}} X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}}.$$

Since $cX_{\mathbf{v}} X_{\mathbf{u}}$ does not contain a monomial in $\widehat{w_{\mathbf{A}}}$, we infer that there exists a monomial $X'_{\mathbf{uvo}}$ include in $c_{\mathbf{ijkl}}$ such that

$$X_{\mathbf{uvo}} = X'_{\mathbf{uvo}} X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}}.$$

Consider the following restricted sum $\mu'_{\mathbf{B}}$ of $\mu_{\mathbf{B}}$ where every polynomial of degree $m_{\mathbf{A}}$ finishes by $X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}}$, and $\mathbf{i}, \mathbf{j}, \mathbf{k}$ is fixed from (B4) (here $X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}}$ is the end of $\widehat{\mu_{\mathbf{A}}}$):

$$\mu'_{\mathbf{B}} = \sum_{\deg = m_{\mathbf{A}}} \sum_{(u,v) \in \mathbf{B}} \sum_{o,q,r,z} \sum_{X_{uvo} = X'_{uvo} X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}}} c_{uvoq} w_{uvrz} X_{uvo},$$

This sum is not empty, every term in that sum finishes by $X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}}$, and that sum is in $\mathscr{I}_{\mathbf{B}}$: the two-sided ideal of $\mathscr{E}$ generated by $\overline{w_{\mathbf{B}}}$. Observe that $\widehat{\mu_{\mathbf{B}}} = \widehat{\mu'_{\mathbf{B}}}$.

Define $\mu''_{\mathbf{B}}$ by $\mu'_{\mathbf{B}} := \mu''_{\mathbf{B}}(X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}})$. Notice that $\mu''_{\mathbf{B}}$ is in $\mathscr{I}_{\mathbf{B}}$. Therefore $\mu''_{\mathbf{B}}$ contains a monomial in $\widehat{\mathscr{I}_{\mathbf{B}}}$. Furthermore, by definition

$$\widehat{\mu_{\mathbf{B}}} = \widehat{\mu'_{\mathbf{B}}} = \widehat{\mu''_{\mathbf{B}}} X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}} = c_{\mathbf{ijkl}} X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{ijk}},$$

consequently $\widehat{\mu''_{\mathbf{B}}} = c_{\mathbf{ijkl}}$ is in $\mathscr{C}_\Gamma$ and therefore by (B0) does not contain monomials in $\widehat{\mathscr{I}_{\mathbf{B}}}$. This is impossible. We studied all cases, so we conclude that $\widehat{\mu_{\mathbf{B}}}$ satisfies Equality (B5).

4.2.4 Conclusion

Let us first show that $m_{\mathbf{A}} = n$. If $m_{\mathbf{A}} < n$, then from Equalities (B3), (B4) and (B5), we have:

$$M_{\mathbf{A}} X_{\mathbf{i}} X_{\mathbf{j}} X_{\mathbf{A}} = M_{\mathbf{B}} X_{\mathbf{u}} X_{\mathbf{v}} X_{\mathbf{B}}.$$

Therefore, $M_{\mathbf{A}} = M_{\mathbf{B}}$. This is impossible since $X_{\mathbf{i}} \neq X_{\mathbf{u}}$. We conclude that $m_{\mathbf{A}} = n$.

Let us now finish our proof, by showing that $\overline{f}$ is in $\mathscr{I}(\Gamma)$. Using Equality (B2), we have modulo E_{n+1}:

$$f = \sum_{\deg=n, ijkl, (i,j)\in\mathbf{A}} s_{ijkl} + \sum_{\deg\leq n, uvoq, (u,v)\in\mathbf{B}} s_{uvoq}.$$

Since f and $\sum_{\deg=n} s_{ijkl}$ are both of degree n, then $\sum_{\deg\leq n} s_{uvoq}$ is at least of degree n, and by Lemma 11 we have $\overline{\sum_{\deg\leq n} s_{uvoq}} \in \mathscr{I}(\Gamma)$. Consequently modulo E_{n+1}, we infer:

$$f \equiv \overline{\sum_{\deg=n} s_{ijkl} + \sum_{\deg\leq n} s_{uvoq}} = \overline{\sum_{\deg=n} s_{ijkl}} + \overline{\sum_{\deg\leq n} s_{uvoq}}$$
$$\equiv \sum_{\deg=n} c_{ijkl}[X_i; X_j] X_{ijkl} + \overline{\sum_{\deg\leq n} s_{uvoq}}.$$

Thus $\overline{f} \in \mathscr{I}_n(\Gamma)$, so $\mathscr{I}(\Gamma) = \mathscr{I}$.

Remark 20. *In the proof of Theorem E, we constructed a filtered $\mathbb{F}_p$-vector space C_Γ, and we showed that if $\mathscr{I} = \mathscr{I}(\Gamma)$, then $E(G)$ is isomorphic to C_Γ as a filtered $\mathbb{F}_p$-vector space. In fact, we can define an algebra structure on C_Γ using the natural surjection $\phi\colon E \to E(G)$ induced by the Magnus isomorphism and show that C_Γ is indeed isomorphic (as a filtered algebra) to $E(G)$.*

Remark 21 (Gocha series and filtrations for groups satisfying the Condition (4.1))**.** *We assume that G admits a presentation which satisfies the Condition* (4.1)*. The gocha series of G is given by:*

$$gocha(G,t) = \frac{1}{\sum_{k=0}^{n}(-1)^k c_k(\Gamma) t^k}, \quad \text{and} \quad h^n(G) = c_n(\Gamma), \text{ for every integer } n.$$

Let us denote by $a_n := \dim_{\mathbb{F}_p} G_n/G_{n+1}$. Then using [92, Theorem 2.9*], we can explicitly compute coefficients a_n for every integer n. See also [45] for an equivariant study.*

4.2.5 Example

Let us give an example:

We define Γ a graph with 6 vertices and five edges given by $\mathbf{E} := \mathbf{A} \sqcup \mathbf{B}$, where $\mathbf{A} := \{(1,2);(1,3)\}$ and $\mathbf{B} := \{(4,5);(4,6);(5,6)\}$. A representation of Γ is given by:

Take G a pro-p group defined by six generators and five relations of the form $l_{\mathbf{A}\cup\mathbf{B}}$ given by:

$$l_{12} \equiv 1 + [X_1; X_2] \pmod{E_3}, \quad \text{and} \quad l_{13} \equiv 1 + [X_1; X_3] \pmod{E_3},$$
$$l_{45} := [x_4; x_5], \quad l_{46} := [x_4; x_6], \quad \text{and} \quad l_{56} := [x_5; x_6].$$

Observe that Γ and the relations $l_{\mathbf{E}}$ satisfy the Condition (4.1). Therefore, by Theorem E, the algebra $\mathscr{E}(G)$ is given by $\mathscr{E}(\Gamma) := \mathscr{E}/\mathscr{I}(\Gamma)$, where

$$\mathscr{I}(\Gamma) := \langle [X_1; X_2], [X_1; X_3], [X_4; X_5], [X_4; X_6], [X_5; X_6] \rangle.$$

Furthermore, thanks to Proposition 27, that we prove in Part 4.3, we have:

$$h^1(G) = c_1(\Gamma) = 6, \quad h^2(G) = c_2(\Gamma) = 5, \quad h^3(G) = c_3(\Gamma) = 1, \quad \text{else } h^n(G) = c_n(\Gamma) = 0.$$

Consequently G has cohomological dimension 3.

4.3 Applications to pro-p groups with quadratic presentation

In this part, we begin to prove Proposition 27, then we illustrate it with some examples. We say that G has a *quadratic presentation* if it is presented by a family of quadratic relations $l := \{l_i\}$ (i.e. l_i is in $F_2 \setminus F_3$).

4.3.1 Proof of Proposition 27

I am thankful to Thomas Weigel for the following argument. We also refer to [73] for further details.

Let us denote by $\Delta_\bullet(G)$ the graded algebra indexed by negative integers: $\Delta_\bullet(G) := \bigoplus_i \Delta_i(G)$ where $\Delta_i(G) := \mathscr{E}_{-i}(G)$. Following notations from Theorem [125, Theorem 5.1.12.(2)] and its proof, if the algebra $\mathscr{E}(G)$ is Koszul then $\mathrm{Ext}^{\bullet,\bullet}_{\Delta_\bullet(G)}$ is the quadratic dual of $\mathscr{E}(G)$ generated by $X_1, \ldots, X_d$ where every X_i is endowed with bidegree $(-1, 2)$. In particular, $\mathrm{Ext}^{s,t}_{\Delta_\bullet(G)} \neq 0$ only if $t = -2s$.

From Theorem [125, Theorem 5.1.12.(2)], we infer a spectral sequence $(E_r^{\bullet,\bullet}; d_r)$ and a filtration $F^\bullet$ on $H^\bullet(G)$ such that:

- $E_1^{\bullet,\bullet} = \mathrm{Ext}^{\bullet,\bullet}_{\Delta_\bullet(G)}(\mathbb{F}_p, \mathbb{F}_p)$,
- $E_\infty^{s,t} = F^s H^{s+t}(G)/F^{s+1}H^{s+t}(G)$.

In particular, we have $d_1 = 0$, so we infer an isomorphism of graded algebras $E_1^{\bullet,\bullet} \simeq E_\infty^{\bullet,\bullet}$. The filtration $F^\bullet$ on $H^\bullet(G)$ is decreasing and from the convergence of the spectral sequence, we obtain:

$$\cdots \supset F^{-(n+1)}H^n(G) = H^n(G) \supset F^{-n}H^n(G) = H^n(G) \supset F^{-(n-1)}H^n(G) = 0 \ldots$$

Consequently, we infer the following isomorphism of graded algebras:

$$H^\bullet(G;\mathbb{F}_p) \simeq \mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p;\mathbb{F}_p).$$

Remark 22. *We propose an alternative proof, using Serre's Lemma [69, Partie* 5*, Lemme* 2.1*], of the fact that we have an isomorphism of graded vetor spaces between* $H^\bullet(G;\mathbb{F}_p)$ *and* $\mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p;\mathbb{F}_p)$.

Let $\mathscr{P} := (\mathscr{P}_i, \delta_i)$ *be a Koszul resolution of* $\mathbb{F}_p$*, then there exists a* $E(G)$*-free resolution* $P := (P_i, d_i)$ *of* $\mathbb{F}_p$ *such that* $\mathrm{Grad}(P) := (\mathrm{Grad}(P_i), \mathrm{Grad}(d_i)) = \mathscr{P}$*, i.e. for every* i*,* $\mathrm{Grad}(P_i) = \mathscr{P}_i$ *and* $\mathrm{Grad}(d_i) = \delta_i$*. Moreover, there exits a family* $p_{i,j}$ *in* P_i *such that*

$$P_i := \prod_j p_{i,j}E(G) \quad \textit{and} \quad \mathscr{P}_i := \prod_j \overline{p_{i,j}}\mathscr{E}(G).$$

Since P_i *(resp.* $\mathscr{P}_i$*) is a free compact* $E(G)$*-module (resp. graded* $\mathscr{E}(G)$*-module), we infer two isomorphisms of discrete* $\mathbb{F}_p$*-vector spaces:*

$$Hom_{E(G)}(P_i;\mathbb{F}_p) \simeq \bigoplus_j p_{ij}^*\mathbb{F}_p, \quad \textit{and} \quad Hom_{\mathscr{E}(G)}(\mathscr{P}_i;\mathbb{F}_p) \simeq \bigoplus_j \overline{p_{ij}}^*\mathbb{F}_p,$$

where p_{ij}^* *(resp.* $\overline{p_{ij}}^*$*) is the function which maps* $\sum_l p_{il}e_l \in P_i$ *with* $e_l \in E(G)$ *(resp.* $\sum_l \overline{p_{il}}f_l \in \mathscr{P}_i$*, with* $f_l \in \mathscr{E}(G)$*) to* $\epsilon(e_j)$ *(resp.* $\epsilon(f_j)$*), for* ϵ *the augmentation map of* $E(G)$ *(or* $\mathscr{E}(G)$*).*

Define by $gr\colon Hom_{E(G)}(P_i;\mathbb{F}_p) \to Hom_{\mathscr{E}(G)}(\mathscr{P}_i;\mathbb{F}_p)$ *the morphism of* $\mathbb{F}_p$*-vector spaces which maps* p_{ij}^* *to* $\overline{p_{ij}}^*$*. We infer the following diagram of discrete* $\mathbb{F}_p$*-vector spaces:*

$$\begin{array}{ccccc}
Hom_{E(G)}(P_{i+1};\mathbb{F}_p) & \xleftarrow[d_{i+1}^*]{} & Hom_{E(G)}(P_i;\mathbb{F}_p) & \xleftarrow[d_i^*]{} & Hom_{E(G)}(P_{i-1};\mathbb{F}_p) \\
\downarrow gr & & \downarrow gr & & \downarrow gr \\
Hom_{\mathscr{E}(G)}(\mathscr{P}_{i+1};\mathbb{F}_p) & \xleftarrow[\delta_{i+1}^*]{} & Hom_{\mathscr{E}(G)}(\mathscr{P}_i;\mathbb{F}_p) & \xleftarrow[\delta_i^*]{} & Hom_{\mathscr{E}(G)}(\mathscr{P}_{i-1};\mathbb{F}_p)
\end{array}$$

Observe that the previous diagram is in general not commutative. Since the resolution $\mathscr{P}$ *is Koszul, we show that the previous diagram is indeed commutative. More precisely, we show that for every* i*, the map* d_i^* *is zero.*

Since d_i *is a filtered morphism, we can write* $d_i(p_{i,l}) := \sum_m p_{i-1,m}\sum_{k=1}^d \alpha_{k,m}X_k + c_{i,l}$ *with* $c_{i,l}$ *an element of degree strictly larger than* i *in* P_{i-1}*, and* $c_{i,l} := \sum_m p_{i-1,m}u_m$*. In*

particular, $\epsilon(u_m) = 0$. *Consequently, we have:*

$$\begin{aligned} d_i^*(p_{i-1,j}^*)(p_{i,l}) &= p_{i-1,j}^* \circ d_i(p_{i,l}) \\ &= p_{i-1,j}^* \left(\sum_m p_{i-1,m} \sum_{k=1}^{d} \alpha_{k,m} X_k + c_{i,l} \right) \\ &= p_{i-1,j}^* \left(\sum_m p_{i-1,m} (\sum_{k=1}^{d} \alpha_{k,m} X_k + u_m) \right) \\ &= \epsilon(\alpha_{k,j} X_k + u_j) \\ &= 0, \end{aligned}$$

therefore we have $d_i^* = 0$.

4.3.2 Free pro-p groups

Assume that G is a free pro-p group, then by the Magnus isomorphism, we infer $\mathscr{E}(G) \simeq \mathscr{E}$. Using Proposition 27, we obtain the well known result:

$$H^\bullet(G) \simeq \mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p; \mathbb{F}_p) = H^1(G).$$

4.3.3 Mild quadratic pro-p group

In this subsubsection, we slightly improve [98, Theorem 1.3].

From [29, Theorem 3.7], if G has a mild quadratic presentation, then $\mathscr{E}(G)$ is a quadratic algebra. In fact, in the proof of [98, Theorem 1.3], Mináč-Pasini-Quadrelli-Tân showed that the algebra $\mathscr{E}(G)$ is Koszul. Denote its quadratic dual by $\mathscr{A}(G)$ (see for instance [108, Chapter 1, Part 2] for more details).

Corollary 12. *Assume that* G *has a mild quadratic presentation. Then* $H^\bullet(G)$ *and* $\mathscr{E}(G)$ *are both quadratic algebras. Furthermore, we have:*

$$H^\bullet(G) \simeq \mathscr{A}(G).$$

Proof. Since $\mathscr{E}(G)$ is Koszul, we can apply Proposition 27. We infer

$$H^\bullet(G) \simeq \mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p; \mathbb{F}_p).$$

Furthermore $\mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p; \mathbb{F}_p) \simeq \mathscr{A}(G)$. Consequently:

$$H^\bullet(G) \simeq \mathrm{Ext}^\bullet_{\mathscr{E}(G)}(\mathbb{F}_p; \mathbb{F}_p) \simeq \mathscr{A}(G).$$

□

4.3.4 Pro-p Right Angled Artin Groups

We say that G_Γ is a Right Angled Artin Group (RAAG) if G_Γ admits a presentation $\mathscr{F}/S_\Gamma$ where $\mathscr{F}$ is the abstract free group on $\{x_1;\dots;x_d\}$ and S_Γ is a normal subgroup of $\mathscr{F}$ generated by $[x_i;x_j]$ for $(i,j)\in\mathbf{E}$.

We say that $G(\Gamma)$ is pro-p RAAG if $G(\Gamma)$ is the pro-p completion of G_Γ. The pro-p group $G(\Gamma)$ admits a presentation F/R_Γ where F is a free pro-p group over $\{x_1;\dots;x_d\}$ and R_Γ is a closed normal subgroup of F generated by $[x_i;x_j]$ for $(i,j)\in\mathbf{E}$.

The algebra $H^\bullet(G(\Gamma))$ is already known. Lorensen [76, Theorem 2.7] showed that

$$H^\bullet(G(\Gamma))\simeq H^\bullet(G_\Gamma).$$

It is also well-known, see [6], that $H^\bullet(G_\Gamma)\simeq\mathscr{A}(\Gamma)$. Consequently

Theorem 24. *Let $G(\Gamma)$ be pro-p RAAG, then we have the following isomorphism:*

$$H^\bullet(G(\Gamma))\simeq\mathscr{A}(\Gamma).$$

We propose another proof of Theorem 24.

Proposition 29. *Let G be a pro-p RAAG with underlying graph Γ, then we have $E(G)=E(\Gamma)$. Therefore, we infer:*

$$\mathscr{E}(G)\simeq\mathscr{E}(\Gamma),\quad \textit{and}\quad H^\bullet(G(\Gamma))\simeq\mathscr{A}(\Gamma).$$

Proof. Here, we just need to observe, following notations of Proposition 28, that $I=\Delta$. Then we infer, using Proposition 28, that $E(G)=E(\Gamma)$. From Lemma 11 and Proposition 28, we conclude that $\mathscr{E}(G)=\mathscr{E}(\Gamma)$.

Consequently, $\mathscr{E}(G)$ is quadratic and Koszul. We finish the proof using Proposition 27. □

Remark 23. *Observe that the $\mathbb{F}_p$-vector space C_Γ constructed in Subpart 20 does depend only on Γ. In particular, using Remark 20 and Proposition 29, we conclude that the filtered vector space C_Γ is isomorphic to the filtered vector space $E(\Gamma)$.*

4.3.5 Prescribed and restricted ramification

We finish this chapter by showing a more precise version (and a proof) of Theorem D:

Theorem 25 (Galois extensions with prescribed ramification and cohomology)**.** *Fix Γ and $l_{\mathbf{E}}$ satisfying the Condition (4.1). Then, there exist a totally imaginary field K and a set T of primes in K such that G_K^T, the Galois group of the maximal pro-p extension of K unramified outside p and which totally splits in T, is presented by set of generators $\{x_1;\dots;x_d\}$ and set of relations $l_{\mathbf{A}}$ satisfying the Condition (4.1).*

Furthermore, there exist a quotient G of G_K^T satisfying $\mathscr{E}(G)\simeq\mathscr{E}(\Gamma)$. In particular, $H^\bullet(G)\simeq\mathscr{A}(\Gamma)$.

Proof. Take $k := \mathbb{Q}(\sqrt{-p})$ and define k_p the maximal p-extension of k unramified outside places above p in k. From [80, Proof of Corollary 4.6] we observe that p is coprime to the class number of k. Consequently, from [59, Theorems 11.5 and 11.8] we infer that $G_k := \mathrm{Gal}(k_p/k)$ is a free pro-p group with 2 generators.

Let F be an open subgroup of G_k with index $|G_k : F|$ larger than d. Then using the Schreier formula (see [102, Theorem 3.3.16]), we infer that the group F is pro-p free with $d' := 1 + |G_k : F|$ generators. Let K be the fixed subfield of k_p by F. Observe that K_p, the maximal p-extension of K unramified outside places in K above p, is equal to k_p, and so $F := \mathrm{Gal}(k_p/K) = G_K$. We define $V' := [\![d+1; d']\!]$.

By the Chebotarev Density Theorem (see for instance [45, Part 2]), there exists a set of primes $T := \{p_{ij}, p_v\}_{(i,j)\in\mathbf{A}, v\in V'}$ in K with Frobenius elements σ_{ij} (resp. σ_v) in F conjugated to an element l_{ij} (resp. l_v) in F satisfying $l_{ij} \equiv [x_i; x_j] \pmod{F_3}$ (resp. $l_v \equiv x_v \pmod{F_3}$). Define $R_{\mathbf{A}}$ the normal closed subgroup of G_K generated by $l_{\mathbf{A}}$ and $l_{V'}$, then we infer $G_K^T = G_K/R_{\mathbf{A}}$, which is mild presented by generators $\{x_1; \ldots; x_d\}$ and set of relations $l_{\mathbf{A}}$ satisfying the Condition (4.1). Introduce K_p^T the maximal Galois subextension of K_p which totally splits in T.

Define $R_{\mathbf{B}}$ the closed normal subgroup of G_K^T generated by images of $l_{\mathbf{B}} := \{l_{uv} := [x_u; x_v]; (u,v) \in \mathbf{B}\}$, and $K(\Gamma)$ the fixed subfield of K_p^T by $R_{\mathbf{B}}$. Then a presentation of $G := \mathrm{Gal}(K(\Gamma)/K)$ is given by F/R, where F is the free pro-p group generated by $\{x_1; \ldots; x_d\}$ and R is the closed normal subgroup of F generated by the family $l_{\mathbf{E}}$.

Since $l_{\mathbf{E}}$ satisfies the Condition (4.1), using Theorem E, we infer that

$$\mathscr{E}(G) \simeq \mathscr{E}(\Gamma).$$

Using Proposition 27, we conclude that:

$$H^\bullet(G) \simeq \mathscr{A}(\Gamma).$$

□

Corollary 13. *For every integer n, there exists an integer $d > n$, a totally imaginary field K and a set T of primes in K such that the Galois group G_K^T:*

(*i*) *is mild on d generators,*

(*ii*) *admits a quotient G presented by d generators and of cohomological dimension n.*

Proof. The case $n = 1$ and $n = 2$ are already well-known. The case $n \geq 3$ is a consequence of Theorem 25. We give more details below.

If $n = 1$, we can take $K := \mathbb{Q}(\sqrt{-p})$ (or the field K given in the proof of Theorem 25), and T empty. Then, as showed in the proof of Theorem 25, the group $G := G_K^\emptyset$ is a free pro-p group with $d = 2$ generators, so of cohomological dimension 1.

From now, we fix $\Gamma_{\mathbf{A}}$ a graph with 3 vertices $\{1; 2; 3\}$ and two edges: $\{1; 2\}$ and $\{1; 3\}$. The graph $\Gamma_{\mathbf{A}}$ is bipartite.

If $n = 2$, we take for instance $\Gamma := \Gamma_{\mathbf{A}}$, and we apply Theorem 25. Consequently we infer a field K and a set T of primes such that the group $G := G_K^T$ is mild presented by $d = 3$ generators, so of cohomological dimension 2.

If $n \geq 3$, take $\Gamma := \Gamma_{\mathbf{A}} \sqcup \Gamma_{\mathbf{B}}$, where $\Gamma_{\mathbf{B}}$ is the complete graph on n vertices. The graph $\Gamma_{\mathbf{A}}$ satisfies the Condition (4.1), has clique number n, and admits $d = n+3$ vertices. Then $\mathscr{A}(\Gamma)$ has cohomological dimension n and admits d generators. We conclude with Theorem 25. $\square$

Chapter 5

On maximal extensions of Pythagorean fields and oriented Graph products

Context

Absolute Galois groups and their quotients play a fundamental role in field theory. For instance, Neukirch and Uchida [129] showed that number fields are determined by their absolute Galois groups. However, notice that p-Sylows of absolute Galois groups are not sufficient for determining underlying fields (see [77]).

In this chapter, we are interested in the class $\mathscr{P}$ of maximal pro-2 extensions of formally real Pythagorean fields of finite type (that we denote by RPF). These fields, and their pro-2 absolute Galois groups, were investigated by Mináč-Spira [87], [94], [88] and [95], Marshall [82], Jacob [51] and Lam [67]. As a consequence of Milnor's conjecture [86] (see also [55]), Witt rings, pro-2 absolute Galois groups and their cohomology are strongly connected to the set of orderings of RPF fields, which are sufficient to characterize them (see [82]). Let us quote Voedvodsky [133] and De Clercq-Florence [17, Part 14.1] (partial proof) for resolution of this conjecture.

Mináč in [87] describes the class $\mathscr{P}$ as the minimal class of pro-2 groups containing $\Delta := \mathbb{Z}/2\mathbb{Z}$ stable by coproducts and some semi-direct products, and Mináč-Spira [94] and [95] showed that RPF fields are characterised by the third Zassenhaus quotient of their pro-2 absolute Galois groups. The goal of this work is to study explicit presentations on $\mathscr{P}$.

For this purpose, we relate the class $\mathscr{P}$ to the well known class of pro-p Right Angled Artin Groups (RAAGs): we refer to [6] for a general introduction. Snopce and Zalesski [122, Theorem 1.2] gave a criterion, on the underlying graphs, for RAAGs occuring as pro-p absolute Galois groups. Blumer, Quadrelli and Weigel [7, Theorem 1.1.(i)] also introduced pro-p oriented RAAGs and characterise, from the underlying graph, the ones who are pro-p absolute Galois groups.

Let us now precisely introduce the main results of this chapter.

The class of Δ-RAAGs

Let $\Delta := \mathbb{Z}/2\mathbb{Z}$ be the multiplicative group of two elements generated by x_0, and let us introduce a class of pro-2 groups that we call Δ-RAAGs; these groups are semi-direct products of (pro-2)-Right Angled Artin Groups by Δ, where the action inverts a "natural" set of generators. More concretely, consider $\Gamma := (\mathbf{X}; \mathbf{E})$ an undirected graph with d vertices $\{1; \dots; d\}$, and denote by $c_n(\Gamma)$ the number of n-cliques of Γ, i.e. maximal subgraphs with n vertices. We say that G_Γ is a pro-2 right Angled Artin Group (RAAG), if we have a presentation:

$$1 \to R \to F \to G_\Gamma \to 1,$$

where $F := F(d)$ is the free pro-2 group on d generators $\{x_1; \dots; x_d\}$ and R is the normal closed subgroup of G_Γ generated by $\{[x_i; x_j]\}_{\{i;j\} \in \mathbf{E}}$ and $[x_i; x_j] := x_i^{-1} x_j^{-1} x_i x_j$.

From [44, Proposition 3.16], we can define an action:

$$\delta \colon \Delta \to \mathrm{Aut}(G_\Gamma), \quad \text{such that } \delta(x_0)(x_i) := x_i^{-1}.$$

We set $G_{\Gamma,\Delta} := G_\Gamma \rtimes_\delta \Delta$, and we define by Δ-RAAGs the class with all objects given by $G_{\Gamma,\Delta}$ where Γ varies along all graphs. Similarly to the class $\mathscr{P}$, the class of Δ-RAAGs is stable by coproducts (see Theorem 30) and by some specific semi-direct products (see Remark 25). The study of Δ-RAAGs is motivated by Proposition 30, which allows us to recover the Zassenhaus filtration of a Δ-RAAG from its underlying graph.

Our results

Let K be a field of characteristic different from 2 and denote by G_K its pro-2 absolute Galois group. Define $L := K(\sqrt{-1})$ and G_L its pro-2 absolute Galois group. We assume that K is a formally real Pythagorean field of finite type (that we denote by RPF), i.e. (i) -1 is not a square, (ii) the sum of two squares is a square, (iii) the group $K^\times/K^{2\times}$ is finite.

Observe that $\Delta \simeq \mathrm{Gal}(L/K)$ and we have an exact sequence of pro-2 groups:

$$1 \to G_L \to G_K \to \Delta \to 1. \tag{5.1}$$

We infer the following result, related to [122, Theorem 1.2] and [7, Theorem 1.1].

Theorem F. *If K is RPF, then the exact sequence* (5.1) *splits, G_L is RAAG and G_K is Δ-RAAG. Conversely, if a Δ-RAAG occurs as a pro-2 absolute Galois group over a field K, then K is RPF.*

As a corollary, we infer:

Corollary. *The pro-2 group*

$$G := < x_1, x_2, x_3, x_4 | \quad [x_1, x_2] = 1, [x_3, x_4] = 1, x_0^2 = 1, x_0 x_j x_0 x_j = 1, \forall j \in [\![1; 4]\!] >$$

does not occur as a pro-2 absolute Galois group.

Mináč and Tân introduced two conjectures characterising pro-p absolute Galois groups among all pro-p groups: the Massey vanishing and the Kernel unipotent conjectures [96]. Contrary to the Kernel unipotent conjecture, the Massey vanishing conjecture was well investigated, see for instance [97] and [47]. Snopce-Zalesski [122], Blumer, Quadrelli and Weigel [7, Corollary 1.2] showed that all pro-p oriented RAAGs occuring as pro-p absolute Galois groups satisfy the Massey vanishing conjecture. Quadrelli [110] also showed that $\mathscr{P}$ satisfies the Massey vanishing conjecture.

Theorem G. *Assume that G is either a pro-p RAAG or a Δ-RAAG occuring as an absolute Galois group, then G satisfies the Kernel unipotent conjecture.*

Structure of the chapter

We begin by studying the Zassenhaus filtration of Δ-RAAGs. Then we show that the class $\mathscr{P}$ is a subclass of Δ-RAAGs. We also prove in this chapter that $\mathscr{P}$ satisfies the Kernel unipotent conjecture. Finally, using our filtrations' results, we observe that Δ-RAAGs which occur as pro-2 absolute Galois groups have necessarily underlying RPF fields. As an application, we give an example of Δ-RAAG which is not an absolute Galois group for any field.

Notations

We introduce useful notations for the chapter.

Algebraic Notation

• We denote by $F(d)$ the free pro-2 group on d generators (or F when the number of generators is clear from the context).

• We recall that G is a finitely presented pro-2 groups with generators $\{x_0; x_1; \dots; x_d\}$ and relations $\{l_1; \dots; l_r\}$. We have the presentation $1 \to R \to F \to G \to 1$, where F is the free pro-2 group with generators $\{x_0; x_1; \dots; x_d\}$ and R is the normal closed subgroup of F generated by $\{l_1; \dots; l_r\}$.

• We define $H^n(G)$ the n-th (continuous) cohomology group of the trivial (continuous) G-module $\mathbb{F}_2$. The cohomological dimension of G is the smallest integer n (which can be infinite) such that for every $m > n$ we have $H^m(G) = 0$.

• Let us denote by $E(G)$ the completed group algebra of G over $\mathbb{F}_2$, and $E_n(G)$ the n-th power of the augmentation ideal of $E(G)$.

• The Zassenhaus filtration of G is defined by $G_n = \{g \in G; \phi(g-1) \in E_n(G)\}$, and we introduce

$$\mathscr{L}(G) := \bigoplus_{n\in\mathbb{N}} G_n/G_{n+1}, \quad \text{and} \quad \mathscr{E}(G) := \bigoplus_{n\in\mathbb{N}} E_n(G)/E_{n+1}(G).$$

We call $\mathscr{L}$ (resp. $\mathscr{E}$) the free graded Lie algebra (resp. graded algebra) on $\{X_1; \dots; X_d\}$ over $\mathbb{F}_2$.

• Finally, we define the gocha series of G by:

$$gocha(G,t) := \sum_{n=0}^{\infty} c_n t^n, \quad \text{where} \qquad c_n := \dim_{\mathbb{F}_2} E_n(G)/E_{n+1}(G)$$

Graphs notations

We introduce a few notations related to graphs.

• Let $\Gamma := (\mathbf{X}, \mathbf{E})$ be a graph with d vertices. We denote by $\coprod$ the disjoint union of graphs and ∇ the join. We introduce $c_n(\Gamma)$ the number of n-cliques of Γ, i.e. maximal complete subgraphs with n vertices and the polynomial

$$\Gamma(t) := \sum_n c_n(\Gamma) t^n.$$

• We denote RAAGs by G_Γ, with $\{x_1; \dots; x_d\}$ as a (canonical) set of generators of G_Γ. We define δ an action of Δ on G_Γ by $\delta(x_0).x_j = x_j^{-1}$. We say that a group is Δ-RAAG, if we can write it as:

$$G_{\Gamma,\Delta} := G_\Gamma \rtimes_\delta \Delta.$$

Finally, we denote by $\mathscr{E}_\Gamma$ the quotient of the algebra of noncommutative polynomials on $\{X_1; \dots; X_d\}$ over $\mathbb{F}_2$ by the two-sided ideal generated by $\{[X_i; X_j]\}_{\{i;j\}\in\mathbf{E}}$. We call $\mathscr{A}_\Gamma$ its quadratic dual.

5.1 The class of Δ-RAAGs

In this part, we study the Zassenhaus filtration on Δ-RAAGs.

5.1.1 Filtrations on Δ-RAAGs

We begin by a result on the Frattini subgroup of Δ-RAAGs.

Lemma 13. *We have* $[G_{\Gamma,\Delta}; G_{\Gamma,\Delta}] = G_{\Gamma,\Delta,2} = G_{\Gamma,2}$.

Proof. For this proof, we use the following equalities:

(*i*) $[x,y] = x^{-2}(xy^{-1})^2y^2$,

(*ii*) $[x_0; x_i] = x_0x_ix_0x_i^{-1} = x_i^{-2}$

From (*i*), we observe that $[G_{\Gamma,\Delta}; G_{\Gamma,\Delta}] \subset G_{\Gamma,\Delta,2}$.

Let us show that $G_{\Gamma,\Delta,2} \subset G_{\Gamma,2}$. Take $x \in G_{\Gamma,2}$. Up to an open subgroup, we can write

$$x := (x_{i_1} \dots x_{i_n})^2,$$

with x_{i_l} in $\{x_0;\dots;x_d,x_1^{-1},\dots,x_d^{-1}\}$.
Consequently, $x\equiv x_{i_1}^2\dots x_{i_n}^2 \pmod{[G_{\Gamma,\Delta};G_{\Gamma,\Delta}]}$ is an element in $G_{\Gamma,\Delta,2}$.

Now, we conclude by showing that $G_{\Gamma,2}\subset[G_{\Gamma,\Delta};G_{\Gamma,\Delta}]$. Again, we take x in $G_{\Gamma,2}$. Then up to an open subgroup, we infer that $x\equiv x_{i_1}^2\dots x_{i_n}^2 \pmod{[G_\Gamma,G_\Gamma]}$, which is from (ii) an element in $[G_{\Gamma,\Delta};G_{\Gamma,\Delta}]$.

□

Let us now infer general results on the Zassenhaus filtrations of Δ-RAAGs.

Proposition 30 (Zassenhaus filtration of Δ-RAAGs)**.** *For every $n\geq 2$, we have:*

$$G_{\Gamma,n}=G_{\Gamma,\Delta,n}.$$

Proof. The proof is done by induction. First we have

$$[G_{\Gamma,\Delta};G_{\Gamma,\Delta}]=G_{\Gamma,\Delta}^2=G_\Gamma^2.$$

Assume $n>2$, then from [19, Theorem 12.9], we have:

$$\begin{aligned}G_{\Gamma,n}&=G_{\Gamma,\lceil n/2\rceil}^2\prod_{i+j=n}[G_{\Gamma,i};G_{\Gamma,j}]\\&=G_{\Gamma,\Delta,\lceil n/2\rceil}^2\prod_{i+j=n}[G_{\Gamma,\Delta,i};G_{\Gamma,\Delta,j}]\\&=G_{\Gamma,\Delta,n}.\end{aligned}$$

□

5.1.2 Third Zassenhaus quotient of Δ-RAAGs

In this part, we study the group $\mathscr{G}_{\Gamma,\Delta}:=G_{\Gamma,\Delta}/G_{\Gamma,\Delta,3}$, where $G_3:=G^4[G^2;G]$. Let us recall that this third Zassenhaus quotient plays a fundamental role in the study of absolute Galois group of RPF, which is called Witt group in that context. We refer to [94] and [95] for further details.

Lemma 14. *We have:*

$$\mathscr{G}_{\Gamma,\Delta}\simeq G_\Gamma/G_{\Gamma,3}\rtimes\Delta,$$

where the action is given by inversion of generators, i.e. $x_0x_ix_0=x_i^{-1}$.

Proof. From Proposition 30, we infer:

$$G_\Gamma\cap G_{\Gamma,\Delta,3}=G_\Gamma\cap G_{\Gamma,3}=G_{\Gamma,3}.$$

Consequently, we obtain an exact sequence:

$$1\to G_\Gamma/G_{\Gamma,3}\to\mathscr{G}_{\Gamma;\Delta}\to\Delta\to 1,$$

which splits and the action of Δ on $G_\Gamma/G_{\Gamma,3}$ is given by $x_0x_ix_0=x_i^{-1}$. □

Corollary 14. *We have*

$$\mathscr{G}_{\Gamma,\Delta}^2 = [\mathscr{G}_{\Gamma,\Delta}; \mathscr{G}_{\Gamma,\Delta}].$$

Proof. Since $\mathscr{G}$ is a 2-group, we have the inclusion $[\mathscr{G}_{\Gamma,\Delta}; \mathscr{G}_{\Gamma,\Delta}] \subset \mathscr{G}^2$.

Let us show the reverse inclusion. We have:

$$\begin{aligned}
[\mathscr{G}_{\Gamma,\Delta}; \mathscr{G}_{\Gamma,\Delta}] &= [G_{\Gamma,\Delta}/G_{\Gamma,\Delta,3}; G_{\Gamma,\Delta}/G_{\Gamma,\Delta,3}] \\
&= [G_{\Gamma,\Delta}; G_{\Gamma,\Delta}]G_{\Gamma,\Delta,3}/G_{\Gamma,\Delta,3} \\
&= G_{\Gamma,\Delta}^2 G_{\Gamma,\Delta,3}/G_{\Gamma,\Delta,3} \\
&= \mathscr{G}_{\Gamma,\Delta}^2.
\end{aligned}$$

□

Remark 24. *Some results of the previous parts were already proved by Mináč-Rogelstad-Tân. We refer to [92, Corollary* 4.8 *and Lemma* 4.12*].*

5.1.3 Gocha series and associated graded algebras

Let us define $\mathscr{J}_{\Gamma,\Delta}$ (resp. $\mathscr{L}(\mathscr{J}_{\Gamma,\Delta})$) by the two-sided ideal of $\mathscr{E}$ (resp. $\mathscr{L}$) generated by:

$$\{[X_i, X_j], \quad \text{and} \quad [X_0; X_k] + X_k^2\}_{(i,j)\in\mathbf{E} \text{ and } 0\leq k\leq d}.$$

We introduce

$$\mathscr{E}_{\Gamma,\Delta} := \mathscr{E}/\mathscr{J}_{\Gamma,\Delta}, \quad \text{and} \quad \mathscr{L}_{\Gamma,\Delta} := \mathscr{L}/\mathscr{L}(\mathscr{J}_{\Gamma,\Delta}).$$

Lemma 15. *We have an isomorphism of graded-$\mathbb{F}_2$ Lie algebras:*

$$\mathscr{L}(G_{\Gamma,\Delta}) \simeq \mathscr{L}_{\Gamma,\Delta}.$$

Proof. Observe first that $\mathscr{L}_{\Gamma,\Delta}$ is a semi-direct product of the Lie-algebra $\mathscr{L}_\Gamma$ by $\mathbb{F}_2 :=< x_0 >$, where the action of x_0 on $\mathscr{L}_\Gamma$ is given by: $x_0 x_i x_0 := x_i^{-1}$.

As graded vector spaces, we have from Proposition 30:

$$\mathscr{L}_1(G_{\Gamma,\Delta}) \simeq \mathbb{F}_2 \bigoplus \mathscr{L}_1(G_\Gamma), \quad \text{and for } n \geq 2, \quad \mathscr{L}_n(G_{\Gamma,\Delta}) \simeq \mathscr{L}_n(G_\Gamma).$$

Consequently, from Proposition 30, we have an isomorphism of graded vector spaces:

$$\mathscr{L}(G_{\Gamma,\Delta}) \simeq \mathscr{L}_{\Gamma,\Delta}.$$

To conclude, we just need to define an epimorphism between $\mathscr{L}_{\Gamma,\Delta}$ and $\mathscr{L}(G_{\Gamma,\Delta})$. This is easy, we have an epimorphism:

$$u\colon \mathscr{L} \to \mathscr{L}(G_{\Gamma,\Delta}), \quad x_i \mapsto x_i.$$

Furthermore, $u([x_i, x_j]) = 0$ and $u([x_0; x_k] + x_k^2) = 0$. Therefore u factors through an epimorphism from $\mathscr{L}_{\Gamma,\Delta}$ to $\mathscr{L}(G_{\Gamma,\Delta})$. □

Theorem 26. *We have*

$$\mathscr{E}(G_{\Gamma,\Delta}) \simeq \mathscr{E}_{\Gamma,\Delta}, \quad \textit{and} \quad gocha(G_{\Gamma,\Delta}, t) = \frac{1+t}{\Gamma(-t)}.$$

Proof. The algebra $\mathscr{E}_{\Gamma,\Delta}$ is the universal envelope of $\mathscr{L}_{\Gamma,\Delta}$. Consequently, using the previous Lemma and Jennings-Lazard formula, we deduce that $\mathscr{E}_{\Gamma,\Delta} \simeq \mathscr{E}(G_{\Gamma,\Delta})$.

Recall that

$$\mathscr{L}_1(G_{\Gamma,\Delta}) \simeq \mathbb{F}_2 \bigoplus \mathscr{L}_{\Gamma,1}, \quad \text{and for } n \geq 2, \quad \mathscr{L}_n(G_{\Gamma,\Delta}) \simeq \mathscr{L}_{\Gamma,n}.$$

Then, from Jennings-Lazard formula [69, Proposition 3.10, Appendice A], we infer:

$$gocha(G_{\Gamma,\Delta}, t) = (1+t) \times gocha(G_\Gamma, t) = \frac{1+t}{\Gamma(-t)}.$$

□

5.2 Pythagorean fields

Let us recall that we denote by G_K (resp. G_L) the pro-2 quotient of the absolute Galois group of a RPF K (resp. of $L := K(\sqrt{-1})$). In Corollary 15, we show that $G_K/G_K^2 \simeq G_L/G_L^2 \times \Delta$, where Δ is a subgroup of order 2 of G_K. Consequently, we define a system of generators of G_K, by $\{x_0, x_1, \ldots, x_d\}$ where x_0 is the generator of Δ and $\{x_1, \ldots, x_d\}$ is a set of generators of G_L.

5.2.1 Semi-direct product and PYT groups

The main goal of this part is to show the following result:

Theorem 27. *Assume that K is RPF. Then there exists a graph Γ such that $G_K = G_{\Gamma,\Delta}$ and $G_L = G_\Gamma$. Consequently:*

$$G_K = G_L \rtimes_\delta \Delta,$$

where $\delta(x_0).x_i := x_i^{-1}$.

We introduce several results before proving Theorem 27. First, we show that we can write G_K as a semi-direct product of G_L by Δ. For this purpose, let us recall [87, Proposition]:

Proposition 31 (Mináč)**.** *There exists a unique morphism $\phi\colon G_K \to \Delta$ such that $\phi(\sigma) = x_0$ for every involution σ in G_K. Furthermore,* $\ker(\phi) = G_L$.

To conclude that G_K is a semi-direct product, this is sufficient to show that the morphism ϕ defined in Proposition 31 admits a section. For this purpose, we will use [92, Proposition 4.9]. Before, let us recall the following definition:

Definition 29 (SAP and superpythagorean fields)**.** *We say that K is*

- *SAP if $G_K = G_{\Gamma_N,\Delta} = F(d) \rtimes_\delta \Delta$, where Γ_N is the free graph on d vertices (i.e. no edges),*
- *superpythagorean if $G_K = G_{\Gamma_C,\Delta} = \mathbb{Z}_2^d \rtimes_\delta \Delta$, where Γ_C is the complete graph on d vertices.*

Example 23. *We give here few examples of RPF fields. We refer to [67, Chapter 8, Part 4] for more examples and further details.*

• *As a first example, we can take $K := \mathbb{R}$. Then $\mathbb{R}$ is RPF and both SAP and superpythagorean. Indeed, we have $G_{\mathbb{R}} \simeq \Delta = \Gamma_{\emptyset,\Delta}$, where $\emptyset$ is the empty graph.*

• *As a second example, let us take $K := \mathbb{R}((x_1))\dots((x_d))$, the field of iterated Laurent series over K. Then, the field K is RPF, and superpythagorean, i.e. we have $G_K = G_{\Gamma_C,\Delta}$, where Γ_C is the complete graph on d vertices.*

Let us recall [92, Theorem 4.2 and Proposition 4.9] with full details:

Proposition 32 (Mináč, Rogelstad, Tân)**.** *For every integer d, there exists two RPF fields N and C satisfying $|C^\times/C^{\times 2}| = |N^\times/N^{\times 2}| = 2^{d+1}$ such that N is SAP, C is superpythagorean. Furthermore, if we fix K a RPF with $|K^\times/K^{\times 2}| = 2^{d+1}$, there exists C and D as before, such that the following commutative diagram, with exact rows, holds:*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & F(d) & \longrightarrow & G_N & \xrightarrow{n} & \Delta & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \pi_N} & & \downarrow & & \\
1 & \longrightarrow & G_L & \longrightarrow & G_K & \xrightarrow{\phi_K} & \Delta & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \pi_C} & & \downarrow & & \\
1 & \longrightarrow & \mathbb{Z}_2^d & \longrightarrow & G_C & \xrightarrow{c} & \Delta & \longrightarrow & 1
\end{array}$$

Furthermore the columns are all epimorphisms, and the first and last rows split.

We are now able to prove the following result

Theorem 28. *There exists a unique morphism $\phi_K \colon G_K \to \Delta$ such that:*

(i) for every involution $\sigma \in G_K$, we have $\phi(\sigma) = x_0$

(ii) the kernel of ϕ_K is G_L,

(iii) the morphism ϕ_K admits a section ψ_K.

Proof. By Proposition 31, the morphism ϕ_K satisfies *(i)* and *(ii)*. Let us show that ϕ_K satisfies *(iii)*.

The maps ϕ_N and ϕ_C introduced in Proposition 32 admit sections ψ_N and ψ_C. Let us define $\psi_K := \pi_N \circ \psi_N$. It is indeed a section of ϕ_K: from Proposition 32 we have

$$\phi_K \circ \psi_K(x_0) = \phi_C \circ \pi_C \circ \pi_N \circ \psi_N(x_0) = x_0.$$

□

Consequently, if K is RPF, we can write:

$$G_K := G_L \rtimes_{\psi_K} \Delta.$$

Corollary 15. *We have $G_K/G_K^2 \simeq G_L/G_L^2 \times \Delta$.*

Proof. Let us use the notations from Proposition 32. Since G_N and G_C are Δ-RAAGs and $G_K^2 \subset G_L$, we deduce from Proposition 32 that $G_K^2 = G_L^2$. Consequently,

$$G_K/G_K^2 \simeq (G_K/G_L) \times (G_L/G_L^2) \simeq \Delta \times G_L/G_L^2.$$

Alternatively, we can also show this result directly using Kummer Theory. □

5.2.2 Mináč' structural results

Let V be an abelian pro-2 groups and $G := H \rtimes_\psi \Delta$ be a semi-direct product, where H is also a pro-2 group.

Definition 30 (Semi-trivial action)**.** *We define an action, that we call semi-trivial and denote by i_V, of G on V by:*

- *for every $h \in H$ and $v \in V$, $i_V(h).v = v$,*
- *for every $v \in V$, $i_V(x_0).v = -v$.*

Remark 25. *Observe that:*

$$V \rtimes_{i_V} G \simeq (V \times H) \rtimes_{i_V \times \psi} \Delta.$$

The action $i_V \times \psi$ of Δ on $V \times H$ is defined by:

- *$(i_V \times \psi)(x_0).h := \psi(h)$ for every $h \in H$,*
- *$(i_V \times \psi)(x_0).v := i_V(x_0).v = -v$ for every $v \in V$.*

Consequently, if we take $V = \mathbb{Z}_2^d$ and Γ_C the complete graph on d vertices, then we have:

$$V \rtimes_{i_V} G_{\Gamma,\Delta} \simeq G_{(\Gamma_C \nabla \Gamma),\Delta},$$

where ∇ denotes the join operation of graphs.
Thus if G is Δ-RAAG, then $V \rtimes_{i_V} G$ is also Δ-RAAG.

Let us recall [87, Theorem]:

Theorem 29. *The class $\mathscr{P}$ is exactly the minimal class of pro-2 groups satisfying the following conditions:*

(i) the group Δ is in $\mathscr{P}$,

(*ii*) *if* $G_1, \dots, G_m$ *are in* $\mathscr{P}$*, then* $G_1 \coprod G_2 \coprod \cdots \coprod G_m$ *is also in* $\mathscr{P}$*,*

(*iii*) *if* n *is an integer and* G_K *is in* $\mathscr{P}$*, then* $\mathbb{Z}_2^n \rtimes_{i_{\mathbb{Z}_2^n}} G_K$ *is in* $\mathscr{P}$*.*

Explanation of the minimality. Observe that $\Delta = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = G_{\mathbb{R}}$ is in $\mathscr{P}$. In [87, Theorem],Ináč showed that the class $\mathscr{P}$ satisfies conditions (*ii*) and (*iii*).Ináč also showed the following alternative, if G_K is in $\mathscr{P}$, then either:

- $G_K = \Delta$,
- or there exists an integer $s > 1$ and a family $G_1, \dots, G_s$ in $\mathscr{P}$ such that $G_K = \coprod_{i=1}^{s} G_i$,
- or, there exists an integer $m > 0$ and a group G in $\mathscr{P}$ such that $G = \mathbb{Z}_2^r \rtimes_i G_K$.

Then we can conclude by strong induction on the number of generators of G_K. □

5.2.3 Structure of G_L

Let us recall from Theorem 28 that we can write $G_K \simeq G_L \rtimes_{\psi_K} \Delta$. From Theorem 29, we study the structure of G_L.

Semi direct products

Assume there exists a group G_{K_1} in $\mathscr{P}$, and an integer n such that $G_K \simeq \mathbb{Z}_2^n \rtimes_i G_{K_1}$. Let us compare G_L and G_{L_1}:

Corollary 16. *We have* $G_L \simeq \mathbb{Z}_2^n \times G_{L_1}$*.*

Proof. From Remark 25, we have:

$$G_K \simeq \mathbb{Z}_2^n \rtimes_i \left(G_{L_1} \rtimes_{\psi_{K_1}} \Delta\right) \simeq (\mathbb{Z}_2^n \times G_{L_1}) \rtimes_{\psi_{K_1} \times i} \Delta.$$

From Theorem 28, G_{L_1} does not have involution, then $G_{L_1} \times \mathbb{Z}_2^n$ also does not. So by Theorem 28, we conclude that $G_L \simeq G_{L_1} \times \mathbb{Z}_2^n$. □

Coproducts

Here we assume that there exists two fields K_1 and K_2 such that $G_K = G_{K_1} \coprod G_{K_2}$. We study G_L from G_{L_1} and G_{L_2}.

First, we need to introduce a technical result, which will also be useful later.

Theorem 30. *Let* f *(resp.* g*) be an action of* Δ *on a finitely generated pro-2 group* A *(resp.* B*). Then*

$$(A \rtimes_f \Delta) \coprod (B \rtimes_g \Delta) \simeq \left(A \coprod B \coprod \mathbb{Z}_2\right) \rtimes_{f*g} \Delta,$$

where $f * g$ *is an action of* Δ *on* $A \coprod B \coprod \mathbb{Z}_2$ *which*

- *acts on A by f,*
- *acts on B by g,*
- *and acts on $\mathbb{Z}_2$ by inversion.*

Theorem 30 is a consequence of [102, Theorem (4.2.1)], which is a profinite version of the Kurosh subgroup Theorem:

Theorem 31. *Let $G_1, \dots, G_n$ be a collection of finitely generated pro-p groups. Assume that $G = \coprod_{i=1}^{n} G_i$ and H is an open subgroup of G. Define $S_i := \bigcup_{j=1}^{n_i} \{s_{i,j}\}$ where $1 \leq i \leq n$ and $n_i = |S_i|$ a system of cosets representatives satisfying:*

$$G = \bigcup_{i=1}^{n} \left(\bigcup_{j=1}^{n_i} G_i s_{i,j} H \right).$$

Then

$$H = \coprod_{i=1}^{n} \left(\coprod_{j=1}^{n_i} G_i^{s_{i,j}} \cap H \right) \coprod \mathbb{Z}_p^d,$$

where

$$d = \sum_{i=1}^{n} ([G : h] - n_i) - [G : H] + 1, \quad \text{and} \quad G_i^{s_{i,j}} = s_{i,j} G_i s_{i,j}^{-1}.$$

Let us now prove Theorem 30

Proof Theorem 30. Let $\{a_i\}$ (resp. $\{b_i\}$) be a minimal system of generators of A (resp. B). Take x_A (resp. x_B) an element of order 2 in $A \rtimes_f \Delta$ (resp. $B \rtimes_g \Delta$).

Now, let us define a map $\phi \colon G \to \Delta$ by:

- $\phi(a) = 0$ for every $a \in A$,
- $\phi(b) = 0$ for every $b \in B$,
- $\phi(x_A) = x_0$ and $\phi(x_B) = x_0$.

We introduce $H := \ker(\phi)$, which is closed and of finite index, so open in G. We apply Theorem [102, Theorem (4.2.1)] by taking $G_A := A \rtimes_f \Delta$, $G_B := B \rtimes_g \Delta$, $S_A := \{1\}$ and $S_B := \{1\}$.

Let us observe that $G = G_A 1 H = G_B 1 H$. Indeed, if we take g in G, then up to a topological argument, there exists h in H such that:

$$g := \prod_{k=1}^{n} \left(a_{i_k}^{\alpha_{i_k}} x_A^{\beta_{i_k}} b_{i_k}^{\gamma_{i_k}} x_B^{\delta_{i_k}} \right) \times h,$$

where $\alpha_{i_k}, \gamma_{i_k}$ are integers and $\beta_{i_k}, \delta_{i_k}$ are in $\{0; 1\}$. We conclude using that $[x_i; G_j] \subset H$ for $i, j \in \{A, B\}$, and $x_A x_B$ and $x_B x_A$ are in H.

Then $G := G_A \coprod G_B$, S_A and S_B satisfy the hypothesis of Theorem [102, Theorem (4.2.1)]. Moreover, $G_A \cap H = A$ and $G_B \cap H = B$. Therefore from Theorem [102, Theorem (4.2.1)], we conclude that:

$$H \simeq A \coprod B \coprod \mathbb{Z}_2.$$

Furthermore $\mathbb{Z}_2$ is generated by $x_A x_B$ as a subgroup of G. The map $\psi\colon \Delta \to G$, which maps x_0 to x_A defines a section of ϕ, and induces an action of Δ on H which is precisely defined by $f * g$.

□

We now infer results on the structure of G_L..

Corollary 17. *We have:*

$$G_L = G_{L_1} \coprod G_{L_2} \coprod \mathbb{Z}_2.$$

Proof. From Theorem 28, we have $G_K \simeq G_L \rtimes_{\psi_K} \Delta$, and from Theorem 30 we have $G_K \simeq (G_{L_1} \coprod G_{L_2} \coprod \mathbb{Z}_2) \rtimes_{\psi_{K_1} * \psi_{K_2}} \Delta$. Using Theorem 28, it is sufficient to show that $G_{L_1} \coprod G_{L_2} \coprod \mathbb{Z}_2$ does not contain involution, to conclude that $G_L \simeq G_{L_1} \coprod G_{L_2} \coprod \mathbb{Z}_2$. This is true since G_{L_1}, G_{L_2} and $\mathbb{Z}_2$ do not contain involution. □

Conclusion

We finish by the central result of this chapter:

Theorem 32. *If K is a RPF field, then G_K is Δ-RAAG. Furthermore, if $G_{K_1} \simeq G_{K_2}$ then $\Gamma_1 \simeq \Gamma_2$, where K_1 and K_2 are RPF fields, and Γ_1 (resp. Γ_2) is the underlying graph of G_{K_1} (resp. G_{K_2}).*

Proof. First of all, from Theorem 28 if G_K is Δ-RAAG, then the actions ψ_K and δ coincide. Indeed G_Γ does not have involution, so $G_L = G_\Gamma$.

Remark 25 and Theorem 30 show that Δ-RAAG is a class satisfying the conditions of Theorem 29. We conclude by the minimality of the class $\mathscr{P}$ given in Theorem 29.

To show the last part of our result, we first observe, by Theorem 28, that $G_{K_1} \simeq G_{K_2}$ implies that $G_{\Gamma_1} \simeq G_{\Gamma_2}$. From [43, Proposition 3.4], we conclude that $\mathscr{E}(\Gamma_1) \simeq \mathscr{E}(\Gamma_2)$ and $H^\bullet(G_{\Gamma_1}) \simeq H^\bullet(G_{\Gamma_2})$. Then from [57] or [126, Corollary 2.14], we conclude that $\Gamma_1 \simeq \Gamma_2$. □

Example 24. *Let us give few examples.*

- *For every integer d, $G_K := \mathbb{Z}_2^d \rtimes_\delta \Delta$ (superpythagorean) and $G_K := F(d) \rtimes_\delta \Delta$ (SAP) are in $\mathscr{P}$.*
- *From Theorem 29, the group $G_{\Gamma,\Delta}$ is in $\mathscr{P}$, for every graph Γ with at most 3 vertices. But the group $G_{\Gamma,\Delta}$ is not in $\mathscr{P}$ for Γ the following graph described by four vertices and two disjoint edges:*

However, from [122, Theorem 2], the group G_Γ is realisable as a group G_L, for some field L containing a square root of -1.

Corollary 18. *Let n, m be a cuple of integers, and define Γ_{Cn} (resp. Γ_{Nm}) the complete graph on n vertices (resp. the free graph on m vertices) then the following groups are realisable as groups in $\mathscr{P}$:*

(i) $G_{(\Gamma_{Cn} \coprod \Gamma_{Nm}),\Delta}$,

(ii) $G_{(\Gamma_{Cn} \nabla \Gamma_{Nm}),\Delta}$, *where ∇ denotes the join of two graphs.*

Proof. The groups $G_{\Gamma_{Cn},\Delta}$ and $G_{\Gamma_{Nm},\Delta}$ are realisable as absolute Galois groups of super-pythagorean and SAP fields. Observe that:

$$G_{(\Gamma_{Cn} \coprod \Gamma_{Nm}),\Delta} = G_{\Gamma_{Cn},\Delta} \coprod G_{\Gamma_{N(m-1)},\Delta}, \quad \text{and} \quad G_{(\Gamma_{Cn} \nabla \Gamma_{Nm}),\Delta} = (G_{\Gamma_{Cn}} \times G_{\Gamma_{Nm}}) \rtimes_\delta \Delta.$$

We conclude using Theorem 32. □

5.3 Kernel unipotent conjecture

In this part, we show that $\mathscr{P}$ satisfies the Kernel unipotent conjecture. Let us first recall this conjecture. We fix an integer n, we define $\mathbb{U}_n$ the group of unipotent upper triangular matrices over $\mathbb{F}_2$, and we introduce:

$$G_{<n>} := \bigcap_\rho \ker\left(\rho \colon G \to \mathbb{U}_{n+1}\right),$$

where ρ describes every n-unipotent representation of G. Observe that we have the following result:

Lemma 16. *For every integer n, $G_n \subset G_{<n>}$.*

Proof. See for instance [96, Lemma 2.5]. □

We say that G satisfies the Kernel n-unipotent conjecture if $G_n = G_{<n>}$, and G satisfies the Kernel unipotent conjecture if G satisfies the Kernel n-unipotent conjecture for every n. Here we show that the Kernel unipotent conjecture is satisfied for the class $\mathscr{P}$. Precisely, we study stability of the Kernel unipotent conjecture up to products and coproducts. For this purpose, for every $g \in G \setminus G_n$ we construct maps $\rho_g \colon G \to \mathbb{U}_{n+1}$ such that $\rho_g(g) \neq 1$.

5.3.1 Stability by products

Let us show that the Kernel unipotent conjecture is stable by products.

Proposition 33. *Assume that G_1 and G_2 are two pro-2 groups satisfying the Kernel unipotent conjecture, then the group $G := G_1 \times G_2$ also satisfies the Kernel unipotent conjecture.*

Proof. By Lemma 16, to show that a group G satisfies the n-kernel unipotent conjecture, it is necessary and sufficient to exhibit, for every non trivial u in G/G_n, a morphism $\rho_u \colon G/G_n \to \mathbb{U}_{n+1}$ such that $\rho_u(u) \neq 1$.

We can write u as a product:

$$u := ab$$

with $a \in G_1$ and $b \in G_2$. Observe that at least a is not in $(G_1)_n$ or b is not in $(G_2)_n$. Let us distinguish all possible cases:

- If a is not in $(G_1)_n$, then there exists a morphism $\rho_a \colon G_1/(G_1)_n \to \mathbb{U}_{n+1}$ such that $\rho_a(a) \neq 1$. Then we can define $\rho_u := \rho_a \times \mathbb{1} \colon G/G_n \simeq G_1/(G_1)_n \times G_2/(G_2)_n \to \mathbb{U}_{n+1}$, where $\mathbb{1}$ is the trivial map from $G_2/(G_2)_n$ to $\mathbb{U}_{n+1}$.
- If a is in (G_1), then b is not in $(G_2)_n$. This case is symmetric to the previous one.

□

5.3.2 Stability by coproducts

We continue this part by showing that the Kernel unipotent conjecture is stable by coproducts:

Proposition 34. *The Kernel unipotent conjecture is stable by coproduct.*

Proof. Assume that G_1 and G_2 satisfy the kernel unipotent conjecture. Let us show that $G := G_1 \coprod G_2$ does alo satisfy the kernel unipotent conjecture. For this purpose, we fix n an integer and we take $g \in G \setminus G_n$. Then we construct a morphism $\rho_g \colon G \to \mathbb{U}_{n+1}$, which maps g to $\rho(g) \neq 1$.

Modulo G_n, there exists an integer k such that:

$$g := g_{\leq k} := g_1 \dots g_k,$$

where g_i is not trivial and either in G_1 or G_2, but g_i and g_{i+1} are not simultaneously in the same group. By induction, we show the following property:
P_k: "For every integer k, there exists a morphism $\rho_{g_{\leq k}} \colon G \to \mathbb{U}_{n+1}$ which maps $g_{\leq k}$ to a nontrivial element in $\mathbb{U}_{n+1}$."

• If $k = 1$, then either $g := g_1$ is in G_1 or G_2. Say for instance $g \in G_1$. Since G_1 satisfies the kernel unipotent conjecture, then there exist a morphism $\rho_{g_1} \colon G_1 \to \mathbb{U}_{n+1}$ which maps g_1 to a nontrivial element. Then define $\rho_g := \rho_{g_1} \coprod \mathbb{1} \colon G \to \mathbb{U}_{n+1}$ where $\mathbb{1} \colon G_2 \to \mathbb{U}_{n+1}$ is the trivial map. Then $\rho_g(g) = \rho_{g_1}(g_1) \neq 1$.

• Assume P_k true, let us show that P_{k+1} is also true. We write:

$$g := g_1 \dots g_k g_{k+1} = g_{\leq k} g_{k+1},$$

with say g_{k+1} in G_2 and g_k in G_1. Recall that g is not in G_n. Let us distinguish two cases:

(*a*) $g_{\leq k}$ is in G_n,

(*b*) $g_{\leq k}$ is not in G_n.

If we are in (*a*), then necessarily, g_{k+1} is not in $G_n \cap G_2 = (G_2)_n$. Since G_2 satisfies the kernel unipotent conjecture, we can take $\rho_g := \mathbb{1} \coprod \rho_{g_{k+1}}$, where $\mathbb{1} \colon G_1 \to \mathbb{U}_{n+1}$ is the trivial map. So, since $g_{\leq k}$ is in G_n, then $\rho_g(g_{\leq k}) = 1$, thus we have:

$$\rho_g(g) := \rho_g(g_{\leq k} g_{k+1}) = \rho_g(g_{k+1}) = \rho_{g_{k+1}}(g_{k+1}) \neq 1.$$

Assume now that we are in case (*b*). Then since P_k is true, we have a map $\rho_{g_{\leq k}} \colon G \to \mathbb{U}_{n+1}$ which sends $g_{\leq k}$ to a nontrivial element. Consequently, we have $\rho_{g_{\leq k}}(g) = \rho_{g_{\leq k}}(g_{\leq k}) \rho_{g \leq k}(g_{k+1})$. Again, we distinguish two cases:

(*i*) $\rho_{g_{\leq k}}(g_{k+1})$ is trivial,

(*ii*) $\rho_{g_{\leq k}}(g_{k+1})$ is not trivial.

If we are in case (*i*), then we can take $\rho_g := \rho_{g_{\leq k}}$. If we are in case (*ii*), then we take $\rho_g(\bullet) := \rho_{g_{\leq k}}(\bullet) \times \rho_{g_{\leq k}}(g_k)^{-1}$. □

5.3.3 Proof of Theorem G

We finish this part by showing Theorem G.

Remark 26. *Indeed, if we consider p a prime not necessarily even, we can easily generalise Propositions 33 and 34. We show the following result:*

Assume that G is RAAG and a pro-p absolute Galois group, then G satisfies the Kernel unipotent conjecture. Equivalently, if G is RAAG and neither contains the square graph C_4 nor the line L_4 then G satisfies the Kernel unipotent conjecture.

Proof. The group $\mathbb{Z}_p$ satisfies kernel unipotent conjecture. Then we conclude by [122, Theorem 1.2] and Propositions 33 and 34. □

Let us now show the Kernel unipotent conjecture for $\mathscr{P}$.

Theorem 33. *Assume that G is in $\mathscr{P}$, then G satisfies the Kernel unipotent conjecture.*

Proof. We already know that the Kernel unipotent conjecture is satisfied for Δ and is stable by coproduct. To conclude, we only need to show that if H is Δ-RAAG and satisfy the Kernel unipotent conjecture, then $G := U \rtimes H$ satisfies the Kernel unipotent conjecture, where the action of H on U is semi-trivial and $U := \mathbb{Z}_2^l$ for some integer l.

We mostly follow the proof from [96, Proposition 5.1]. First, we observe that we have

$$G/G_n \simeq U/U_n \rtimes H/H_n \simeq \prod_{i\in I} \mathbb{Z}/2^{s+1}\mathbb{Z} \rtimes H/H_n, := \prod_i C_i \rtimes H/H_n$$

where $s := \log_2\lceil n\rceil$ (see [19, Exercise 4, p.289]), and $I := [\![1; l]\!]$. Now, consider $x := uh$ not trivial in G/G_n, where $u \in U/U_n$ and $h \in H/H_n$. We construct $\rho_x \colon G/G_n \to \mathbb{U}_{n+1}$ such that $\rho_x(x) \neq 1$. For this purpose, we distinguish two cases.

(i) First assume that $h \neq 1$. Since H satisfies the Kernel unipotent conjecture, there exists $\eta_h \colon H/H_n \to \mathbb{U}_{n+1}$ such that $\eta_h(h) \neq 1$. Let us define ρ_x by $\rho_x|_{H/H_n} := \eta_h$ and $\rho_x|_{U/U_n} := \mathbb{1}$ the trivial morphism. This morphism is well defined and $\rho_x(x) = \rho_x(u)\rho_x(h) = \eta_h(h) \neq 1$.

(ii) Now, we assume that $h = 1$. From Remark 25, we have the decomposition

$$G/G_n := (U/U_n \times V/V_n) \rtimes \Delta, \quad \text{where} \quad H \simeq V \rtimes \Delta.$$

Then, $u \neq 1$ and we can write $u := (u_i)_{i=1}^l \in \prod_{i=1}^l C_i$, where there exists at least one i_0 such that $u_{i_0} \neq 1$. Define τ_i a generator of C_i and B the matrix with zero's everywhere except on the diagonal and the first upper one. We also write $u_{i_0} := \tau_{i_0}^a \neq 1$. Then we define a morphism $\rho_x \colon G/G_n \to \mathbb{U}_{n+1}$ by $\rho_x(\tau_{i_0}) := B$, $\rho_x(\tau_i) = 1$ when $i \neq i_0$, and $\rho_x(x_0) = A$, where A is a matrix satisfying $ABA := B^{-1}$ and $A^2 = 1$ (see [54, p.154]). This morphism is well defined, and we have:

$$\rho_x(x) := \rho_x(\tau_{i_0}^a) = B^a \neq 1,$$

since 2^{s+1} does not divide a, and B is of order 2^{s+1}. □

5.4 Detection of absolute Galois groups and cohomology

We conclude this chapter by discussing methods to detect the class $\mathscr{P}$. Let us call $\mathscr{P}^+$ the class of RAAG groups of the form G_L, where $L := K(\sqrt{-1})$ for K a RPF.

5.4.1 Cohomology and filtrations

We begin this part by discussing the cohomology of groups in $\mathscr{P}$. [122, Theorem 2] showed that if G is in $\mathscr{P}^+$ then the graph Γ is chordal and does not contain as subgraph the graph:

$$i_1 \text{ ——— } i_2 \text{ ——— } i_3 \text{ ——— } i_4$$

It is also shown that if G_Γ satisfy the previous condition then $H^\bullet(G_\Gamma)$ is universally Koszul, and G_Γ is absolutely torsion-free. However, this condition is not sufficient to classify groups in $\mathscr{P}^+$ as we noticed in example 24. We now focus on that class.

For this purpose, we recall [91, Theorems E and F], and [90, Theorem F, (3)]:

Proposition 35. *If $G_{\Gamma,\Delta}$ is in $\mathscr{P}$, then $H^\bullet(G_{\Gamma,\Delta})$ is universally Koszul and the quadratic dual of $\mathscr{E}_{\Gamma,\Delta}$.*

Proof. From [90, Theorem F, (3)] we infer that $H^\bullet(G_{\Gamma,\Delta})$ is universally Koszul. Furthermore $G_{\Gamma,\Delta}$ has a quadratic presentation. Then from [91, Theorem F], we conclude that $H^\bullet(G_{\Gamma,\Delta})$ is the quadratic dual of $\mathscr{E}_{\Gamma,\Delta}$. In particular, $\mathscr{E}_{\Gamma,\Delta}$ is also Koszul.

□

Let us now use results from [88] to characterise groups in $\mathscr{P}$ from their Hilbert series.

Theorem 34. *Let us fix a graph Γ. If the group $G_{\Gamma,\Delta}$ is in $\mathscr{P}$ then*

$$\Gamma(t) = (1+t)^{s-1} + t\left((1+t)^{s-1}a_{s-1} + \cdots + a_0\right),$$

where a_i and s are integers, a_{s-1} and s are nontrivial, and we have the equality $a_0 + \cdots + a_{s-1} + s = n$.

Conversely, if

$$\Gamma(t) = (1+t)^{s-1} + t\left((1+t)^{s-1}a_{s-1} + \cdots + a_0\right),$$

where a_i and s are integers defined as before, then there exists a graph Γ' such that $\Gamma'(t) = \Gamma(t)$, and $G_{\Gamma',\Delta}$ is in $\mathscr{P}$.

Proof. First assume that $G_{\Gamma,\Delta}$ is in $\mathscr{P}$, then we can write $G_{\Gamma,\Delta} = G_K$, for some K a RPF field. Then from Theorem 27, we have $G_L \simeq G_\Gamma$, and so by [43, Proposition], the Poincaré series of L is:

$$\Gamma(t) := \sum_n c_n(\Gamma)t^n,$$

where $c_n(\Gamma)$ is the number of n-cliques (complete subgraphs with n vertices) of Γ. From [88, Theorem 11], we conclude that $\Gamma(t) = (1+t)^{s-1} + t\left((1+t)^{s-1}a_{s-1} + \cdots + a_0\right)$ for some a_i satisfying the condition of the theorem.

The converse is a consequence of [88, Theorem 11].

□

Let us relate our results with the Milnor conjecture:

Proposition 36. *Assume that $G_{\Gamma,\Delta}$ is in $\mathscr{P}$, and let K be a RPF field such that $G_{\Gamma;\Delta} := G_K$. Then, we have the following isomorphisms of graded algebras:*

$$GW(K) \simeq m_\bullet K \simeq H^\bullet(K) \simeq \mathscr{A}_{\Gamma,\Delta},$$

where $GW(K)$ is the mod 2 graded Witt ring of K and $m_\bullet K$ is the Milnor K-theory of K.

Proof. This is a consequence of Proposition 35 and the Milnor conjecture (we refer to [86] for further details). □

5.4.2 Detection of pro-2 absolute Galois group

Let us conclude this chapter with our final result:

Theorem 35. *Let K be a field, we have the following equivalence:*

- *There exists a graph Γ such that $G_{\Gamma,\Delta} \simeq G_K$,*
- *K is RPF.*

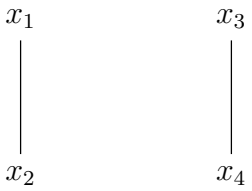
Furthermore, if K is RPF, then it is uniquely determined by an underlying graph Γ.

Proof. We showed in Theorem 27 that K is RPF implies $G_K \simeq G_{\Gamma;\Delta}$ for some graph Γ.

Conversely, assume that there exists a graph Γ such that $G_K \simeq G_{\Gamma;\Delta}$, then from [95, Proposition 2.1], we infer that G_3 is the pro-2 absolute Galois group of $K^{(3)}$, the compositum of all galois extensions of degree dividing 4 of K. From [94, Theorems 2.7 and 2.11] and Corollary 14, we infer that K is RPF.

We conclude with Theorem 32. □

Example 25. *From Theorems 29 and 35, we observe that the group $G := G_{\Gamma,\Delta} := (\mathbb{Z}_2^2 \coprod \mathbb{Z}_2^2) \rtimes_\delta \Delta$, where δ inverts the system of generators of the RAAG $\mathbb{Z}_2^2 \coprod \mathbb{Z}_2^2$, is not in $\mathscr{P}$. We can illustrate this group with the graph Γ, described by 4 vertices and two disjoint edges:*



Consequently by Theorem 35, the group $G_{\Gamma;\Delta}$ is not a pro-2 maximal absolute Galois group for some field K.

Chapter 6

A complete answer to a question from Mináč-Rogelstad-Tân

Let G be a finitely presented pro-p group with set of generators $\{x_1;\dots;x_d\}$ and relations $\{l_1;\dots;l_r\}$. We answer positively to the following question from Mináč-Rogelstad-Tân [92, Question (2.13)]:

If $\mathscr{L}(\mathbb{Z}_p;G)$ is torsion-free, do we have for every integer n, $c_n(\mathbb{Z}_p;G)=c_n(\mathbb{F}_p;G)$?

Theorem 19 gives a positive answer when G is mild using cohomological techniques [59, Proposition 4.3] and graded/filtered algebra results originally introduced by Lazard [69]. This chapter answers to the previous question, without cohomological restriction, using techniques developed in Chapter 4.

First we show the following general result (without torsion-freeness hypothesis):

Lemma 17. *For every integer n, we have:*

$$\dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)\leq \mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p).$$

Proof. Write $k:=\dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)$. Consider $v_1;\dots;v_k$ a basis of $\mathscr{I}_n(\mathbb{F}_p)$. Then we can find a family $u_1;\dots;u_k$ in $\mathscr{I}_n(\mathbb{Z}_p)$ such that $u_i\equiv v_i \pmod{p\mathbb{Z}_p}$. Let us show that the family u is free in $\mathscr{I}_n(\mathbb{Z}_p)$. For this purpose, assume that there exists a family $\alpha_1;\dots;\alpha_k$ in $\mathbb{Z}_p$ such that $\sum_i\alpha_iu_i=0$. Reducing modulo p, we infer that for every i, α_i is in $p\mathbb{Z}_p$. Consequently, we can write

$$\sum_i\alpha_iu_i=p^l\sum_i\alpha_i'u_i,$$

with at least one α_i not in $p\mathbb{Z}_p$. Since $\mathscr{I}_n(\mathbb{Z}_p)\subset\mathscr{E}_n(\mathbb{Z}_p)$, then $\mathscr{I}_n(\mathbb{Z}_p)$ is torsion-free. Consequently $\sum_i\alpha_i'u_i=0$, then $\sum_i\alpha_i'v_i\equiv 0 \pmod p$, so every α_i' is in $p\mathbb{Z}_p$: this is a contradiction. Therefore, the family u is free. Then $k:=\dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)\leq\mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p)$. □

Corollary 19. *If $\dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)=\mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p)$, then $\mathscr{E}_n(\mathbb{Z}_p,G)$ is torsion-free.*

Proof. Assume that $k:=\dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)=k':=\mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p)$. We show here that $\mathscr{E}_n(\mathbb{Z}_p,G)$ is torsion-free. For this purpose, let us take u in $\mathscr{E}_n(\mathbb{Z}_p)$ such that pu is in $\mathscr{I}_n(\mathbb{Z}_p)$. We need to show that u is in $\mathscr{I}_n(\mathbb{Z}_p)$.

Since $k = k'$, we can take the family $\{u_1, \ldots, u_k\}$ as a basis of $\mathscr{I}_n(\mathbb{Z}_p)$ defined in Lemma 17. So we infer a family $\{\alpha_i\}$ in $\mathbb{Z}_p$ such that:

$$pu := \sum_i \alpha_i u_i.$$

Reducing modulo p, we infer that for all i, α_i is in $p\mathbb{Z}_p$. Consequently, u is in $\mathscr{I}_n(\mathbb{Z}_p)$. □

Assume that $\mathscr{L}(\mathbb{Z}_p, G)$ is torsion-free. This implies in particular that $\mathscr{E}(\mathbb{Z}_p, G)$ is torsion-free. Let us state our main result:

Theorem 36. *If $\mathscr{L}(\mathbb{Z}_p, G)$ is torsion-free, then we have $gocha(\mathbb{F}_p, t) = gocha(\mathbb{Z}_p, t)$.*

Proof. Consider the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I(\mathbb{Z}_p) & \longrightarrow & E(\mathbb{Z}_p) & \longrightarrow & E(\mathbb{Z}_p, G) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (\mathrm{mod}\ p)} & & \downarrow{\scriptstyle (\mathrm{mod}\ p)} & & \downarrow{\scriptstyle (\mathrm{mod}\ p)} & & \\
0 & \longrightarrow & I(\mathbb{F}_p) & \longrightarrow & E(\mathbb{F}_p) & \longrightarrow & E(\mathbb{F}_p, G) & \longrightarrow & 0
\end{array}$$

Where the vertical maps are all surjective. Then, we infer the following diagram for every integer n:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathscr{I}_n(\mathbb{Z}_p) & \longrightarrow & \mathscr{E}_n(\mathbb{Z}_p) & \longrightarrow & \mathscr{E}_n(\mathbb{Z}_p, G) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (\mathrm{mod}\ p)} & & \downarrow{\scriptstyle (\mathrm{mod}\ p)} & & \downarrow{\scriptstyle (\mathrm{mod}\ p)} & & \\
0 & \longrightarrow & \mathscr{I}_n(\mathbb{F}_p) & \longrightarrow & \mathscr{E}_n(\mathbb{F}_p) & \longrightarrow & \mathscr{E}_n(\mathbb{F}_p, G) & \longrightarrow & 0
\end{array}$$

Observe that $\mathscr{E}(\mathbb{Z}_p)$ is torsion-free, and from [44, Theorem 3.5] or [92, Remark 3.3], we have $\mathrm{rank}_{\mathbb{Z}_p}\mathscr{E}_n(\mathbb{Z}_p) = \dim_{\mathbb{F}_p}\mathscr{E}_n(\mathbb{F}_p)$. We need to show that $\mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p) = \dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)$.

Let us take the notations from the proof of Lemma 17, and write $k := \dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)$. In Lemma 17, we showed that $k \leq \mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p)$. Let us now show that $k \geq \mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p)$, so u is a generating family of $\mathscr{I}_n(\mathbb{Z}_p)$. Take ρ in $\mathscr{I}_n(\mathbb{Z}_p)$. Since $\mathscr{E}(\mathbb{Z}_p, G)$ is torsion-free, then up to a multiplication by a power of p, we can assume that ρ is not in $p\mathscr{E}(\mathbb{Z}_p)$. Thus we can lift ρ to an element $P \in I(\mathbb{Z}_p)$ of degree n satisfying $P \equiv \rho \pmod{E_{n+1}(\mathbb{Z}_p)}$. In particular, we can write $P := \rho + (P - \rho)$, with $(P - \rho) \in E_{n+1}(\mathbb{Z}_p)$.

Consider P' the image of P modulo p. We define by ρ' the polynomial of degree n in P', i.e. we have the equality $P' \equiv \rho' \pmod{\mathscr{E}_{n+1}(\mathbb{F}_p)}$, so we can write $P' := \rho' + (P' - \rho')$ with $P' - \rho' \in E_{n+1}(\mathbb{F}_p)$. Since we assumed that ρ is not in $p\mathscr{E}(\mathbb{Z}_p)$ and is homogeneous of degree n, we infer that $\rho \equiv \rho' \neq 0 \pmod{p}$. Consequently, ρ' is the leading polynomial of P' which is in $I_n(\mathbb{F}_p)$. Therefore, ρ' is in $\mathscr{I}_n(\mathbb{F}_p)$.

Let us write $\rho' := \sum_i \beta_i v_i \in \mathscr{I}_n(\mathbb{F}_p)$. Then we define $\rho_0 := \sum_i \alpha_i u_i$ with α_i in $\mathbb{Z}_p$ a lift of β_i; which is in $\mathscr{I}_n(\mathbb{Z}_p)$, by the definition of the family u. We also have $\rho_0 \equiv \rho' \equiv \rho \pmod{p\mathbb{Z}_p}$. Consequently, we can write:

$$\rho := \rho_0 + p\rho_{\geq 1},$$

for some $\rho_{\geq 1} \in \mathscr{E}_n(\mathbb{Z}_p)$. Moreover since $p\rho_{\geq 1} = \rho - \rho_0 \in \mathscr{I}_n(\mathbb{Z}_p)$, we deduce that $\rho_{\geq 1}$ is in $\mathscr{I}_n(\mathbb{Z}_p)$. Assuming that $\rho_{\geq 1}$ is not in $p\mathscr{E}_n(\mathbb{Z}_p)$, we can write from the previous argument $\rho_{\geq 1} := \rho_1 + p\rho_{\geq 2}$, where $\rho_{\geq 2}$ is in the $\mathbb{Z}_p$-span of u. Inductively, we can write ρ as a sum:

$$\rho := \sum_{l \geq 0} p^l \rho_l,$$

where every ρ_l is in $u_1\mathbb{Z}_p \oplus \cdots \oplus u_k\mathbb{Z}_p$ and either not in $p\mathscr{E}(\mathbb{Z}_p)$ or equals 0.

By a topological argument, we conclude that u is a generating family of $\mathscr{I}_n(\mathbb{Z}_p)$ so u is a basis of $\mathscr{I}_n(\mathbb{Z}_p)$. Then $\mathrm{rank}_{\mathbb{Z}_p}\mathscr{I}_n(\mathbb{Z}_p) = \dim_{\mathbb{F}_p}\mathscr{I}_n(\mathbb{F}_p)$. □

Chapter 7

Conclusion

This thesis employs techniques from graded Lie algebras associated with pro-p groups filtrations, originally developed by Lazard, to achieve significant advancements in pro-p Galois theory. Our research primarily focuses on applications in number fields and Pythagorean fields. Firstly, we investigate the realization of number field extensions with specified ramification and high cohomological dimension (two or higher). Secondly, we explore 2-maximal extensions of Formally real Pythagorean fields of finite type.

On one hand, building upon foundational work by Anick, Labute, and the "cutting tower strategy" introduced by Hajir, Maire, and Ramakrishna, we analyze tame quotients of absolute Galois groups over number fields. These extensions have infinite splitting and despite having finite abelianization property (a consequence of Class Field Theory), have cohomological dimension two. On the other, drawing insights from graph theory, we construct nontrivial extensions of number fields with ramification above p and large cohomological dimensions, employing principles rooted in Right Angled Artin Algebras.

Lazard's application of graded algebra techniques to pro-p groups led to the formulation of Gocha's alternative, shedding light on potential analytic structures within these groups. Extending Lazard's findings, we present an equivariant version of Gocha's alternative, named from Golod and Shafarevich (which is spelled Chafarevich in french), supported by concrete arithmetic examples using software systems such as PARI/GP, Macaulay2, Sagemath and GAP. Additionally, we address a query posed by Mináč-Rogelstad-Tân concerning the relationship between the Zassenhaus filtration and the lower central series, providing first a solution for mild groups, then a complete positive answer.

This thesis also delves into the presentations of pro-2 absolute Galois groups of Formally real Pythagorean fields of finite type (RPF). Expanding upon Mináč' characterization of pro-2 absolute Galois groups as a minimal class stable under coproducts, some semi-direct products, and containing $\Delta := \mathbb{Z}/2\mathbb{Z}$, we utilize graph products theory to define the class of Δ-RAAGs and infer presentations for these Galois groups. As a consequence, we identify which Δ-RAAGs serve as pro-2-absolute Galois groups over certain fields and verify the Kernel unipotent conjecture for them.

Identifying realizable Galois groups over specific fields remains a challenging, age-old problem. This thesis contributes partial solutions by exploring the structural properties

of pro-p groups, expanding the horizons of pro-p Galois theory, and offering new insights into the nature and structure of Galois groups over diverse fields. Looking forward, future research avenues include:

(i) Exploring pro-p groups that satisfy significant conjectures such as the Massey Vanishing or Kernel unipotent conjectures, which are not pro-p absolute Galois groups over fields containing primitive p-roots of unity.

(ii) Paving the way for the study of unramified extensions with cohomological dimensions exceeding two by investigating their associated graded algebras; such extensions, according to the Fontaine-Mazur conjecture, would not be analytic.

(iii) Extending the study of formality properties (in the sense of Suciu-Wang) on pro-p groups to uncover new relations between underlying groups and their filtrations, akin to the insights gained from Gocha's alternative.

(iv) Understanding which fields satisfy the Strong Massey Vanishing conjecture, and more generally the formality property (in the sense of Merkurjev, Posiltseski and Scavia).

In conclusion, this thesis marks a significant advancement in pro-p Galois theory, pushing the boundaries of our understanding and paving the way for future investigations into the intricate structures of Galois groups over various fields.

Bibliography

[1] D. Anick. "Generic Algebras and CW Complexes". In: *Algebraic Topology and Algebraic K-Theory: Proceedings of a Symposium in Honor of John C. Moore.(AM-113)*. Vol. 113. Princeton University Press. 2016, p. 247.

[2] D. Anick. "Inert sets and the Lie algebra associated to a group". In: *Journal of Algebra* 111.1 (1987), pp. 154–165.

[3] D. Anick. "Non-Commutative Graded Algebras and their Hilbert Series". In: *Journal of Algebra* 78.1 (1982), pp. 120–140.

[4] D. Anick. "On the Homology of Associative Algebras". In: *Transactions of the American Mathematical Society* 296.2 (1986), pp. 641–659.

[5] D. Anick. "On Monomial Algebras of finite global dimension". In: *Transactions of The American Mathematical Society* 291.1 (1985), pp. 291–310.

[6] L. Bartholdi, H. Härer, and T. Schick. "Right Angled Artin Groups and partial commutation, old and new". In: *L'Enseignement Mathématique* 66.1 (2020), pp. 33–61.

[7] S. Blumer, C. Quadrelli, and T. Weigel. "Oriented right-angled Artin pro-ℓ groups and maximal pro-ℓ Galois groups". In: *International Mathematics Research Notices* 2024.8 (2024), pp. 6790–6819.

[8] N. Boston. "Some cases of the Fontaine–Mazur conjecture, II". In: *Journal of Number Theory* 75.2 (1999), pp. 161–169.

[9] N. Boston. "Some cases of the Fontaine-Mazur conjecture". In: *Journal of Number Theory* 42.3 (1992), pp. 285–291.

[10] N. Boston. *The proof of Fermat's last theorem*. Unpublished, 2003. URL: `https://people.math.wisc.edu/~nboston/869.pdf`.

[11] E. Boughattas and D. Neftin. "The Grunwald problem and homogeneous spaces with non-solvable stabilisers". In: *arXiv:2404.09874* (2024).

[12] E. Boughattas and H. Zhang. *L'inégalité de Golod et Shafarevich*. Unpublished, 2017. URL: `https://www.normalesup.org/~boughatt/academique/inegalite_gs.pdf`.

[13] L. Bröcker. "Über die Anzahl der Anordnungen eines kommutativen Körpers". In: *Beiträge zur Geometrischen Algebra: Proceedings des Symposiums über Geometrische Algebra vom 29. März bis 3. April 1976 in Duisburg*. Springer. 1977, pp. 59–61.

[14] A. Brumer. "Pseudocompact algebras, profinite groups and class formations". In: *Bulletin of the American Mathematical Society* 72.2 (1966), pp. 321–324.

[15] J. Cassels and A. Fröhlich. *Algebraic number theory: Proceedings of an instructional conference*. Academic press, 1967.

[16] M. W. Davis. *The Geometry and Topology of Coxeter Groups. (LMS-32)*. Princeton: Princeton University Press, 2008.

[17] C. De Clercq and M. Florence. "Smooth profinite groups and applications". In: *arXiv:1710.10631* (2018).

[18] R. Diestel. "Graph Theory 5th ed". In: *Graduate texts in mathematics* 173.33 (2017).

[19] J. Dixon, M. Du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*. 61. Cambridge University Press, 2003.

[20] D. Dummit and J. Labute. "On a new characterization of Demuskin groups". In: *Inventiones mathematicae* 73 (1983), pp. 413–418.

[21] I. Efrat. "Linking Invariants for Valuations and Orderings on Fields". In: *arXiv:2403.07482* (2024).

[22] I. Efrat and D. Haran. "On Galois groups over pythagorean and semi-real closed fields". In: *Israel Journal of Mathematics* 85 (1994), pp. 57–78.

[23] I. Efrat and J. Mináč. "Galois groups and cohomological functors". In: *Transactions of the American Mathematical Society* 369.4 (2017), pp. 2697–2720.

[24] I. Efrat and C. Quadrelli. "The Kummerian property and maximal pro-p Galois groups". In: *Journal of Algebra* 525 (2019), pp. 284–310.

[25] Ido Efrat and Ján Mináč. "Small Galois groups that encode valuations". In: *Acta Arithmetica* 156.1 (2012), pp. 7–17.

[26] R. Elman and T.-Y. Lam. "Quadratic forms over formally real fields and pythagorean fields". In: *American Journal of Mathematics* 94.4 (1972), pp. 1155–1194.

[27] M. Ershov and A. Jaikin-Zapirain. "Groups of positive weighted deficiency and their applications". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2013.677 (2013), pp. 71–134.

[28] S. Filip. "The Lie algebra of the fundamental group of a surface as a symplectic module". In: *arXiv:1308.1529* (2013).

[29] P. Forré. "Strongly free sequences and pro-p-groups of cohomological dimension 2." In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2011.658 (2011), pp. 173–192.

[30] R. Fröberg. "Determination of a class of Poincaré series". In: *Mathematica Scandinavica* 37.1 (1975), pp. 29–39.

[31] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[32] F. Golmakani. "Classification of W-groups of Pythagorean Formally Real fields". PhD thesis. The University of Western Ontario, 2018.

[33] E. Golod and I. Shafarevich. "On the class field tower". In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 28.2 (1964), pp. 261–272.

[34] G. Gras. "Les θ-régulateurs locaux d'un nombre algébrique: Conjectures p-adiques". In: *Canadian Journal of Mathematics* 68.3 (2016), pp. 571–624.

[35] G. Gras. "On the T-ramified, S-split p-class field towers over an extension of degree prime to p". In: *Journal of Number Theory* 129 (Nov. 2009), 2843–2852.

[36] M. Griffin. "The Pythagorean closure of fields". In: *Mathematica Scandinavica* 38.2 (1976), pp. 177–191.

[37] K. Haberland, H. Koch, and T. Zink. "Galois cohomology of algebraic number fields". In: *VEB Deutscher Verlag der Wissenschafte, Berlin* (1978).

[38] F. Hajir, M. Larsen, C. Maire, and R. Ramakrishna. "On tamely ramified infinite Galois extensions". In: *arXiv:2401.05927* (2024).

[39] F. Hajir and C. Maire. "Prime decomposition and the Iwasawa mu-invariant". In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 166. 3. Cambridge University Press. 2019, pp. 599–617.

[40] F. Hajir and C. Maire. "Tamely ramified towers and discriminant bounds for number fields". In: *Compositio Mathematica* 128.1 (2001), pp. 35–53.

[41] F. Hajir, C. Maire, and R. Ramakrishna. "Cutting towers of number fields". In: *Annales mathématiques du Québec* 45.2 (2021), pp. 321–345.

[42] F. Hajir, C. Maire, and R. Ramakrishna. "On Ozaki's theorem realizing prescribed p-groups as p-class tower groups". In: *Algebra & Number Theory* 18.4 (2024), pp. 771–786.

[43] O. Hamza. "On extensions of number fields with given quadratic algebras and cohomology". In: *arXiv:2309.06396* (2023).

[44] O. Hamza. "Zassenhaus and lower central filtrations of pro-p groups considered as modules". In: *Journal of Algebra* 633 (2023), pp. 172–204.

[45] O. Hamza and C. Maire. "A note on asymptotically good extensions in which infinitely many primes split completely". In: *Archiv der Mathematik* 115.5 (2020), pp. 523–534.

[46] O. Hamza, C. Maire, J. Mináč, and N.D Tân. "On Maximal extension of Pythagorean fields and oriented Graph Products". In: *preparation* (2024).

[47] Y. Harpaz and O. Wittenberg. "The Massey vanishing conjecture for number fields". In: *Duke Mathematical Journal* 172.1 (2023), pp. 1 –41.

[48] M. Hartl. "On Fox and augmentation quotients of semidirect products". In: *Journal of Algebra* 324.12 (2010), pp. 3276–3307.

[49] N. Hindman and D. Strauss. "Algebra in the Stone-Čech compactification". In: *Algebra in the Stone-Cech Compactification*. de Gruyter, 2011.

[50] Y. Ihara. "How many primes decompose completely in an infinite unramified Galois extension of a global field?" In: *Journal of the Mathematical Society of Japan* 35.4 (1983), pp. 693–709.

[51] B. Jacob. "On the structure of Pythagorean fields". In: *Journal of Algebra* 68.2 (1981), pp. 247–267.

[52] B. Jacob. "The Galois cohomology of Pythagorean fields". In: *Inventiones mathematicae* 65.1 (1981), pp. 97–113.

[53] A. Jaikin-Zapirain and H. Souza. "Sylvester domains and pro-p groups". In: *arXiv:2402.14130* (2024).

[54] G.J. Janusz. "Faithful Representations of p Groups at Characteristic p, II". In: *Journal of Algebra* 22.1 (1972), pp. 137–160.

[55] D. Karagueuzian, J. Labute, and J. Mináč. "The Bloch-Kato Conjecture and Galois Theory". In: *Annales des Sciences Mathematiques du Quebec* (Dec. 2010).

[56] S. Katok. *p-adic Analysis Compared with Real*. Vol. 37. American Mathematical Soc., 2007.

[57] K. H. Kim, L. Makar-Limanov, J. Neggers, and F. W. Roush. "Graph algebras". In: *Journal of Algebra* 64.1 (1980), pp. 46–51.

[58] H. Koch. *Algebraic Number Theory*. Algebraic Number Theory v. 62. Springer Berlin Heidelberg, 1997.

[59] H. Koch. *Galois theory of p-extensions*. Springer Science & Business Media, 2002.

[60] H. Koch. "Über Pro-p-Gruppen der kohomologischen Dimension 2". In: *Mathematische Nachrichten* 78.1 (1977), pp. 285–289.

[61] J. Labute. "Algebres de Lie et pro-p-groupes définis par une seule relation". In: *Inventiones mathematicae* 4 (1967), pp. 142–158.

[62] J. Labute. "Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 596 (2006), pp. 155–182.

[63] J. Labute. "On the descending central series of groups with a single defining relation". In: *Journal of Algebra* 14.1 (1970), pp. 16–23.

[64] J. Labute. "The Determination of the Lie Algebra Associated to the Lower Central Series of a Group". In: *Transactions of the American Mathematical Society* 288.1 (1985), pp. 51–57.

[65] J. Labute. "The Genesis of a Theorem". In: *arXiv:2406.08233* (2024).

[66] J. Labute and J. Mináč. "Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification". In: *Journal of Algebra* 332.1 (2011), pp. 136–158.

[67] T.-Y. Lam. *Introduction to quadratic forms over fields*. Vol. 67. American Mathematical Soc., 2005.

[68] T.-Y. Lam. *Orderings, valuations and quadratic forms*. Vol. 52. American Mathematical Soc., 1983.

[69] M. Lazard. "Groupes analytiques p-adiques". In: *Publications Mathématiques de l'IHÉS* 26 (1965), pp. 5–219.

[70] P. Lebacque. "Quelques résultats effectifs concernant les invariants de Tsfasman-Vladut". In: *Ann. Inst. Fourier* 65 (2015), pp. 63–99.

[71] J.-M. Lemaire. *Algebres connexes et homologie des espaces de lacets*. Vol. 422. Springer, 2006.

[72] G. Leoni. "The Zassenhaus p-restricted Lie algebra functor". PhD thesis. Universita degli Studi di Milano-Bicocca, 2024.

[73] G. Leoni and T. Weigel. "Strongly collapsing pro-p groups". In: preparation.

[74] D. Lim and C. Maire. "On the analyticity of the maximal extension of a number field with prescribed ramification and splitting". In: *arXiv:2308.03368* (2023).

[75] J.L. Loday and B. Vallette. *Algebraic operad*. Springer, 2012.

[76] K. Lorensen. "Groups with the same cohomology as their pro-p completions". In: *Journal of Pure and Applied Algebra* 214.1 (2010), pp. 6–14.

[77] A. Lubotzky and D. Neftin. "Sylow-conjugate number fields". In: *Israel Journal of Mathematics* 257.2 (2023), pp. 465–480.

[78] R.C. Lyndon and P.E. Schupp. *Combinatorial group theory*. Vol. 188. Springer, 1977.

[79] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial group theory: Presentations of groups in terms of generators and relations*. Courier Corporation, 2004.

[80] C. Maire. "On Galois representations with large image". In: *Transactions of the American Mathematical Society* 370.10 (2023), pp. 7087–7106.

[81] C. Maire. "Some examples of FAB and mild pro-p-groups with trivial cup-product". In: *Kyushu Journal of Mathematics* 68.2 (2014), pp. 359–376.

[82] M. Marshall. "Classification of finite spaces of orderings". In: *Canadian Journal of Mathematics* 31.2 (1979), pp. 320–330.

[83] A. Merkurjev and F. Scavia. "Degenerate fourfold Massey products over arbitrary fields". In: *arXiv:2208.13011* (2022).

[84] A. Merkurjev and F. Scavia. "On the Massey Vanishing Conjecture and Formal Hilbert 90". In: *arXiv:2308.13682* (2023).

[85] A. Merkurjev and F. Scavia. "The Massey Vanishing Conjecture for fourfold Massey products modulo 2". In: *arXiv:2301.09290* (2023).

[86] J. Milnor. "Algebraic K-theory and quadratic forms". In: *Inventiones mathematicae* 9.4 (1970), pp. 318–344.

[87] J Minác. "Galois groups of some 2-extensions of ordered fields". In: *Comptes Rendus Mathématiques de l'Académie des Sciences* 8 (1986), pp. 103–108.

[88] J. Minác. "Poincaré Polynomials, Stability Indices and Number of Orderings. I, Advances in Number Theory (Kingston, ON, 1991)". In: *Oxford Sci. Publ.* (1993), pp. 515–528.

[89] J. Minác. "Poincaré groups and ordered fields". In: *Comptes Rendus Mathématiques de l'Académie des Sciences* 8 (Jan. 1986).

[90] J. Mináč, M. Palaisti, F. Pasini, and Duy Tân. "Enhanced Koszul properties in Galois cohomology". In: *Research in the Mathematical Sciences* 7.2 (2020), pp. 1–34.

[91] J. Mináč, F. Pasini, C. Quadrelli, and N.D. Tân. "Koszul algebras and quadratic duals in Galois cohomology". In: *Advances in Mathematics* 380 (2021), p. 107569.

[92] J. Mináč, M. Rogelstad, and N. Tân. "Dimensions of Zassenhaus filtration subquotients of some pro-p-groups". In: *Israel Journal of Mathematics* 212.2 (2016), pp. 825–855.

[93] J. Mináč, M. Rogelstad, and N. Tân. "Relations in the maximal pro-p quotients of absolute Galois groups". In: *Transactions of the American Mathematical Society* 373.4 (2020), pp. 2499–2524.

[94] J. Minâĉ and M. Spira. "Formally real fields, Pythagorean fields, C-fields and W-groups". In: *Mathematische Zeitschrift* 205.1 (1990), pp. 519–530.

[95] J. Minác and M. Spira. "Witt rings and Galois groups". In: *Annals of Mathematics* 144.1 (1996), pp. 35–60.

[96] J. Mináč and N. D. Tân. "The Kernel Unipotent Conjecture and the vanishing of Massey products for odd rigid fields". In: *Advances in Mathematics* 273 (2015), pp. 242–270.

[97] J. Mináč and N.D. Tân. "Triple Massey products and Galois theory". In: *Journal of the European Mathematical Society* 19.1 (2016), pp. 255–284.

[98] J. Mináč, F. W. Pasini, C. Quadrelli, and N. D. Tân. "Mild pro-p groups and the Koszulity conjectures". In: *Expo. Math.* 40.3 (2022), pp. 432–455.

[99] M. Morishita. *Knots and primes: an introduction to arithmetic topology*. Springer Science & Business Media, 2011.

[100] M. Morishita. "On certain analogies between knots and primes". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2002.550 (2002), p. 141.

[101] J. Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[102] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Vol. 323. Springer Science & Business Media, 2013.

[103] N. Nikolov. "Algebraic properties of profinite groups". In: *arXiv:1108.5130* (2011).

[104] N. Nikolov and D. Segal. "On Finitely Generated Profinite Groups, I: Strong Completeness and Uniform Bounds". In: *Annals of Mathematics* 165.1 (2007), pp. 171–238.

[105] M. Ozaki. "Construction of maximal unramified p-extensions with prescribed Galois groups". In: *Inventiones mathematicae* 183.3 (2011), pp. 649–680.

[106] M. Palaisti. "Enhanced Koszulity in Galois cohomology". PhD thesis. The University of Western Ontario (Canada), 2019.

[107] T. Panov and T. Rahmatullaev. "Polyhedral products, graph products and p-central series". In: *arXiv:2402.11556* (2024).

[108] A. Polishchuk and L. Positselski. *Quadratic Algebras*. University lecture series. American Mathematical Society, 2005.

[109] C. Quadrelli. "Massey products in Galois cohomology and the elementary type conjecture". In: *Journal of Number Theory* 258 (2024), pp. 40–65.

[110] C. Quadrelli. "Massey products in Galois cohomology and Pythagorean fields". In: *Communications in Algebra* (2024), pp. 1–16.

[111] A. Quéguiner-Mathieu. *Galois Cohomology, Quadratic Forms and Milnor K-theory*. URL: `https://www.math.univ-paris13.fr/\~{}queguin/publi.htm`.

[112] L. Ribes and P. Zalesskii. *Profinite groups*. Springer, 2000.

[113] D. Riley and A. Shalev. "Restricted Lie algebras and their envelopes". In: *Canadian Journal of Mathematics* 47.1 (1995), pp. 146–164.

[114] M. Rogelstad. "Combinatorial techniques in the Galois theory of p-extensions". PhD thesis. The University of Western Ontario (Canada), 2015.

[115] M. Rougnant. "Sur la propagation de la propriété mild au-dessus d'une extension quadratique imaginaire de $\mathbf{Q}$". In: *Annales mathématiques du Québec* 41.2 (2017), pp. 309–335.

[116] M. Rougnant. "Sur quelques aspects des extensions à ramification restreinte". PhD thesis. Université de Franche-Comté, 2018.

[117] A. Schmidt. "Über pro-p-fundamentalgruppen markierter arithmetischer kurven". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 640 (2010), pp. 203–235.

[118] J.-P. Serre. "Travaux de Wiles (et Taylor,...), partie I". In: *Asterisque-Société Mathématique de France* 237 (1996), pp. 319–332.

[119] J.P. Serre. "Galois cohomology". In: *Local Fields*. Springer, 1979, pp. 150–163.

[120] J.P. Serre. *Représentations linéaires des groupes finis*. Collection Méthodes. Hermann, 1978.

[121] M. G. Smith and J. S. Wilson. "On subgroups of finite index in compact Hausdorff groups". In: *Archiv der Mathematik* 80.2 (2003), pp. 123–129.

[122] I. Snopce and P. Zalesskii. "Right-angled Artin pro-p groups". In: *Bulletin of the London Mathematical Society* 54.5 (2022), pp. 1904–1922.

[123] H. Souza and T. Zapata. "Grupos de Demushkin". In: preparation.

[124] J. Stix. "Rational points and arithmetic of fundamental groups, volume 2054 of". In: *Lecture Notes in Mathematics* (2013).

[125] P. Symonds and T. Weigel. "Cohomology of p-adic analytic groups". In: *New horizons in pro-p groups*. Springer, 2000, pp. 349–410.

[126] N. T. Trà. "Zassenhaus filtrations and right-angled Artin groups". In: *Journal of Algebra and Its Applications* 0.0 (0), p. 2550187.

[127] M. Tsfasman and S. Vladut. "Infinite global fields and the generalized Brauer-Siegel theorem". In: *Mosc. Math. J.* 2 (2002), pp. 329–402.

[128] H. Tverberg. "On the irreducibility of polynomials taking small values". In: *Mathematica Scandinavica* 32.1 (1973), pp. 5–21.

[129] K. Uchida. "Isomorphisms of Galois groups of solvably closed Galois extensions". In: *Tohoku Mathematical Journal, Second Series* 31.3 (1979), pp. 359–362.

[130] V.A. Ufnarovski. *Combinatorial and asymptotic methods in algebra, Algebra VI (57) 1-196*. Springer, Berlin Heidelberg New York, 1995.

[131] Ya. A. Veryovkin. "Graded components of the Lie algebra associated with the lower central series of a right-angled Coxeter group". In: *Proceedings of the Steklov Institute of Mathematics* 318.1 (2022), pp. 26–37.

[132] Ya. A. Veryovkin. "The associated Lie algebra of a right-angled Coxeter group". In: *Proceedings of the Steklov Institute of Mathematics* 305 (2019), pp. 53–62.

[133] V. Voevodsky. "Motivic cohomology with $\mathbf{Z}/2$-coefficients". In: *Publications Mathématiques de l'IHÉS* 98 (2003), pp. 59–104.

[134] D. Vogel. *Circular sets of primes of imaginary quadratic number fields*. Working Paper. Regensburg, 2006.

[135] R. Wade. "The lower central series of a right-angled Artin group". In: *L'Enseignement Mathématique* 61.3 (2016), pp. 343–371.

[136] L. Washington. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 2012.

[137] Th. Weigel. "Graded Lie algebras of type FP". In: *Israel Journal of Mathematics* 205.1 (2015), pp. 185–209.

[138] J.S. Wilson. "Finite index subgroups and verbal subgroups in profinite groups". In: *Séminaire Bourbaki* 2009 (2010), pp. 1012–1026.

[139] M. Yamagishi. "A note on free pro-p-extensions of algebraic number fields". In: *Journal de théorie des nombres de Bordeaux* 5.1 (1993), pp. 165–178.

Curriculum Vitae

Name:	Oussama Hamza
Post-Secondary Education and Degrees:	Ecole Normale Supérieure de Lyon Lyon, France 2016 - 2020 B.Sc and M.Sc University of Western Ontario London, ON, Canada 2020 - 2024 PhD
Honours and Awards:	Special Prize Société Mathématique de France, teamed with Baptiste Cerclé and Martin Fatou (2018)
Related Work Experience:	Teaching Assistant The University of Western Ontario 2020 - 2024 Ecole Normale Supérieure de Lyon Civil Trainee 2016 - 2020

(Pre-)Publications:

• Hamza, O. & Maire, Ch. (2020). A note on asymptotically good extensions in which infinitely many primes split completely. *Archiv der Math*

• Hamza, O. (2023). Zassenhaus and lower central filtrations of pro-p groups considered as modules. *Journal of Algebra*

• Hamza, O. (2023). On extensions of number fields with given quadratic algebras and cohomology. *arXiv preprint arXiv:2309.06396* [Submitted].

• Hamza, O., Maire, Ch.,Ináč J. & Nguyen, D.T. (2024). On maximal extensions of Pythagorean fields and oriented Graph products. [To be submitted].

Selection of some talks:

• Hamza, O.(2024, June). *On maximal extensions of Pythagorean fields and Graph products.* Workshop on Galois cohomology and Massey products, Fields Institute, Ottawa, Canada.

• Hamza, O.(2024, February). *On extensions of number fields with given quadratic algebras and cohomology.* Madrid Group Theory Seminar, Institute of Mathematical Sciences, Madrid, Spain.

• Hamza, O. (2023, January). *Filtrations, arithmetic and explicit examples in an equivariant context.* Number Theory Seminar (online), Lethbridge University, Canada.

• Hamza, O. (2022 June). *Hilbert Series and Mild groups.* Summer school COGENT, Institut Fourrier, France.