12-8-2014 12:00 AM

Cohomology of Absolute Galois Groups

Claudio Quadrelli, *The University of Western Ontario*

Supervisor: Jan Minac, *The University of Western Ontario*
Joint Supervisor: Thomas Weigel, *The University of Western Ontario*
A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

COHOMOLOGY
OF ABSOLUTE GALOIS GROUPS

(Thesis format: monograph)

by

Claudio Quadrelli

Graduate Program in Mathematics

Dottorato di Ricerca in Matematica Pura e Applicata

A thesis submitted in partial fulfillment

of the requirements for the degree of Doctor of Philosophy

– The School of Graduate and Postdoctoral Studies
Western University, London-ON, Canada

– Scuola Unica di Dottorato di Ricerca
Università degli Studi di Milano-Bicocca, Milan, Italy

Abstract

The main problem this thesis deals with is the characterization of profinite groups which are realizable as absolute Galois groups of fields: this is currently one of the major problems in Galois theory. Usually one reduces the problem to the pro-p case, i.e., one would like to know which pro-p groups occur as *maximal pro-p Galois groups*, i.e., maximal pro-p quotients of absolute Galois groups. Indeed, pro-p groups are easier to deal with than general profinite groups, yet they carry a lot of information on the whole absolute Galois group.

We define a new class of pro-p groups, called *Bloch-Kato pro-p group*, whose Galois cohomology satisfies the consequences of the Bloch-Kato conjecture. Also we introduce the notion of *cyclotomic orientation* for a pro-p group. With this approach, we are able to recover new substantial information about the structure of maximal pro-p Galois groups, and in particular on θ-abelian pro-p groups, which represent the "upper bound" of such groups.

Also, we study the restricted Lie algebra and the universal envelope induced by the Zassenhaus filtration of a maximal pro-p Galois group, and their relations with Galois cohomology via Koszul duality.

Altogether, this thesis provides a rather new approach to maximal pro-p Galois groups, besides new substantial results.

Keywords: Galois cohomology, pro-p groups, Bloch-Kato conjecture, Elementary Type Conjecture, powerful groups, cyclotomic orientations, Koszul duality in Galois theory.

Dedication

A Elisa

"E propri adess, che te me fet vidé 'n suris,
la radio parla de questo cielo semper püsé gris.
E propri adess, che te strenget la me mann,
g'ho dumà 'l temp de tirà söö tri strasc e 'namm."

Acknowledgments

"Vita che la se incastra e l'è disegnada a lisca de pess,
vita che la sbrisiga verso quel sit 'd te gh'eet vöja de vèss.
Unda che la te porta fin a la spunda de là
per fatt sentii püsé forta la vöja de turnà a caa."[1]
(D. Van de Sfroos)

First of all, I am bound to thank my first advisor, *maestro*, and so far also work-mate (and friend), Prof. Thomas S. Weigel from Milano-Bicocca. In particular, I am grateful to him also for never letting me rest on my laurels, and for being a "warmduscher" only in real life, and never in Mathematics.

And of course, I am very grateful to my second advisor, Prof. Ján Mináč from Western, a wonderful teacher – whose enthusiasm for Mathematics (and not only) is really contagious, and whose laugh is very well known by many mathematicians –, great scorer (in Mathematics and in soccer), work mate and friend as well. And thanks also to his secretary, driver, proof-reader, actress, singer (and when she has some free time, also wife), Leslie... without her, what would be of Professor Mináč?

Sincere thanks to the member of my defense board: Prof. D. Riley and Prof. E. Schost from Western, Prof. R. Schoof from Roma Tor Vergata and Prof.ssa F. Dalla Volta from Milano-Bicocca. I am particularly grateful to D. Riley as Department Chair because of his effort to let me visit Western University as undergraduate and to let me became Ph.D. student there; and I am grateful to him as professor for all the things I learned from him about pro-p groups and restricted Lie algebras.

Many thanks to all the people who were department chairs and graduate chairs during my student career: L. De Michele, F. Magri and S. Levi – resp. G. Tessitore and R. Paoletti – from Milano-Bicocca, and D. Riley and A. Bovin (whose death is a great loss for the department) – resp. D. Christensen and R. Shafikov – from Western. And thanks to the members of my advisory board at Western, G. Denham and L. Renner.

My sincere thanks to S.K. Chebolu, from Illinois State University, for his mathematical insight and for his friendship. I hope we will be working together for a long time

[1] "Life, blocks fitting together, life shaped like a fishbone; life, which slips toward the place where you'd like to be. Wave, which pulls you to the other shore, to make you feel homesick once more and again". From the song *La terza onda*.

There are some mathematicians I have met during my "graduate career" whom I would like to thank for the interest shown towards my work: L. Bary-Soroker, I. Efrat, G. Fernandez-Alcober, D. Krashen, J. Labute, Ch. Maire, D. Neftin, J. Sonn, P. Symonds, D. Vogel, P. Zalesskiĭ. And thanks to my young collegues, in particular to A. Chapman and J. Gärtner.

Two people from the Math Deaprtment in Milan deserve my thanks: Tommaso T., whom I consider as my old "mathematical brother", and Giusy C., the true "pillar" of the department. Same treatment is deserved by N.D. Tân, from Western, for his thoughtful questions and for his "homeworks", without which Section 4.4 would not exists.

Last – but not least – I have to thank my mates, who have been good companions throughout my whole studies... they would be too many, but I can't help to mention at least some. From my undergraduate studies: Chiara B., Claudio S., Cristian C., Davide C., Davide M., Matteo C., Mattia B., Paolo Nicola C., Stefano P.; and from my graduate studies: Chiara O., Dario C., Francesca S., Jacopo C., Linda P., Marina T., Sara V., Simone C.

A special mention is deserved by office-mates in Milan: Gianluca P. (one of the few people in the world able to understand, appreciate and enjoy my humor, together with Paolo Nicola!), Martino B. (the first to leave the office), Nicola S. (even if he's an analyst!), Federico William P. (even if he's abusive!), Elena V. (even if she studies... ehm, better not mentioning it), and also Ilaria C. and Raimundo B. for their "loud presence" (cit.).

Thanks to my landlady in London-ON, Alison W., and my roommates (in particular Silke D.), for providing me a welcoming home while staying in Canada.

I can't help to thank explicitly at least some (but only for the lack of space) of my dearest friends (who are not mentioned above): Teo C., the "Syncefalia", Samu & Giulia, Coco & JPF, Teo & Chiara B., il Biondo, il White, and many other people from the Oratorio di Binago.

Last, but not least, thanks to my parents, Alfredo and Paola, for what I am is also because of them; and to my sister, Giulia, for always supporting me (also with cakes and cookies). And to Elisa (and any word here would seem inadequate, as indeed she often leaves me speechless).

Contents

Abstract ii
Dedication iii
Acknowledgments iv

Introduction 1

Chapter 1. Preliminaries 11
1. Group cohomology and Galois cohomology 11
2. Preliminaries on pro-p groups 16
3. Restricted Lie algebras 19
4. Cohomology of Galois groups and Kummer theory 23

Chapter 2. The Bloch-Kato conjecture 27
1. Quadratic algebras 27
2. The Rost-Voevodsky Theorem 29
3. Bloch-Kato pro-p groups 30
4. Oriented pro-p groups 34
5. The Elementary Type conjecture 42

Chapter 3. The upper bound: θ-abelian groups 47
1. θ-abelian pro-p groups and the cup product 47
2. θ-abelian pro-p groups and powerful pro-p groups 49
3. Rigid fields and θ-abelian Galois groups 55
4. Finite quotients and θ-abelian groups 60
5. The Zassenhaus filtration for θ-abelian groups 65

Chapter 4. Products, relations, and the ETC 67
1. The group $H^1(G, \mathbb{Z}_p(1))$ 67
2. Free products 71
3. The cyclotomic fibre product 74
4. Relations 83
5. Cyclo-oriented ETC 91

Chapter 5. Koszulity for cyclo-oriented pro-p groups 93
1. Koszul duality 93
2. Koszul duality and the ETC 95

3. Koszul duality for cyclo-oriented pro-p groups 100
4. Koszul algebras and Koszul pro-p groups 103

Bibliography 107
Curriculum Vitæ et Studiorum 111

Introduction

> "Die Zahlentheorie nimmt unter den mathematischen Disziplinen eine änlich idealisierte Stellung ein wie die Mathematik selbst unter den anderen Wissenschaften."[2]
> (J. Neukirch)

One may very well say that the Theory of Profinite Groups is "daughter" of Galois Theory. Indeed profinite groups arose first in the study of the Galois groups of infinite Galois extensions of fields, as such groups are profinite groups, and they carry with them a natural topology, the *Krull topology*, which is induced by the Galois subextensions of finite degree, and under this topology they are Hausdorff compact and totally disconnected topological groups: these properties characterize precisely profinite groups. Also, the Krull topology allows us to state the Fundamental Theorem of Galois Theory also for infinite Galois extensions: one has a bijective correspondence between subextensions and *closed* subgroups, and in particular between *finite* subextensions and *open* subgroups.

In particular, the tight relation between profinite groups and Galois groups is stated by the following theorem, proved first by H.Leptin in 1955 (cf. [**Le55**]).

THEOREM 0.1. *Let G be a profinite group. Then there exists a Galois extension of fields L/K such that $G = \mathrm{Gal}(L/K)$.*

The proof of this theorem one commonly refers to nowadays is due to L. Ribes (1977, see also [**RZ10**, § 2.11]). Note that the aforementioned theorem does not say anything about the nature of the field K nor about the extension L/K. In fact, the essence of the whole Galois theory is to "lose information", as one passes from a field, i.e., an algebraic structure with two compatible operations, to a (profinite) group, i.e., an algebraic (and topological) structure with only one operation (compatible with the topology).

[2] "Number Theory, among the mathematical disciplines, occupies a similar ideaized position to that held by Mathematics itself among the sciencies". From the introduction of Neukirch's book *Algebraic Number Theory*, and quoted at the beginning of the Introduction of [**NSW**].

Every field K comes equipped with a distinguished Galois extension: the *separable closure* $\bar{K}^{\text{sep}}$. Its Galois group $G_K = \text{Gal}(\bar{K}^{\text{sep}}/K)$ is called the **absolute Galois group** of K. Such extension collects all (finite and infinite) Galois extensions of K; in particular, all Galois groups of K are "encoded" in G_K: this is why absolute Galois groups of fields have a prominent place in Galois theory.

Unfortunately (or fortunately, otherwise I would have wasted the last four years of my life), it is impossible to have a result like Theorem 0.1 for absolute Galois groups: not every profinite group is realizable as absolute Galois group, and in general it is a very hard problem to understand which profinite group is an absolute Galois group. For example, the celebrated Artin-Schreier Theorem states that the only finite group which is realizable as absolute Galois group is the finite group of order two (for example, as $\text{Gal}(\mathbb{C}/\mathbb{R})$, see Section 2.3 for the complete statement of the Artin-Schreier Theorem).

Thus, the problem to understand which profinite groups are realizable as absolute Galois groups – and also to recover some arithmetic information from the group – has caught the attention of algebraists and number theorists in the last decades, and many are working on it from different points of view, and using various tools.

A very powerful one is Galois Cohomology. Actually, the first comprehensive exposition of the theory of profinite groups appeared in the book *Cohomologie Galoisienne* by J-P. Serre in 1964, which is a milestone of Galois theory. The introduction of Galois cohomological techniques is doubtlessly one of the major landmarks of 20th century algebraic number theory and Galois theory. For example, class field theory for a field K is nowadays usually formulated via cohomological duality properties of the absolute Galois group G_K.

A recent remarkable developement in Galois cohomology is the complete proof of the **Bloch-Kato conjecture** by V. Voevodsky, with the substantial contribution of M. Rost (and the "patch" by C. Weibel). The first formulation of this conjecture is due to J. Milnor, with a later refinement by J. Tate (see Section 2.2 for a more detailed history of the conjecture). The conjecture states that there is a tight relation between the cohomology of the absolute Galois group G_K of a field K (a group-theoretic object), and the *Milnor $\mathcal{K}$-ring* of K (an arithmetic object). In particular, one has that the *Galois symbol*

$$\mathcal{K}_n^M(K)/m.\mathcal{K}_n^M(K) \xrightarrow{h_K} H^n\left(G_K, \mu_m^{\otimes n}\right) \tag{0.1}$$

from the n-th Milnor $\mathcal{K}$-group of K modulo m to the n-th cohomology group of G_K with coefficients in $\mu_m^{\otimes n}$, with μ_m the group of m-th roots of unity lying in $\bar{K}^{\mathrm{sep}}$, is an isomorphism for every $n \geq 1$ and for every $m \geq 2$ such that the characteristic of the field K does not divide m.

Therefore, after the proof of what is nowadays called the Rost-Voevodsky theorem, one has these two hopes:

(1) to recover information about the structure of the absolute Galois group from the structure of its cohomology;
(2) to recover arithmetic information from the structure of the cohomology of the absolute Galois group – and thus, possibly, from the group structure of G_K itself.

Yet, in general it is still rather hard to handle an absolute Galois group. Thus, for a prime number p, we shall focus our attention to the *pro-p groups* "contained" in an absolute Galois group G_K: the pro-p-Sylow subgroups of G_K (which are again absolute Galois groups) and, above all, the **maximal pro-p Galois group** $G_K(p)$ of K, i.e., the maximal pro-p quotient of the absolute Galois group G_K.[3] Indeed, pro-p groups are much more understood than profinite groups, and this reduction is not an "abdication", as such groups bring substantial information on the whole absolute Galois group, and in some cases they determine the structure of the field. Also, many arguments form Galois cohomology and from the study of Galois representations suggest that one should focus on pro-p quotient (cf. [**BT12**, Introduction]).

In particular, the Bloch-Kato conjecture has the following corollary: if the field K contains a primitive p-th root of unity (and usually one should assume that $\sqrt{-1}$ lies in K, if $p = 2$), then the Galois symbol induces the isomorphisms of (non-negatively) graded $\mathbb{F}_p$-algebras

$$\frac{\mathcal{K}_\bullet^M(K)}{p.\mathcal{K}_\bullet^M(K)} \simeq H^\bullet\left(G_K, \mu_p\right) \simeq H^\bullet\left(G_K(p), \mathbb{F}_p\right), \tag{0.2}$$

where the finite field $\mathbb{F}_p$ is a trivial $G_K(p)$-module, and $H^\bullet$ denotes the cohomology ring, equipped with the *cup product*. Since the Milnor $\mathcal{K}$-ring $\mathcal{K}_\bullet^M(K)$ is a *quadratic algebra* – i.e., a graded algebra generated by elements of degree one and whose relations are generated in degree two.

[3]Note that every pro-p-Sylow subgroup of an absolute Galois group, i.e., every absolute Galois group which is pro-p, is also the maximal pro-p quotient of itself, thus the class of maximal pro-p Galois groups is more general than the class of absolute Galois pro-p groups, and every result which holds for maximal pro-p Galois groups, holds also for absolute Galois groups which are pro-p.

also the $\mathbb{F}_p$-cohomology ring of the maximal pro-p Galois group $G_K(p)$ is a quadratic algebra over the field $\mathbb{F}_p$ This provides the inspiration for the definition of a **Bloch-Kato pro-p group**: a pro-p group such that the $\mathbb{F}_p$-cohomology ring of every closed subgroup is quadratic. Bloch-Kato pro-p groups were first introduced in [**BCMS**], and then defined and studied in [**Qu14**].

Another tool to study maximal pro-p Galois group is provided by the *cyclotomic character*, induced by the action of the absolute Galois group G_K on the roots of unity lying in $\bar{K}^{\text{sep}}$: in the case K contains μ_p, then the cyclotomic character induces a continuous homomorphism from the maximal pro-p Galois group $G_K(p)$ to the units of the ring of p-adic integers $\mathbb{Z}_p^\times$, called the *arithmetic orientation* of $G_K(p)$.

Thus, a continuous homomorphism of pro-p groups $\theta\colon G \to \mathbb{Z}_p^\times$ is called an orientation for G, and if G is a Bloch-Kato pro-p group and certain conditions on the induced Tate-twist module $\mathbb{Z}_p(1)$ are satisfied, the **orientation** is said to be **cyclotomic** (in particular, the group $H^2(G, \mathbb{Z}_p(1))$ has to be torsion-free, see Subsection 2.4.2), and the group G is said to be **cyclo-oriented**. Cyclo-oriented pro-p groups are a generalization of maximal pro-p Galois groups; we may say that they are "good candidates" for being realized as maximal pro-p Galois groups, as they have the right cohomological properties.

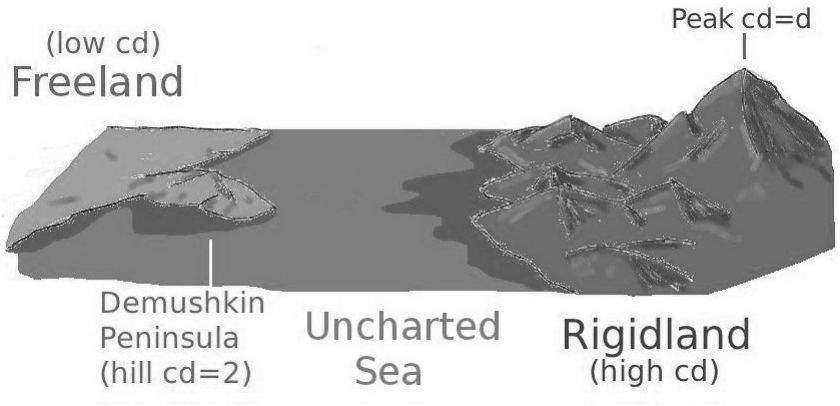
For a pro-p group G with cyclotomic orientation θ such that either $\text{im}(\theta)$ is trivial or $\text{im}(\theta) \simeq \mathbb{Z}_p$ – which is always the case if $p \neq 2$ – one has an epimorphism of graded $\mathbb{F}_p$-algebras

$$\bigwedge_\bullet (H^1(G, \mathbb{F}_p)) \twoheadrightarrow H^\bullet(G, \mathbb{F}_p) \ , \tag{0.3}$$

i.e., the $\mathbb{F}_p$-cohomology ring of G is an epimorphic image of the exterior algebra over $\mathbb{F}_p$ generated by the grup $H^1(G, \mathbb{F}_p)$.

If G is finitely generated, then we are given two bound-cases: when the morphism (0.3) is trivial and when it is an isomorphism. The former case is precisely the case of a free pro-p group, in the latter case the group is said to be **θ-abelian**. One may represent this situation with the picture below.[4]

[4] I displayed this picture the first time in a talk during a workshop organized at the Technion, Haifa, in honor of Prof. J. Sonn.



In fact, from the "mountain" side it is possible to recover the full structure of the group G, and also the arithmetic of the base field, in the case G is a maximal pro-p Galois group, as stated by the following theorem (see Theorem 3.12 and Theorem 3.18).

THEOREM 0.2. *Let G be a finitely generated cyclo-oriented pro-p group. Then the following are equivalent:*

(1) *the epimorphism* (0.3) *is an isomorphism;*
(2) *the cohomological dimension of G is equal to the minimal number of generators of G;*
(3) *G has a presentation*

$$G = \left\langle \sigma, \tau_1, \dots, \tau_d \;\middle|\; \sigma\tau_i\sigma^{-1} = \tau_i^{1+p^k}, \tau_i\tau_j = \tau_j\tau_i \;\forall\; i,j = 1,\dots,d \right\rangle$$

with $d \geq 1$ and $k \in \mathbb{N} \cup \{\infty\}$ such that $\mathrm{im}(\theta) = 1 + p^k\mathbb{Z}_p$.

Moreover, if G is the maximal pro-p Galois group of a field K containing a primitive p-th root of unity, the above conditions hold if, and only if, K is a p-rigid field, i.e., K has a p-Henselian valuation of rank d.

This last point has particular relevance, since there is much interest in construction of non-trivial valuations of fields. Such constructions became particularly important in recent years in connection with the so-called *birational anabelian geometry*, (cf. [**BT12**], [**Po94**]). This line of research originated from ideas of A. Grothendieck and of J. Neukirch: as stated, the goal is to recover the arithmtic structure of a field from its various canonical Galois groups. The point is that usually the first step is to recover enough valuations from their cohomological "footprints".

The "mountain-case" is discriminant for Bloch-Kato pro-p groups also in the sense specified by the following Tits alternative-type result (see Theorem 3.3).

THEOREM 0.3. *Let G be a Bloch-Kato pro-p group. Then either the epimorphism* (0.3) *is an isomorphism, or G contains a free non-abelian closed subgroup.*

Thus, every Bloch-Kato pro-p group which is floating in the "uncharted sea" contains a trace from the West shore. On the other hand, it is possible to generalize the situation of θ-abelian groups in the following way. Set the **θ-centre** of a cyclo-oriented pro-p group G to be the (normal) subgroup

$$\mathrm{Z}_\theta(G) = \left\{ \tau \in \ker(\theta) \;\middle|\; \sigma\tau\sigma^{-1} = \tau^{\theta(\sigma)} \text{ for all } \sigma \in G \right\} \tag{0.4}$$

Then $\mathrm{Z}_\theta(G)$ is the maximal abelian normal subgroup of G (cf. Proposition 4.18), and the short exact sequence

$$1 \longrightarrow \mathrm{Z}_\theta(G) \longrightarrow G \longrightarrow G/\mathrm{Z}_\theta(G) \longrightarrow 1 \tag{0.5}$$

splits (cf. Theorem 4.13). Note that in the case of a θ-abelian group, one has $\mathrm{Z}_\theta(G) = \ker(\theta)$, and the short exact sequence (0.5) clearly splits, as the presentation in Theorem 0.2 provides an explicit complement of the θ-centre in G. And as in Theorem 0.2, the θ-centre of a maximal pro-p Galois group detects the existence of non-trivial valuations, and its presence can be deduced also from the cohomology ring (cf. Theorem 4.19).

THEOREM 0.4. *Let K be a field containing a primitive p-th root of unity, with maximal pro-p Galois group $G_K(p)$ equipped with arithmetic orientation $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$. The following are equivalent:*

1. *the θ-centre of $G_K(p)$ is non-trivial;*
2. *the $\mathbb{F}_p$-cohomology ring of $G_K(p)$ is the skew-commutative tensor product of an exterior algebra with a quadratic algebra;*
3. *the field K has a p-Henselian valuation of rank equal to the rank of $\mathrm{Z}_\theta(G)$ as abelian pro-p group.*

The above result is particularly relevant for the importance of being able to find valuations, as underlined above. Indeed, with Theorem 0.4 we come full circle, as it completes the picture with the results contained in [**EK98**] and [**Ef06**]. Also, it shows that cyclotomic orientations provide an effective way to express such results.

It is possible to go a bit further, in order to see how the existence of a cyclotomic orientation for a pro-p group affects the structure of the whole group. For example, we show that the torsion in the abelianization of a finitely generated pro-p group with cyclotomic orientation is

induced by the "cyclotomic action" of the group (cf. Theorem 4.25). Note that the existence of a cyclotomic orientation is a rather restrictive condition: for example, certain free-by-Demushkin groups cannot be equipped with a cyclotomic orientation, as shown in Subsection 4.2.1.

Given a pro-p group G, one may associate to G another graded $\mathbb{F}_p$-algebra, besides the $\mathbb{F}_p$-cohomology ring: the graded algebra $\mathrm{gr}_\bullet(G)$ induced by the *augmentation ideal* of the completed group algebra $\mathbb{F}_p[\![G]\!]$.

In many relevant cases – such as free pro-p groups, Demushkin groups, θ-abelian groups – the $\mathbb{F}_p$-cohomology ring and the graded algebra of a maximal pro-p Galois group happen to be related via **Koszul duality** of quadratic algebra, and both algebras are **Koszul algebras** (for the definition of Koszul dual of a quadratic algebra see Definition 17, and for the definition of Koszul algebra see Definition 19).

Moreover, one has that if the relations of G satisfy certain "reasonable" conditions, then $H^\bullet(G, \mathbb{F}_p)$ and $\mathrm{gr}_\bullet(G)$ are Koszul dual (cf. Theorem 5.12). Thus, we conjecture that if K is a field containing a primitive p-th root of unity with finitely generated maximal pro-p Galois group $G_K(p)$, then $\mathbb{F}_p$-cohomology ring and the graded algebra of $G_K(p)$ are Koszul dual, and also that both algebras are Koszul algebras (cf. Question 4).

Here we study the graded algebra $\mathrm{gr}_\bullet(G)$ of a pro-p group G via the *restricted Lie algebra* induced by the **Zassenhaus filtration** of G. The study of the graded algebras induced by filtrations of pro-p groups has gained much interest recently, in particular the algebras induced by the Zassenhaus filtration, as well as the algebras induced by the p-descending central series (see [**La70, La85, La06**], [**MSp96**], [**CM08, CEM**]). For example, we prove the following result (Theorem 3.19), the proof of which uses indeed the Zassenhaus filtration of G, which generalizes [**CMQ**, Theorem A]:

THEOREM 0.5. *It is possible to detect whether a finitely generated Bloch-Kato pro-p group G is θ-abelian from the third element of its p-descending central series.*

Also, the Zassenhaus filtration is proving to be closely related to Massey products, which have shifted from their original field of application (topology) toward number theory: see [**Gä11**], [**Ef14**] and [**MT14**].

Albeit we have still only a glimpse of the structure of maximal pro-p Galois groups but in few specific cases (such as the two shores of the picture) there is a conjecture which states how a finitely generated

maximal pro-p Galois group should look like, the so called **Elementary Type Conjecture** (or ETC). Formulated first by I. Efrat in [**Ef97b**], the ETC states that finitely generated maximal pro-p Galois groups have a rather rigid structure: namely, they can be built starting from "elementary blocks" such as $\mathbb{Z}_p$ and Demushkin groups, via rather easy group-theoretic operations, such as free pro-p products and cyclotomic fibre products (defined in Definition 15).

The only evidences we have for this conjecture are:

(1) we have no counterexamples;
(2) it seems "just" it should be so;

which are not very strong. Yet, we show that all the classes of pro-p groups we study – Bloch-Kato pro-p groups, cyclo-oriented pro-p groups, Koszul duality groups and Koszul groups –, which are kind of generalizations of maximal pro-p Galois groups, are closed with respect to free pro-p products and cyclotomic fibre products, and this provides at least more sense to this conjecture.

Therefore, the aim of this thesis is to show that our approach toward Galois theory via the cohomology of maximal pro-p Galois groups (in particular studying Bloch-Kato pro-p groups and cyclotomic orientations) is particularly powerful and effective, as indeed it provides new consistent knowledge on maximal pro-p Galois groups, and it promises to bring more results in the future.

The thesis is structured in the following chapters:

(1) The first introductory chapter presents the theoretical background of the thesis. In particular, it introduces some preliminaries on pro-p groups, together with cohomology of profinite groups, Galois cohomology and restricted Lie algebras.

(2) First we introduce quadratic algebras and their properties. Then we present the Bloch-Kato conjecture, and we define Bloch-Kato pro-p groups and cyclo-oriented pro-p groups. Here we explore the first properties of these groups – for example, we prove an Artin-Schreier-type result for cyclo-oriented pro-p groups (cf. Corollary 2.14). Also, we introduce Demushkin groups and the ETC.

(3) Here we study the "mountain side" of cyclo-oriented pro-p groups, i.e., θ-abelian groups. We study the cup produt of such groups and we prove Theorem 0.3. In order to describe

the group structure of θ-abelian groups we study *locally powerful* pro-p groups, and we show that the two classes of group coincides (cf. Theorem 3.12). In order to explain the "arithmetic role" of θ-abelian groups we introduce p-rigid fields, and we prove Theorem 0.2. Then we compute the Zassenhaus filtration for such groups and we prove Theorem 0.5. Part of the content of this chapter is published in [**Qu14**] and [**CMQ**].

(4) In the fourth chapter we study free products and cyclotomic fibre products of cyclo-oriented pro-p groups. In particular, we show that (0.5) splits and we prove Theorem 0.4. Also, we show that the defining relations of a finitely generated cyclo-oriented pro-p group which induce torsion in the abelianization are induced by the cyclotomic action of the orientation (cf. Theorem 4.25). Part of the material contained in this chapter is being developed in [**QW2**].

(5) First we define the koszul dual of a quadratic algebra, and we study Koszul duality for cyclo-oriented pro-p groups. Then we define Koszul algebras. Part of the material contained in this chapter is being developed in [**MQRTW**].

CHAPTER 1

Preliminaries

1. Group cohomology and Galois cohomology

Throughout the whole thesis, subgroups are assumed to be closed with respect to the profinite topology, and the generators are assumed to be topological generators (i.e., we consider the closed subgroup generated by such elements).

1.1. Cohomology of profinite group. We recall briefly the construction of the cohomology groups for profinite groups, and the property we will use further. We refer mainly to [**NSW**, Ch. I].

Let G be a profinite group.

Definition 1. A **topological G-module** M is an abelian Hausdorff topological group which is an abstract G-module such that the action

$$G \times M \longrightarrow M$$

is a continuous map (with $G \times M$ equipped with the product topology).

For a closed subgroup $H \leq_c G$, we denote the subgroup of H-invariant elements in M by M^H, i.e.

$$M^H = \{m \in M \mid h.m = m \text{ for all } h \in H\}.$$

Assume now that M is a discrete module. For every $n \geq 1$, let $G^{\times n}$ be the direct product of n copies of G. For a G-module M, define $C^n(G, M)$ to be the **group of (inhomogeneous) cochains** of G with coefficients in M, i.e., $C^n(G, M)$ is the abelian group of the continuous maps $G^{\times n} \to M$, with the group structure induced by M. (Note that, if M is discrete, then a continuous map from $G^{\times n}$ to M is a map which is locally constant.) Also, define $C^0(G, M) = M$.

The $n+1$-coboundary operator $\partial^{n+1}\colon C^n(G,M) \to C^{n+1}(G,M)$ is given by

$$\begin{aligned}
\partial^1 a(g) &= g.a - a \quad \text{for } a \in M \\
\partial^2 f(g_1,g_2) &= g_1.f(g_2) - f(g_1g_2) + f(g_1), \quad f \in C^1(G,M) \\
&\vdots \\
\partial^{n+1} f(g_1,\ldots,g_{n+1}) &= g_1.f(g_2,\ldots,g_{n+1}) + \\
&\quad \sum_{i=1}^{n} (-1)^i f(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}) \\
&\quad +(-1)^{n+1} f(g_1,\ldots,g_n) \quad \text{for } f \in C^n(G,M).
\end{aligned}$$

Then one sets $Z^n(G,M) = \ker(\partial^{n+1})$, called the group of (inhomogeneous) n-cocycles, and $B^n(G,M) = \mathrm{im}(\partial^n)$, called the group of (inhomogeneous) n-coboundaries.

DEFINITION 2. For $n \geq 0$, the quotient

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

is called the **n-th cohomology group** of G with coefficients in the G-module M.

One has the following facts:

FACT 1.1. (i) *The 0-th cohomology group of a profinite group G with coefficients in M is the subgroup of G-invariant elements, i.e.,*

$$H^0(G,M) = M^G.$$

In particular, if G acts trivially on M, one has $H^0(G,M) = M$.

(ii) *The 1-cocycles are the continuous maps $f\colon G \to M$ such that*

$$f(g_1g_2) = f(g_1) + g_1.f(g_2) \quad \textit{for every } g_1, g_2 \in G.$$

They are also called crossed homomorphisms. The 1-coboundaries are the continuous maps $a\colon G \to M$ such that $a(g) = g.a - a$ for every $g \in G$. In particular, if G acts trivially on M, one has

$$H^1(G,M) = \mathrm{Hom}(G,M),$$

where $\mathrm{Hom}(G,M)$ is the group of (continuous) group homomorphisms from G to M.

The following proposition states a fundamental property of group cohomology (cf. [**NSW**, Theorem 1.3.2]).

PROPOSITION 1.2. *For an exact sequence* $0 \to A \to B \to C \to 0$ *of* G*-modules, one has connecting homomorphisms*

$$\delta^n \colon H^n(G, C) \longrightarrow H^{n+1}(G, A)$$

for every $n \geq 0$*, such that*

$$\cdots \longrightarrow H^n(G, A) \longrightarrow H^n(G, B) \longrightarrow H^n(G, C) \xrightarrow{\delta^n} H^{n+1}(G, A) \longrightarrow \cdots$$

is a long exact sequence.

Also, the following result states the behavior of low-degree cohomology with respect of normal subgroups and quotients (cf. [**NSW**, Prop. 1.6.7]).

PROPOSITION 1.3. *Let* N *be a normal closed subgroup of* G*. Then one has an exact sequence*

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\inf^1_{G,N}} H^1(G, A) \xrightarrow{\mathrm{res}^1_{G,N}} H^1(N, A)^G \xrightarrow{tg_{G,N}} H^2(G/N, A^N) \xrightarrow{\inf^2_{G,N}} H^2(G, A)$$

called the five term exact sequence. The map $tg_{G,N}$ *is called transgression.*

Let A, B, C be G-modules with bilinear pairings

$$A \times B \longrightarrow A \otimes_{\mathbb{Z}} B \longrightarrow C. \tag{1.1}$$

Then (1.1) induces the map

$$H^n(G, A) \times H^m(G, B) \xrightarrow{\cup} H^{n+m}(G, C)$$

called the **cup-product**, which has a very important role in the Bloch-Kato conjecture, as we shall see later. The cup-product has the following property (cf. [**NSW**, Prop. 1.4.4]).

PROPOSITION 1.4. *The cup-product is associative and skew-commutative, i.e., for $\alpha \in H^n(G,A)$, $\beta \in H^m(G,B)$ and $\gamma \in H^h(G,C)$, one has*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \quad \textit{and} \quad \alpha \cup \beta = (-1)^{nm} \beta \cup \alpha,$$

with the identifications

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \quad \textit{and} \quad A \otimes B = B \otimes A.$$

REMARK 1.5. In the case the G-module is a ring k such that $k \otimes_{\mathbb{Z}} k = k$ (e.g., $k = \mathbb{Z}, \mathbb{F}_p$), the cup product makes the cohomology of G with M-coefficients a graded-commutative k-algebra.

For a profinite group G the *first Bockstein homomorphism*

$$\beta^1 \colon H^1(G, \mathbb{F}_p) \longrightarrow H^2(G, \mathbb{F}_p) \tag{1.2}$$

is the connecting homomorphism arising from the short exact sequence of trivial G-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

In the case $p = 2$, the first Bockstein morphism is related to the cup product in the following way (cf. [**EM11**, Lemma 2.4]).

LEMMA 1.6. *Let G be a profinite group. Then, for every $\chi \in H^1(G, \mathbb{F}_2)$ one has $\beta^1(\chi) = \chi \cup \chi$.*

1.2. Continuous cohomology. Fix a profinite group G. The complete group algebra of G over $\mathbb{Z}_p$ is the topological inverse limit

$$\mathbb{Z}_p[\![G]\!] = \varprojlim_{U \lhd_o G} \mathbb{Z}_p[G/U],$$

where U runs through the open normal subgroups of G, and $\mathbb{Z}_p[G/U]$ is the group algebra defined in the usual way for finite groups. Then $\mathbb{Z}_p[\![G]\!]$ is a compact $\mathbb{Z}_p$-algebra. Thus, if M is a topological G-module which is also a (continuous) $\mathbb{Z}_p$-module, then M is a topological $\mathbb{Z}_p[\![G]\!]$-module.

Let $\mathbb{Q}_p$ be the field of p-adic numbers. Then the embedding $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ induces a short exact sequence

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Q}_p \longrightarrow \mathbb{I}_p \longrightarrow 0 \tag{1.3}$$

which defines the discrete $\mathbb{Z}_p$-module $\mathbb{I}_p$. In particular, $\mathbb{Z}_p$ and $\mathbb{I}_p$ can be considered as topological $\mathbb{Z}_p[\![G]\!]$-modules, the former complete and the latter discrete, with the topology inherited from $\mathbb{Q}_p$. An essential tool for working with profinite groups and $\mathbb{Z}_p$-modules is **Pontryagin duality**.

DEFINITION 3. Let M be a Hausdorff, abelian and locally compact $\mathbb{Z}_p$-module (e.g., a pro-p group, a compact $\mathbb{Z}_p$-module or a discrete $\mathbb{Z}_p$-module). We call the group

$$M^\vee = \mathrm{Hom}_{\mathrm{cts}}(M, \mathbb{I}_p)$$

the **Pontryagin dual** of M.

For every $\mathbb{Z}_p$ module M, one has $(M^\vee)^\vee = M$. In particular, if M is a compact $\mathbb{Z}_p$-module, then $M^\vee$ is a discrete $\mathbb{Z}_p$-module, and conversely. Thus, Pontryagin duality induces an equivalence (of categories) between the two categories of compact $\mathbb{Z}_p$-modules and discrete $\mathbb{Z}_p$-modules.

For a profinite group G, the category of compact $\mathbb{Z}_p[\![G]\!]$-modules has sufficiently many projectives, and the category of discrete $\mathbb{Z}_p[\![G]\!]$-modules has sufficiently many injectives. Hence, it is possible to define Ext-functors for the two categories in the usual way – see [**Br66**], [**NSW**, § V.2]) and [**SW00**]. Then, one has the following result.

PROPOSITION 1.7. *For continuous $\mathbb{Z}_p[\![G]\!]$-module N, one has the isomorphisms*

$$H^n(G, N) \simeq \mathrm{Ext}^n_{\mathbb{Z}_p[\![G]\!]}(\mathbb{Z}_p, N)$$

for every $n \geq 0$ Moreover, if N is discrete, one has the canonical isomorphisms

$$H_n(G, N^\vee) \simeq H^n(G, N)^\vee.$$

For a detailed exposition on continuous cohomology of profinite groups (which would go far beyond the aims of this thesis) see the aforementioned works by A. Brumer, by J. Neukirch and by P. Symonds and Th. Weigel. For a brief introduction to cohomology and homology of profinite groups, see also [**Ri13**, § 3.4-7].

For a (topologically) finitely generated torsion-free $\mathbb{Z}_p[\![G]\!]$-module M, one has also the following property. Set $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$ and $N = \mathbb{I}_p \otimes_{\mathbb{Z}_p} M$. In particular, V is a $\mathbb{Q}_p$-vector space of finite dimension, and N is a discrete divisible p-primary torsion group, and (1.3) induces the short exact sequence

$$0 \longrightarrow M \longrightarrow V \longrightarrow N \longrightarrow 0. \tag{1.4}$$

Then one has the following result (cf. [**Ta76**, Prop. 2.3] and [**NSW**, Prop. 2.7.11]).

PROPOSITION 1.8. *For every $n \geq 0$ one has isomorphisms*

$$H^n(G, V) \simeq H^n(G, M) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

and in the exact cohomology induced by (1.4)*, the kernel of the boundary homomorphism $\delta^n \colon H^{n-1}(G, N) \to H^n(G, M)$ is the maximal divisible $\mathbb{Z}_p$-submodule of $H^{n-1}(G, N)$, and its image is the torsion $\mathbb{Z}_p$-submodule of $H^n(G, M)$.*

DEFINITION 4. The cohomological dimension $\mathrm{cd}(G)$ of a profinite group G is the least non-negative integer n such that

$$H^m(G, M) = 0 \quad \text{for all } m > n$$

and for every discrete G-module M which is a torsion abelian group, and it is infinite if no such integer exists.

If G is a pro-p group, then $\mathrm{cd}(G) \leq n$ if, and only if $H^{n+1}(G, \mathbb{F}_p) = 0$, where $\mathbb{F}_p$ is a trivial G-module.

2. Preliminaries on pro-p groups

Let G be a profinite group, and let m be a positive integer. We define G^m and $[G, G]$ to be the closed subgroups of G generated by the m-th powers of G, resp. by the commutators[1] of G. I.e.,

$$G^m = \langle g^m \,|g \in G\rangle \leq_c G \quad \text{and} \quad [G, G] = \langle [g_1, g_2] \,|g_1, g_2 \in G\rangle \leq_c G.$$

DEFINITION 5. Let G be a profinite group.

(i) A subset $\mathcal{X}$ of G is said to be a *system of (topological) generators* of G if the closed subgroup of G generated by $\mathcal{X}$ is G itself. Moreover, the system $\mathcal{X}$ is said to be *minimal* if any proper subset of $\mathcal{X}$ generates a proper subgroup of G.

(ii) The group G is *finitely generated* if it has a generating system which is a finite subset. The minimal number of generators of G – i.e., the (finite) cardinality of a minimal generating system

[1] We use the left notation for the conjugation of group elements: namely,

$${}^x y = xyx^{-1} \quad \text{and} \quad [x, y] = {}^x y \cdot y^{-1} = xyx^{-1}y^{-1}.$$

$\mathcal{X}$ of G – will be denoted by $d(G)$, and sometimes it will be called the "dimension" of G.[2]

(iii) Let F be a free profinite group. A short exact sequence of profinite groups

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G \longrightarrow 1 \ , \tag{1.5}$$

is called a *presentation* of G. The the elements R are called the *relations* of G, and the generators of R as (closed) normal subgroup of F are called *defining relations* of G. If G is finitely generated, then the presentation (1.5) is said to be *minimal* if $d(F) = d(G)$. Moreover, if the minimal number of generators of R as normal subgroup is finite, then it is denoted by $r(G)$, and G is said to be *finitely presented*. In particular, it is possible to present explicitly G in the following way:

$$G = \langle x \in \mathcal{X} \mid \rho = 1, \rho \in \mathcal{R} \rangle,$$

with $\mathcal{R} \subset R$ a minimal system of defining relations. Finally, if G is a pro-p group, then

$$r(G) = \dim_{\mathbb{F}_p} \left(H^2(G, \mathbb{F}_p) \right) \tag{1.6}$$

(cf. [**NSW**, Prop. 3.9.5]).

(iv) The *rank* of G is defined by

$$\mathrm{rk}(G) = \sup\{d(C) \mid C \leq_c G\} = \sup\{d(C) \mid C \leq_o G\}$$

(see [**DdSMS**, § 3.2]).

2.1. Filtrations of pro-p groups. Recall that the terms of the *lower central series* are defined by

$$\gamma_1(G) = G, \quad \gamma_2(G) = [G, G], \quad \dots \quad \gamma_i(G) = [\gamma_{n-1}(G), G]$$

for every $i \geq 1$.

The *Frattini subgroup* $\Phi(G)$ of a profinite group G is the intersection of all the maximal proper open subgroups of G. The Frattini subgroup of G is a closed subgroup, and if $\mathcal{X} \subset G$ is a system of generators of G, then $\mathcal{X}\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$ (cf. [**DdSMS**, Prop. 1.9]). Note that if (1.5) is a minimal presentation of G, then $R \subseteq \Phi(F)$.

[2]Following the notation of [**DdSMS**]: indeed this makes sense in the case of analytic pro-p groups.

If G is a pro-p group, then one has the following (cf. [**DdSMS**, Prop. 1.13]).

PROPOSITION 1.9. *If G is pro-p, then*

$$\Phi(G) = G^p[G, G],$$

and the quotient group $G/\Phi(G)$ is a $\mathbb{F}_p$-vector space. In particular, G is finitely generated if, and only if, $G/\Phi(G)$ has finite dimension as $\mathbb{F}_p$-vector space, and $d(G) = \dim(G/\Phi(G))$.

The **p-descending central series** of a pro-p group is a sort of "p-refinement" of the central series, and it is defined by

$$\lambda_1(G) = G, \quad \lambda_2(G) = \Phi(G), \quad \dots \quad \lambda_{i+1}(G) = \lambda_i(G)^p \left[G, \lambda_i(G)\right],$$

for every $i \geq 1$.

REMARK 1.10. In [**DdSMS**] the notation $P_i(G)$ is used instead of $\lambda_i(G)$, and D. Segal informally refers to this series as "the pigs series". Other authors, as I. Efrat and J. Mináč, use the notation $G^{(i)}$ instead of $\lambda_i(G)$ (see [**CEM, CMQ, EM11**]). Finally, authors from the "Neukirch's school" use the notation G^i instead of $\lambda_i(G)$, and G_i instead of $\gamma_i(G)$ (see [**NSW**, § III.8] and [**Gä11**]).

The p-descending central series has the following properties.

PROPOSITION 1.11. *Let G be a pro-p group.*

(i) $[\lambda_i(G), \lambda_j(G)] \leq \lambda_{i+j}(G)$ *for all* $i, j \geq 1$.
(ii) *If G is finitely generated then $\lambda_i(G)$ is open for every $i \geq 1$, and the set $\{\lambda_i(G), i \geq 1\}$ is a basis of neighbourhoods of* $1 \in G$.

The **Zassenhaus filtration** of an arbitrary group G (not necessarily a pro-p group) is the descending series defined by $D_1(G) = G$ and

$$D_i(G) = D_{\lceil i/p \rceil}(G)^p \prod_{j+h=i} [D_j(G), D_h(G)]$$

for every $i \geq 1$, where $\lceil i/p \rceil$ is the least integer m such that $pm \geq i$. This series is also called *Jennings filtration* and the groups $D_i(G)$ are called *dimension subgroups* of G in characteristic p. Note that if G is pro-p, then $D_2(G) = \Phi(G)$. Such series has the following properties (cf. [**DdSMS**, § 11.1]).

PROPOSITION 1.12. (i) *For each $i, j \geq 1$, one has*

$$[D_i(G), D_j(G)] \leq D_{i+j}(G) \quad \textit{and} \quad D_i(G)^p \leq D_{pi}(G),$$

and it is the fastest descending series with these properties.[3]

(ii) *For each $i \geq 1$, one has the formula*

$$D_i(G) = \prod_{jp^h \geq i} \gamma_j(G)^{p^h}, \tag{1.7}$$

due to M. Lazard.

(iii) *If G is a finitely generated pro-p group, then G has finite rank if, and only if, $D_i(G) = D_{i+1}(G)$ for some $i \geq 1$ (this result is due to M. Lazard and D. Riley).*

3. Restricted Lie algebras

Unless stated otherwise, if L is a Lie algebra (over an arbitrary commutative ring), we denote by $(\_,\_)\colon L \times L \to L$ its Lie bracket, and for $v \in L$ the notation

$$\mathrm{ad}(v)\colon L \longrightarrow L, \quad w \longmapsto (v, w)$$

denotes the adjoint endomorphism. Throughout this section, let $\mathbb{F}$ denote a field of characteristic $p > 0$.

DEFINITION 6. A restricted Lie algebra over $\mathbb{F}$ is a $\mathbb{F}$-Lie algebra L equipped with a map

$$\_^{[p]}\colon L \longrightarrow L$$

satisfying the following properties:

(i) $(av)^{[p]} = a^p v^{[p]}$, with $a \in \mathbb{F}$ and $v \in L$;

(ii) $(v + w)^{[p]} = v^{[p]} + w^{[p]} + \sum_{i=1}^{p-1} \frac{s_i(v,w)}{i}$, where $v, w \in L$, and the $s_i(v, w)$ denote the coefficients of λ^{i-1} in the formal expression $\mathrm{ad}(\lambda v + w)^{p-1}(v)$;

(iii) $\mathrm{ad}(v^{[p]}) = \mathrm{ad}(v)^p$, with $v \in L$.

In fact it is possible to see a restricted Lie algebra over $\mathbb{F}$ as a subalgebra of a $\mathbb{F}$-algebra. For any associative $\mathbb{F}$-algebra A, let A_L be the induced Lie algebra, i.e., $A_L = A$ and

$$(a, b) = ab - ba \quad \text{for all } a, b \in A.$$

[3]Namely, if $\{\tilde{D}_i(G)\}$ is another descending series satisfying these two properties, then $\tilde{D}_i(G) \supseteq D_i(G)$ for every $i \geq 1$.

A Lie subalgebra L of A_L is said to be restricted if $a^p \in L$ for every $a \in L$. Equivalently, a $\mathbb{F}$-Lie algebra L together with a unitary operation $\_^{[p]}$ is said to be restricted if there exists an associative $\mathbb{F}$-algebra A and a Lie algebras monomorphisms $\iota\colon L \to A_L$ such that

$$\iota\left(a^{[p]}\right) = \iota(a)^p \quad \text{for every } a \in L.$$

The pair (A, ι) is called a *restricted envelope* for L.

An ideal $\mathfrak{r}$ of a restricted Lie algebra L is an ideal of the underlying Lie algebra of L which is also closed under the operation $\_^{[p]}$. Thus the quotient $L/\mathfrak{r}$ is again a restricted $\mathbb{F}$-Lie algebra. A homomorphism of restricted Lie algebras is a homomorphism of Lie algebras that commutes with the operations $\_^{[p]}$.

Definition 7. Let L be a restricted Lie algebra over $\mathbb{F}$. An associative $\mathbb{F}$-algebra $\mathcal{U}_p(L)$ equipped with a monomorphism of restricted Lie algebras

$$\psi_L\colon L \longrightarrow \mathcal{U}_p(L) \tag{1.8}$$

is called **universal restricted envelope** of L, if it is a restricted envelope for L and it satisfies the usual universal property: for any restricted Lie algebras homomorphism $\phi\colon L \to B_L$, with B a $\mathbb{F}$-algebra, there exists a unique $\mathbb{F}$-algebra homomorphism $\tilde{\phi}\colon \mathcal{U}_p(L) \to B$ such that $\tilde{\phi} \circ \psi_L = \phi$.

For every restricted Lie algebras there exists a unique universal restricted envelope [**Gä11**, Prop. 1.2.4], and the morphism ψ_L is injective [**Gä11**, Prop. 1.2.5].

Free restricted Lie algebras over $\mathbb{F}$ are defined via the usual property. It is possible to construct such a restricted Lie algebra as follows. Given a set of indeterminates $\mathcal{X} = \{X_i, i \in \mathcal{I}\}$, let $\mathbb{F}\langle\mathcal{X}\rangle$ be the free associative $\mathbb{F}$-algebra on $\mathcal{X}$, and let L be the restricted subalgebra of $\mathbb{F}\langle\mathcal{X}\rangle_L$ generated by $\mathcal{X}$. Then L is the free restricted $\mathbb{F}$-Lie algebra with free generating set $\mathcal{X}$, denoted by $L_p(\mathcal{X})$. In particular, one has the following (cf. [**Gä11**, Prop. 1.2.7]).

Proposition 1.13. *The restricted universal envelope of the free restricted Lie algebra $L_p(\mathcal{X})$ is the algebra $\mathbb{F}\langle\mathcal{X}\rangle$, via the monomorphism which sends every X_i to itself.*

3.1. The restricted Lie algebra induced by the Zassenhaus filtration. We are interested in restricted Lie algebras, as the Zassenhaus filtration of a pro-p group induces a structure of restricted Lie algebra over $\mathbb{F}_p$. Indeed, given a pro-p group put

$$L_i(G) = D_i(G)/D_{i+1}(G) \quad \text{and} \quad L_\bullet(G) = \bigoplus_{i=1}^{\infty} L_i(G)$$

for $i \geq 1$. Then every $L_i(G)$ is a $\mathbb{F}_p$-vector space, and the graded space $L_\bullet(G)$ comes equipped with two further operations. Let $v \in L_i(G)$, $v = xD_{i+1}(G)$, and $w \in L_j(G)$, $w = yD_{j+1}(G)$, for some $x, y \in G$. Then one may define

$$\begin{aligned} (v, w) &= [x, y]D_{i+j+1} \in L_{i+j}(G), \\ v^{[p]} &= x^p D_{pi+1} \in L_{pi}(G), \end{aligned}$$

which make $L_\bullet(G)$ a restricted Lie algebra over $\mathbb{F}_p$ (cf. [**DdSMS**, Theorem 12.8.(i)]).

Moreover, the restricted $\mathbb{F}_p$-Lie algebra $L_\bullet(G)$ of a pro-p group G is thightly related to the group algebra $\mathbb{F}_p[G]$. Let $\omega_{\mathbb{F}_p[G]}$ be the augmentation ideal of $\mathbb{F}_p[G]$ (i.e., $\omega_{\mathbb{F}_p[G]}$ is the two-sided ideal of $\mathbb{F}_p[G]$ generated by the elements $x - 1$, with $x \in G$), and put

$$\begin{aligned} &\mathrm{gr}_1(G) = \mathbb{F}_p[G]/\omega_{\mathbb{F}_p[G]} \simeq \mathbb{F}_p, \quad \mathrm{gr}_{i+1}(G) = \omega^i_{\mathbb{F}_p[G]}/\omega^{i+1}_{\mathbb{F}_p[G]}, \\ &\mathrm{gr}_\bullet(G) = \bigoplus_{i=1}^{\infty} \mathrm{gr}_i(G) \end{aligned}$$

for $i \geq 1$. Then every $\mathrm{gr}_i(G)$ is a $\mathbb{F}_p$-vector space, and $\mathrm{gr}_\bullet(G)$ is a graded associative $\mathbb{F}_p$-algebra. Then one has the following result, due to S. Jennings (cf. [**DdSMS**, Theorems 12.8-12.9]).

THEOREM 1.14. *Let $\vartheta\colon L_\bullet(G) \to \mathrm{gr}_\bullet(G)$ be the morphism of graded $\mathbb{F}_p$-algebras defined by*

$$\vartheta(xD_{i+1}) = (x - 1) + \omega_G^{i+1}, \quad \textit{for } xD_{i+1} \in L_i(G), i \geq 1.$$

Then ϑ is a monomorphism of restricted Lie algebras, and $\mathrm{gr}_\bullet(G)$ is the universal restricted envelope of $L_\bullet(G)$. In particular, one has

$$D_i(G) = (1 + \omega_G^i) \cap G$$

for every $i \geq 1$.

Let x be an element of G, and let $i \geq 1$ such that $x \in D_i(G) \smallsetminus D_{i+1}(G)$. Then the image $\bar{x}$ of x in the quotient $D_i(G)/D_{i+1}(G)$ is said to be the *initial form* of x in $L_\bullet(G)$ (and in $\mathrm{gr}_\bullet(G)$).

REMARK 1.15. The restricted Lie algebra $L_\bullet(G)$ of a pro-p group G and the restricted envelope $\mathrm{gr}_\bullet(G)$ are to be intended as "linearizations" of the group itself: since Lie algebras and associative algebras are easier to handle than groups, they are supposed to provide new tools to study pro-p groups.

3.2. Restricted Lie algebras of free groups. The class of pro-p groups for which the induced restricted Lie algebras are best understood are free pro-p groups. Let F be a finitely generated free pro-p groups with minimal generating system $\{x_1, \ldots, x_d\}$, with $d = d(F)$, and let $\mathcal{X} = \{X_1, \ldots, X_d\}$ be a set of non commutative indeterminates. Then one has the following (cf. [**Gä11**, Theorem 1.3.8]).

THEOREM 1.16. *Let F be a finitely generated free pro-p group, and let $\mathcal{X}$ be as above, with $d = d(F)$. The restricted Lie algebra over $\mathbb{F}_p$ induced by the Zassenhaus filtration of F is free, i.e., one has*

$$L_\bullet(F) \xrightarrow{\sim} L_p(\mathcal{X}), \quad \bar{x}_i \longmapsto X_i$$

for every $i = 1, \ldots, d$, where $\bar{x}_i \in L_1(F)$ is the initial form of x_i.

In particular, by Proposition 1.13 and Theorem 1.14, the graded algebra $\mathrm{gr}_\bullet(F)$ is isomorphic to the algebra $\mathbb{F}_p\langle\mathcal{X}\rangle$, considered with the grading induced by the degree of the monomials.

REMARK 1.17. Let $\mathbb{F}_p\langle\langle\mathcal{X}\rangle\rangle$ be the *Magnus algebra*, i.e., the $\mathbb{F}_p$-algebra of formal series on the non-commutative indeterminates $\mathcal{X}$. It is well known that one has a continuous isomorphisms $\mathbb{F}_p[\![F]\!] \simeq \mathbb{F}_p\langle\langle\mathcal{X}\rangle\rangle$ given by $x_i \mapsto 1 + X_i$ for every $i = 1, \ldots, d(F)$. Then the powers of the augmentation ideal $\omega_{\mathbb{F}_p[\![F]\!]}$ of $\mathbb{F}_p[\![F]\!]$, and the powers of the ideal $\langle X_1, \ldots, X_{d(F)}\rangle$ of the Magnus algebra induce an isomorphism of graded $\mathbb{F}_p$-algebras $\mathrm{gr}_\bullet(F) \simeq \mathbb{F}_p\langle\mathcal{X}\rangle$ given by $\bar{x}_i \mapsto X_i$ for every $i = 1, \ldots, d(F)$.

One has also the following useful property (cf. [**Gä11**, Prop. 1.2.6])

PROPOSITION 1.18. *Let L be a restricted $\mathbb{F}$-Lie algebra and let $\mathfrak{r} \lhd L$ be an ideal. Let $\mathcal{R}$ denote the left ideal of $\mathcal{U}_p(L)$ generated by $\psi_L(\mathfrak{r})$ Then $\mathcal{R}$ is a two-sided ideal and the canonical epimorphism $L \twoheadrightarrow L/\mathfrak{r}$ induces an exact sequence*

$$0 \longrightarrow \mathcal{R} \longrightarrow \mathcal{U}_p(L) \longrightarrow \mathcal{U}_p(L/\mathfrak{r}) \longrightarrow 0 \ .$$

4. Cohomology of Galois groups and Kummer theory

Fix a field K, and let L/K be a Galois extension of fields. Then the multiplicative group $L^\times$ is a module of the Galois group $\mathrm{Gal}(L/K)$. The celebrated Hilbert's Satz 90 (Noether's version) states that the first cohomology group of $\mathrm{Gal}(L/K)$ with coefficients in $L^\times$ is trivial, i.e.,

$$H^1\left(\mathrm{Gal}(L/K), L^\times\right) = 1. \tag{1.9}$$

Given a field K and a positive integer m, let $\mu_m = \mu_m(K)$ be the group of the roots of unity of order m contained in K, namely,

$$\mu_m(K) = \left\{\zeta \in K^\times \mid \zeta^m = 1\right\}.$$

Thus, one has the short exact sequence of G_K-modules

$$1 \longrightarrow \mu_m(\bar{K}^{\mathrm{sep}}) \longrightarrow (\bar{K}^{\mathrm{sep}})^\times \xrightarrow{m} (\bar{K}^{\mathrm{sep}})^\times \longrightarrow 1, \tag{1.10}$$

which induces the exact sequence in cohomology

$$K^\times \xrightarrow{m} K^\times \longrightarrow H^1\left(G_K, \mu_m(\bar{K}^{\mathrm{sep}})\right) \longrightarrow H^1\left(G_K, (\bar{K}^{\mathrm{sep}})^\times\right) = 0,$$

and hence an isomorphism $K^\times/(K^\times)^m \simeq H^1(G_K, \mu_m(\bar{K}^{\mathrm{sep}}))$. In particular, assume that the field K contains a primitive m^{th}-root of unity, i.e., $\mu_m(\bar{K}^{\mathrm{sep}}) \subseteq K$. Then μ_m is a trivial G_K-module which is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. This yields the isomorphism

$$\phi_K \colon \frac{K^\times}{(K^\times)^m} \xrightarrow{\sim} H^1\left(G_K, \mathbb{Z}/m\mathbb{Z}\right) = \mathrm{Hom}\left(G_K, \mathbb{Z}/m\mathbb{Z}\right), \tag{1.11}$$

where the equality follows from Fact 1.1, called the *Kummer isomorphism*. In particular, fix an isomorphism of G-modules $\mu_m \simeq \mathbb{Z}/m\mathbb{Z}$. Then one has

$$\phi_K(\bar{a})(\sigma) = \frac{\sigma\left(\sqrt[m]{a}\right)}{\sqrt[m]{a}} \in \mu_m, \tag{1.12}$$

with $\bar{a} = a \bmod (K^\times)^m$ (cf. [**CMQ**, (3.1)]).

Now let $K(p)$ be the **p-closure** of K, i.e., $K(p)/K$ is the maximal p-extension of K, and let $G_K(p) = \mathrm{Gal}(K(p)/K)$ be the *maximal pro-p Galois group* of K. Assume that K contains all the roots of unity of p-power order. Then Hilbert's Sats 90 holds for the extension $K(p)/K$,

and (1.12), together with a fixed isomorphism of trivial $G_K(p)$-modules $\mu_p \simeq \mathbb{F}_p$, yields an isomorphism

$$K^\times/(K^\times)^p \simeq H^1(G_K(p), \mathbb{F}_p) \tag{1.13}$$

Recall from Proposition 1.9 that for a pro-p group G, the quotient $G/\Phi(G)$ is a $\mathbb{F}_p$-vector space. Then one has the following (cf. [**NSW**, Prop. 3.9.1]).

COROLLARY 1.19. *Let G be a pro-p group. Then the cohomology group $H^1(G, \mathbb{F}_p)$ is the Pontryagin dual of the quotient $G/\Phi(G)$, i.e.,*

$$H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p) = \mathrm{Hom}(G/\Phi(G), \mathbb{I}_p) = (G/\Phi(G))^\vee, \tag{1.14}$$

and the groups $H^1(G, \mathbb{F}_p)$ and $G/\Phi(G)$ are isomorphic as (discrete) $\mathbb{F}_p$-vector spaces. In particular, if G is finitely generated, then

$$\dim_{\mathbb{F}_p}(H^1(G, \mathbb{F}_p)) = \dim_{\mathbb{F}_p}(G/\Phi(G)) = d(G).$$

Thus, if $\mathcal{X} = \{x_i, i \in \mathcal{I}\} \subset G$ is a minimal system of generators of G, the dual $\mathcal{X}^\vee$ is a basis for $H^1(G, \mathbb{F}_p)$, with $\mathcal{X}^\vee = \{\chi_i, i \in \mathcal{I}\}$ such that $\chi_i(x_j) = \delta_{ij}$ for every $i, j \in \mathcal{I}$. Therefore, the isomorphisms (1.13) and (1.14) yield the isomorphism of discrete $\mathbb{F}_p$-vector spaces

$$K^\times/(K^\times)^p \simeq G_K(p)/\Phi\left(G_K(p)\right)$$

(with K satisfying the above conditions). Hence, if $\{a_i, i \in \mathcal{I}\} \subset K^\times \smallsetminus (K^\times)^p$ is a set of representatives of $K^\times/(K^\times)^p$, one has the minimal generating sistem $\mathcal{X}$ of $G_K(p)$ such that

$$\frac{x_j(\sqrt[p]{a_i})}{\sqrt[p]{a_i}} = \begin{cases} \zeta & \text{if } i = j \\ 1 & \text{if } i \neq j \end{cases} \tag{1.15}$$

with $\zeta \in K$ a fixed primitive p-th root of unity, and the dual basis $\mathcal{X}^\vee \subset H^1(G_K(p), \mathbb{F}_p)$.

Finally, one has this classic result (see also [**Ge13**, § 3.6] and [**BT12**, § 3]).

PROPOSITION 1.20. *Assume K contains a primitive p-th root of unity, and let $K(\sqrt[p]{K}) = K(\sqrt[p]{a}, a \in K)$. Then $K(\sqrt[p]{K})/K$ is Galois, and it is the compositum of all finite cyclic extensions of K of degree p. Its Galois group is*

$$\mathrm{Gal}\left(K(\sqrt[p]{K})/K\right) = G_K(p)/\Phi(G_K(p)) \simeq \left(K^\times/(K^\times)^p\right)^\vee,$$

i.e., $G_{K(\sqrt[p]{K})} = \Phi(G_K(p))$.

One has an arithmetical interpretation also for the second cohomology group of a Galois group. Indeed, for a Galois extension L/K one has canonical isomorphisms

$$H^2(\mathrm{Gal}(L/K), \bar{L}^\times) \xrightarrow{\sim} \mathrm{Br}(L/K) \ ,$$

where $\mathrm{Br}(L/K)$ is the *Brauer group* of L/K (cf. [**NSW**, Theorem 6.3.4]). In particular, one has $H^2(G_K, (\bar{K}^{\mathrm{sep}})^\times) \simeq \mathrm{Br}(K)$, with $\mathrm{Br}(K)$ the Brauer group of K. Thus, for a positive integer m the short exact sequence (1.10), together with Hilbert's Satz 90, induces the exact sequence in cohomology

$$0 \longrightarrow H^2(G_K, \mu_m) \longrightarrow \mathrm{Br}(K) \xrightarrow{m} \mathrm{Br}(K) \ ,$$

which implies the following.

Corollary 1.21. *Let m be a positive integer such that the characteristic of K does not divide m. Then $H^2(G_K, \mu_m)$ is (canonically) isomorphic to $\mathrm{Br}_m(K)$, the subgroup of the Brauer group of K of exponent m.*

CHAPTER 2

The Bloch-Kato conjecture

1. Quadratic algebras

Fix a ring R, and let $A_\bullet$ be a non-negatively graded R-algebra, i.e., $A_\bullet = \bigoplus_{n\geq 0} A_n$ with $A_0 = R$ and A_n a R-module for every $n \geq 1$, together with a product such that if $a \in A_n$ and $b \in A_m$, then $ab \in A_{n+m}$.

A graded algebra $A_\bullet$ is said to be **quadratic** if A_n is generated by products of n elements of A_1, with $n > 0$, and the defining relations of $A_\bullet$ are generated by elements of degree 2: namely

$$A_\bullet \simeq \frac{\mathcal{T}^\bullet(A_1)}{\mathcal{R}}, \quad \mathcal{T}^\bullet(A_1) = \bigoplus_{n\geq 0} A_1^{\otimes n}, \tag{2.1}$$

where $\mathcal{R}$ is a two-sided ideal of $\mathcal{T}^\bullet(A_1)$ generated by elements of $A_1 \otimes_R A_1$.

Examples 1. Let $\mathbb{F}$ be a field, and let V be a $\mathbb{F}$-vector space.

(a) The symmetric algebra $S_\bullet(V)$ is a quadratic $\mathbb{F}$-algebra, as

$$S_\bullet(V) = \frac{\mathcal{T}^\bullet(V)}{\langle v \otimes w - w \otimes v\rangle}, \quad v, w \in V.$$

(b) The exterior algebra $\bigwedge_\bullet(V)$ is a quadratic $\mathbb{F}$-algebra, as

$$\bigwedge_{n\geq 0}(V) = \frac{\mathcal{T}^\bullet(V)}{\langle v \otimes w + w \otimes v\rangle}, \quad v, w \in V.$$

Definition 8. Fix a field K. For a positive integer n, the n^{th} **Milnor $\mathcal{K}$-group** of K is the quotient

$$\mathcal{K}_n^M(K) = \left(K^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} K^\times\right)/I_n,$$

where I_n is the subgroup generated by the elements $a_1 \otimes \cdots \otimes a_n$ such that $a_i + a_j = 1$ for some $i \neq j$. (Such relations are called of *Steinberg*

type.) Moreover, set $\mathcal{K}_0^M = \mathbb{Z}$. Then the **Milnor $\mathcal{K}$-ring** of K is the quadratic $\mathbb{Z}$-algebra

$$\mathcal{K}_\bullet^M(K) = \bigoplus_{n\geq 0} \mathcal{K}_n^M(K) = \frac{\mathcal{T}^\bullet(K^\times)}{\langle a \otimes b \mid a+b=1\rangle},$$

equipped with the addition induced by the multiplication of K, and with the multiplication induced by the tensor product.

Given $a_1, \ldots, a_n \in K^\times$, the symbol $\{a_1, \ldots, a_n\}$ denotes the image of $a_1 \otimes \cdots \otimes a_n$ in $\mathcal{K}_n^M(K)$. A particular feature of Milnor $\mathcal{K}$-rings of fields is the anti-commutativity:

$$\{a,b\} = -\{b,a\} \quad \text{for all } a,b \in K^\times \tag{2.2}$$

(cf. [**Ef06**, Prop. 24.1.2]). Therefore, the algebra $\mathcal{K}_\bullet^M(K)$ is in fact a quotient of the exterior algebra $\bigwedge_\bullet K^\times$.

For a positive integer m, one may consider the Milnor $\mathcal{K}$-ring modulo m, i.e.,

$$\mathcal{K}_\bullet^M(K)/m = \bigoplus_{n\geq 0} \mathcal{K}_n^M(K)/m.\mathcal{K}_n^M(K).$$

Then $\mathcal{K}_\bullet^M(K)/m$ is a quadratic, anti-commutative $\mathbb{Z}/m\mathbb{Z}$-algebra. In particular, one has the following (cf. [**Ef06**, Prop. 24.1.3]).

Proposition 2.1. *For positive integers m, one has*

$$\mathcal{K}_\bullet^M(K)/m = \frac{\mathcal{T}^\bullet\left(K^\times/(K^\times)^m\right)}{\langle \bar{a} \otimes \bar{b} \mid a+b \in (K^\times)^m\rangle},$$

where $\bar{a} = a \bmod (K^\times)^m$ and $\bar{b} = b \bmod (K^\times)^m$.

1.1. Constructions with quadratic algebras. Let $A_\bullet$ and $B_\bullet$ be two quadratic algebras over a field $\mathbb{F}$. There are several constructions which produce a new quadratic algebra $C_\bullet$ generated by A_1 and B_1, i.e.,

$$C_\bullet = \frac{\mathcal{T}^\bullet(A_1 \oplus B_1)}{\mathcal{R}},$$

with $\mathcal{R}$ the two-sided ideal generated by $\mathcal{R}_1 \leq (A_1 \oplus B_1)^{\otimes 2}$.

Let $\mathcal{R}_1^A \leq A_1 \otimes A_1$ and $\mathcal{R}_1^B \leq B_1 \otimes B_1$ be the relations of $A_\bullet$, resp. of $B_\bullet$. Then one has the following constructions.

(a) The *direct product* $C_\bullet = A_\bullet \sqcap B_\bullet$ (also denoted as $A_\bullet \oplus B_\bullet$) is such that $C_n = A_n \oplus B_n$ for every $n \geq 1$. Thus, one has

$$\mathcal{R}_1 = \mathcal{R}_1^A \oplus \mathcal{R}_1^B \oplus (A_1 \otimes B_1) \oplus (B_1 \otimes A_1).$$

In particular, $ab = ba = 0$ for any $a \in A_n$, $b \in B_m$, $n, m \geq 1$.

(b) The *free product* $C_\bullet = A_\bullet \sqcup B_\bullet$ (also denoted as $A_\bullet * B_\bullet$) is the associative algebra generated freely by $A_\bullet$ and $B_\bullet$. One has

$$\mathcal{R}_1 = \mathcal{R}_1^A \oplus \mathcal{R}_1^B.$$

(c) The *symmetric tensor product* $A_\bullet \otimes^1 B_\bullet$ (also called 1-tensor product) is such that $ab = ba$ for any $a \in A_n$, $b \in B_m$, $n, m \geq 1$. Thus,

$$\mathcal{R}_1 = \mathcal{R}_1^A \oplus \mathcal{R}_1^B \oplus \langle ab - ba \rangle,$$

with $a \in A_1$ and $b \in B_1$.

(d) The *skew-commutative tensor product* $A_\bullet \otimes^{-1} B_\bullet$ (also called (-1)-tensor product, or graded tensor product, see [**Ef06**, § 23.2]) is such that $ab = (-1)^{nm} ba$ for any $a \in A_n$, $b \in B_m$, $n, m \geq 1$. Thus,

$$\mathcal{R}_1 = \mathcal{R}_1^A \oplus \mathcal{R}_1^B \oplus \langle ab + ba \rangle,$$

with $a \in A_1$ and $b \in B_1$.

See [**PP05**, § 3.1] for further details.

2. The Rost-Voevodsky Theorem

Assume now that the characteristic of K does not divide m, and let μ_m be the group of the m^{th}-roots of unity as in (1.10). The isomorphism (1.11) induces the isomorphism $\mathcal{K}_1(K)/m \simeq H^1(G_K, \mu_m)$. Thus the cup-product induces a morphism

$$\frac{K^\times}{(K^\times)^m} \otimes_{\mathbb{Z}/m\mathbb{Z}} \cdots \otimes_{\mathbb{Z}/m\mathbb{Z}} \frac{K^\times}{(K^\times)^m} \longrightarrow H^n\left(G_K, \mu_m^{\otimes n}\right) \tag{2.3}$$

defined by $\bar{a}_1 \otimes \cdots \otimes \bar{a}_n \mapsto \chi_{a_1} \cup \cdots \cup \chi_{a_n}$, whith the χ_{a_i}'s as in (1.15). In fact, J. Tate showed in [**Ta76**] that the map (2.3) factors through $\mathcal{K}_n^M(K)/m$, thus one has the homomorphism

$$h_K \colon \mathcal{K}_n^M(K)/m \longrightarrow H^n\left(G_K, \mu_m^{\otimes n}\right)$$

(cf. [**NSW**, Theorem 6.4.2]) called the **Galois symbol** (or the **norm residue map**) of degree n.

THEOREM 2.2 (Bloch-Kato Conjecture). *For every field K and for every positive m prime to* $\mathrm{char}(K)$*, the Galois symbol h_K is an isomorphism for every degree n.*

For $m = 2$ this was conjectured first by J. Milnor in the late '60s, whereas the full formulation of the conjecture was stated by S. Bloch and K. Kato in [**BK86**]. The complete proof required several steps:

(i) for $n = 1$ the Galois symbol is just the Kummer isomorphism;
(ii) for $n = 2$ it was proved by A.S. Merkur'ev and A.A. Suslin in the early '80s (cf. [**MS82**]);
(iii) for $n = 3$ and $m = 2$ it was proved by Merkur'ev and Suslin in the late '80s (cf. [**MS90**]) and, independently, by M. Rost;
(iv) for any n and m a power of 2 it was proved by V. Voevodsky at the beginning of the century (cf. [**Vo03**]).

For this, Voevodsky was awarded the Fields Medal in 2002. Later, he announced a proof of the full conjecture in a preprint. Yet, it required a while to see a complete (and published) proof, which appeared in 2011 (cf. [**Vo11**]). Also Rost gave a remarkable and substantial contribution to achieve the final proof – further, C. Weibel solved some technical problems via what is now known as the "Chuck Weibel's patch" – so that now the Bloch-Kato Conjecture is adressed as the **Rost-Voevodsky theorem**, see also [**We08, We09**].

3. Bloch-Kato pro-p groups

Let p be a prime. If K contains a primitive p^{th}-root of unity, then μ_p is isomorphic to $\mathbb{F}_p$ as (trivial) G_K-modules. In particular, one has $\mu_p^{\otimes n} \simeq \mathbb{F}_p$ for every $n \geq 1$. Therefore, one has the cup product

$$H^n(G_K, \mathbb{F}_p) \times H^m(G_K, \mathbb{F}_p) \xrightarrow{\cup} H^{n+m}(G_K, \mathbb{F}_p) \ ,$$

with $n, m \geq 0$, and by Remark 1.5 we may define the graded-commutative $\mathbb{F}_p$-algebra

$$H^\bullet(G_K, \mathbb{F}_p) = \bigoplus_{n \geq 0} H^n(G_K, \mathbb{F}_p),$$

equipped with the cup-product. Since the Galois symbol is defined by the cup product, h_K induces an isomorphism of graded $\mathbb{F}_p$-algebras

$$h_K \colon \mathcal{K}^M_\bullet(K)/p \xrightarrow{\sim} H^\bullet(G_K, \mathbb{F}_p) \ ,$$

which implies that the $\mathbb{F}_p$-cohomology ring of G_K is a quadratic $\mathbb{F}_p$-algebra.

For a profinite group G let $\mathcal{O}_p(G)$ be the subgroup

$$\mathcal{O}_p(G) = \langle C \in \mathrm{Syl}_\ell(G) \mid \ell \neq p \rangle \,,$$

where $\mathrm{Syl}_\ell(G)$ is the set of the Sylow pro-ℓ subgroups; namely one has the short exact sequence

$$1 \longrightarrow \mathcal{O}_p(G) \longrightarrow G \longrightarrow G(p) \longrightarrow 1, \tag{2.4}$$

with $G(p)$ the maximal pro-p quotient of G, i.e., the Galois group of the extensions $K(p)/K$ (cf. [**Qu14**, § 2]). Therefore, in the case G is the absolute Galois group G_K of a field with the above properties, $\mathcal{O}_p(G_K)$ is the absolute Galois group of the p-closure $K(p)$, and by the Bloch-Kato Conjecture the cohomology ring $H^\bullet(\mathcal{O}_p(G_K), \mathbb{F}_p)$ is quadratic, and thus generated by $H^1(\mathcal{O}_p(G_K), \mathbb{F}_p)$. Since $\mathcal{O}_p(G_K)$ is p-perfect, by Fact 1.1 one has

$$H^1\left(\mathcal{O}_p(G_K), \mathbb{F}_p\right) = \mathrm{Hom}_{\mathbb{F}_p}\left(\mathcal{O}_p(G_K), \mathbb{F}_p\right) = 0,$$

and hence $H^n(\mathcal{O}_p(G_K), \mathbb{F}_p) = 0$ for every $n \geq 1$. Thus in the Lyndon-Hochschild-Serre spectral sequence (cf. [**NSW**, § II.4]) induced by (2.4), the terms

$$E_2^{rs} = H^r\left(G_K(p), H^s(\mathcal{O}_p(G_K))\right)$$

vanish for $s > 0$, and the spectral sequence collapses at the E_2-term. Hence the inflation map

$$\inf^n_{G_K, \mathcal{O}_p(G_K)} \colon H^n\left(G_K(p), \mathbb{F}_p\right) \longrightarrow H^n\left(G_K, \mathbb{F}_p\right) \tag{2.5}$$

is an isomorphism for every $n \geq 0$ (cf. [**NSW**, Lemma 2.1.2]). This proves the following.

Proposition 2.3. *Let K be a field containing a primitive p^{th}-root of unity, with p a fixed prime. Then the $\mathbb{F}_p$-cohomology ring $H^\bullet(G_K(p), \mathbb{F}_p)$ of the maximal pro-p Galois group of K is a quadratic $\mathbb{F}_p$-algebra.*

Definition 9 ([**Qu14**]). Let G be a pro-p group. Then G is said to be a **Bloch-Kato pro-p group** if for every closed subgroup $C \leq G$ the $\mathbb{F}_p$-cohomology ring $H^\bullet(C, \mathbb{F}_p)$ is a quadratic $\mathbb{F}_p$-algebra.

Thus, the maximal pro-p Galois group $G_K(p)$ of a field K containing μ_p is a Bloch-Kato pro-p group: indeed, every closed subgroup of the maximal pro-p Galois group of a field is again a maximal pro-p Galois group (and this justifies such a requirement in the definition).

By Proposition 1.4, the cohomology ring of a pro-p group G with $\mathbb{F}_p$-coefficients is skew-commutative. In particular, for G a Bloch-Kato pro-p group let $\{\chi_i, i \in \mathcal{I}\}$ be a basis for $H^1(G, \mathbb{F}_p)$ as $\mathbb{F}_p$-vector space, and let $\mathcal{R}$ be the defining relations of $H^\bullet(G, \mathbb{F}_p)$ as in (2.1), i.e.,

$$H^\bullet(G, \mathbb{F}_p) \simeq \frac{\mathcal{T}^\bullet\left(H^1(G, \mathbb{F}_p)\right)}{\mathcal{R}}. \tag{2.6}$$

Then one has $\chi_i \otimes \chi_j + \chi_j \otimes \chi_i \in \mathcal{R}$ for every $i, j \in \mathcal{I}$, and (2.6) induces an epimorphism of quadratic $\mathbb{F}_p$-algebras

$$\bigwedge_\bullet H^1(G, \mathbb{F}_p) \twoheadrightarrow H^\bullet(G, \mathbb{F}_p) \ , \tag{2.7}$$

so that, in the case p odd, we may consider the exterior algebra generated by $H^1(G, \mathbb{F}_p)$ as an "upper bound" for the $\mathbb{F}_p$-cohomology of Bloch-Kato pro-p groups, namely, this is the case when the ideal $\mathcal{R}$ is the smallest possible. On the other hand, the ideal $\mathcal{R}$ may be generated by the whole group $H^2(G, \mathbb{F}_p)$, i.e., the $\mathbb{F}_p$-cohomology ring of G is concentrated in degrees 0 and 1, and this case can be considered as "lower bound". The latter case is completely explained by the following classic result (cf. [**NSW**, Prop. 3.3.2 and Prop. 3.5.17]).

Proposition 2.4. *Let G be a pro-p group.*

(i) *for $n \geq 0$, one has $\mathrm{cd}(G) = n$ if, and only if, $H^{n+1}(G, \mathbb{F}_p) = 0$.*
(ii) *the group G is free if, and only if, $\mathrm{cd}(G) = 1$.*

In particular, if p is odd and G is a finitely generated Bloch-Kato pro-p group, then (2.7) and Proposition 2.4 imply the following (see also [**Qu14**, Prop. 4.1 and Prop. 4.3]).

Corollary 2.5. *For G Bloch-Kato and p odd, one has the following:*

(i) *$\mathrm{cd}(G) \leq d(G)$, and the equality holds if, and only if (2.7) is an isomorphism;*
(ii) *$r(G) \leq \binom{d(G)}{2}$.*

The celebrated Artin-Schreier theorem states that the only non-trivial finite subgroups of an absolute Galois group is the cyclic group

of order two.[1] A similar condition holds for Bloch-Kato pro-p groups: a Bloch-Kato pro-p group G may have torsion only if $p = 2$. In particular one has the following.

PROPOSITION 2.6. *Bloch-Kato pro-p group G is torsion if, and only if, G is abelian and of exponent 2, and moreover any of such group is a Bloch-Kato pro-2 group.*

PROOF. Let p be any prime and let C_p be the cyclic group of order p, and assume that G admits a finite subgroup. Then G has C_p as a (closed) subgroup. If p is odd, then the cohomology ring $H^\bullet(C_p, \mathbb{F}_p)$ is not quadratic, as $H^2(C_p, \mathbb{F}_p)$ contains an element which is not a combination of cup products of elements in $H^1(C_p, \mathbb{F}_p)$, i.e., the map (2.7) is not an epimorphism in degree 2. Thus G can't be a Bloch-Kato pro-p group.

Moreover, if $p = 2$ and G has 2^n-torsion, with $n > 1$, the above argument works also for C_{2^n} instead of C_p, with C_{2^n} the cyclic group of order 2^n.

On the other hand, if $p = 2$ and G is abelian and of exponent 2, then the cohomology ring $H^\bullet(G, \mathbb{F}_2)$ is isomorphic to the symmetric $\mathbb{F}_2$-algebra $S_\bullet(H^1(G, \mathbb{F}_2))$, and thus G is Bloch-Kato. □

For Bloch-Kato pro-p groups one may deduce the following result from [**CEM**].

THEOREM 2.7. *Let G be a Bloch-Kato pro-p group. Then the inflation map induces an isomorphism*

$$H^\bullet(G/\lambda_3(G), \mathbb{F}_p)_{dec} \xrightarrow{\sim} H^\bullet(G, \mathbb{F}_p),$$

where $H^\bullet(\_, \mathbb{F}_p)_{dec}$ is the decomposable part of the cohomology ring, i.e., the subalgebra generated by products of elements of degree one. Moreover, if $\phi\colon G_1 \to G_2$ is a homomorphism of Bloch-Kato pro-p group, then the induced map in cohomology

$$\phi^*\colon H^\bullet(G_2, \mathbb{F}_p) \longrightarrow H^\bullet(G_1, \mathbb{F}_p)$$

is an isomorphism if, and only if, the induced map on the quotients $G_1/\lambda_3(G_1) \to G_2/\lambda_3(G_2)$ is an isomorphism.

[1] In particular, the Artin-Schreier theorem states that if the absolute Galois group G_K of a field K is finite (and non-trivial), then $G_K \simeq \mathbb{Z}/2\mathbb{Z}$ and K is a *real closed field*, i.e., K is of characteristic 0 with an unique *ordering* such that every positive element is a square and every polynomial in $K[X]$ of odd degree has a zero in K.

We shall study more in detail the quotient $G/\lambda_3(G)$ in Section 4

4. Oriented pro-p groups

Fix a prime p and a field K, and let $\mu_{p^\infty} = \mu_{p^\infty}(K)$ be the group of all the roots of unity of p-power order, i.e., $\mu_{p^\infty}(K) = \varinjlim_{k\geq 0} \mu_{p^k}(K)$. In particular, μ_{p^∞} is a discrete torsion $\mathbb{Z}_p$-module, and one has

$$\mathrm{Aut}_K\left(\mu_{p^\infty}(\bar{K}^{\mathrm{sep}})\right) \simeq \mathbb{Z}_p^\times,$$

with $\mathrm{Aut}_K(\mu_{p^\infty})$ the group of K-automorphisms (cf. [**Wr92**, Lemma 1]). Therefore, the action of the absolute Galois group on the separable closure induces an homomorphism of pro-p groups

$$\theta_{(p,K)}\colon G_K \longrightarrow \mathbb{Z}_p^\times, \tag{2.8}$$

called the p-cyclotomic character of K.

If $K \supseteq \mu_p$, then the p-closure $K(p)$ contains $\mu_{p^\infty}(\bar{K}^{\mathrm{sep}})$, and the maximal pro-$p$ Galois group $G_K(p)$ acts on μ_{p^∞}, namely, the cyclotomic character $\theta_{p,K}$ is trivial on the subgroup $\mathcal{O}_p(G)$, and it factors in a unique way through a homomorphism $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$. We will call the map θ the *arithmetical orientation* of the Galois group $G_K(p)$. This is the arithmetical justification for the following definition.

Definition 10. Let G be a profinite group. A continuous homomorphism of profinite groups $\theta\colon G \to \mathbb{Z}_p^\times$ will be called a **p-orientation** of G, and the group G will be called a **p-oriented** profinite group.

Thus, absolute Galois groups (and maximal pro-p Galois groups of fields containing a primitive p^{th}-root of unity) are naturally equipped with a p-orientation.

A p-orientation $\theta\colon G \to \mathbb{Z}_p^\times$ of a profinite group G induces a natural continuous action of G on $\mathbb{Z}_p$ in the following way: for every $g \in G$, the multiplication by $\theta(g)$ induces an automorphisms of $\mathbb{Z}_p$. Thus $\mathbb{Z}_p(1)$ will denote the $\mathbb{Z}_p[\![G]\!]$-module isomorphic to $\mathbb{Z}_p$ as $\mathbb{Z}_p$-module,[2] and with the G-action induced by the orientation θ. Also, for $m \in \mathbb{Z}$, one has the $\mathbb{Z}_p[\![G]\!]$-module $\mathbb{Z}_p(m)$, together with the action induced by θ^m, i.e., $g.\lambda = \theta(g)^m \cdot \lambda$ for every $g \in G$ and $\lambda \in \mathbb{Z}_p$.

[2]In the arithmetical case, the module $\mathbb{Z}_p(m)$ is called the m^{th} *Tate twist* of $\mathbb{Z}_p$, as this construction was used first by J. Tate in [**Ta76**] (see also [**NSW**, (7.3.6)]).

4.1. θ-abelian pro-p groups. From now on we will concentrate on pro-p groups with p-orientations (and we will omit the "p" in the notation, for simplicity).

REMARK 2.8. If G is a pro-p group, then the image of an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ is again a pro-p group.

- If p is odd, then $\mathbb{Z}_p^\times$ is virtually pro-p, and the Sylow pro-p group is $1+p\mathbb{Z}_p$, with $|\mathbb{Z}_p^\times : (1+p\mathbb{Z}_p)| = p-1$. In particular, one has that $\mathrm{im}(\theta)$ is contained in $1+p\mathbb{Z}_p$, and it is isomorphic to $\mathbb{Z}_p$.
- If $p=2$, then $\mathbb{Z}_2^\times$ is pro-2, and it is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}_2$. Thus, one has that $\mathrm{im}(\theta)$ is torsion-free and isomorphic to $\mathbb{Z}_2$ if, and only if, $\mathrm{im}(\theta) \leq 1+4\mathbb{Z}_2$.

In a pro-p group with orientation, one has a distinguished subgroup.

DEFINITION 11. Let (G,θ) be an oriented pro-p group. The closed subgroup defined by

$$\mathrm{Z}_\theta(G) = \left\{ h \in \ker(\theta) \;\middle|\; ghg^{-1} = h^{\theta(g)} \text{ for all } g \in G \right\}$$

will be called the **θ-centre** of G. Moreover, the group G will be called **θ-abelian**, if $\mathrm{Z}_\theta(G) = \ker(\theta)$.

Namely, the θ-centre of an oriented pro-p group is given by the "copies" of the module $\mathbb{Z}_p(1)$, induced by the orientation, lying inside G. It is easy to see that $\mathrm{Z}_\theta(G)$ is an abelian normal subgroup of G. If a pro-p group with an orientation (G,θ) is θ-abelian, then it has a very simple structure (see [**Qu14**, Prop. 3.4] and [**CMQ**, Remark 3.3]).

PROPOSITION 2.9. *Let (G,θ) be a pro-p group with an orientation, ans suppose that $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$. Then G is θ-abelian if, and only if, there exists a minimal generating system $\mathcal{X} = \{x_0, x_i, i \in \mathcal{I}\} \subset G$, such that G has a presentation*

$$G = \left\langle x_0, x_i \;\middle|\; x_0 x_i x_0^{-1} = x_i^{\theta(x_0)}, [x_i, x_j] = 1, i,j \in \mathcal{I} \right\rangle. \tag{2.9}$$

In particular, G can be expressed as a fibre product

$$G \simeq \mathrm{im}(\theta) \ltimes \mathbb{Z}_p(1)^{\mathcal{I}},$$

with the action induced by the orientation.

4.2. Cyclotomic orientations. Let K be a field containing the pth roots of unity μ_p, and let $G_K(p)$ be the maximal pro-p Galois group. For every $n \geq 0$, the p^nth power induces the short exact sequence of $\mathbb{Z}_p[\![G_K(p)]\!]$-modules

$$0 \longrightarrow \mu_{p^n} \longrightarrow K(p)^\times \xrightarrow{p^n} K(p)^\times \longrightarrow 0. \tag{2.10}$$

Since μ_{p^n} is isomorphic to $\mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)$ as $G_K(p)$-modules, (2.10) induces the commutative diagram in cohomology

$$\begin{array}{ccccc} K^\times/(K^\times)^{p^n} & \xrightarrow{\sim} & H^1\left(G_K(p), \mu_{p^n}\right) & = & H^1\left(G_K(p), \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)\right) \\ \downarrow & & \downarrow{\scriptstyle p^{n-1}} & & \downarrow \\ K^\times/(K^\times)^{p^m} & \xrightarrow{\sim} & H^1\left(G_K(p), \mu_{p^m}\right) & = & H^1\left(G_K(p), \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)\right) \end{array}$$

for every $n > m \geq 1$, where the left-hand side horizontal arrows are isomorphisms by (1.13). In particular, one has the epimorphism

$$H^1\left(G_K(p), \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)\right) \xrightarrow{\pi_{nm}} H^1\left(G_K(p), \mathbb{Z}_p(1)/p^m\mathbb{Z}_p(1)\right) \tag{2.11}$$

for every $n > m \geq 1$. In particular, $\{H^1\left(G_K(p), \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)\right), \pi_{nm}\}$ is a projective system, and by [**NSW**, Corollary 2.7.6] one has the isomorphism $H^1(G, \mathbb{Z}_p(1)) \simeq \varprojlim_n H^1(G_K(p), \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1))$.

Definition 12. Let (G, θ) be a pro-p group with an orientation. Then θ is called a **cyclotomic** orientation (and G is said to be **cyclo-oriented**) if the following hold:

(i) G is a Bloch-Kato pro-p group;
(ii) $H^2(C, \mathbb{Z}_p(1))$ is a torsion-free abelian group for all closed subgroups C of G.

Remark 2.10. If F is a free pro-p group, then $\mathrm{cd}(F) = 1$ by Proposition 2.4. Then for any orientation $\theta\colon F \to \mathbb{Z}_p^\times$ one has $H^2(F, \mathbb{Z}_p(1)) = 0$, so that (F, θ) is cyclo-oriented for any θ.

One has the following elementary fact.

LEMMA 2.11. *Let (G,θ) be a pro-p group with orientation. Then $H^2(G,\mathbb{Z}_p(1))$ is a torsion-free abelian group if, and only if, the map*

$$H^1(G,\mathbb{Z}_p(1)) \longrightarrow H^1(G,\mathbb{F}_p) \tag{2.12}$$

induced by the short exact sequence of $\mathbb{Z}_p[\![G]\!]$-modules

$$0 \longrightarrow \mathbb{Z}_p(1) \xrightarrow{\ p\ } \mathbb{Z}_p(1) \longrightarrow \mathbb{F}_p \longrightarrow 0 \tag{2.13}$$

is an epimorphism.

PROOF. The short exact sequence (2.13) induces the exact sequence in cohomology

$$H^1(G,\mathbb{Z}_p(1)) \longrightarrow H^1(G,\mathbb{F}_p) \longrightarrow H^2(G,\mathbb{Z}_p(1)) \xrightarrow{\ p\ } H^2(G,\mathbb{Z}_p(1)),$$

and $H^2(G,\mathbb{Z}_p(1))$ is torsion-free if, and only if, the right-hand side arrow is injective, namely, if, and only if, the middle arrow is trivial and the left-hand side arrow is surjective. □

Consequently, by (2.11) one has that $H^1(G_K(p),\mathbb{Z}_p(1))$ projects onto $H^1(G_K(p),\mathbb{F}_p)$, so that one has the following.

THEOREM 2.12. *Let K be a field containing a primitive p-th root of unity, and let $G_K(p)$ be its maximal pro-p Galois group. Then the arithmetical orientation $\theta\colon G_K(p)\to\mathbb{Z}_p^\times$ is cyclotomic.*

The following result is a refinement of Proposition 2.6 for pro-2 groups with a cyclotomic orientation.

PROPOSITION 2.13. *Let (G,θ) be a pro-2 group with cyclotomic orientation.*

(i) *If G is non-trivial and torsion, then $G\simeq C_2$ and $\mathrm{im}(\theta)=\{\pm1\}$.*
(ii) *If $\mathrm{im}(\theta)$ is torsion free, then G is torsion free.*

PROOF. (i) By Proposition 2.6, G is an elementary abelian 2-group. Let $K=\ker(\theta)$. Then $(K,\theta|_K)$ is an elementary abelian pro-2 group with trivial cyclotomic 2-orientation, namely, $\theta|_K\equiv 1$ and $\mathbb{Z}_2(m)\simeq\mathbb{Z}_2(0)=\mathbb{Z}_2$ as K-modules for all $m\in\mathbb{Z}$. Since K is torsion, one has $H^1(K,\mathbb{Q}_2)=\mathrm{Hom}(K,\mathbb{Q}_2)=0$, and the connecting map $H^1(K,\mathbb{I}_2)\to$

$H^2(K, \mathbb{Z}_2)$ induced in cohomology by the exact sequence (1.3) for $p = 2$ is injective. Thus one has the embedding

$$K^\vee = H^1(K, \mathbb{I}_2) \hookrightarrow H^2(K, \mathbb{Z}_2) = H^2(K, \mathbb{Z}_2(1)) \ ,$$

which is torsion-free. Consequently $K^\vee = 0$ and K is the trivial group, and $\theta\colon G \to \mathbb{Z}_2^\times$ is injective. This shows (i), and (ii) is a direct consequence of (i). □

From Proposition 2.6, Proposition 2.13 and Sylow's theorem one deduces the following corollary, which can be considered as a local version of the Artin-Schreier theorem for profinite groups with cyclotomic p-orientation.

COROLLARY 2.14. *Let p be a prime number, and let (G, θ) be a pro-p group with cyclotomic orientation.*

(i) *If p is odd, then G has no p-torsion.*
(ii) *If $p = 2$, then every non-trivial 2-torsion subgroup is isomorphic to C_2, the cyclic group of order 2. Moreover, if $\mathrm{im}(\theta)$ has no 2-torsion, then G has no 2-torsion.*

REMARK 2.15. Let $\theta\colon \mathbb{Z}_2 \to \mathbb{Z}_2^\times$ be given by $\theta(1 + \lambda) = -1$ and $\theta(\lambda) = 1$ for all $\lambda \in 2\mathbb{Z}_2$. Then θ is a 2-orientation of $G = \mathbb{Z}_2$ satisfying $\mathrm{im}(\theta) = \{\pm 1\}$. As $\mathrm{cd}_2(\mathbb{Z}_2) = 1$, θ is also cyclotomic by Remark 2.10. This shows that for a torsion free pro-2 group G with cyclotomic 2-orientation $\theta\colon G \to \mathbb{Z}_2^\times$, $\mathrm{im}(\theta)$ is not necessarily torsion free.

On the other hand, if $\mathrm{im}(\theta) \leq 1 + 4\mathbb{Z}_2$ for a cyclo-oriented pro-2 group (G, θ), one has the following.

PROPOSITION 2.16. *Let (G, θ) be a pro-2 group with cyclotomic 2-orientation satisfying $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$. Then $\chi \cup \chi = 0$ for all $\chi \in H^1(G, \mathbb{F}_2)$.*

PROOF. Set $\mathbb{Z}_4(1) = \mathbb{Z}_2(1)/4\mathbb{Z}_2(1)$. By Remark 2.8, $\mathbb{Z}_4(1)$ is a trivial $\mathbb{Z}_2[\![G]\!]$-module, thus $\mathbb{Z}_4 \simeq \mathbb{Z}/4\mathbb{Z}$ as abelian groups. Since the group $H^2(G, \mathbb{Z}_2(1))$ is torsion-free, one has a commutative diagram with exact rows

(2.14)

$$\begin{array}{ccccccc}
H^1(G, \mathbb{Z}_2(1)) & \xrightarrow{4} & H^1(G, \mathbb{Z}_2(1)) & \longrightarrow & H^1(G, \mathbb{Z}_4(1)) & \longrightarrow & 0 \\
\Big\downarrow{\scriptstyle 2} & & \Big\| & & \Big\downarrow{\scriptstyle \pi} & & \\
H^1(G, \mathbb{Z}_2(1)) & \xrightarrow{2} & H^1(G, \mathbb{Z}_2(1)) & \longrightarrow & H^1(G, \mathbb{F}_2) & \longrightarrow & 0
\end{array}$$

with π the canonical morphism. Hence by the weak four lemma applied to the diagram (2.14) extended by another column of 0's to the right, π is surjective. In particular, the first Bockstein morphism

$$\beta^1 \colon H^1(G, \mathbb{F}_2) \longrightarrow H^2(G, \mathbb{F}_2)$$

is the trivial map, and the claim follows by Lemma 1.6. □

Let (G, θ) be a cyclo-oriented pro-p group. The above result, together with Remark 2.8, shows that if $\mathrm{im}(\theta)$ is pro-p-cyclic (possibly trivial), then the cup product in $H^\bullet(G, \mathbb{F}_p)$ is skew-commutative, and Corollary 2.5 holds also in the case $\mathrm{im} \simeq \mathbb{Z}_2$. In particular, from (2.7) one gets the epimorphism of quadratic $\mathbb{F}_p$-algebras

$$\frac{\mathcal{T}^\bullet\left(H^1(G, \mathbb{F}_p)\right)}{\langle \chi \otimes \chi \rangle} \twoheadrightarrow H^\bullet(G, \mathbb{F}_p) \tag{2.15}$$

for all cyclo-oriented pro-p groups (G, θ) with $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, or $\mathrm{im}(\theta) = \{1\}$ for p odd.

4.3. Modules of cyclo-oriented groups. Given an oriented pro-p group (G, θ), the orientation induces a G-action also on the $\mathbb{Z}_p$-modules $\mathbb{Q}_p$ and $\mathbb{I}_p$. Thus, one may define the $\mathbb{Z}_p[\![G]\!]$-modules $\mathbb{Q}_p(m)$ and $\mathbb{I}_p(m)$, for $m \in \mathbb{Z}$, and (1.3) induces the short exact sequence

$$0 \longrightarrow \mathbb{Z}_p(m) \longrightarrow \mathbb{Q}_p(m) \longrightarrow \mathbb{I}_p(m) \longrightarrow 0. \tag{2.16}$$

Fact 2.17. *For $m \in \mathbb{Z}$, one has $\mathbb{I}_p(m)^\vee \simeq \mathbb{Z}_p(-m)$.*

Proof. By definition, one has $\mathbb{I}_p \simeq \mathbb{Z}_p^\vee$ as $\mathbb{Z}_p$-modules. Thus, for $\lambda \in \mathbb{I}_p$, $\phi \in \mathbb{I}_p(m)^*$ and $g \in G$ one has

$$(g.\phi)(\lambda) = \phi\left(g^{-1}.\lambda\right) = \phi\left(\theta(g^{-1})^m \cdot \lambda\right) = \theta(g)^{-m} \cdot \phi(\lambda),$$

and this yields the claim. □

Lemma 2.18. *For G a profinite group and $\theta \colon G \to \mathbb{Z}_p^\times$ an orientation, the Pontryagin dual induces the natural isomorphism of functors*

$$\mathbb{Z}_p(m)^\times \hat{\otimes}_G \mathrm{Hom}(\_, \mathbb{I}_p) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_p(m), \_)^\vee, \quad m \in \mathbb{Z}.$$

PROOF. Let N be a discrete left $\mathbb{Z}_p[\![G]\!]$-module, and let $\lambda \in \mathbb{Z}_p(m)^\times$ and $f \in \mathrm{Hom}(N, \mathbb{I}_p)$. Then define $\phi_{\lambda\otimes f} \in \mathrm{Hom}_G(\mathbb{Z}_p(m), N)^\vee$ such that $\phi_{\lambda\otimes f}(h) = f(h(\lambda))$ for every $h \in \mathrm{Hom}_G(\mathbb{Z}_p(m), N)$. Then, for every $g \in G$, one has

$$\begin{aligned}\phi_{\lambda.g\otimes f}(h) &= f(h(\lambda.g)) = f\left(h(g^{-1}.\lambda)\right) = \\ &= f\left(g^{-1}.h(\lambda)\right) = g.f(h(\lambda)) = \phi_{\lambda\otimes g.f}(h),\end{aligned}$$

and this yields the claim. □

In particular, for $m = 0$ Lemma 2.18 implies the isomorphism

$$\mathrm{Tor}_n^{\mathbb{Z}_p[\![G]\!]}\left(\mathbb{Z}_p, M^\vee\right) \simeq \mathrm{Ext}^n_{\mathbb{Z}_p[\![G]\!]}\left(\mathbb{Z}_p, M\right)^\vee, \tag{2.17}$$

with M a discrete module (see also [**NSW**, Corollary 5.2.9]).

PROPOSITION 2.19. *Let G be a profinite group with a p-orientation θ. Then for every $m \in \mathbb{Z}$ the following are equivalent:*

(i) *$H^{m+1}(G, \mathbb{Z}_p(m))$ is a torsion-free $\mathbb{Z}_p$-module.*
(ii) *$H^m(G, \mathbb{I}_p(m))$ is a p-divisible $\mathbb{Z}_p$-module.*
(iii) *$H_m(G, \mathbb{Z}_p(-m))$ is a torsion-free $\mathbb{Z}_p$-module.*

PROOF. The exact sequence (2.16) induces the exact sequence in cohomology

(2.18)

$$H^n\left(G, \mathbb{Z}_p(m)\right) \longrightarrow H^n\left(G, \mathbb{Q}_p(m)\right) \longrightarrow H^n\left(G, \mathbb{I}_p(m)\right) \xrightarrow{\delta^m} H^{m+1}\left(G, \mathbb{Z}_p(m)\right) \longrightarrow H^{m+1}\left(G, \mathbb{Q}_p(m)\right)$$

for $m \geq 0$. Then by Proposition 1.8, one has that $\ker(\delta)$ is the maximal p-divisible subgroup of $H^m(G, \mathbb{I}_p(m))$, and $\mathrm{im}(\delta)$ is the torsion subgroup of $H^{m+1}(G, \mathbb{Z}_p(m))$. Thus, $H^{m+1}(G, \mathbb{Z}_p(m))$ is a torsion-free $\mathbb{Z}_p[\![G]\!]$-module if, and only if, δ is the zero map, i.e., $\ker(\delta) = H^m(G, \mathbb{I}_p(m))$. This establishes the equivalence between (i) and (ii).

Now set $M = \mathbb{I}_p(m)$. Then (2.17) and Fact 2.17 imply that

$$H_m(G, \mathbb{Z}_p(-m)) \cong H^m\left(G, \mathbb{I}_p(m)\right)^\vee.$$

By duality, it follows that $H_m(G, \mathbb{Z}_p(-m))$ is a profinite torsion-free $\mathbb{Z}_p[\![G]\!]$-module if, and only if, $H^m(G, \mathbb{I}_p(m))$ is a discrete p-divisible $\mathbb{Z}_p[\![G]\!]$-module. This establishes the equivalence between (ii) and (iii). □

The above result has the following consequence.

COROLLARY 2.20. *Let (G,θ) a cyclo-oriented pro-p group. The abelianization $\ker(\theta)/[\ker(\theta),\ker(\theta)]$ of the kernel of the orientation θ is a torsion-free group.*

PROOF. Since the restriction $\theta|_{\ker(\theta)}$ is trivial, $\mathbb{Z}_p(1)$ is a trivial $\mathbb{Z}_p[\![\ker(\theta)]\!]$-module. Thus, one has

$$H_1(\ker(\theta),\mathbb{Z}_p(1)) = H_1(\ker(\theta),\mathbb{Z}_p) \simeq \frac{\ker(\theta)}{[\ker(\theta),\ker(\theta)]}.$$

Therefore, $\ker(\theta)/[\ker(\theta),\ker(\theta)]$ is torsion-free by Proposition 2.19. □

On the other hand, the following result describes the torsion of $H^1(G,\mathbb{Z}_p(1))$ as $\mathbb{Z}_p$-module ([**QW1**, Lemma 3.2]).

LEMMA 2.21. *Let (G,θ) be a cyclo-oriented pro-p group such that $\mathrm{im}(\theta) = 1+p^k\mathbb{Z}_p \simeq \mathbb{Z}_p$ for some $k \geq 1$. The torsion $\mathbb{Z}_p$-submodule of $H^1(G,\mathbb{Z}_p(1))$ is isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$.*

PROOF. The exact sequence of G-modules (2.16) with $m=1$ induces the exact cohomology sequence

$$\cdots \longrightarrow H^0(G,\mathbb{Q}_p(1)) \longrightarrow H^0(G,\mathbb{I}_p(1)) \xrightarrow{\delta^0} H^1(G,\mathbb{Z}_p(1)) \longrightarrow H^1(G,\mathbb{Q}_p(1)) \longrightarrow \cdots$$

As θ is non-trivial, one has $H^0(G,\mathbb{Q}_p(1)) = \mathbb{Q}_p(1)^G = 0$. Moreover, $H^1(G,\mathbb{Q}_p(1))$ is a torsion free $\mathbb{Z}_p$-module, and thus by Proposition 1.8 δ induces an isomorphism between $\mathbb{I}_p(1)^G$ and the torsion submodule of $H^1(G,\mathbb{Z}_p(1))$. Since

$$\mathbb{I}_p(1)^G = \frac{1}{p^k}\mathbb{Z}_p(1)/\mathbb{Z}_p(1) \simeq \mathbb{Z}_p/p^k\mathbb{Z}_p$$

as $\mathbb{Z}_p$-modules, this yields the claim. □

5. The Elementary Type conjecture

5.1. Demushkin groups. Let $\mathbb{F}$ be a field and let V, W be two $\mathbb{F}$-vector spaces. Recall that a *non-degenerate pairing* of V and W is a $\mathbb{F}$-bilinear form $V \times W \to \mathbb{F}$ which induces injections $V \hookrightarrow W^*$ and $W \hookrightarrow V^*$, where V^* and W^* are the $\mathbb{F}$-duals. If V and W have finite dimensions, then such monomorphisms are isomorphisms.

Definition 13. A finitely generated pro-p group G is called a **Demushkin group** if the cohomology ring $H^\bullet(G, \mathbb{F}_p)$ satisfies the following properties:

(i) $H^1(G, \mathbb{F}_p) = 1$ is isomorphic to $\mathbb{F}_p$ as $\mathbb{F}_p$-vector spaces.
(ii) the cup product $\cup\colon H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is a non-degenerate pairing.

If G is an infinite Demushkin group, then G is a Poincaré group of cohomological dimension $\mathrm{cd}(G) = 2$. On the other hand, the only torsion Demushkin group is the cyclic group of order 2 (cf. [**NSW**, (3.9.9) and (3.9.10)]). In particular, one may find a basis $\{\chi_1, \ldots, \chi_d\}$ of $H^1(G, \mathbb{F}_p)$, with $d = d(G)$, such that

$$\chi_1 \cup \chi_2 = \chi_3 \cup \chi_4 = \ldots = \chi_{d-1} \cup \chi_d, \quad \text{for } 2 \mid d,$$
$$\chi_1 \cup \chi_1 = \chi_2 \cup \chi_3 = \ldots = \chi_{d-1} \cup \chi_d, \quad \text{for } 2 \nmid d,$$

and $H^2(G, \mathbb{F}_p)$ is generated by such element.

Demuskin groups are arithmetically interesting, as they appear as Galois group of p-adic fields. In particular, if K is a *p-adic local field* (i.e., a finite extension of the field $\mathbb{Q}_p$) containing the roots of unity of order p, then the maximal pro-p Galois group $G_K(p)$ is a Demushkin group with $d(G_K(p)) = |K : \mathbb{Q}_p| + 2$ (cf. [**NSW**, Theorem 7.5.11]). From this, it follows that arithmetical Demushkin groups are also Bloch-Kato pro-p groups.

By (1.6), a Demushkin group G is a *one-relator* pro-p group, i.e., $r(G) = 1$. Thus, one has that either

$$G/[G,G] \simeq \mathbb{Z}_p^d \quad \text{or} \quad G/[G,G] \simeq \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}_p^{d-1},$$

with $k \geq 1$. Set $q_G = 0$ in the former case and $q_G = p^k$ in the latter. The structure of Demushkin groups has been studied in the '60s by S.P. Demuškin, J.-P. Serre and finally by J. Labute, who completed the case $p = 2$ and equipped Demushkin groups with a suitable orientation. Altogether, one has the following (cf. [**La67**]).

THEOREM 2.22. *Let G be a finitely generated one-relator pro-p group, and set q_G as above. Then G is a Demushkin group if, and only if, it is isomorphic to the pro-p group with a presentation $\langle x_1, \dots, x_d | r = 1\rangle$ with $d = d(G)$, such that*

(i) *if p is odd or if $p = 2$ and $q_G \neq 2$, one has*

$$r = x_1^{-q_G}[x_1, x_2][x_3, x_4] \cdots [x_{d-1}, x_d];$$

(ii) *if $q_G = 2$ and d is odd, one has*

$$r = x_1^{-2}x_2^{-2^f}[x_2, x_3][x_4, x_5] \cdots [x_{d-1}, x_d],$$

for some $f = 2, 3, \dots, \infty$;

(iii) *if $q_G = 2$ and d is even, one has*

$$r = x_1^{-2-\alpha}[x_1, x_2]x_3^{-2^f}[x_3, x_4] \cdots [x_{d-1}, x_d],$$

for some $f = 2, 3, \dots, \infty$ and $\alpha \in 4\mathbb{Z}_2$.

Moreover, let $\theta\colon G \to \mathbb{Z}_p^\times$ be the orientation defined by

(i) *$\theta(x_2) = (1 - q_G)$ and $\theta(x_i) = 1$ for $i \neq 2$, if $q_G \neq 2$;*
(ii) *$\theta(x_1) = -1$, $\theta(x_3) = (1 - 2^f)$ and $\theta(x_i) = 1$ for $i \neq 1, 3$, if $q_G = 2$ and d is odd;*
(iii) *$\theta(x_2) = -(1+\alpha)^{-1}$, $\theta(x_4) = (1-2^f)$ and $\theta(x_i) = 1$ for $i \neq 2, 4$, if $q_G = 2$ and d is even.*

Then θ is a cyclotomic orientation for G.

REMARK 2.23. Note that in [**La67**], the author uses a different notation:

(a) he uses the "right-action notation" for the commutator, i.e., $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$, that is why we get the signs minus in the relations;
(b) he uses χ instead of θ for the orientation (and he does not use such term, as he calls χ simply a "continuous homomorphism");
(c) he uses $\mathbf{U}_p$ instead of $\mathbb{Z}_p^\times$.

It is interesting to compute also the restricted Lie algebra $L_\bullet(G)$ induced by the Zassenhaus filtration, when G is a Demushkin group. Let $\mathcal{X} = \{x_1, \dots, x_d\}$, $d = d(G)$, be a minimal generating system for

G such that G has a presentation with a relation r as described in Theorem 2.22. Then r lies in $D_2(G) \smallsetminus D_3(G)$, and one has

$$r \equiv \begin{cases} [x_1, x_2] + \ldots + [x_{d-1}, x_d] \bmod D_3(G) & \text{if } q_G \neq 2 \\ x^2 + [x_1, x_2] + \ldots + [x_{d-1}, x_d] \bmod D_3(G) & \text{if } q_G = 2,\ 2 \mid d \\ x^2 + [x_2, x_3] + \ldots + [x_{d-1}, x_d] \bmod D_3(G) & \text{if } q_G = 2,\ 2 \nmid d \end{cases}$$

(where we used the additive notation for the quotient $D_2(G)/D_3(G)$). If $q_G \neq 2$, then [**Gä11**, Theorem 2.4.6] and Theorem 1.14 imply that the restricted Lie algebra $L_\bullet(G)$ is the quotient of the free restricted $\mathbb{F}_p$-Lie algebra $L_p(\mathcal{X})$ over the ideal $\mathfrak{r}$ generated by the image of r in $L_2(F)$, where F is the free pro-p group generated by $\mathcal{X}$. Moreover, by Proposition 1.18 one has

$$\operatorname{gr}_\bullet(G) \simeq \mathcal{U}_p(L_\bullet(G)) \simeq \frac{\mathbb{F}_p\langle\mathcal{X}\rangle}{\langle [X_1, X_2] + \ldots + [X_{d-1}, X_d]\rangle}, \tag{2.19}$$

where $\mathcal{X} = \{X_1 \ldots, X_d\}$, with the grading induced by the degrees of the monomials.

5.2. Free products and the Elementary Type Conjecture. Let G be a profinite group, and let $\{G_i, i \in \mathcal{I}\}$ be a collection of profinite groups with $\mathcal{I}$ a set of indices. For every $i \in \mathcal{I}$, let $\iota_i \colon G_i \to G$ be a continuous homomorphism. If the set $\mathcal{I}$ is not finite, assume further that for every open neighborhood U of 1 in G, U contains all but a finite number of the images $\operatorname{im}(\iota_i)$ (if this condition is satisfied, the family $\{\iota_i, i \in \mathcal{I}\}$ is said to be *convergent*).

The profinite group G, together with the maps ι_i, is said to be the **free profinite product** of the groups G_i if the following universal property is satisfied: whenever $\{\psi_i \colon G_i \to H, i \in \mathcal{I}\}$ is a convergent family of continuous homomorphisms into a profinite group H, there exists a unique continuous homomorphism $\psi \colon G \to H$ such that

$$\begin{array}{ccc} G_i & \xrightarrow{\iota_i} & G \\ {\scriptstyle \psi_i}\downarrow & \swarrow_{\psi} & \\ H & & \end{array} \tag{2.20}$$

commutes for every $i \in \mathcal{I}$. Such free product is denoted by

$$G = \coprod_{i \in \mathcal{I}} G_i.$$

If the groups G_i's are all pro-p, then G is the **free pro-p product** if (2.20) commutes for every $i \in \mathcal{I}$ and for any pro-p group H (see, e.g., [**RZ10**, § 9.1] and [**Ri13**, § 2.7] for details). In particular, if $\mathcal{I}$ is finite, let G^{abs} denote the free *abstract* product of the G_i's. Then G is the projective limit $\varprojlim_{\mathcal{N}} G^{abs}/N$, where $\mathcal{N}$ is the family of normal subgroups of G^{abs}

$$\mathcal{N} = \left\{ N \;\middle|\; |G^{abs} : N| = p^m, N \cap G_i \leq G_i \text{ open for all } i \right\}. \tag{2.21}$$

One may denote the free pro-p product also by

$$G = G_1 *_{\hat{p}} \cdots *_{\hat{p}} G_n.$$

It is well known that free profinite products of absolute Galois groups of fields are absolute Galois groups. Moreover, the free pro-p product of absolute Galois groups which are pro-p is a pro-p group which is realizable as absolute Galois group for some fields (see, e.g., [**Er01**] and [**HJK**] for details).

Yet, such a general statement is still missing for maximal pro-p Galois groups of fields. So far, only partial results are known: for example

(a) the free pro-p product of two arithmentic Demushkin groups is realizable as maximal pro-p Galois group of fields (this is a consequence of [**Ef97b**, Main Theorem]);
(b) the free pro-p product of θ-abelian maximal pro-p groups (and of $\mathbb{Z}/2\mathbb{Z}$ in the case $p = 2$) is realizable as maximal pro-p Galois group of fields (this can be deduced from [**Ef97a**]).

The possibility to use free pro-p products to construct new maximal pro-p Galois groups provided the inspiration to formulate the **Elementary Type Conjecture** (=ETC) on maximal pro-p Galois groups, which states how a finitely generated maximal pro-p Galois group of a field should "look like".

This conjecture originates form the theory of Witt rings: the *ETC on Witt rings of fields* was concieved in the early '80s to study maximal 2-extension of fields via Witt rings, and it states that the Witt rings of fields of characteristic not 2 can be constructed from elementary "building blocks" by means of two standard operations (cf. [**Ef06**, § 29.3]). Later, B. Jacob and R. Ware translated the conjecture in the context of maximal pro-2 Galois groups of fields, and they obtained a classification of such galois groups with small number of generators (cf. [**JW89**] and [**JW91**]). In this case, finitely generated pro-2 Galois

groups can be built from some "basic" pro-2 groups, i.e., $\mathbb{Z}_2$, Demushkin groups and $\mathbb{Z}/2\mathbb{Z}$.

In the '90s, I. Efrat stated a stronger pro-p arithmetical version of the ETC which mimics Jacob and Ware's "pro-2 translation": the maximal pro-p Galois groups of fields of characteristic not p can be constructed from elementary "building blocks", such as $\mathbb{Z}_p$, Demushkin groups and $\mathbb{Z}/2\mathbb{Z}$, by iterating two rather simple operations, i.e., free pro-p products and certain fibre products (which we will define in Section 4.3), and it was stated explicitly in [**Ef97b**, Question 4.8] and reformulated in [**En04**, Definition 1].

The ETC has been proven in some particular cases, such as maximal pro-p Galois groups of algebraic extensions of $\mathbb{Q}$, or fields satisfying certain condition on valuations. A general answer for this conjecture seems to be still quite far from being obtained (so far).

CHAPTER 3

The upper bound: θ-abelian groups

1. θ-abelian pro-p groups and the cup product

In this chapter we shall study the "mountain boundary case" of Bloch-Kato pro-p groups, namely, the case

$$\bigwedge_{\bullet} H^1(G, \mathbb{F}_p) \xrightarrow{\sim} H^\bullet(G, \mathbb{F}_p). \tag{3.1}$$

REMARK 3.1. Most of the content of this chapter is contained (sometimes in a different shape) in [**Qu14**] and [**CMQ**], plus some generalizations for the two cases $p = 2$ and $d(G) = \infty$.

In particular, one has the following fact.

LEMMA 3.2. *Let (G, θ) be a pro-p group with orientation, and assume that θ is cyclotomic with $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ if $p = 2$. Then the epimorphism* (2.15) *is an isomorphism if, and only if, the map*

$$H^1(G, \mathbb{F}_p) \wedge H^1(G, \mathbb{F}_p) \xrightarrow{\wedge_2(\cup)} H^2(G, \mathbb{F}_p) \ , \tag{3.2}$$

induced by the cup product, is injective. In particular, if G is finitely generated, then (3.2) *is an isomorphism if, and only if,*

$$\mathrm{cd}(G) = d(G). \tag{3.3}$$

PROOF. The proof is an easy argument from elementary linear algebra, together with Proposition 2.16 for the case $p = 2$. See also [**Qu14**, Prop. 4.3]. □

Since every closed subgroup of a maximal pro-p Galois group is again a maximal pro-p Galois, it is worth asking what does the injectivity of the morphism $\wedge_2(\cup)$ for every closed subgroup imply in the case of Bloch-Kato pro-p groups. In particular, one has the following Tits alternative-type result.

THEOREM 3.3. *Let (G,θ) be a Bloch-Kato pro-p group, and assume that θ is cyclotomic with $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ if $p=2$. Then G does not contain non-abelian closed free pro-p group if, and only if, the map*

$$\wedge_2(\cup)\colon H^1(C,\mathbb{F}_p) \wedge H^1(C,\mathbb{F}_p) \longrightarrow H^2(C,\mathbb{F}_p) \tag{3.4}$$

is injective for every closed subgroup C of G.

PROOF. Assume that G contains a closed subgroup C such that (3.4) is not injective. Let $\{\chi_i, i \in \mathcal{I}\}$ be an $\mathbb{F}_p$-basis of the $H^1(C,\mathbb{F}_p)$. Thus there exists a non-trivial element

$$\eta = \sum_{i,j\in\mathcal{J}} a_{ij}\chi_i \wedge \chi_j \in \ker\left(\wedge_2(\cup)\right),$$

with $\mathcal{J} \subseteq \mathcal{I}$ finite. As $\eta \neq 0$, there exist $m,n \in \mathcal{J}$, $m \neq n$, such that $a_{mn} \neq 0$. Let $\{x_i, i \in \mathcal{I}\} \subset C$ be a minimal generating system of C such that every χ_i is dual to x_i for all i, and let S be the subgroup of G generated by x_m and x_n. Then by duality (1.14) the map

$$\mathrm{res}^1_{C,S}\colon H^1(C,\mathbb{F}_p) \longrightarrow H^1(S,\mathbb{F}_p)$$

is surjective, and, by construction,

$$\ker\left(\mathrm{res}^1_{C,S}\right) = \mathrm{Span}_{\mathbb{F}_p}\left\{\,\chi_i \mid i \in \mathcal{I},\ i \neq n,m\,\right\}.$$

From the surjectivity of $\mathrm{res}^1_{C,S}$ and the commutativity of the diagram

$$\begin{array}{ccc} H^1(C,\mathbb{F}_p) \wedge H^1(C,\mathbb{F}_p) & \xrightarrow{\wedge_2(\cup)} & H^2(C,\mathbb{F}_p) \\ \downarrow{\scriptstyle \mathrm{res}^1_{C,S}} \quad \downarrow{\scriptstyle \mathrm{res}^1_{C,S}} & & \downarrow{\scriptstyle \mathrm{res}^2_{C,S}} \\ H^1(S,\mathbb{F}_p) \wedge H^1(S,\mathbb{F}_p) & \xrightarrow{\wedge_2(\cup)} & H^2(S,\mathbb{F}_p) \end{array} \tag{3.5}$$

one concludes that the lower horizontal arrow of (3.5) is the 0-map. Since S is Bloch-Kato, one has that $H^2(S,\mathbb{F}_p) = 0$, i.e., S is a 2-generated free pro-p group by Proposition 2.4, a contradiction.

Conversely, if G contains a non-abelian free pro-p group C, then $H^2(C,\mathbb{F}_p) = 0$, and (3.4) is not injective. □

The following theorem is the key to study the group structure of Bloch-Kato pro-p groups whose $\mathbb{F}_p$-cohomology ring is an exterior algebra. It is due to P. Symonds and Th. Weigel (cf. [**SW00**, Theorem 5.1.6]).

THEOREM 3.4. *Let G be a finitely generated pro-p group. Then the map* (3.2) *is injective if, and only if, G is powerful.*

2. θ-abelian pro-p groups and powerful pro-p groups

2.1. Powerful pro-p groups and Lie algebras. Recall from Section 1.2 that G^m is generated by the m-th powers of G, for $m \geq 1$. A pro-p group is said to be *powerful* if

$$[G, G] \leq \begin{cases} G^p & \text{for } p \text{ odd} \\ G^4 & \text{for } p = 2. \end{cases}$$

Moreover, G is called *uniformly powerful*, or simply *uniform*, if G is finitely generated, powerful, and

$$|\lambda_i(G) : \lambda_{i+1}(G)| = |G : \Phi(G)| \quad \text{for all } i \geq 1$$

Thus, one has the following characterization for uniform pro-p groups ([**DdSMS**, Ch. 3-4]).

THEOREM 3.5. *A finitely generated powerful pro-p group G is uniform if, and only if, G is torsion-free.*

Finally, a pro-p group G is called *locally powerful* if every finitely generated closed subgroup K of G is powerful. Moreover, for uniform pro-p groups, one has the following property (cf. [**DdSMS**, Prop. 4.32]).

PROPOSITION 3.6. *Let G be a d-generated uniform pro-p group, and let $\{x_1, \ldots, x_d\}$ be a generating set for G. Then G has a presentation $G = \langle x_1, \ldots, x_d | R \rangle$ with relations*

$$R = \left\{ [x_i, x_j] = x_1^{\lambda_1(i,j)} \cdots x_d^{\lambda_d(i,j)}, 1 \leq i < j \leq d \right\}, \tag{3.6}$$

and for all i, j one has $\lambda_n(i, j) \in p.\mathbb{Z}_p$ if p is odd, and $\lambda_n(i, j) \in 4.\mathbb{Z}_2$ if $p = 2$.

If G is a uniform pro-p group, then it is possible to associate a $\mathbb{Z}_p$-Lie algebra $\log(G)$ to it (see [**DdSMS**, § 4.5] and [**Qu14**, § 3.1]),

i.e., $\log(G)$ is the $\mathbb{Z}_p$-free module generated by the generators of G, equipped with the sum

$$x + y = \lim_{n\to\infty} x +_n y, \quad x +_n y = \left(x^{p^n} y^{p^n}\right)^{p^{-n}}, \tag{3.7}$$

and the Lie brackets

$$(x, y) = \lim_{n\to\infty} (x, y)_n, \quad (x, y)_n = \left[x^{p^n}, y^{p^n}\right]^{p^{-2n}}. \tag{3.8}$$

REMARK 3.7. Note that the $\mathbb{Z}_p$-Lie algebra $\log(G)$ of a uniform pro-p group is not related to the restricted $\mathbb{F}_p$-Lie algebra $L_p(G)$ as defined in Section 1.3.

The following result lists the properties of the $\mathbb{Z}_p$-Lie algebras associated to uniform pro-p groups we will need in the continuation (cf. [**Qu14**, § 3.1 and § 3.3]).

PROPOSITION 3.8. (i) *If G is uniform with minimal generating system $\{x_1, \ldots, x_n\}$, then it is possible to write every element $g \in G$ as $g = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$, with $\lambda_i \in \mathbb{Z}_p$, in a unique way. Thus the map*

$$G \longrightarrow \log(G), \quad x_1^{\lambda_1} \cdots x_n^{\lambda_n} \longmapsto \lambda_1 x_1 + \ldots + \lambda_n x_n$$

is a homeomorphism in the $\mathbb{Z}_p$-topology (cf. [**DdSMS**, Theorem 4.9]*).*

(ii) *If G is locally powerful and torsion-free, let C be a finitely generated subgroup of G. Then one can construct the Lie algebra $\log(C)$, which is in fact a subalgebra of $\log(G)$. In particular, the $\mathbb{Z}_p$-submodule $\mathrm{Span}_{\mathbb{Z}_p}\{x \in \mathcal{S}\}$ of $\log(G)$ is closed under Lie brackets for every finite subset $\mathcal{S} \subseteq G$.*

(iii) *An uniform pro-p group G with orientation θ is θ-abelian if, and only if, the associated $\mathbb{Z}_p$-Lie algebra $\log(G)$ has a basis $\{v_1, \ldots, v_d\}$, with $d = d(G)$, such that*

$$(v_1, v_i) = \lambda v_i \quad \textit{and} \quad (v_i, v_j) = 0$$

for all $1 < i, j \leq d$, where $\mathrm{im}(\theta) = 1 + \lambda\mathbb{Z}_p$ and $\lambda \in p\mathbb{Z}_p$, or $\lambda \in 4\mathbb{Z}_2$ if $p = 2$ (cf. [**Qu14**, Prop. 3.6]*)*

2.2. Locally powerful pro-p groups. In spite of a rather convoluted definition, torsion-free locally powerful pro-p groups have a very simple (and rigid) structure: in fact such a group is naturally equipped with an orientation θ which makes it θ-abelian.

THEOREM 3.9. *Let G be a torsion-free pro-p group. Then G is locally powerful if, and only if, there exists an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that (G,θ) is θ-abelian.*

PROOF. If G is θ-abelian, then, by Proposition 2.9, G is locally powerful and torsion-free.

Conversely, let G be a torsion-free locally powerful pro-p group, and assume first that G is finitely generated, with $d(G) = d \geq 2$, Thus by Proposition 3.6, G has a presentation $G = \langle x_1, \ldots, x_d | R\rangle$ with relations as in (3.6). Let $H_{ij} \leq_c G$ be the closed subgroup generated by the elements x_i, x_j. Since H_{ij} is uniform as well, we have that

$$H_{ij} = \left\langle x_i, x_j \,\middle|\, [x_i, x_j] = x_i^{\lambda_i(i,j)} x_j^{\lambda_j(i,j)}, \lambda_i, \lambda_j \in p.\mathbb{Z}_p \right\rangle,$$

so that $R = \{[x_i, x_j] = x_i^{\lambda_i(i,j)} x_j^{\lambda_j(i,j)}, 1 \leq i < j \leq d\}$ is the set of relations.

Since an abelian pro-p group is $\mathbf{1}$-abelian, where $\mathbf{1}$ is the trivial orientation, we may assume that G is not abelian, i.e., we may assume without loss of generality that x_1 and x_2 do not commute.

Step 1: First suppose that $d = 2$. It is well known that if G is non-abelian, then G has a presentation $\langle x, y | [x,y] y^{-p^k}\rangle$ for some uniquely determined positive integer k (with $k \geq 2$ if $p = 2$, see [**DdSMS**, Ch. 4, Ex. 13]) – in fact G is a 2-generated Demushkin group. Thus, G is θ-abelian by Proposition 2.9, with $\theta(x) = 1 + p^k$ and $\theta(y) = 1$.

Step 2: Suppose $d = 3$. By the previously mentioned remark we may choose x_1, x_2 such that $[x_1, x_2] = x_2^\lambda$, with $\lambda \in p.\mathbb{Z}_p$ (resp. $\lambda \in 4.\mathbb{Z}_2$ if $p = 2$). Thus

$$G = \left\langle x_1, x_2, x_3 \,\middle|\, [x_1, x_2] = x_2^\lambda, [x_1, x_3] = x_1^{\lambda_1} x_3^{\lambda_2}, [x_2, x_3] = x_2^{\mu_1} x_3^{\mu_2} \right\rangle,$$

with $\lambda_i, \mu_i \in p.\mathbb{Z}_p$ (resp. in $4.\mathbb{Z}_2$). Let H_{ij} be the subgroups as defined above, with $1 \leq i < j \leq 3$, and let $L = \log(G)$. Clearly, $(x_i, x_j)_n \in H_{ij}$ for all n. Hence $(x_i, x_j) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_i, x_j\}$. In particular, the Lie brackets in L are such that

$$(x_1, x_2) = \alpha x_2, \quad (x_2, x_3) = \beta_2 x_2 + \beta_3 x_3, \quad (x_1, x_3) = \gamma_1 x_1 + \gamma_3 x_3,$$

with $\alpha, \beta_i, \gamma_i \in p.\mathbb{Z}_p$ (resp. in $4.\mathbb{Z}_2$).

By the Jacobi identity, one has

$$\begin{aligned} 0 &= ((x_1,x_2),x_3) + ((x_2,x_3),x_1) + ((x_3,x_1),x_2) \\ &= (\alpha x_2, x_3) + (\beta_2 x_2 + \beta_3 x_3, x_1) - (\gamma_1 x_1 + \gamma_3 x_3, x_2) \\ &= -\beta_3\gamma_1 x_1 + (\alpha\beta_2 - \alpha\beta_2 - \alpha\gamma_1 + \beta_2\gamma_3)\, x_2 + (\alpha\beta_3 - \beta_3\gamma_3 + \beta_3\gamma_3)\, x_3, \end{aligned}$$

hence $\beta_3\gamma_1 x_1 = 0$, and thus $\beta_3 = 0$ or $\gamma_1 = 0$.

(1) If $\beta_3 = 0$, then by definition $(x_2, x_3) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_2\}$, i.e., the $\mathbb{Z}_p$-module generated by x_2 is an ideal of L. Therefore we may choose without loss of generality x_1 and x_3 such that $(x_1, x_3) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_3\}$, and $(x_i, x_2) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_2\}$ for $i = 1, 3$.

(2) If $\gamma_1 = 0$, then by definition $(x_1, x_3) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_3\}$, i.e., the $\mathbb{Z}_p$-module generated by x_2 and x_3 is an ideal of L. Therefore we may choose without loss of generality x_2 and x_3 such that $(x_2, x_3) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_2\}$, and $(x_1, x_i) \in \mathrm{Span}_{\mathbb{Z}_p}\{x_i\}$ for $i = 2, 3$.

Altogether the Lie brackets in L are

$$(x_1, x_2) = \alpha' x_2, \quad (x_2, x_3) = \beta' x_2, \quad (x_1, x_3) = \gamma' x_3,$$

with $\alpha', \beta', \gamma' \in p.\mathbb{Z}_p$ (resp. in $4.\mathbb{Z}_2$). The matrix of $\mathrm{ad}(\gamma x_3)$ with respect to the basis $\{x_1, x_2, x_3\}$ is given by

$$\mathrm{ad}(\gamma' x_3) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \beta'\gamma' & 0 \\ -\gamma'^2 & 0 & 0 \end{pmatrix}.$$

In particular, its trace is $\mathrm{tr}(\mathrm{ad}(\gamma' x_3)) = \beta'\gamma'$. Since $\mathrm{ad}(\gamma' x_3) = (\mathrm{ad}(x_1), \mathrm{ad}(x_3))$, one has $\mathrm{tr}(\mathrm{ad}(\gamma' x_3)) = \beta'\gamma' = 0$. Therefore $\beta' = 0$ or $\gamma' = 0$.

(1) If $\beta' = 0$, let $v_1 = x_1 + x_2$ and $v_2 = x_2 + x_3$. Then $(v_1, v_2) = \alpha' x_2 + \gamma' x_3$. By Proposition 3.8, one has that (v_1, v_2) is a $\mathbb{Z}_p$-linear combination of v_1 and v_2. Thus (v_1, v_2) is necessarily a multiple of v_2, i.e., $\alpha' = \gamma'$.

(2) If $\gamma' = 0$ and $\beta' \neq 0$, let $v = x_1 + x_2$. Then $(v, x_3) = \beta' x_2$. Again by Proposition 3.8, one has that $(v, x_3) \in \mathrm{Span}_{\mathbb{Z}_p}\{v, x_3\}$. In particular, no multiple of x_2 lies in $\mathrm{Span}_{\mathbb{Z}_p}\{v, x_3\}$. Therefore, this case is impossible.

(3) If $\beta' = \gamma' = 0$ then $\alpha' = 0$ by (1). So L, and hence G, is abelian. But this case was excluded previously.

This yields $\beta' = 0$ and $\alpha' = \gamma' \neq 0$, with $\alpha' \in p.\mathbb{Z}_p$ (resp. in $4.\mathbb{Z}_2$), and the claim follows from Proposition 3.8.

Step 3: Suppose that G is locally powerful, torsion-free with $d(G) = n+1 \geq 4$, and let G be generated by $x_1, \ldots, x_{n+1}$. Since G is non-abelian we may assume without loss of generality that x_1 and x_2 do not commute.

Let $H \leq_c G$ be the subgroup generated by $x_1, \ldots, x_n$. Thus by induction there is a unique (non-trivial) orientation $\theta\colon H \to \mathbb{Z}_p^\times$ such that H is θ-abelian. In particular, we may assume that $[x_1, x_i] = x_i^\lambda$ and $[x_i, x_j] = 1$ for all $2 \leq i, j \leq n$, where

$$\lambda = \theta(x_1) - 1 \in p.\mathbb{Z}_p \smallsetminus \{0\}$$

(resp. in $4.\mathbb{Z}_2 \smallsetminus \{0\}$ for $p = 2$).

Furthermore, let $H_i \leq_c G$ be the subgroup generated by x_1, x_i, x_{n+1}, for $2 \leq i \leq n$. By induction, for each i there exists an orientation $\theta_i\colon H_i \to \mathbb{Z}_p^\times$ such that H_i is θ_i-abelian.

Since $\theta_i(x_1) = \theta(x_1) = 1 + \lambda$ and $\theta_i(x_i) = \theta(x_i) = 1$ for all i, then necessarily $\theta_i(x_{n+1}) = 1$ for all i; i.e.,

$$[x_1, x_{n+1}] = x_{n+1}^\lambda \quad \text{and} \quad [x_i, x_{n+1}] = 1$$

for all i. Hence we may extend θ to G such that $\theta(x_{n+1}) = 1$. Thus G is θ-abelian.

Step 4: Assume now that G is not finitely generated, and let C be any finitely generated subgroup of G. Thus G is θ_C-abelian, for some orientation $\theta_C\colon C \to \mathbb{Z}_p^\times$. Also, let $L_C = \log(C)$ be the Lie algebra associated to C

Also, let V_C be the commutator subalgebra $(L_C, L_C) \leq L_C$, and let Z_C be the kernel of θ_C, considered as ideal of L_C. Then $(v, w) = 0$ for every $v \in Z_C$ and $w \in V_C$, and $V_C = \lambda_C Z_C$, for some $\lambda \in p\mathbb{Z}_p$ (and $\lambda \in 4\mathbb{Z}_2$ for $p = 2$). Note that V_C and Z_C are abelian Lie algebras for every C. Let

$$H = \overline{\bigcup_{C<G} V_C} \quad \text{and} \quad Z = \overline{\bigcup_{C<G} Z_C},$$

where the line denotes the closure in the $\mathbb{Z}_p$-topology. Then H and Z are abelian subgroups of G, H is the commutator subgroup of G, and $G/Z \simeq \mathbb{Z}_p$.

For every element $x \in G \smallsetminus Z$, one has $\mathrm{ad}(x)z = \lambda_x z$, for some $\lambda_x \in p\mathbb{Z}_p$ (resp., $\lambda_x \in 4\mathbb{Z}_p$). Let $x_0 \in G \smallsetminus Z$ such that λ_{x_0} has the minimal p-adic value. Then we may define an orientation $\theta\colon G \to \mathbb{Z}_p^\times$

such that $\ker(\theta) = Z$ and $\theta(x_0) = 1 + \lambda_{x_0}$. Then $\theta_C = \theta|_C$ for every finitely generated subgroup C, so that G is θ-abelian. □

REMARK 3.10. Theorem 3.9 is the union of [**Qu14**, Theorem A] (for the finitely generated case) and [**CMQ**, Prop. 3.5] (for the infinitely generated case).

Recall from Definition 5 the definition of rank of a pro-p group. The following is a well-known result.

FACT 3.11. *A non-abelian free pro-p group has infinite rank.*

From Theorem 3.3 and Theorem 3.9 one gets the following.

THEOREM 3.12. *Let G be a Bloch-Kato pro-p group (and assume further that G has a cyclotomic orientation θ' such that $\mathrm{im}(\theta') \simeq \mathbb{Z}_2$ for $p = 2$). Then the following are equivalent.*

(i) *G is locally powerful.*
(ii) *G does not contain non-abelian closed free pro-p subgroups.*
(iii) *There exists an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that G is θ-abelian.*

Moreover, if G is finitely generated, the above conditions and the below ones are equivalent.

(iv) *G is powerful.*
(v) *G is p-adic analytic.*[1]
(vi) *the cohomology ring $H^\bullet(G, \mathbb{F}_p)$ is an exterior $\mathbb{F}_p$-algebra.*
(vii) $\mathrm{cd}(G) = d(G)$.
(viii) *$d(C) = d(G)$ for every open subgroup C of G, i.e., G has constant generating number on open subgroups.*

PROOF. The equivalence between (i), (ii) and (iii) follows directly from Theorem 3.3 and Theorem 3.9. Now assume that G is finitely generated.

Condition (i) implies (iv) by definition. Conversely, if G is powerful, then the rank $\mathrm{rk}(G)$ is finite [**DdSMS**, Theorem 3.13]. Thus, by Fact 3.11, G contains no non-abelian free subgroups, and by Theorem 3.3 G is θ-abelian, for some orientation $\theta\colon G \to \mathbb{Z}_p^\times$. This establishes the equivalence between (iv) and the first three conditions.

[1] A topological group G is said to be a *p-adic analytic group* if G has the structure of analytic manyfold over $\mathbb{Q}_p$, and the function

$$f\colon G \times G \longrightarrow G, \quad (x, y) \longmapsto xy^{-1}$$

is analytic (see also [**DdSMS**, Ch. 8])

By [**DdSMS**, Theorem 8.18], condition (i) implies condition (v), whereas condition (v) implies condition (ii) follows by [**DdSMS**, Theorem 8.32].

Conditions (vi) and (vii) are equivalent by Lemma 3.2, and conditions (iv) and (vi) are equivalent by Theorem 3.4.

If G is locally powerful, then it has finite rank by the argument above, thus every open subgroup C of G is powerful. Thus, (i) implies (viii) by [**DdSMS**, Prop. 4.4]. Conversely, if (viii) holds, then one has $\mathrm{rk}(G) = d(G)$, and G contains no non-abelian free subgroups. □

For a finitely generated pro-p group G, consider the property

$$d(C) - n = |G : C|(d(G) - n) \tag{3.9}$$

for all open subgroups C of G, with n a fixed poritive integer. In the early '80s, K. Iwasawa observed that pro-p groups satisfying (3.9) have interesting representation-theoretic properties, and he raised the question of determining the groups satisfying (3.9) for each $n \geq 1$.

For $n = 1$, (3.9) becomes the well-known (topological) Schreier index formula, which characterizes free pro-p groups [**NSW**, Corollary 3.9.6]. In [**DL83**], D. Dummit and Labute answer Iwasawa's question for $n = 2$ in the case of groups with one defining relation: G is a Demushkin group if and only if G is a one-relator torsion-free pro-p group satisfying (3.9) with $n = 2$.

Hnece, Theorem 3.12(viii) provides the answer to Iwasawa's question with $n = d(G)$ in the category of finitely generated Bloch-Kato pro-p groups. A similar answer has been proven in [**KS11**] for the category of p-adic analytic pro-p groups. It is interesting to remark that the groups listed in [**KS11**, Theorem 1.1.(1)-(2), (4)] are θ-abelian for some orientation θ (in fact the groups listed in (4) are not powerful, as the image of the orientation is torsion), whereas the groups listed in [**KS11**, Theorem 1.1.(3)] are not Bloch-Kato (and thus they cannot be realized as maximal pro-p Galois groups), for they have non-trivial 3-torsion.

3. Rigid fields and θ-abelian Galois groups

Let K be a field containing a root of unity of order p, and let $G_K(p)$ be the maximal pro-p Galois group of K, with arithmentic orientation $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$. The condition of θ-abelianity of the group $G_K(p)$ can be translated in the arithmentic "language" (i.e., in conditions on the field K) in some different ways.

Recall from (1.13) that the first $\mathbb{F}_p$-cohomology group of $G_K(p)$ is isomorphic to the quotient $K^\times/(K^\times)^p$ as $\mathbb{F}_p$-vector space. Also, fix an isomorphism of $G_K(p)$-modules $\mu_p \simeq \mathbb{F}_p$. Then by (2.5) and by Corollary 1.21 one has that the second $\mathbb{F}_p$-cohomology group of $G_K(p)$ is canonically isomorphic to the subgroup $\mathrm{Br}_p(K)$ of the Brauer group of $\mathrm{Br}(K)$.

It is possible to define a map from $K^\times/(K^\times)^p \wedge K^\times/(K^\times)^p$ to $\mathrm{Br}_p(K)$ as follows. For $a, b \in K^\times$, the **cyclic K-algebra** generated by a and b is the K-algebra

$$(a,b)_K = \frac{K\langle u, v\rangle}{\langle u^p = a, v^p = b, uv = \zeta vu\rangle},$$

where $\zeta \in K^\times$ is the fixed primitive p^{th}-root of the unity (which depends on the isomorphism $\mu_p \simeq \mathbb{F}_p$). For $a, b \in K^\times$, the cyclic algebra $(a,b)_K$ represents a class of the Brauer group $\mathrm{Br}(K)$. Moreover, for every $a, b \in K^\times$, the algebra $(a^p, b)_K$ splits, so that in fact the class of $(a,b)_K$ lies in $\mathrm{Br}_p(K)$, and we may define a map

$$K^\times/(K^\times)^p \wedge K^\times/(K^\times)^p \xrightarrow{(-,-)_K} \mathrm{Br}_p(K) \ . \tag{3.10}$$

In their work on the case $n = 2$ of the Bloch-Kato conjecture, Merkur'ev and Suslin proved that one has a commutative diagram (3.11)

$$\begin{array}{ccc} K^\times/(K^\times)^p \wedge K^\times/(K^\times)^p & \xrightarrow{(-,-)_K} & \mathrm{Br}_p(K) \\ \downarrow \wr & & \uparrow \wr \\ H^1(G_K(p), \mathbb{F}_p) \wedge H^1(G_K(p), \mathbb{F}_p) & \xrightarrow{\wedge_2(\cup)} & H^2(G_K(p), \mathbb{F}_p) \end{array}$$

where the upper horizontal arrow (and thus also the lower one) is an epimorphism of vector spaces over $\mathbb{F}_p$.

3.1. p-rigid fields. Let a be a p-power free unit of K (i.e., $a \in K^\times \smallsetminus (K^\times)^p$). Then $K(\sqrt[p]{a})/K$ is a Galois extension of degree p, with cyclic Galois group generated by an element $\bar\sigma \in \mathrm{Gal}(K(\sqrt[p]{a})/K)$ of order p. Recall that the **norm** $\mathfrak{N}$: $K(\sqrt[p]{a}) \to K$ of the extension

$K(\sqrt[p]{a})/K$ is defined by

$$\begin{aligned}\mathfrak{N}(\gamma) &= \gamma\cdot\bar{\sigma}(\gamma)\cdots\bar{\sigma}^{p-1}(\gamma)\\ &= \prod_{i=0}^{p-1}\left(c_0+c_1\zeta^i\sqrt[p]{a}+\ldots+c_{p-1}\zeta^{i(p-1)}\sqrt[p]{a^{p-1}}\right),\end{aligned}$$

with $\gamma = c_0 + c_1\sqrt[p]{a} + \ldots + c_{p-1}\sqrt[p]{a^{p-1}}$.

Definition 14. Let K be a field containing a primitive p-th root of unity (and containing also $\sqrt{-1}$, if $p=2$).

(i) An element $a\in K^\times$ which is p-power free is said to be **p-rigid** if $\mathfrak{N}(K(\sqrt[p]{a}))$ is contained in the set $\bigcup_{n=0}^{p-1} a^n K^p$.
(ii) The field K is said to be **p-rigid** if all of the elements in $K\smallsetminus K^p$ are p-rigid.

Remark 3.13. (i) Since $\mathfrak{N}(K)=K^p$, every p-power of K is a norm of $K(\sqrt[p]{a})/K$.
(ii) The restriction of the norm on the multiplicative group $K(\sqrt[p]{a})^\times$ is a group homomorphism.
(iii) If p is odd, then $\mathfrak{N}(\sqrt[p]{a^m}) = a^m$, with m a positive integer, whereas if $p=2$ then $\mathfrak{N}(\sqrt{a}) = -a$.

The notion of p-rigidity of fields was introduced by K. Szymiczek in [**Sz77**], and it was developed and studed first in the case $p=2$, and then in the case of an odd prime. The notion of p-rigidity is important expecially for the consequences on the existence of valuations (see [**Ef06**, § 11.3-11.4]).

Examples 2. (a) Let ℓ be a prime different to p and k a positive integer such that $p \mid (\ell^k-1)$, and let K be the field $\mathbb{F}_{\ell^k}(\!(X)\!)$, i.e, K is the field of Laurent series on the indeterminate X with coefficients in the finite field $\mathbb{F}_{\ell^k}$. Then K is p-rigid [**Wr92**, p. 727].
(b) Let ζ be a primitive p-th root of unity and ℓ a prime different to p. Then the p-adic field $\mathbb{Q}_\ell(\zeta)$ is p-rigid [**CMQ**, Exam. 3.1].

In the case $p=2$, one may understand a 2-rigid field by studying the structure of the Witt ring of quadratic forms of the field. The consequences of 2-rigidity were studied in several papers, and today many results about 2-rigid fields are known, and these fields are rather well understood (see, for example, [**Wr81**], [**AEJ**], [**JW89**] and [**LS02**]).

The problem to generalize the results obtained in the case $p=2$ for odd primes has been considered rather hard for long time. A first difficulty is that there is no usable version of Witt ring for higher degree

forms. Thus, one has to find an "odd substitute" of a quaternionic pairing. (Indeed, quaternionic pairings were developed as a tool for studying abstract Witt rings.) The first attempts to use the cup product in Galois cohomology to study the maximal pro-p Galois groups of p-rigid fields are to be found in [**Wr92**] first, and then, more explicitly, in [**HJ95**]. On the other hand, [**EK98**] makes no use of cohomological tools.

It is worth to stress that all the contribuitions to p-rigid fields listed so far make use of instruments provided by the theory of valuations, whereas our approach (based only on Galois cohomology and the theory of pro-p groups) makes it possible to study p-rigid without any "help" from valuation theory. In fact, the following result is the key to relate p-rigid fields with the cohomology of maximal pro-p Galois groups.

PROPOSITION 3.14. *Let K be a field containing a root of unity of order p (and also $\sqrt{-1}$, if $p = 2$). Then K is p-rigid if, and only if, the map $\wedge_2(\cup)$ in the $\mathbb{F}_p$-cohomology of the Galois group $G_K(p)$ is a monomorphism.*

PROOF. The definition of p-rigidity states that for every a, the norms of $K(\sqrt[p]{a})/K$ modulo $(K^\times)^p$ are precisely the $\mathbb{F}_p$-multiples of the $\bar{a}^i$'s, with $\bar{a}^i = a^i \bmod (K^\times)^p$ and $0 \leq i \leq p-1$, i.e.,

$$\mathfrak{N}(\sqrt[p]{a}) = \mathrm{Span}_{\mathbb{F}_p}\{\bar{a}, \ldots, \bar{a}^{p-1}\} \leq K^\times/(K^\times)^p.$$

It is well known that the class of $(a,b)_K$ is trivial in $\mathrm{Br}(K)$ if, and only if, b is a norm of $K(\sqrt[p]{a})/K$ – in particular, if b is a p-power of K or if $\bar{b}$ is $\mathbb{F}_p$-linearly dependent to $\bar{a}$ in $K^\times/(K^\times)^p$, by Remark 3.13.

Consequently, K is p-rigid if, and only if, the algebra $(a,b)_K$ splits if, and only if, $\bar{b}$ is $\mathbb{F}_p$-linearly dependent to $\bar{a}^i$ in $K^\times/(K^\times)^p$ for some i, namely, the map (3.10) is a monomorphism. Therefore the claim follows from the commutative diagram (3.11). □

This provides a first immediate consequence.

COROLLARY 3.15. *Let K be a field containing a primitive p-th root of unity (and also $\sqrt{-1}$, if $p = 2$), and assume that the quotient $K^\times/(K^\times)^p$ is finite. Then K is p-rigid if, and only if, the maximal pro-p Galois group $G_K(p)$ is θ-abelian, with $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$ the arithmetical orientation.*

Note that under the assumption that K contains $\sqrt{-1}$, one has that either $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ or $\theta \equiv \mathbf{1}$.

In order to study explicitly the structure of maximal pro-p Galois group of p-rigid fields, R. Ware introduced in [**Wr92**] also the notion

of hereditary p-rigidity: a field K is said to be hereditarily p-rigid if every subextension of the p-closure $K(p)$ is p-rigid. As Ware pointed out, to conclude that K is hereditary p-rigid, it is enough to check that each finite extension L/K is p-rigid. In [**EK98**], A. Engler and J. Koenigsmann showed that p-rigidity implies hereditary p-rigidity, and later also the author, with S.K. Chebolu and J. Mináč, proved the same result using a different argument (cf. [**CMQ**, § 3.3]). The former proof makes use of techniques from the theory of valuations.

THEOREM 3.16. *If a field K containing a primitive p-th root of unity (and $\sqrt{-1}$ for $p = 2$) is p-rigid, then every p-extension L of K is rigid.*

REMARK 3.17. Note that if the quotient $K^\times/(K^\times)^p$ is finite, then it is possible to prove that a p-rigid field is also hereditarily p-rigid without making use of arithmetical tools. Indeed, assume that the field K (containing a primitive p-th root of unity and also $\sqrt{-1}$ if $p = 2$) is p-rigid. Then by Proposition 3.14 and Theorem 3.4 the maximal pro-p Galois group $G_K(p)$ is powerful, and by Theorem 3.12 it is also locally powerful. Thus again by Proposition 3.14 and Theorem 3.4 every p-extension L of K is p-rigid.

Therefore, one has an "arithmetical version" of Theorem 3.12.

THEOREM 3.18. *Let K be a field containing a primitive p-th root of unity (and $\sqrt{-1}$ for $p = 2$), and let G be the maximal pro-p Galois group of K, equipped with the arithmetical orientation $\theta\colon G \to \mathbb{Z}_p^\times$. Then, K is p-rigid if, and only if:*

(i) *G is θ-abelian and $\mathrm{im}(\theta) = 1 + p^k\mathbb{Z}_p$, where k is the maximum positive integer such that $\mu_{p^k} \subseteq K$ and $\mu_{p^{k+1}} \nsubseteq K$ (in case $\mu_{p^\infty} \subseteq K$, then $k = \infty$ and $\theta \equiv \mathbf{1}$);*
(ii) *there are no p-extensions L/K such that the maximal pro-p Galois group $G_L(p)$ is free and non-abelian;*
(iii) *G is solvable;*[2]

Assume further that the quotient $K^\times/(K^\times)^p$ is finite. Then, K is p-rigid if, and only if:

(iv) *G is powerful;*
(v) *the cohomology ring $H^\bullet(G, \mathbb{F}_p)$ is isomorphic to the exterior $\mathbb{F}_p$-algebra $\bigwedge_{i\geq 0} K^\times/(K^\times)^p$;*

[2]I.e., G admits a finite normal series of closed subgroups such that each successive quotient is abelian

(vi) *one has*

$$\mathrm{cd}(G) = \dim_{\mathbb{F}_p}\left(K^\times/(K^\times)^p\right) = \frac{1}{p}\left|K^\times/(K^\times)^p\right|.$$

(vii) *for every finite p-extension L/K one has*

$$\dim_{\mathbb{F}_p}\left(L^\times/(L^\times)^p\right) = \dim_{\mathbb{F}_p}\left(K^\times/(K^\times)^p\right).$$

The above result extends and generalizes the results proved in [**Wr92**] and some in [**EK98**]. In particular, Corollary 2, Theorem 2 and Theorem 4 in the former paper require the assumption that K contains also a root of unity of order p^2, which is not necessary in our result.

4. Finite quotients and θ-abelian groups

It is possible to obtain further characterizations of θ-abelian pro-p groups which involve finite quotients, and which have a particular arithmetical interpretation.

For a pro-p group G, let $\Phi_2(G)$ be the Frattini subgroup of the Frattini subgroup, i.e.,

$$\Phi_2(G) = \Phi\left(\Phi(G)\right).$$

Thus, $G^{p^2} \leq \Phi_2(G)$, so that the quotient $G/\Phi_2(G)$ has exponent p^2. In particular, if G is finitely generated, then the quotient $G/\Phi_2(G)$ is a finite p-group. Also, one has

$$\lambda_3(G) = \Phi_2(G) \cdot [G, \Phi(G)], \tag{3.12}$$

where $\lambda_3(G)$ is the third element of the p-descending central series (see Subsection 1.2.1).

If G is θ-abelian for some orientation θ, then one has a tighter relation between $\lambda_3(G)$ and $\Phi_2(G)$.

THEOREM 3.19. *Let G be a finitely generated Bloch-Kato pro-p group. Then there exists an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that G is θ-abelian if, and only if, one has the equality*

$$\Phi_2(G) = \lambda_3(G).$$

PROOF. Assume first that G is θ-abelian, for some orientation θ. Then one has

$$\Phi_2(G) = \Phi(G)^p[\Phi(G), \Phi(G)] = G^{p^2} = \lambda_3(G)$$

– in fact one has $\lambda_i(G) = G^{p^{i-1}}$ for every $i \geq 1$.

Conversely, assume that $\Phi_2(G) = \lambda_3(G)$. Since

$$[D_2(G), D_2(G)] \leq D_4(G) \quad \text{and} \quad D_2(G)^p \leq D_{2p}(G),$$

one has

$$\Phi_2(G) = D_2(G)^p\,[D_2(G), D_2(G)] \leq D_4(G),$$

as $\Phi(G) = D_2(G)$. Moreover, one has the inclusion $\gamma_3(G) \leq \lambda_3(G)$. Therefore, one has the chain of inclusions

$$\gamma_3(G) \leq \lambda_3(G) = \Phi_2(G) \leq D_4(G). \tag{3.13}$$

We shall split the proof of this implication in three cases.

(i) Assume $p > 3$. By Lazard's formula (1.7), one has

$$D_3(G) = \prod_{ip^h \geq 3} \gamma_i(G)^{p^h} = \gamma_3(G) \cdot G^p,$$

$$D_4(G) = \prod_{ip^h \geq 4} \gamma_i(G)^{p^h} = \gamma_4(G) \cdot G^p.$$

Therefore, (3.13) implies

$$D_3(G) = \gamma_3(G) \cdot G^p \leq \lambda_3(G) = \Phi_2(G) \cdot G^p \leq D_4(G),$$

as $G^p \leq D_4(G)$. Thus, one has the equality $D_3(G) = D_4(G)$. Hence, Proposition 1.12 implies that $\mathrm{rk}(G)$ is finite, and thus by Theorem 3.12 there is an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that G is θ-abelian.

(ii) Assume $p = 2$. From (1.7) one obtains

$$D_3(G) = \prod_{i2^h \geq 3} \gamma_i(G)^{2^h} = \gamma_3(G) \cdot \gamma_2(G)^2 \cdot G^4,$$

$$D_4(G) = \prod_{i2^h \geq 4} \gamma_i(G)^{2^h} = \gamma_4(G) \cdot \gamma_2(G)^2 \cdot G^4.$$

Therefore, (3.13) implies

$$D_3(G) = \gamma_3(G)\gamma_2(G)^2G^4 \leq \Phi_2(G)\gamma_2(G)^2G^4 \leq D_4(G),$$

as $\gamma_2(G)^2G^4 \leq D_4(G)$. Thus, one has the equality $D_3(G) = D_4(G)$. Hence, Proposition 1.12 implies that $\mathrm{rk}(G)$ is finite, and thus by Theorem 3.12 there is an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that G is θ-abelian.

(iii) Assume $p = 3$. By (1.7), one has

$$D_4(G) = \prod_{i3^h \geq 4} \gamma_i(G)^{3^h} = \gamma_4(G) \cdot \gamma_2(G)^3 \cdot G^9,$$
$$D_5(G) = \prod_{i3^h \geq 5} \gamma_i(G)^{3^h} = \gamma_5(G) \cdot \gamma_2(G)^3 \cdot G^9.$$

Therefore, from (3.13) one obtains the chain of inclusions

$$\gamma_4(G) = [G, \gamma_3(G)] \leq [G, D_4(G)] = [D_1, D_4(G)] \leq D_5(G),$$

which implies

$$D_4(G) = \gamma_4(G) \cdot \gamma_2(G)^3 \cdot G^9 \leq D_5(G),$$

as $G^9, \gamma_2(G)^3 \leq D_5(G)$. Thus, one has the equality $D_4(G) = D_5(G)$. Hence, Proposition 1.12 implies that $\mathrm{rk}(G)$ is finite, and thus by Theorem 3.12 there is an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that G is θ-abelian.

□

Corollary 3.20. *Let G be a finitely generated Bloch-Kato pro-p group. Then there exists an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that G is θ-abelian if, and only if, one has*

$$\Phi(G)/\Phi_2 \leq \mathrm{Z}\left(G/\Phi_2\right). \tag{3.14}$$

Proof. Assume that G is θ-abelian. Then by Theorem 3.19 one has $\lambda_3(G) = \Phi_2(G)$, and $\lambda_2(G)/\lambda_3(G)$ is central in $G/\lambda_3(G)$.

Conversely, assume that $\Phi(G)/\Phi_2$ is central in $G/\Phi_2(G)$. This implies that the commutator subgroup $[G, \Phi(G)]$ is contained in $\Phi_2(G)$. Since

$$\Phi_2(G) = \Phi\left(\Phi(G)\right) \geq \left(\Phi(G)\right)^p \quad \text{and} \quad \lambda_3(G) = \left(\Phi(G)\right)^p [G, \Phi(G)],$$

it follows that $\Phi_2(G)$ contains $\lambda_3(G)$, and thus $\lambda_3(G) = \Phi_2(G)$. □

4.1. Rigid fields and small Galois groups. The above results can be translated in the arithmetical "language" in terms of finite extensions. Let K be a field containing a root of unity of order p, and let G be the maximal pro-p Galois group $G_K(p)$. Recall that by Proposition 1.20 the quotient $G/\Phi(G)$ is the Galois group of the extension of $K(\sqrt[p]{K})/K$. Set $L = K(\sqrt[p]{K})$. Then $L(\sqrt[p]{L})/K$ is again a Galois extension, and one has

$$\mathrm{Gal}\left(L(\sqrt[p]{L})/L\right) = \frac{\Phi(G)}{\Phi_2(G)} \quad \text{and} \quad \mathrm{Gal}\left(L(\sqrt[p]{L})/K\right) = \frac{G}{\Phi_2(G)},$$

as $\Phi_2(G)$ is the maximal pro-p Galois group of the field $L(\sqrt[p]{L})$. An important subextension of $L(\sqrt[p]{L})$ is the following: let $A \subseteq L^\times$ be the set

$$A = \left\{a \in L^\times \;\middle|\; L\left(\sqrt[p]{a}\right)/K \text{ is Galois}\right\}.$$

Consider the field $L(\sqrt[p]{A})$. The following well-known fact (cf. [**CMQ**, Lemma 2.2]) is necessary to determine the Galois group of $L(\sqrt[p]{A})/K$.

Fact 3.21. *Let K be a field containing a primitive p^{th}-root of unity, and let L/K be a p-extension with $a \in L^\times$. Then $L(\sqrt[p]{a})/K$ is Galois if, and only if,*

$$\frac{\sigma(a)}{a} \in L^p$$

for every $\sigma \in \mathrm{Gal}(L/K)$.

Proposition 3.22. *Let K be a field containing a root of unity of order p (and containing also $\sqrt{-1}$ in the case $p = 2$), and let L/K and $A \subseteq L^\times$ be as above. Then the subgroup $\lambda_3(G)$ of G is the maximal pro-p Galois group of $L(\sqrt[p]{A})$, i.e.,*

$$G/\lambda_3(G) = \mathrm{Gal}\left(L(\sqrt[p]{A})/K\right).$$

Proof. By Proposition 1.20 one knows that

$$\frac{L^\times}{(L^\times)^p} \simeq \left(\frac{\Phi(G)}{\Phi_2(G)}\right)^\vee.$$

By Fact 3.21, the set A corresponds to the G-invariant submodule $(L^\times/(L^\times)^p)^G$ of $L^\times/(L^\times)^p$, considered as discrete G-module.

On the other hand, (3.12) implies that the quotient $\Phi(G)/\lambda_3(G)$ is isomorphic to the G-coinvariant quotient of the discrete G-module

$\Phi(G)/\Phi_2(G)$. Therefore, by duality one has the isomorphisms of discrete G-modules

$$\frac{A}{(L^\times)^p} = \left(\frac{L^\times}{(L^\times)^p}\right)^G \simeq \left(\left(\frac{\Phi(G)}{\Phi_2(G)}\right)_G\right)^\vee \simeq \left(\frac{\Phi(G)}{\lambda_3(G)}\right)^\vee,$$

so that the claim follows by Kummer duality. □

Theorem 3.19 and Proposition 3.22 have the following consequence.

COROLLARY 3.23. *Let $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$ be the arithmetical orientation of the maximal pro-p Galois group of K. Then $G_K(p)$ is θ-abelian if, and only if, the extension $L(\sqrt[p]{a})/K$ is Galois for every $a \in L$.*

The equality of Galois groups $\lambda_3(G_K(p)) = \Phi_2(G_K(p))$ is equivalent to the equality of extensions

$$L(\sqrt[p]{A})/K = L(\sqrt[p]{L})/K. \tag{3.15}$$

Therefore, K is p-rigid if, and only if, equality (3.15) holds. [3] This is the main result in [**CMQ**], and it completes the the result obtained by D. Leep and T. Smith for 2-rigid fields in [**LS02**].

In the case $p = 2$ the quotient $G_K(p)/\lambda_3(G_K(p))$ has been extensively studied under the name of "W-group", in particular in connection with quadratic forms (see, e.g., [**MSp90**]). It was further shown that in this case such quotient has great arithmetical significance, as it encodes information about orderings and valuations of K. In the case p odd the quotient $G_K(p)/\lambda_3(G_K(p))$ has been studied by S.K. Chebolu, J. Mináč and Efrat in [**CEM**] (see also Theorem 2.7).

Also, one has the following (cf. [**CMQ**, § 4.2]).

THEOREM 3.24. *Let K be a field containing a root of unity of order p (and containing also $\sqrt{-1}$ in the case $p = 2$). Then K is p-rigid if, and only if the p-closure of K is obtained by adjoining the p-power roots of all the elements of K, namely,*

$$K(p) = K\left(\sqrt[p^m]{a}, m \geq 1, a \in K\right).$$

Note that if the field K is p-rigid, then one needs only the quotient $K^\times/(K^\times)^p$ and the image of the arithmetical orientation $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$ to recover the entire structures of the maximal pro-p Galois group $G_K(p)$ and of the p-closure $K(p)/K$.

[3] Note that the following notation is rather common in papers on rigid fields: $K^{(2)} = L$, $K^{(3)} = L(\sqrt[p]{A})$ and $K^{\{3\}} = L(\sqrt[p]{L})$, see for example [**CMQ**, § 2.3]

5. The Zassenhaus filtration for θ-abelian groups

The rather simple structure of a θ-abelian pro-p group makes it possible to compute explicitly the Zassenhaus filtration and the induced quotients.

Let (G,θ) be a θ-abelian pro-p group, with $k \in \mathbb{N} \cup \{\infty\}$ such that $\mathrm{im}(\theta) = 1+p^k\mathbb{Z}_p$ (in particular, $k=\infty$ if, and only if, $\theta \equiv \mathbf{1}$, as $p^\infty = 0$ in the pro-p topology). Then one has

$$\gamma_i(G) = \ker(\theta)^{p^{k(i-1)}} \quad \text{for every } i > 1.$$

For every $n \geq 1$ set $\ell = \lceil \log_p(n) \rceil$, i.e., ℓ is the least integer such that $n \leq p^\ell$. Hence, by Lazard's formula (1.7), one has

$$D_n(G) = G^{p^\ell} \prod_{ip^h \geq n} \ker(\theta)^{p^{k(i-1)+h}}, \quad \text{with } i \geq 2. \tag{3.16}$$

We shall show that for every i,h such that $i \geq 2$ and $ip^h \geq n$, one has the inequality

$$k(i-1)+h \geq \ell, \tag{3.17}$$

so that $\ker(\theta)^{p^{k(i-1)+h}} \leq G^{p^\ell}$, and $D_n(G) = G^{p^\ell}$. If $h \geq \ell$, then inequality (3.17) follows immediately. Otherwise, notice that $i > p^{\ell-h-1} \geq 1$, as $ip^h \geq n > p^{\ell-1}$, which implies

$$k(i-1) > k\left(p^{(\ell-h)-1}-1\right). \tag{3.18}$$

Therefore, for $\ell - h \geq 2$, the inequality (3.18) implies $k(i-1) \geq \ell - h$, and thus (3.17), whereas for $\ell - h = 1$ (3.17) follows from the fact that $i \geq 2$.

Altogether, this shows that

$$D_n(G) = G^{p^\ell} \quad \text{for } p^{\ell-1} < n \leq p^\ell. \tag{3.19}$$

Consequently, the quotients induced by the Zassenhaus filtration are

$$L_i(G) = \frac{D_i(G)}{D_{i+1}(G)} \simeq \begin{cases} G/\Phi(G) & \text{for } i \text{ a } p^{th}\text{-power} \\ 0 & \text{otherwise} \end{cases} \tag{3.20}$$

as $\mathbb{F}_p$-vector spaces. Therefore, $L_\bullet(G)$ is an abelian restricted Lie algebra over $\mathbb{F}_p$, and by Proposition 1.18 the restricted envelope is the polynomial $\mathbb{F}_p$-algebra in $d(G)$ indeterminates, i.e.,

$$\mathrm{gr}_\bullet(G) \simeq \mathcal{U}_p(L_\bullet(G)) \simeq \mathbb{F}_p\left[X_1,\ldots,X_{d(G)}\right], \tag{3.21}$$

with the grading induced by the degrees of the monomials.

REMARK 3.25. It is worth to stress that the Zassenhaus filtration loses completely the information about the image of the orientation θ – as it happens for Demuškin groups, see (2.19).

THEOREM 3.26. *Let (G, θ) be a finitely generated pro-p group with a cyclotomic orientation, and assume further that $\mathrm{im}(\theta) \leq 1 + 4\mathbb{Z}_2$ if $p = 2$. Then the following are equivalent:*

(i) *G is θ-abelian;*
(ii) *the algebra $L_\bullet(G)$ is an abelian restricted Lie algebra over $\mathbb{F}_p$;*
(iii) *the algebra $\mathrm{gr}_\bullet(G)$ is a commutative polynomial $\mathbb{F}_p$-algebra.*

PROOF. Assume first that G is θ-abelian. Then (ii) and (iii) follow from (3.20) and (3.21).

Assume that the algebra $L_\bullet(G)$ is abelian. Then (3.21) follows immediately. Moreover, one has $L_i(G) = D_i(G)/D_{i+1}(G)$ whenever i is not a p-power. In particular, $D_i(G) = D_{i+1}(G)$ for every such i's, so that [**DdSMS**, Theorem 11.4] implies that G has finite rank, and (i) follows by Theorem 3.12.

Assume now that $\mathrm{gr}_\bullet(G)$ is a commutative polynomial $\mathbb{F}_p$-algebra. Since the map $\psi_{L_\bullet(G)} \colon L_\bullet(G) \to \mathrm{gr}_\bullet(G)$ is a monomorphism, also the restricted Lie algebra $L_\bullet(G)$ has to be commutative, so that (iii) implies (ii). □

COROLLARY 3.27. *Let K be a field containing a primitive p-th root of unity such that the quotient $K^\times/(K^\times)^p$ is finite, and assume further that $\sqrt{-1}$ lies in K if $p = 2$. Then the following are equivalent:*

(i) *K is p-rigid;*
(ii) *the algebra $L_\bullet(G_K(p))$ induced by the maximal pro-p Galois group $G_K(p)$ is an abelian restricted Lie algebra over $\mathbb{F}_p$;*
(iii) *the algebra $\mathrm{gr}_\bullet(G_K(p))$ is a commutative polynomial $\mathbb{F}_p$-algebra.*

CHAPTER 4

Products, relations, and the ETC

1. The group $H^1(G, \mathbb{Z}_p(1))$

Let (G, θ) be a cyclo-oriented pro-p group. Our first goal is to study the structure of the cohomology group $H^1(G, \mathbb{Z}_p(1))$ and the continuous crossed homomorphism $f\colon G \to \mathbb{Z}_p(1)$ which represent the cohomology classes.

The following result is a consequence of [**La67**, Prop. 6].

PROPOSITION 4.1. *Let (G, θ) be a finitely generated pro-p group with orientation. Then θ is cyclotomic if, and only if, one may arbitrarily prescribe the values of a continuous crossed homomorphisms $f\colon G \to \mathbb{Z}_p(1)$ on a minimal system of generators of G.*

PROOF. First of all, recall that by Proposition 2.11, θ is a cyclotomic orientation for G if, and only if, one has the epimorphism (2.12).

Assume first that it is possible to arbitrarily prescribe the values of a crossed homomorphism f on a minimal system of generators of G. Then it is easy to see that (2.12) is an epimorphism: indeed, for every $\chi \in H^1(G, \mathbb{F}_p)$, χ is the image of a crossed homomorphism $f\colon G \to \mathbb{Z}_p(1)$ such that $f(x) \equiv \chi(x) \bmod p$ for every generator x of G.

Conversely, assume that (2.12) is an epimorphism. The composition of projections $\mathbb{Z}_p(1) \twoheadrightarrow \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1) \twoheadrightarrow \mathbb{F}_p$ for every $n \geq 1$ implies that the map

$$H^1(G, \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)) \longrightarrow H^1(G, \mathbb{F}_p)$$

is surjective for every $n \geq 1$. In particular, condition (1) of [**La67**, Prop. 6] holds, and this yields the thesis. □

For $x, y \in G$ and $f\colon G \to \mathbb{Z}_p(1)$ a continuous crossed homomorphism, one has the formula

$$f([x, y]) = (\theta(x) - 1)f(y) - (\theta(y) - 1)f(x). \tag{4.1}$$

Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1 \tag{4.2}$$

be a minimal presentation for a finitely generated cyclo-oriented pro-p group (G, θ). Since $R \leq \Phi(G)$, we may extend θ to an orientation $\tilde{\theta}\colon F \to \mathbb{Z}_p^\times$ such that $\theta \circ \pi = \tilde{\theta}$. Note that $(F, \tilde{\theta})$ is again a cyclo-oriented pro-p group by Remark 2.10. Then, one has the following.

FACT 4.2. (i) *A continuous crossed homomorphism $f\colon G \to \mathbb{Z}_p(1)$ is uniquely determined by the values of f on a minimal set of generators of G. In particular, we may arbitrarily prescribe such values (cf.* [**La67**, Prop. 6 (3)]*).*

(ii) *For a crossed homomorphism $f\colon G \to \mathbb{Z}_p(1)$, let $\tilde{f}\colon F \to \mathbb{Z}_p(1)$ be the lift of f induced by the values of f on a minimal set of generators of G, i.e., $\tilde{f} = f \circ \pi$. Then one has $\tilde{f}|_R \equiv \mathbf{0}$.*

(iii) *If a crossed homomorphism $h\colon F \to \mathbb{Z}_p(1)$ is zero on a set of defining relations of R, then $h|_R \equiv \mathbf{0}$. Indeed, if $\rho \in R$ and $h(\rho) = 0$, (4.1) implies that*

$$\begin{aligned} h\left({}^x\rho\right) &= h\left([x,\rho]\rho^{-1}\right) \\ &= h([x,\rho]) + \theta([x,\rho])h(\rho^{-1}) \\ &= (\theta(x)-1)h(\rho) - (\theta(\rho)-1)h(x) + 1 \cdot 0 = 0, \end{aligned}$$

as $\theta(\rho) = 1$.

For every crossed homomorphism $f\colon G \to \mathbb{Z}_p(1)$, the restriction $f|_{\ker(\theta)}\colon \ker(\theta) \to \mathbb{Z}_p(1)$ is a morphism of pro-p groups. In particular, if the orientation θ is trivial, then $\mathbb{Z}_p(1)$ is a trivial $\mathbb{Z}_p[\![G]\!]$-module, and

$$H^1(G, \mathbb{Z}_p(1)) \simeq \mathrm{Hom}(G, \mathbb{Z}_p).$$

Moreover, recall that from Corollary 2.20 one has that the abelianization of $\ker(\theta)$ is torsion-free. Thus one has the isomorphism of abelian pro-p groups

$$\frac{\ker(\theta)}{[\ker(\theta), \ker(\theta)]} \simeq \mathrm{Hom}(\ker(\theta), \mathbb{Z}_p) \simeq H^1(\ker(\theta), \mathbb{Z}_p(1)).$$

REMARK 4.3. Using Proposition 4.4 and Fact 4.2 allows us to prove Corollary 2.20 in a more "direct" way. Indeed, let (G, θ) be a cyclo-oriented pro-p group with θ trivial. Let 4.2 be a minimal presentation for G, and assume for contradiction that there is a relation $\rho \in R$ and a

generator $x \in F$ such that $\rho \equiv x^{p^m} \bmod [F,F]$ for some finite m. With an abuse of notation, consider x as element of G, and let $\chi \in H^1(G, \mathbb{F}_p)$ be the dual of x. Also, let the crossed homomorphism $\tilde{f}\colon F \to \mathbb{Z}_p(1)$ be a "lift" of χ, i.e., the cohomology class of $\tilde{f}$ is equivalent to χ modulo p. By assumption, $\mathbb{Z}_p(1)$ is a trivial $\mathbb{Z}_p[\![G]\!]$-module, and thus also a trivial $\mathbb{Z}_p[\![F]\!]$-module. Hence $\tilde{f}$ is an homomorphism, and

$$0 = \tilde{f}(\rho) = \tilde{f}\left(x^{p^m}\right) = p^m \tilde{f}(x) = p^m,$$

a contradiction. Thus, the abelianization $G/[G,G]$ is torsion-free.

Assume now that $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$. The orientation θ induces an action of G on $H^1(\ker(\theta), \mathbb{Z}_p(1))$, given by

$$(g.f)(z) = \theta(g) \cdot f\left(g^{-1}z\right), \quad g \in G, z \in \ker(\theta), \tag{4.3}$$

for $f \in H^1(\ker(\theta), \mathbb{Z}_p(1))$. Note that every $g \in G$ can be written as $g = x^\lambda z$, with $z \in \ker(\theta)$ and $x \in G$ such that $\theta(x)$ generates $\mathrm{im}(\theta)$. Thus, if $f\colon G \to \mathbb{Z}_p(1)$ is a continuous crossed homomorphism such that $f(x^\lambda) = 0$ for every $\lambda \in \mathbb{Z}_p$ (i.e., we may consider f as element of $\mathrm{Hom}(\ker(\theta), \mathbb{Z}_p)$), then Fact 1.1 implies that

$$f\left(x^\lambda z\right) = \theta\left(x^\lambda\right) \cdot f(z) \implies \theta\left(x^{-\lambda}\right) \cdot f\left(x^\lambda z\right) = f(z)$$

for every $\lambda \in \mathbb{Z}_p$ and $z \in \ker(\theta)$, namely, by (4.3) G acts trivially on f. Therefore, $H^1(\ker(\theta), \mathbb{Z}_p(1))^G$ embeds in $H^1(G, \mathbb{Z}_p(1))$.

Moreover, for every crossed homomorphism f and for every $x, y \in G$, one has

$$f(xy) \equiv f(x) + f(y) \mod q,$$

with q a p-th power such that $\mathrm{im}(\theta) = 1 + q\mathbb{Z}_p$. Also, by Fact 1.1 every $\lambda \in \mathbb{Z}_p(1)$ induces a crossed homomorphism

$$\lambda\colon G \longrightarrow \mathbb{Z}_p(1), \quad \lambda(x) = (\theta(x) - 1)\lambda$$

which is a 1-coboundary. Note that $\lambda|_{\ker(\theta)} \equiv \mathbf{0}$, so that λ factors through the quotient $G/\ker(\theta)$, and the image of λ is $q\lambda\mathbb{Z}_p$. Therefore, by Lemma 2.21, the reduction modulo q induces the isomorphism

$$\mathrm{tor}_{\mathbb{Z}_p}\left(H^1(G, \mathbb{Z}_p(1))\right) \xrightarrow{\sim} H^1(G/\ker(\theta), \mathbb{Z}/q\mathbb{Z}). \tag{4.4}$$

Moreover, the five term exact sequence induced by the quotient $G/\ker(\theta)$ (cf. [**NSW**, Prop. 1.6.7]) induces the exact sequence in cohomology

$$0 \to H^1(G/\ker(\theta), \mathbb{Z}_p(1)) \to H^1(G, \mathbb{Z}_p(1)) \to H^1(\ker(\theta), \mathbb{Z}_p(1))^G \to H^2(G/\ker(\theta), \mathbb{Z}_p(1)) \longrightarrow \cdots$$

which becomes

$$0 \to H^1(G/\ker(\theta), \mathbb{Z}/q\mathbb{Z}) \to H^1(G, \mathbb{Z}_p(1)) \to H^1(\ker(\theta), \mathbb{Z}_p)^G \to 0$$

as $\mathrm{cd}(G/\ker(\theta)) = 1$. Consequently, one has the following.

Proposition 4.4. *Let (G, θ) be a cyclo-oriented pro-p group. Then one has the isomorphism of $\mathbb{Z}_p$-modules*

$$H^1(G, \mathbb{Z}_p(1)) \simeq H^1(G/\ker(\theta), \mathbb{Z}/q\mathbb{Z}) \oplus H(\ker(\theta), \mathbb{Z}_p)^G.$$

Examples 3. (a) Let (G, θ) be a finitely generated θ-abelian pro-p group with $d(G) = d$ and a presentation (2.9), with $\mathcal{I} = 1, \ldots, d-1$, and set $\theta(x_0) = 1 + p$. Then $H^1(G, \mathbb{Z}_p(1))$ is the $\mathbb{Z}_p$-module generated by the classes of the continuous crossed homomorphisms $f_i \colon G \to \mathbb{Z}_p(1)$, with $f_i(x_j) = \delta_{ij}$ for $i, j = 0, \ldots, d-1$. In particular,

$$H^1(G, \mathbb{Z}_p(1)) \simeq \mathbb{F}_p \oplus \mathbb{Z}_p^{d-1}$$

as $\mathbb{Z}_p$-modules, and $\mathrm{ord}(f_0) = p$, as pf_0 is the crossed homomorphism induced by $1 \in \mathbb{Z}_p(1)$. Note that for every $i \geq 1$ one has

$$(x_0.f_i)(x_i) = \theta(x_0) \cdot f\left(x_i^{\theta(x_0^{-1})} x_0^{-1}\right) = \theta(x_0)\theta(x_0)^{-1} f_i(x_i) + 0$$

i.e., the action of G fixes $\mathrm{Hom}(\mathrm{Z}_\theta(G), \mathbb{Z}_p(1))$.

(b) Let G be as above, but equip it with the trivial orientation $\theta' \colon G \to \mathbb{Z}_p^\times$, $\theta' \equiv \mathbf{0}$. Then by Corollary 2.20 (G, θ') is not cyclo-oriented, as the abelianization of $G = \ker(\theta')$ is not torsion-free. Moreover, $H^1(G, \mathbb{Z}_p) \simeq \mathbb{Z}_p$, and such group does not projects onto $H^1(G, \mathbb{F}_p)$ – in particular, it is not possible

to lift the dual of x_i from $H^1(G, \mathbb{F}_p)$ to $\mathrm{Hom}(G, \mathbb{Z}_p)$ for every $i \geq 1$, as one would have $p = f_i(x_i^p) = f_i([x_0, x_i]) = 0$.

2. Free products

Recall from Subsection 2.5.2 the definition of free product in the category of pro-p groups. The class of Bloch-Kato pro-p groups is closed under free pro-p products (cf. [**Qu14**, Theorem 5.2]). We want now to extend such closure to the class of cyclo-oriented pro-p groups.

Then for two oriented pro-p groups (G_1, θ_1) and (G_2, θ_2), the orientations θ_1 and θ_2 induce a new orientation on the free product, i.e., one has the commutative diagram

$$\begin{array}{ccc} G_i & \xrightarrow{\iota_i} & G_1 *_{\hat{p}} G_2 \\ {\scriptstyle \theta_i}\downarrow & \swarrow_{\tilde{\theta}} & \\ \mathbb{Z}_p^\times & & \end{array} \tag{4.5}$$

with $i = 1, 2$. Thus, we may define the free pro-p product for oriented pro-p groups, and one has the following.

THEOREM 4.5. *Let (G_1, θ_1) and (G_2, θ_2) be two cyclo-oriented pro-p groups, and assume further that $\mathrm{im}(\theta_i)$ has non non-trivial torsion for both i. Then the orientation $\tilde{\theta}$ defined as in (4.5) is a cyclotomic orientation for the free product $G_1 *_{\hat{p}} G_2$.*

PROOF. Set $G = G_1 *_{\hat{p}} G_2$. First, as stated above, the group G is a Bloch-Kato pro-p group. Thus, it is enough to show that $H^2(C, \mathbb{Z}_p(1))$ is torsion-free for every C.

By [**NSW**, Theorem 4.1.5], the group $H^1(G, \mathbb{F}_p)$ decomposes as $H^1(G_1, \mathbb{F}_p) \oplus H^1(G_2, \mathbb{F}_p)$. Thus, the inclusions ι_1, ι_2 induce the commutative diagram

$$\begin{array}{ccc} H^1(G, \mathbb{Z}_p(1)) & \longrightarrow & H^1(G_1, \mathbb{F}_p) \oplus H^1(G_2, \mathbb{F}_p) \\ \downarrow{\scriptstyle \mathrm{res}^1_{G,G_i}} & & \downarrow \\ H^1(G_i, \mathbb{Z}_p(1)) & \twoheadrightarrow & H^1(G_i, \mathbb{F}_p) \end{array} \tag{4.6}$$

for $i = 1, 2$, where the lower arrow is surjective by hypothesis and by Lemma 2.11. In particular, the groups G_1 and G_2 are properly embedded in G (cf. [**Qu14**, Fact 4.5]).

Moreover, by (4.5), one has that $\tilde{\theta}|_{G_i} = \theta_i$ for $i = 1, 2$. Thus, the restrictions $H^1(\ker(\tilde{\theta}), \mathbb{Z}_p) \to H^1(\ker(\theta_1), \mathbb{Z}_p)$ are surjective. Also, the monomorphisms $\bar{\iota}_i \colon G_i/\ker(\theta_i) \to G/\ker(\tilde{\theta})$ induce epimorphisms $H^1(G/\ker(\tilde{\theta}), \mathbb{Z}/\tilde{q}\mathbb{Z}) \twoheadrightarrow H^1(G_i/\ker(\theta_i), \mathbb{Z}/q_i\mathbb{Z})$, with $\mathrm{im}(\theta_i) = 1 + q_i\mathbb{Z}_p$ and $\mathrm{im}(\tilde{\theta}) = 1 + \tilde{q}\mathbb{Z}_p$, if the respective orientation is not trivial. Therefore, Proposition 4.4 implies that

$$\mathrm{res}^1_{G,G_i} \colon H^1(G, \mathbb{Z}_p(1)) \longrightarrow H^1(G_i, \mathbb{Z}_p(1)) \tag{4.7}$$

is surjective for $i = 1, 2$. Thus the map $H^1(G, \mathbb{Z}_p(1)) \to H^1(G_i, \mathbb{F}_p)$ is surjective for each i, and therefore also the upper arrow of (4.6) is surjective, and by Lemma 2.11 $H^2(G, \mathbb{Z}_p(1))$ is torsion-free.

Now let C be a closed subgroup of G. Then by the proof of [**Qu14**, Theorem 5.2], one has $C = F *_{\hat{p}} C_1 *_{\hat{p}} C_2$, with F a free pro-p group and for every i,

$$C_i = \coprod_{r \in \mathcal{R}_i} (C \cap G_i^r)$$

where $\mathcal{R}_i$ is a set of representatives of the coset space $C\backslash G/G_i$. [1] Note that every $C \cap G_i^r$ is a subgroup of a group isomorphic to G_i, thus it is again cyclo-oriented. Thus, for every $r' \in \mathcal{R}_i$ one has the commutative diagram

$$\begin{array}{ccc} H^1(C_i, \mathbb{Z}_p(1)) & \longrightarrow & \bigoplus_{\mathcal{R}_i} H^1(C \cap G_i^r, \mathbb{F}_p) \\ \downarrow{\scriptstyle \mathrm{res}_{C_i, C\cap G_i^{r'}}} & & \downarrow \\ H^1(C \cap G_i^{r'}, \mathbb{Z}_p(1)) & \twoheadrightarrow & H^1(C \cap G_i^{r'}, \mathbb{F}_p) \end{array}$$

with the right-hand side vertical arrow is surjective by [**Qu14**, Eq. (5.1)]. Hence, also C_i (and consequently C) is cyclo-oriented. □

2.1. Free-by-Demushkin groups. In the short paper [**Wü85**], T. Würfel proves the following theorem.

THEOREM 4.6. *Let K be a field such that* $\mathrm{char}(K) \neq p$ *and $\mu_{p^\infty} \subseteq K$, and suppose that the maximal pro-p Galois group $G_K(p)$ is finitely generated with one defining relation. Then there exists a normal closed*

[1] This construction is called the free pro-p product of a *sheaf* of pro-p groups, see [**Qu14**, § 5.1] for further details and references.

subgroup N of G which is pro-p free such that the quotient G/N is a Demushkin group, and the inflation map

$$H^2(C/N, \mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\inf^2_{C,N}} H^2(C, \mathbb{Z}/p^n\mathbb{Z}) \tag{4.8}$$

is an isomorphism for every closed subgroup C of G containing N.

He concludes with the following question: is it always true that such $G_K(p)$ is a *free-by-Demushkin group*, i.e., G is decomposable as free pro-p product $G = G/N *_{\hat{p}} F$, with F a finitely generated free pro-p group, if the map (4.8) is an isomorphism?

In [**KZ05**], D. Kochloukova and P. Zalesskiĭ construct a pro-p group as described in Theorem 4.6 such that (4.8) is an isomorphism, but which is not a free-by-Demushkin group. Also they observe that such group is not realizable as maximal pro-p Galois group of any field. Such group is defined by the presentation

$$G = \langle x, y, z \,|z^p[x, y] = 1\rangle\,. \tag{4.9}$$

Let N be the normal subgroup of G generated by z, and set $D = G/N$. Then N is an (infinitely generated) free pro-p group, and D is a 2-generated abelian group. In particular, D is a 2-generated Demushkin group with $q_D = 0$.

We want to show that no orientations $\theta\colon G \to \mathbb{Z}_p^\times$ make (G, θ) a cyclo-oriented pro-p group. Assume for contradiction that G has a cyclotomic orientation θ. Since the abelianization $G/[G, G]$ is isomorphic to $\mathbb{Z}_p^2 \oplus \mathbb{Z}/p\mathbb{Z}$, by Remark 4.3 the orientation θ can not be trivial. Also,

$$1 = \theta\left(z^p[x, y]\right) = \theta\left(z^p\right)\theta([x, y]) = \theta(z)^p,$$

thus $\theta(z) = 1$. Let $f\colon G \to \mathbb{Z}_p(1)$ be the continuous crossed homomorphism representing a lift of the dual of z in $H^1(G, \mathbb{F}_p)$, i.e., $f(z) = 1$ and $f(x), f(y) = 0$ (such f exists by Proposition 4.4 and Fact 4.2, as we are assuming that θ is cyclotomic). Then, using (4.1), one obtains

$$\begin{aligned} f\left(z^p[x, y]\right) &= f(z^p) + \theta(z)f([x, y]) \\ &= pf(z) + (\theta(x) - 1)f(y) - (\theta(y) - 1)f(x) \\ &= p. \end{aligned}$$

But $f(z^p[x, y]) = f(1) = 0$, a contradiction.

3. The cyclotomic fibre product

The other basic operation involved in the ETC is the *cyclotomic fibre product* induced by the arithmetic orientation of a maximal pro-p Galois group.

DEFINITION 15. Let (G, θ) be an oriented pro-p group, and let Z be a pro-p-cyclic group, i.e., $Z \simeq \mathbb{Z}_p$. The **cyclotomic fibre product** $\tilde{G} = G \ltimes_\theta Z$ is the fibre product induced by the split short exact sequence

$$1 \longrightarrow Z \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1 \tag{4.10}$$

with $Z \simeq \mathbb{Z}_p(1)$ as $\mathbb{Z}_p[\![G]\!]$-module. The group $\tilde{G}$ comes equipped with an orientation $\tilde{\theta}\colon \tilde{G} \to \mathbb{Z}_p^\times$ such that $\tilde{\theta}|_G = \theta$ and $\tilde{\theta}|_Z \equiv \mathbf{0}$.

The class of maximal pro-p Galois groups is closed under iterated cyclotomic fibre products, as shown by the following.

PROPOSITION 4.7. *Let K be a field containing a primitive p-th root of unity with cyclotomic orientation $\theta\colon G_K(p) \to \mathbb{Z}_p^\times$, and let A be an abelian free pro-p group, i.e., $A \simeq \mathbb{Z}_p^m$, for some $m \geq 1$. Then the cyclotomic fibre product $G_K(p) \ltimes_\theta A$ is realizable as maximal pro-p Galois group $G_L(p)$ for some field $L \supset K$.*

The above result is well known, and it can be deduced, e.g., from [**En04**, § 1, p. 512]. Also, it is clear that the cyclotomic fibre product "enlarges" the θ-centre of an oriented pro-p group. In particular, one has the following elementary fact.

FACT 4.8. *If (G, θ) is an oriented pro-p group and Z is as above, then for $\tilde{G} = G \ltimes_\theta Z$ one has $\mathrm{Z}_{\tilde{\theta}}(\tilde{G}) = \mathrm{Z}_\theta(G) \times Z$.*

As Theorem 4.13 will show, every θ-centre of oriented Bloch-Kato pro-p groups can be obtained as the result of a cyclotomic fibre products.

3.1. The θ-centre. Let $C \leq G$ be a closed subgroup of a pro-p group G. Then C is called *isolated* if for every element $g \in G$ there exists $m \geq 1$ such that $g^{p^m} \in C$ if, and only if, $g \in C$. It follows that a closed normal subgroup $N \lhd G$ is isolated if, and only if, G/N is torsion free.

PROPOSITION 4.9. *Let (G, θ) be an oriented torsion free Bloch-Kato pro-p group. Then $\mathrm{Z}_\theta(G)$ is an isolated subgroup of G.*

PROOF. Assume first that θ is trivial. Then $\mathrm{Z}_\theta(G)$ is the centre $\mathrm{Z}(G)$. Suppose there exists $x \in G \smallsetminus \mathrm{Z}(G)$ and $m \geq 1$ such that $x^{p^m} \in \mathrm{Z}(G)$. Without loss of generality, we may assume that $m = 1$, i.e., $x^p = z \in \mathrm{Z}(G)$. As G is torsion free, one has $z \neq 1$. Since $x \notin \mathrm{Z}(G)$, there exists an element $g \in G$ such that $gxg^{-1} \neq x$. Set C to be the closed subgroup of G generated by x and g. As C is a Bloch-Kato pro-p group and $z \in \mathrm{Z}(C)$, C must be abelian by Theorem 3.12. Hence $gxg^{-1} = x$, a contradiction, and this yields the claim.

Assume now that $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, and let p be odd. As $\mathrm{Z}_\theta(G)$ is a closed normal subgroup of G, it suffices to show that $G/\mathrm{Z}_\theta(G)$ is torsion free. Since $\mathrm{Z}_\theta(G) = \mathrm{Z}(\ker(\theta))$, the θ-centre of G is isolated in $\ker(\theta)$. Thus $\ker(\theta)/\mathrm{Z}_\theta(G)$ is torsion free. As $G/\ker(\theta) \simeq \mathrm{im}(\theta)$ is torsion free, this yields the claim in this case.

Now let $p = 2$, and put $K = \ker(\theta)$. Since $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$, $\mathrm{Z}(K)$ is isolated in K. Moreover, $\mathrm{Z}(K)$ is a profinite left $\mathbb{Z}_2[\![G/K]\!]$-module which is a torsion free abelian pro-2 group. As

$$\mathrm{Z}_\theta(G) = \{z \in \mathrm{Z}(K) \mid (g - \theta(g)\mathrm{id}_K)z = 0 \text{ for all } g \in G\}\,, \tag{4.11}$$

$\mathrm{Z}_\theta(G)$ is an isolated subgroup of $\mathrm{Z}(K)$. Hence $\mathrm{Z}_\theta(G)$ is an isolated subgroup of K.

Suppose $\mathrm{Z}_\theta(G)$ is not isolated in G. Then there exists $x \in G \smallsetminus \mathrm{Z}_\theta(G)$ such that $x^2 = z \in \mathrm{Z}_\theta(G)$ and $z \neq 1$. As $x \notin \mathrm{Z}_\theta(G)$, the previously mentioned remark shows that $x \notin K$, i.e., $\theta(x) \neq 1$. Hence $z = xzx^{-1} = z^{\theta(x)}$. As every element in $\mathbb{Z}_2^\times$ acts fixed point freely on the closed subgroup generated by z, one concludes that $\theta(x) = 1$, a contradiction, and this yields the claim. □

The following fact is straightforward.

FACT 4.10. *Let $\phi_\bullet \colon A_\bullet \to B_\bullet$ be a morphism of positively graded $\mathbb{F}_p$-algebras such that $\phi_1 \colon A_1 \to B_1$ is surjective, and that $B_\bullet$ is generated by B_1. Then $\phi_n \colon A_n \to B_n$ is surjective for all $n \geq 0$.*

PROPOSITION 4.11. *Let G be a Bloch-Kato pro-p group of finite cohomological dimension, and let Z be a closed normal subgroup of G isomorphic to $\mathbb{Z}_p$ such that G/Z is torsion-free. Then $Z \not\subseteq \Phi(G)$.*

PROOF. Let $d = \mathrm{cd}(G)$. As $Z \simeq \mathbb{Z}_p$, one has $\mathrm{cd}(Z) = 1$ and $H^1(U, \mathbb{F}_p) \simeq \mathbb{F}_p$ for all open subgroups U of Z. Thus, the *virtual* cohomological dimension of G/Z is $\mathrm{vcd}(G/Z) = d - 1$ (cf. [**NSW**, Theorem 3.3.9]). Since G/Z is torsion-free one has $\mathrm{cd}(G/Z) < \infty$, hence [**NSW**, Prop. 3.3.5] implies that $\mathrm{cd}(G/Z) = d - 1$.

Suppose that $Z \subseteq \Phi(G)$. Then $\inf^1_{G,Z}\colon H^1(G/Z, \mathbb{F}_p) \to H^1(G, \mathbb{F}_p)$ is an isomorphism. Since G is a Bloch-Kato pro-p group, Fact 4.10 implies that

$$\inf^n_{G,Z}\colon H^n(G/Z, \mathbb{F}_p) \longrightarrow H^n(G, \mathbb{F}_p) \tag{4.12}$$

is surjective for all $n \geq 0$. In particular, if $(E_r^{s,t}, d_r)$ denotes the Hochschild-Serre spectral sequence associated to the extension of pro-p groups $Z \to G \to G/Z$ with $\mathbb{F}_p$-coefficients, then $E_\infty^{s,t}$ must be concentrated on the bottom row. However, $H^1(Z, \mathbb{F}_p)$ is a trivial G/Z-module isomorphic to $\mathbb{F}_p$, and thus

$$E_2^{d-1,1} = H^{d-1}\left(G/Z, H^1(Z, \mathbb{F}_p)\right) \neq 0. \tag{4.13}$$

For $r \geq 2$ the pages of the spectral sequence $(E_r^{s,t}, d_r)$ are concentrated in the rectangle $\{0, \ldots, d-1\} \times \{0, 1\}$. Thus the place $(d-1, 1)$ can never be hit by a differential non-trivially, and $d_r^{d-1,1} = 0$ for all $r \geq 2$. Hence $E_\infty^{d-1,1} = E_2^{d-1,1} \neq 0$. A contradiction, and this yields the claim. □

Proposition 4.11 has the following consequence.

PROPOSITION 4.12. *Let G be a finitely generated Bloch-Kato pro-p group, and let Z be a closed normal subgroup of G isomorphic to $\mathbb{Z}_p$ such that G/Z is torsion-free. Then there exists a Z-complement in G, i.e., the extension of pro-p groups $1 \to Z \to G \to G/Z \to 1$ splits.*

PROOF. By Proposition 4.11 one has $Z \not\subseteq \Phi(G)$. Hence there exists an open subgroup C_1 of index p such that $C_1 Z = G$ and $Z_1 = C_1 \cap Z = Z^p$. Moreover, Z_1 is a closed normal subgroup in C_1 such that C_1/Z is torsion-free and $Z_1 \simeq \mathbb{Z}_p$. Thus again by Proposition 4.11 one has $Z_1 \not\subseteq \Phi(C_1)$. Repeating this process one finds open subgroup C_m of G of index p^k such that

$$C_m Z = G \quad \text{and} \quad Z_m = C_m \cap Z = Z^{p^m}.$$

Hence $\bigcap_{m \geq 1} C_m$ is a Z-complement in G. □

THEOREM 4.13. *Let (G, θ) be a finitely generated cyclo-oriented pro-p group. Then there exists a closed subgroup $G_\circ$ of G which is a complement for $\mathrm{Z}_\theta(G)$, i.e., the short exact sequence*

$$1 \longrightarrow \mathrm{Z}_\theta(G) \longrightarrow G \longrightarrow G/\mathrm{Z}_\theta(G) \longrightarrow 1 \tag{4.14}$$

splits, with $G_\circ \simeq G/\mathrm{Z}_\theta(G)$, so that $G = G_\circ \ltimes_\theta \mathrm{Z}_\theta(G)$.

We want now to compute the Zassenhaus filtration for a cyclo-oriented pro-p group with non-trivial θ-centre, as we did for θ-abelian groups in Section 3.5.

Let (G,θ) be as in Theorem 4.13, with $G = G_\circ \ltimes_\theta \mathrm{Z}_\theta(G)$ and $\mathrm{Z}_\theta(G)$ non-trivial. Also let p^k be the p-power such that $\mathrm{im}(\theta) = 1 + p^k\mathbb{Z}_p$. Then it is easy to see that for each $i \geq 1$ one has

$$\gamma_i(G) = \gamma_i(G_\circ) \ltimes_{\theta_{\gamma_i}} \mathrm{Z}_\theta(G)^{p^{k(i-1)}},$$

with $\theta_{\gamma_i} = \theta|_{\gamma_i(G_\circ)}$. Therefore, an argument as in (3.19) shows that

$$D_n(G) = D_n(G_\circ) \ltimes_{\theta_n} \mathrm{Z}_\theta(G)^{p^\ell} \quad \text{for } p^{\ell-1} < n \leq p^\ell, \tag{4.15}$$

with $\theta_n = \theta|_{D_n(G_\circ)}$. Consequently, the quotients induced by the Zassenhaus filtration are

$$L_i(G) \simeq \begin{cases} L_i(G_\circ) \oplus \mathrm{Z}_\theta(G)/\mathrm{Z}_\theta(G)^p & \text{for } i \text{ a } p^{th}\text{-power} \\ L_i(G_\circ) & \text{otherwise} \end{cases} \tag{4.16}$$

as vector spaces over $\mathbb{F}_p$.

Proposition 4.14. *Let (G,θ) be a cyclo-oriented pro-p group, and assume that $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ for $p = 2$. Then the restricted Lie algebra $L_\bullet(G)$ induced by the Zassenhaus filtration decomposes as*

$$L_\bullet(G) = L_\bullet(G_\circ) \oplus A_\bullet$$

with $G_\circ \leq G$ as in Theorem 4.13, and $A_\bullet$ an abelian restricted Lie algebra such that $\dim(A_1) = d(\mathrm{Z}_\theta(G)) = d$. Also, one has

$$\mathrm{gr}_\bullet(G) \simeq \mathcal{U}_p(L_\bullet(G)) \simeq \mathrm{gr}_\bullet(G_\circ) \otimes^1 \mathbb{F}_p[Z_1,\ldots,Z_d], \tag{4.17}$$

where $\otimes^1$ denotes the symmetric tensor product (defined in Subsection 2.1.1), and the grading in the polynomial part is induced by the degrees of the monomials.

Proof. The first statement follows from (4.16). As for the second one, since $(L_\bullet(G_\circ), A_\bullet) = 0$, one has that $\psi_L(L_\bullet(G_\circ))$ and $\psi_L(A_\bullet)$ commute in $\mathcal{U}_p(L_\bullet(G))$, and (4.17) holds. □

3.2. Cohomology of cyclotomic fibre products. The next result is the cohomological "translation" of Theorem 4.13, namely, it shows how the presence of the θ-centre decomposes the $\mathbb{F}_p$-cohomology ring.

THEOREM 4.15. *Let (G,θ) be a finitely generated Bloch-Kato pro-p group with orientation such that $\mathrm{Z}_\theta(G)$ is non-trivial, and let $G_\circ$ be the complement of the θ-centre. Then one has the isomorphism of $\mathbb{F}_p$-vector spaces*

$$H^2(G,\mathbb{F}_p) \simeq H^2(G_\circ,\mathbb{F}_p) \oplus (V \wedge W) \oplus (W \wedge W), \tag{4.18}$$

with $V = H^1(G_\circ,\mathbb{F}_p)$ and $W = H^1(\mathrm{Z}_\theta(G),\mathbb{F}_p)$.

PROOF. We shall prove the result by induction on the minimal number of generators of $\mathrm{Z}_\theta(G)$.

Assume first that $\mathrm{Z}_\theta(G) \simeq \mathbb{Z}_p$, and let $z \in \mathrm{Z}_\theta(G)$ be a generator. Moreover, let $\psi \in W$ be the dual of z, and pick a $\mathbb{F}_p$-basis $\{\chi_i, i \in \mathcal{I}\}$ of V, so that $\{\psi, \chi_i\}$ is a basis for $H^1(G,\mathbb{F}_p)$.

Let $\chi \in V$ be any non-trivial $\mathbb{F}_p$-linear combination of the χ_i's, and let $x \in G_\circ \smallsetminus \Phi(G)$ be such that χ is dual to x. Set $C \leq G$ be the closed subgroup generated by x and z. By construction, C is a 2-generated $\theta|_C$-abelian pro-p group, and by Theorem 3.12 the cohomology ring $H^\bullet(C,\mathbb{F}_p)$ is the exterior $\mathbb{F}_p$-algebra generated by $\mathrm{res}^1_{G,C}(\chi)$ and $\mathrm{res}^1_{G,C}(\psi)$. In particular, one has

$$\mathrm{res}^2_{G,C}(\chi \cup \psi) = \mathrm{res}^1_{G,C}(\chi) \cup \mathrm{res}^1_{G,C}(\psi) \neq 0,$$

hence $\chi \cup \psi \neq 0$ in $H^2(G,\mathbb{F}_p)$. Therefore, all the cup products $\chi_i \cup \psi$, with $i \in \mathcal{I}$, are $\mathbb{F}_p$-linearly independent, and $V \wedge W$ is a subspace of $H^2(G,\mathbb{F}_p)$.

Moreover, the short exact sequence of pro-p groups (4.14) induces the five term exact sequence

(4.19)

$$\begin{array}{l} 0 \longrightarrow H^1(G_\circ,\mathbb{F}_p) \xrightarrow{\inf^1_{G,G_\circ}} V \oplus W \xrightarrow{\mathrm{res}^1_{G,\mathrm{Z}_\theta(G)}} W^G \xrightarrow{\mathrm{tg}_{G,\mathrm{Z}_\theta(G)}} \\ \qquad\qquad H^2(G_\circ,\mathbb{F}_p) \xrightarrow{\inf^2_{G,G_\circ}} H^2(G,\mathbb{F}_p). \end{array}$$

Since $W^G = H^1(\mathrm{Z}_\theta(G), \mathbb{F}_p)$, one has that $\mathrm{res}^1_{G,\mathrm{Z}_\theta(G)}$ is surjective, for the θ-centre is properly embedded in G [**Qu14**, Fact 4.5]. Thus, the transgression map $\mathrm{tg}_{G,\mathrm{Z}_\theta(G)}$ is trivial, and $\inf^2_{G,G_\circ}$ is injective. In particular, the image of $\inf^2_{G,G_\circ}$ is isomorphic to $H^2(G_\circ, \mathbb{F}_p)$.

Since the intersection between $V \wedge W$ and $\inf^2_{G,G_\circ}(H^2(G_\circ, \mathbb{F}_p))$ is trivial, one has

$$\begin{aligned} r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) &\geq \dim_{\mathbb{F}_p}(V \wedge W) + \dim_{\mathbb{F}_p} H^2(G_\circ, \mathbb{F}_p) \\ &= \dim_{\mathbb{F}_p}(V) + r(G_\circ), \end{aligned}$$

by Definition 5. By hypothesis, the minimal number of relations of G is exactly $r(G) = r(G_\circ) + \dim_{\mathbb{F}_p}(V)$, thus $H^2(G, \mathbb{F}_p)$ is generated by $\inf^2_{G,G_\circ} H^2(G_\circ, \mathbb{F}_p)$ and $V \wedge W$.

Assume now that $d(\mathrm{Z}_\theta(G)) > 1$, and let Z_1, Z_2 be subgroups of the θ-centre such that $Z_2 \simeq \mathbb{Z}_p$ and $\mathrm{Z}_\theta(G) = Z_1 \times Z_2$. Moreover, set $W_i = H^1(Z_i, \mathbb{F}_p)$, with $i = 1, 2$, and $\tilde{G}_\circ = G_\circ \ltimes_\theta Z_1$. Thus, $H^1(\tilde{G}_\circ, \mathbb{F}_p) = V \oplus W_1$, and by induction one has

$$H^2(\tilde{G}_\circ, \mathbb{F}_p) \simeq H^2(G_\circ, \mathbb{F}_p) \oplus (V \wedge W_1) \oplus (W_1 \wedge W_1).$$

Also, the above argument shows that

$$H^2(G, \mathbb{F}_p) \simeq H^2(\tilde{G}_\circ, \mathbb{F}_p) \oplus ((V \oplus W_1) \wedge W_2),$$

and the claim follows. □

Remark 4.16. By Theorem 4.15, the $\mathbb{F}_p$-cohomology ring of the cyclo-oriented pro-p group is the skew-commutative tensor product

$$H^\bullet(G, \mathbb{F}_p) = H^\bullet(G_\circ, \mathbb{F}_p) \otimes^{-1} \left(\bigwedge_{n \geq 0} W \right),$$

which can be considered also as a *graded tensor product*[2]. In particular, the $\mathbb{F}_p$-cohomology ring of a Bloch-Kato pro-p group can be considered

[2]Let $A_\bullet$ and $B_\bullet$ be two (non-negatively) graded rings. The *tensor product* in the category of graded rings is defined by

$$A_\bullet \otimes_{\mathrm{gr}} B_\bullet = \coprod_{k \geq 0} \left(\bigoplus_{i+j=k} A_i \otimes B_j \right),$$

with the multiplication law $(a \otimes b)(a' \otimes b') = (-1)^{i'j} aa' \otimes bb'$ for $a \in A_i$, $a' \in A_{i'}$, $b \in B_j$ and $b' \in B_{j'}$ (cf. [**Ef06**, § 23.2]).

as a *κ-structure* (cf. [**Ef06**, Ch. 23]), and $H^\bullet(G, \mathbb{F}_p)$ is the *extension* of κ-structures $H^\bullet(G_\circ, \mathbb{F}_p)[W]$ [**Ef06**, p. 211].

EXAMPLE 1. Let $G_\circ$ be a Demushkin group with cyclotomic orientation $\theta\colon G_\circ \to \mathbb{Z}_p^\times$ such that $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, and let $\{\chi_1, \ldots, \chi_d\}$ be a suitable basis for $H^1(G_\circ, \mathbb{F}_p)$, with $d = d(G_\circ)$. Also, let Z be isomorphic to $\mathbb{Z}_p(1)$ as $\mathbb{Z}_p[\![G]\!]$-modules, and let ψ be a generator of $H^1(Z, \mathbb{F}_p)$. Then for $G = G_\circ \ltimes_\theta Z$, the $\mathbb{F}_p$-vector space $H^2(G, \mathbb{F}_p)$ is generated by the elements

$$\chi_1 \cup \chi_2 = \ldots = \chi_{d-1} \cup \chi_d \quad \text{and} \quad \chi_i \cup \psi \text{ for every } i,$$

and $\dim(H^2(G, \mathbb{F}_p)) = d + 1$.

Theorem 4.15 shows that the class of Bloch-Kato pro-p groups is closed under cyclotomic fibre products. We want to extend the closure to the class of cyclo-oriented pro-p groups.

THEOREM 4.17. *Let (G, θ) be a finitely generated cyclo-oriented pro-p group, and let $\tilde{G} = G \ltimes_\theta Z$ be the cyclotomic fibre product with Z and $\tilde{\theta}$ as in Definition 15. Then $(\tilde{G}, \tilde{\theta})$ is again a cyclo-oriented pro-p group.*

PROOF. By Theorem 4.15, $\tilde{G}$ is a Bloch-Kato pro-p group, so it remains to show that $H^2(\tilde{G}, \mathbb{Z}_p(1))$ is a torsion-free $\mathbb{Z}_p$-module. Thus, by Lemma 2.11, it is enough tho show that the morphism

$$H^1(\tilde{G}, \mathbb{Z}_p(1)) \to H^1(\tilde{G}, \mathbb{F}_p) \tag{4.20}$$

induced by (2.13) is surjective.

Let z be a generator of Z. Then $H^1(Z, \mathbb{Z}_p(1))$ is the $\mathbb{Z}_p$-module generated by the morphism $f\colon Z \to \mathbb{Z}_p(1)$ defined by $f(z) = 1$. Note that by (4.3) $\tilde{G}$ fixes f, as

$$(g.f)(z) = \theta(g) \cdot f\left(z^{\theta(g^{-1})} g^{-1}\right) = \theta(g)\theta(g)^{-1} \cdot 1 + 0 = 1$$

for every $g \in G$. Thus, $H^1(Z, \mathbb{Z}_p(1))^G = H^1(Z, \mathbb{Z}_p(1))$. In particular, this implies that the restriction map

$$\mathrm{res}^1_{\tilde{G},Z}\colon H^1(\tilde{G}, \mathbb{Z}_p(1)) \longrightarrow H^1(Z, \mathbb{Z}_p(1))$$

is surjective.

Therefore, by the five term exact sequence induced by (4.10) with coefficients in $\mathbb{Z}_p(1)$, one has the commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & H^1(G,\mathbb{Z}_p(1)) & \xrightarrow{\inf^1_{\tilde{G},Z}} & H^1(\tilde{G},\mathbb{Z}_p(1)) & \xrightarrow{\mathrm{res}^1_{\tilde{G},Z}} & H^1(Z,\mathbb{Z}_p(1)) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & H^1(G,\mathbb{F}_p) & \to & H^1(G,\mathbb{F}_p)\oplus H^1(Z,\mathbb{F}_p) & \to & H^1(Z,\mathbb{F}_p) & \to & 0 \end{array}$$

where the left-hand side vertical arrow is surjective by hypothesis, and the right-hand side one is surjective since $f \bmod p$ generates $H^1(Z,\mathbb{F}_p)$. Hence, by the snake lemma, also (4.20) is surjective.

Moreover, every closed subgroup $\tilde{C}$ of $\tilde{G}$ decomposes as cyclotomic fibre product $\tilde{C} = C \ltimes_{\theta|_C} Z'$, with C a subgroup of G and Z' a subgroup of Z, and by the above argument $H^2(\tilde{C},\mathbb{Z}_p(1))$ is torsion-free. □

3.3. Arithmetic. Let K be a field. Recall that a **valuation** of K is a group homomorphism v from $K^\times$ into an ordered abelian group $(\Gamma,\leq)$ such that for every $\alpha,\beta \in K^\times$ with $x \neq -y$, one has

$$v(x+y) \geq \min\{v(x), v(y)\}.$$

The *rank* of the valuation v is the rank of the abelian group $\mathrm{im}(v) \leq \Gamma$.

A valuation $v\colon K^\times \to \Gamma$ is said to be **p-Henselian** if it extends uniquely to the p-closure $K(p)$, i.e., there exists a unique valuation $w\colon K(p)^\times \to \Gamma$ such that $w|_{K^\times} = v$. (For more details on valuation theory see [**Ef06**].)

Assume now that K has characteristic prime to p. We are to show the relation between the structure of the maximal pro-p Galois group $G_K(p)$ of K (and of its $\mathbb{F}_p$-cohomology ring) and the existence of certain valuations of K.

PROPOSITION 4.18. *Let (G,θ) be a cyclo-oriented pro-p group, and assume that $\mathrm{im}(\theta)$ is either pro-p-cyclic or trivial. Then the θ-centre $\mathrm{Z}_\theta(G)$ is the maximal normal abelian subgroup of G*

PROOF. If G is abelian, then θ is trivial, and $\mathrm{Z}_\theta(G) = G$. Thus, assume that G is not abelian, and let N be the maximal normal abelian subgroup of G. Note that $N \leq \ker(\theta)$, as $(N,\theta|_N)$ is cyclo-oriented.

Fix an element $z \in N$, and choose any $x \in G$. Let $C \leq G$ be the closed subgroup generated by x and z: then either $C \simeq \mathbb{Z}_p$ or $d(C) = 2$.

In the former case, x and z commute, and moreover $C \leq \ker(\theta)$: thus, one has

$$ {}^{x}z = z = z^{\theta(x)}. \tag{4.21}$$

In the latter case, Theorem 3.12 implies that either C is a 2-generated free pro-p group, or C is θ'-abelian, for some orientation $\theta' \colon C \to \mathbb{Z}_p^\times$. Since N is normal, the commutator subgroup $[C, C]$ of C is contained in N, hence $[C, C]$ is abelian, and C is θ'-abelian. Since $\theta|_C$ is a cyclotomic orientation for C, one has $\theta' = \theta|_C$, and $z \in \mathrm{Z}_{\theta|_C}(C)$: thus, one has

$$ {}^{x}z = z^{\theta|_C(x)} = z^{\theta(x)}. \tag{4.22}$$

Thus for every $z \in N$ and $x \in G$ one has (4.21) or (4.22). Therefore, $N \leq Z_\theta(G)$, and thus they coincide, as the θ-centre is abelian. □

The following result shows the arithmetic meaning of the θ-centre of the maximal pro-p Galois group of a field, with θ the arithmetic orientation.

THEOREM 4.19. *Let K be a field of characteristic* $\mathrm{char}K \neq p$ *containing a primitive p-th root of unity, and also $\sqrt{-1}$ if $p = 2$. Let $\theta \colon G_K(p) \to \mathbb{Z}_p^\times$ be the cyclotomic orientation, and assume that the maximal pro-p Galois group $G_K(p)$ is finitely generated. Then the following are equivalent:*

(i) *the θ-centre $\mathrm{Z}_\theta(G)$ is non-trivial;*
(ii) *there exist two $\mathbb{F}_p$-vector subspaces $V, W < H^1(G_K(p), \mathbb{F}_p)$ such that*

$$H^1\left(G_K(p), \mathbb{F}_p\right) = V \oplus W, \quad \textit{and}$$
$$H^2\left(G_K(p), \mathbb{F}_p\right) = \wedge_2(\cup)(V) \oplus (V \wedge W) \oplus (W \wedge W),$$

with $\wedge_2(\cup)$ as in (3.2).
(iii) *there exists a non-trivial p-Henselian valuation $v \colon K^\times \to \Gamma$ with residue characteristic different to p.*

Moreover, if the conditions above hold, then

$$d\left(\mathrm{Z}_\theta(G_K(p))\right) = \dim_{\mathbb{F}_p}(W) = \mathrm{rk}(v).$$

PROOF. Assume first that $d(G_K(p)) = 1$ and $K \supseteq \mu_{p^\infty}$. Then $G_K(p)$ is isomorphic to $\mathbb{Z}_p$, and the p-closure of K is $K(p) = K(\mu_{p^\infty})$. Thus, K has non non-trivial valuations. Moreover, θ is not trivial and $\mathrm{Z}_\theta(G_K(p))$ is trivial. Therefore we may assume that $d(G_K(p)) \geq 2$.

We have the second statement as a consequence of Theorem 4.15, so that the implication (i) $\Rightarrow$ (ii) is established.

If condition (ii) hold then [**HJ95**, Theorem 2.11] implies that the field K is *V-rigid* (cf. [**HJ95**, Definition 2.1]), and there exists a non-trivial p-Henselian (and non-p-adic) valuation v of K of rank $\mathrm{rk}(v) = \dim(W)$.

Thus by [**Ef06**, Corollary 26.6.2], there exists a valuation $v\colon K^\times \to \Gamma$ which is $(K^\times)^p$-compatible, and therefore it is also p-Henselian. Moreover, one has that $|v(K^\times) : v(K^\times)^p| \geq |V|$, hence the rank of v is at least $\dim_{\mathbb{F}_p} H^1(\mathrm{Z}_\theta, \mathbb{F}_p) = \mathrm{rk}(\mathrm{Z}_\theta(G))$. This establishes the implication from (ii) to (iii).

The equivalence between (i) and (iii) follows from Proposition 4.18 and from [**EK98**, Theorem 3.1] in the case $p \neq 2$, and from [**EN94**, § 4] in the case $p = 2$. In particular, the equality $\mathrm{rk}(v) = d(\mathrm{Z}_\theta(G))$ follows by induction. □

Remark 4.20. Unfortunately the paper [**HJ95**] contains some essential mistakes due to wrong interpretation of the Bloch-Kato conjecture. These mistakes affected also some subsequent articles on the relations between Galois cohomology and Henselian valuations, written in the late '90s. In the '00s, I. Efrat become aware of such mistakes, and in fact his later results on valuations – in particular, the ones contained in his book [**Ef06**] – are correct.

Recall that in Remark 4.16 we stated condition (ii) in terms of *extensions of κ-structures*. Thus, one may prove the implication (ii) $\Rightarrow$ (iii), i.e., the existence of non-trivial p-Henselian valuations, also using [**Ef06**, § 26.5]. In particular, [**Ef06**, Corollary 26.6.2] says that there exists a valuation v of K which is $(K^\times)^p$-compatible (i.e., $v(\alpha) \geq 1$ for every p-power α), and therefore v is also p-Henselian. Therefore, the proof of Theorem 4.19 is not invalidated by the mistakes contained in [**HJ95**].

4. Relations

We want now to analise more in depth the relations of a minimal presentation (4.2) for a finitely generated cyclo-oriented pro-p group (G, θ), with orientation θ such that either $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$ or $\theta \equiv \mathbf{1}$. So far we have studied explicitly the group-structure of two types of cyclo-oriented pro-p groups with non-trivial relations:

(a) θ-abelian groups, and more in general cyclo-oriented groups (G, θ) with non-trivial θ-centre;
(b) Demushkin groups, with an orientation as in Theorem 2.22.

In the former case, we may find a minimal system of generators $\{x_1, \dots, x_{d-c}, z_1, \dots, z_c\}$ with the x_i's which generate $G_\circ$ and the z_i's which generate $\mathrm{Z}_\theta(G)$, such that $\theta(x_1) = 1 + q$, with $q = p^k$ for some $k = \mathbb{N} \cup \{\infty\}$, and $\theta(x_i) = 1$ for $i \geq 2$. Thus one has the relations

$$z_i^{-q}[x_1, z_i] = 1 \quad \text{and} \quad [x_j, z_i] = 1, \tag{4.23}$$

with $i = 1, \dots, c$ and $j = 2, \dots, d - c$. In fact, the relations (4.23) are the "commutator translation" of the cyclotomic action induced by θ on the θ-centre.

In the latter case, by Theorem 2.22 we may find a minimal system of generators $\{x_1, \dots, x_d\} \subset G$, with $\theta(x_2) = 1 - q_G$, such that one has the relation

$$x_1^{-q_G}[x_1, x_2] \cdots [x_{d-1}, x_d] = 1,$$

thus

$$x_1^{q_G}[x_2, x_1] \equiv 1 \mod [\ker(\theta), \ker(\theta)]. \tag{4.24}$$

Namely, we have the cyclotomic action, as in (4.23), but "perturbed" by the commutator subgroup of the kernel of the orientation θ.

Recall that θ-abelian pro-p groups and Demushkin groups (together with free pro-p groups) are the two "bounds" for cyclo-oriented pro-p groups. Therefore, it is natural to ask the following question: for a finitely generated cyclo-oriented pro-p group (G, θ), with $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, do (4.23) and (4.24) represent "models" for the behavior of the relations of G, such that they are induced by the cyclotomic action modulo $[\ker(\theta), \ker(\theta)]$? Namely...

Question 1. *Given a finitely generated cyclo-oriented pro-p group (G, θ), with $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, is it possible to find a minimal presentation* (4.2) *with generating system $\{x_1, \dots, x_{d(G)}\}$ and defining relations $r_1, \dots, r_{r(G)}$ such that $x_i \in \ker(\theta)$ for $i = 2, \dots, d(G)$ and either $r_j \in [F, F]$ or*

$$r_j \equiv x_i^{1-\theta(x_1)}[x_1, x_i] \mod [\ker(\theta), \ker(\theta)] \tag{4.25}$$

with $i \in \{2, \dots, d(G)\}$?

We shall call a relation as in (4.25) a relation of **cyclotomic type**. For a cyclo-oriented pro-p group with trivial orientation, the answer to Question 1 is clearly positive, as Corollary 2.20 and Remark 4.3 imply the following.

PROPOSITION 4.21. *Let (G,θ) be a finitely generated pro-p group with trivial cyclotomic orientation $\theta \equiv \mathbf{0}$, and let (4.2) be a minimal presentation for G. Then $R \leq [F,F]$.*

The following collects some useful facts.

FACT 4.22. *Let (G,θ) a finitely generated cyclo oriented pro-p group, and let G^{ab} be the abelianization $G/[G,G]$.*

(i) *There are positive integers f, t, k_j, with $f+t = d(G) = d$, such that*

$$G^{\mathrm{ab}} \simeq \mathbb{Z}_p^f \oplus \left(\bigoplus_{j=1} \mathbb{Z}/p^{k_j}\mathbb{Z} \right).$$

(ii) *One may find a minimal system of generators $\{x_1, \dots, x_d\}$ such that for $1 \leq i \leq t$ the images $\bar{x}_i$ in G^{ab} generate the torsion-free part, and for $t+1 \leq i \leq d$ the $\bar{x}_i$'s generate the torsion part (in particular the order of $\bar{x}_i$ is p^{k_j} for $j = i - f$).*

(iii) *Also, one has $\theta(x_i) = 1$ for $i > f$, and one may choose the x_i's for $i \leq f$ such that $\theta(x_i) = 1$ also for $2 \leq i \leq f$.*

4.1. The module N^{ab}. For a finitely generated pro-p group G with cyclotomic orientation θ such that $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, let N be the kernel of θ, and set

$$N^{\mathrm{ab}} = \frac{N}{[N,N]},$$

i.e., N^{ab} is the abelianization of the $\ker(\theta)$. Recall that by Corollary 2.20, N^{ab} is a torsion-free abelian pro-p group.

The action induced by the conjugation – i.e.,

$$x.\bar{y} = \overline{{}^x y} \equiv xyx^{-1} \mod [N,N],$$

with $x \in G$ and $y \in N$ – makes N a continuous $\mathbb{Z}_p[\![G]\!]$-module, and a trivial $\mathbb{Z}_p[\![N]\!]$-module. Hence, set $\Gamma = G/N$, and let k be such that $\mathrm{im}(\theta) = 1 + q\mathbb{Z}_p$, with $q = p^k$. Then, Γ is isomorphic to $\mathbb{Z}_p$ as pro p-group, and it may be identified with $1+q\mathbb{Z}_p = \mathrm{im}(\theta)$. In particular, the complete group ring $\mathbb{Z}_p[\![\Gamma]\!]$ is the *Iwasawa algebra*, and N^{ab} becomes a $\mathbb{Z}_p[\![\Gamma]\!]$-module, i.e., an **Iwasawa module** (cf. [**NSW**, 5.3.6]).

Let g be an element of G such that $\theta(g) = 1 + q$. Without loss of generality, we may assume that $g = x_1$, with x_1 as in Fact 4.22. Let γ be te image of x_1 in Γ. Then γ is a generator of Γ. Also, the Iwasawa algebra $\mathbb{Z}_p[\![\Gamma]\!]$ is isomorphic to the power series ring $\mathbb{Z}_p[\![X]\!]$, via the

morphism[3] given by $\gamma \mapsto 1+X$, so that $X \mapsto \gamma - 1$, and N^{ab} becomes a $\mathbb{Z}_p[\![X]\!]$-module via

$$\begin{aligned} X.\bar{y} = (\gamma-1).\bar{y} = x_1.\bar{y} - \bar{y} &= \overline{{}^{x_1}y \cdot y^{-1}} \\ &\equiv [x_1, y] \mod [N,N] \end{aligned} \tag{4.26}$$

for every $y \in N$. Hence, one has

$$\begin{aligned} \lambda X^m.\bar{y} &\equiv [x_{1,m}\, y]^{\lambda} \mod [N,N] \\ &\equiv \left[x_{1,m}\, y^{\lambda}\right] \mod [N,N] \end{aligned} \tag{4.27}$$

with $\lambda \in \mathbb{Z}_p$, $m \geq 1$ and $[x_{i,m}\, y] = [x_1[x_1 \dots [x_1, y]]]$.

Recall that a polynomial $\wp \in \mathbb{Z}_p[\![X]\!]$ is said to be a *Weierstraß polynomial* if

$$\wp = X^m + \alpha_{m-1}X^{m-1} + \ldots + \alpha_2 X^2 + \alpha_1 X + \alpha_0,$$

with $\alpha_0, \dots, \alpha_{m-1} \in p\mathbb{Z}_p$ (cf. [**NSW**, Definition 5.3.2]). Thus, one has the following.

Proposition 4.23. *For a finitely generated cyclo-oriented pro-p group G with $N = \ker(\theta)$, there are positive integers f, t and irreducible Weierstraß polynomials $\wp_j$, with $j = 1, \dots, t$, such that the $\mathbb{Z}_p[\![\Gamma]\!]$-module N^{ab} is isomorphic to a submodule of finite index of the $\mathbb{Z}_p[\![X]\!]$-module*

$$M = \mathbb{Z}_p[\![X]\!]^f \oplus \left(\bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[\![X]\!]}{\wp_j^{m_j}} \right), \tag{4.28}$$

with $m_j \geq 1$.

Proof. Since N^{ab} is an Iwasawa module, the Structure Theorem for Iwasawa modules implies that there exist positive integers a_h, with $h = 1, \dots, s$, together with suitable $f, t, s \geq 0$ and $\wp_j$'s such that one has a morphism of $\mathbb{Z}_p[\![X]\!]$-modules

$$\phi \colon N^{\mathrm{ab}} \longrightarrow \mathbb{Z}_p[\![X]\!]^f \oplus \left(\bigoplus_{h=1}^{s} \frac{\mathbb{Z}_p[\![X]\!]}{p^{a_h}} \right) \oplus \left(\bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[\![X]\!]}{\wp_j^{m_j}} \right),$$

and ϕ has finite kernel and finite cokernel (cf. [**NSW**, Theorem 5.3.8]).

Since N^{ab} is a torsion-free $\mathbb{Z}_p$-module, the kernel of ϕ is trivial, and the p-torsion part (the quotients $\mathbb{Z}_p[\![X]\!]/p^{a_h}$) disappears. Thus,

[3]Note that this is the same map as in Remark 1.17

one has that $\phi\colon N^{\mathrm{ab}} \to M$ is injective, and N^{ab} is isomorphic to a $\mathbb{Z}_p[\![X]\!]$-submodule of M of finite index. $\square$

For every $j = 1, \ldots, t$, set

$$\wp_j^{m_j} = X^{h_j} + \alpha_{(j,h_j-1)}X^{h_j-1} + \ldots + \alpha_{(j,1)}X + \alpha_{j,0}.$$

Therefore, for every $\bar{y} \in N^{\mathrm{ab}}$, one has $\wp_j^{m_j}.\bar{y} = 0$, and thus by (4.27)

$$r = [x_{1,h_j}\, y] \cdot [x_{1,h_j-1}\, y]^{\alpha(j,h_j-1)} \cdots [x_1, y]^{\alpha_{(j,1)}} y^{\alpha_{j,0}} \in [N, N]. \tag{4.29}$$

Now let $y \in N$ belong to a generating system of G (e.g., $y = x_i$ for an $i \geq 2$, with x_i as in Fact 4.22), and let $f_y\colon G \to \mathbb{Z}_p(1)$ be the continuous crossed homomorphism such that $f_y(y) = 1$ and $f_y(x) = 0$ for any other generator of G (in particular, $f_y(x_1) = 0$). Such a crossed homomorphism exists by Fact 4.2. Since $f_y|_N$ is a group homomorphism and $f_y|_{[N,N]} \equiv \mathbf{0}$, by (4.1) one has

$$f_y\left([x_{1,m}\, y]^{\alpha}\right) = \alpha(\theta(x_1) - 1) f_y([x_{1,m-1}\, y]) = \ldots = \alpha q^m$$

(notice that $[x_{1,m}\, y] \in N$ for any $m \geq 0$). Hence, by (4.29),

$$f_y(r) = \alpha_{j,0} + \alpha_{(j,1)}q + \ldots + \alpha_{(j,h_j-1)}q^{h_j-1} + q^{h_j} = \wp_j^{m_j}(q). \tag{4.30}$$

On the other hand, one has $f_y(r) = 0$, as $r \in [N, N]$, so that $\wp_j^{m_j}(q) = 0$, and $X - q$ divides $\wp_j$. Since $\wp_j$ is an irreducible polynomial, it follows that in fact $\wp_j = X - q$ for every $j = 1, \ldots, t$. In particular, one has the monomorphism of $\mathbb{Z}_p[\![X]\!]$-modules

$$\phi\colon N^{\mathrm{ab}} \longrightarrow M = \mathbb{Z}_p[\![X]\!]^f \oplus \left(\bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[\![X]\!]}{(X-q)^{m_j}} \right), \tag{4.31}$$

with $m_j \geq 1$.

Proposition 4.24. *Let (G, θ) be a finitely generated pro-p group with cyclotomic orientation θ such that $\mathrm{im}(\theta) \simeq \mathbb{Z}_p$, and with minimal presentation (4.2). Let $x_1, y \in G$ be as above, and let $r \in R$ be a relation induced by the polynomial $(X-q)^m$, with $m \geq 1$, i.e.,*

$$r \equiv y^{(-q)^m}[x_1, y]^{m(-q)^{m-1}} \cdots [x_{1,m-1}\, y]^{-mq}[x_{1,m}\, y] \mod [N, N]. \tag{4.32}$$

Then r can occur as defining relation only if $m = 1$.

PROOF. Consider the short exact sequence

$$1 \longrightarrow C \longrightarrow G \longrightarrow \bar{G} \longrightarrow 1 \ , \tag{4.33}$$

where C is the closed normal subgroup of G generated by all the generators x_i's with $i \neq 1$ and $x_i \neq y$, and $\bar{G} = G/C$. Then $\bar{G}$ has a minimal presentation $1 \to \bar{R} \to \bar{F} \to \bar{G} \to 1$, where $d(\bar{F}) = d(\bar{G}) = 2$, and $\bar{R}$ is generated as normal subgroup of $\bar{F}$ by

$$\bar{r} = y^{(-q)^m}[x_1, y]^{m(-q)^{m-1}} \cdots [x_{1,m-1}\, y]^{-mq}[x_{1,m}\, y],$$

where we consider x_1 and y as elements of $\bar{G}$ and of $\bar{F}$ as well with an abuse of notation. Then (4.33) induces the five term exact sequence (4.34)

$$\begin{array}{l} 0 \longrightarrow H^1(\bar{G}, \mathbb{F}_p) \xrightarrow{\inf^1_{G,\bar{G}}} H^1(G, \mathbb{F}_p) \xrightarrow{\mathrm{res}^1_{G,C}} H^1(C, \mathbb{F}_p)^G \xrightarrow{\mathrm{tg}_{G,C}} \\ \qquad\qquad H^2(\bar{G}, \mathbb{F}_p) \xrightarrow{\inf^2_{G,\bar{G}}} H^2(G, \mathbb{F}_p). \end{array}$$

By construction of C, the map $\mathrm{res}^1_{G,C}$ is surjective, so that the transgression map is trivial, and $\inf^2_{G,\bar{G}}$ is injective. In particular, one has the commutative diagram

$$\begin{array}{ccc} H^1(\bar{G}, \mathbb{F}_p) \times H^1(\bar{G}, \mathbb{F}_p) & \xrightarrow{\cup} & H^2(\bar{G}, \mathbb{F}_p) \\ \downarrow \inf^1_{G,\bar{G}} \quad \downarrow \inf^1_{G,\bar{G}} & & \downarrow \inf^2_{G,\bar{G}} \\ H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) & \xrightarrow{\cup} & H^2(G, \mathbb{F}_p) \end{array} \tag{4.35}$$

where the vertical arrows are monomorphisms by (4.34).

Assume now that $m > 1$. In this case the relation $\bar{r}$ lies in $\lambda_3(\bar{F})$, thus by [**CEM**, Corollary 9.2] the cohomology ring $H^\bullet(\bar{G}, \mathbb{F}_p)$ is not a quadratic $\mathbb{F}_p$-algebra. In particular, let $\chi, \psi \in H^1(\bar{G}, \mathbb{F}_p)$ be the duals of x_1 and y. Since $\bar{r} \in \lambda_3(\bar{F})$ and $r(\bar{G}) = 1$, [**NSW**, Propositions 3.9.12-13] imply that $\chi \cup \psi = 0$. On the other hand, one has

$$H^2(\bar{G}, \mathbb{F}_p) \simeq \mathbb{F}_p, \quad \text{as } \dim_{\mathbb{F}_p}\left(H^2(\bar{G}, \mathbb{F}_p)\right) = r(\bar{G}) = 1.$$

Set $A = \mathrm{im}(\mathrm{inf}^2_{G,\bar{G}}) \leq H^2(G, \mathbb{F}_p)$. By (4.35) one has that

$$A \neq 0 \quad \text{and} \quad \mathrm{inf}^1_{G,\bar{G}}(\chi) \cup \mathrm{inf}^1_{G,\bar{G}}(\psi) = 0,$$

thus, A is not induced by the cup product of χ and ψ. Also, by the Hochschild-Serre spectral sequence $E_2^{st} = H^s(\bar{G}, H^t(C, \mathbb{F}_p))$ associated to (4.33), A is not generated by cup products of elements of $H^1(C, \mathbb{F}_p)^{\bar{G}}$, nor by cup products of $\mathrm{inf}^1_{G,\bar{G}}(\chi)$ and $\mathrm{inf}^1_{G,\bar{G}}(\psi)$ with elements of $H^1(C, \mathbb{F}_p)^G$.

Therefore, for $m > 1$ A is not generated by elements of $H^1(G, \mathbb{F}_p)$, i.e., the cohomology ring $H^\bullet(G, \mathbb{F}_p)$ is not a quadratic $\mathbb{F}_p$-algebra, a contradiction. Thus, $m = 1$ and one has $r \equiv y^{-q}[x_1, y] \bmod [N, N]$.[4] □

Therefore, the relations of G which induce the torsion-module part in the image of N^{ab} in M via ϕ must be of cyclotomic type, and from (4.31) and Proposition 4.24 one deduces the following.

THEOREM 4.25. *Let (G, θ) be a cyclo-oriented pro-p with $\mathrm{im}(\theta) = 1 + q\mathbb{Z}_p$ and $N = \ker(\theta)$, and let $N/[N, N]$ be a $\mathbb{Z}_p[\![X]\!]$-module with the action induced by* (4.26) *and* (4.27). *Then* (4.31) *induces the isomorphism of $\mathbb{Z}_p[\![X]\!]$-modules*

$$\frac{N}{[N, N]} \xrightarrow{\sim} \mathbb{Z}_p[\![X]\!]^f \oplus \left(\frac{\mathbb{Z}_p[\![X]\!]}{X - q}\right)^t \tag{4.36}$$

with $f + t = d(G) - 1$.

In particular, Theorem 4.25 provides a positive answer to Question 1.

EXAMPLES 4. (a) Let (G, θ) be a finitely generated θ-abelian pro-p group with $\mathrm{im}(\theta) = 1 + p\mathbb{Z}_p$. Then $N = \mathrm{Z}_\theta(G)$, and one has

$$N^{\mathrm{ab}} \simeq \left(\frac{\mathbb{Z}_p[\![X]\!]}{X - p}\right)^{d(G)-1}.$$

[4] In fact this argument does not work properly, but this one does: assume that one has a defining relation as (4.32), with $m \geq 2$; then

$$y^{-q}[x_1, y] \not\equiv 1 \bmod [N, N] \quad \text{and} \quad \left(y^{-q}[x_1, y]\right)^m \equiv 1 \bmod [N, N],$$

i.e., N^{ab} has non-trivial torsion, a contradiction.

(b) Let (G,θ) be a Demushkin group with $p \neq 2$ and $\mathrm{im}(\theta) = 1 + p\mathbb{Z}_p$, and let x_i, $1 \leq i \leq d(G)$, be as in Theorem 2.22. Then N is generated by $x_1, x_3, \ldots, x_{d(G)}$, and one has

$$N^{\mathrm{ab}} \simeq \frac{\mathbb{Z}_p[\![X]\!]}{X-p} \oplus \mathbb{Z}_p[\![X]\!]^{d(G)-2},$$

where the torsion-module part is induced by $\bar{x}_1$.

COROLLARY 4.26. *Let (G,θ) be a finitely generated cyclo-oriented pro-p group with $\mathrm{im}(\theta) = 1 + q\mathbb{Z}_p$, with $q = p^k$ and $k \in \mathbb{N} \cup \{\infty\}$. Then one has*

$$G/[G,G] \simeq \mathbb{Z}_p^{d(G)-t} \oplus \left(\mathbb{Z}_p/q\mathbb{Z}_p\right)^t,$$

with t as in Theorem 4.25. In particular, if $G_K(p)$ is the maximal pro-p Galois group of a field K containing a primitive p-th root of unity (and also $\sqrt{-1}$ if $p = 2$), then

$$\frac{G_K(p)}{[G_K(p), G_K(p)]} \simeq \mathbb{Z}_p^{d-t} \oplus (\mathbb{Z}/q\mathbb{Z})^t \quad \textit{or} \quad \frac{G_K(p)}{[G_K(p), G_K(p)]} \simeq \mathbb{Z}_p^t,$$

the former case if K contains a primitive q-th root of unity but not a pq-th one, and the latter if K contains all roots of unity of p-power order, with $d = \dim_{\mathbb{F}_p}(K^\times/(K^\times)^p)$.

Thus, for a finitely generated pro-p group G with non-trivial cyclotomic orientation $\theta\colon G \to \mathbb{Z}_p^\times$, one may define the *1-torsion rank* $t_1(G)$ and the *1-free rank* $f_1(G)$ of G to be the rank as $\mathbb{Z}_p$-module of the $\mathbb{Z}_p[\![\Gamma]\!]$-torsion part of $H_1(\ker(\theta), \mathbb{Z}_p)$, resp. of the $\mathbb{Z}_p[\![\Gamma]\!]$-free part of $H_1(\ker(\theta), \mathbb{Z}_p)$; i.e.,

$$t_1(G) = t \quad \text{and} \quad f_1(G) = f,$$

with t and f as in Theorem 4.25.

By Examples 4 one easily deduces that if $\mathrm{Z}_\theta(G)$ is not trivial, then also the $\mathbb{Z}_p[\![\Gamma]\!]$-torsion part of $H_1(\ker(\theta), \mathbb{Z}_p)$ is non-trivial, i.e., $t_1(G) \geq d(\mathrm{Z}_\theta(G))$.

Then, one may formulate the following questions.

QUESTION 2. *Let G be a finitely generated pro-p group with non-trivial cyclotomic orientation $\theta\colon G \to \mathbb{Z}_p^\times$.*

(i) *Assume that $t_1(U) = 0$ for every open subgroup U of G. Then G is a free pro-p group.*

(ii) *Assume that* $t_1(U) = 1$ *for every open subgroup* U *of* G*, and assume also that* $\mathrm{Z}_\theta(G)$ *is trivial. Then* G *is a cyclotomic fibre product* $F \ltimes_\theta Z$*, with* F *a free pro-*p *group and* $Z \simeq \mathbb{Z}_p$*, or* G *is a Demushkin group, or* G *is the free pro-*p *product* $F *_{\hat{p}} \tilde{G}$*, with* F *a free pro-*p *group and* $\tilde{G}$ *one of the former two groups (fibre product or Demushkin).*

(iii) *Assume that* $\mathrm{Z}_\theta(G)$ *is trivial and* $t_1(G) \geq 2$*. Then there exist two closed subgroups* G_1 *and* G_2 *of* G *such that* $G = G_1 *_{\hat{p}} G_2$*.*

These questions will provide me some work (and hopefully a job) in the next future.

5. Cyclo-oriented ETC

Now it makes sense to try to extend the Elementary Type Conjecture to the whole class of finitely generated pro-p groups with a cyclotomic orientation. In order to do this, we define the class of elementary type cyclo-oriented pro-p groups.

Definition 16. For p a prime number, let $\mathcal{ET}_p$ be the minimal class of finitely generated pro-p groups with an orientation such that

(i) the pro-cyclic group $\mathbb{Z}_p$, together with an orientation $\theta\colon \mathbb{Z}_p \to \mathbb{Z}_p^\times$ (possibly the trivial one), is in $\mathcal{ET}_p$;
(ii) if $p = 2$, then the cyclic group $\mathbb{Z}/2\mathbb{Z}$ of order 2, together with the non-trivial orientation $\theta\colon \mathbb{Z}/2\mathbb{Z} \to \{\pm 1\} \subset \mathbb{Z}_2^\times$, is in $\mathcal{ET}_2$;
(iii) every Demushkin group equipped with an orientation as described in Theorem 2.22 is in $\mathcal{ET}_p$;
(iv) if the group (G, θ) is in $\mathcal{ET}_p$, then also the cyclotomic fibre product $G \ltimes_\theta \mathbb{Z}_p(1)$ is in $\mathcal{ET}_p$;
(v) if the groups (G_1, θ_1) and (G_2, θ_2) are in $\mathcal{ET}_p$, then also the free pro-p product $G_1 *_{\hat{p}} G_2$ with the induced orientation $\tilde{\theta}$ is in $\mathcal{ET}_p$.

Then $\mathcal{ET}_p$ is called the class of **elementary type** pro-p groups with a cyclotomic orientation.

By Theorem 4.5 and Theorem 4.17, every element of $\mathcal{ET}_p$ is a finitely generated cyclo-oriented pro-p group. In particular, every element of $\mathcal{ET}_p$ can be realized as maximal pro-p Galois group of a field. We can now state a new formulation of the ETC.

Question 3. *Let* K *be a field.*

(i) *Assume that the absolute Galois group* G_K *of* K *is a finitely generated pro-*p *group. Then* G_K *is in* $\mathcal{ET}_p$*.*

(ii) *Assume that K contains a primitive p-th root of unity, and that the maximal pro-p Galois group $G_K(p)$ is finitely generated. Then $G_K(p)$ is in $\mathcal{ET}_p$.*

Obviously, a positive answer to (ii) provides also a positive answer to (i).

Note that Question 2 is coherent with the ETC, and a positive answer would be a contribution to the ETC.

Moreover, the recent results obtained independently by Th. Weigel and P. Zalesskiĭ, and by K. Wingberg on free decomposability of pro-p groups provide new tools also to study the ETC (cf. [**WZ13**] and [**Wn13**]).

CHAPTER 5

Koszulity for cyclo-oriented pro-p groups

1. Koszul duality

Let $A_\bullet$ be a quadratic algebra over a field $\mathbb{F}$, and let A_1 and $\mathcal{R}$ be as in (2.1), with A_1 of finite dimension over $\mathbb{F}$. In particular, set $\mathcal{R}_1$ to be the $\mathbb{F}$-vector subspace of $A_1 \otimes A_1$ which generates $\mathcal{R}$ as two-sided ideal of $\mathcal{T}^\bullet(A_1)$.

Since A_1 is finitely generated, one has the isomorphism of $\mathbb{F}$-vector spaces

$$A_1^* \otimes A_1^* \simeq (A_1 \otimes A_1)^* . \tag{5.1}$$

Let $\mathcal{R}_1^\perp \leq (A_1 \otimes A_1)^*$ be the annihilator of $\mathcal{R}_1$, namely,

$$\mathcal{R}_1^\perp = \{f \in (A_1 \otimes A_1)^* \mid f(v) = 0 \text{ for all } v \in \mathcal{R}_1\}.$$

By (5.1) we may consider $\mathcal{R}_1^\perp$ as a subspace of $A_1^* \otimes A_1^*$. In particular, one has that $\mathcal{R}_1^\perp \simeq (A_1^{\otimes 2}/R_1)^*$. Then, the short exact sequences of $\mathbb{F}$-vector spaces

$$0 \longrightarrow \mathcal{R}_1 \longrightarrow A_1^{\otimes 2} \longrightarrow A_2 \longrightarrow 0,$$

$$0 \longleftarrow \mathcal{R}_1^* \longleftarrow \left(A_1^{\otimes 2}\right)^* \longleftarrow \mathcal{R}_1^\perp \longleftarrow 0,$$

where one is the dual of the other, induce the following definition.

Definition 17. Let $A_\bullet$ be a quadratic algebra over a field $\mathbb{F}$ with $\dim(A_1)$ finite. The **Koszul dual** $A_\bullet^!$ of $A_\bullet$ is the quadratic algebra over $\mathbb{F}$ given by

$$A_\bullet^! = \frac{\mathcal{T}^\bullet(A_1^*)}{\mathcal{R}^\perp},$$

where $\mathcal{R}^\perp$ is the two-sided ideal of $\mathcal{T}^\bullet(A_1^*)$ generated by $\mathcal{R}_1^\perp$.

Note that the Koszul dual is an involution, as $(A_\bullet^!)^! = A_\bullet$ for every quadratic algebra.

EXAMPLES 5. (a) Let V be a finite-dimensional $\mathbb{F}$-vector space, and let $A_\bullet$ be the tensor algebra $\mathcal{T}^\bullet(V)$. Then $\mathcal{R} = 0$, and the Koszul dual $A^!_\bullet$ is the algebra of *dual numbers*

$$\mathcal{T}^\bullet(V)^! = \mathbb{F} \oplus V^*,$$

with trivial multiplication.

(b) Let $\{v_1, \ldots, v_n\}$ be a basis for the $\mathbb{F}$-vector space V, and let $A_\bullet$ be the symmetric algebra $S_\bullet(V)$. Then a basis for $\mathcal{R}_1^\perp$ is

$$\left\{v_i^* \otimes v_j^* + v_j^* \otimes v_i^*, 1 \leq i, j \leq n\right\},$$

with $v_i^* \in V^*$ the dual of v_i. Hence, the Koszul dual of $S_\bullet(V)$ is the exterior algebra $\bigwedge_\bullet(V^*)$, and conversely $\bigwedge_\bullet(V)^! = S_\bullet(V^*)$.

The Koszul dual behaves with respect to the constructions of quadratic algebras defined in Subsection 2.1.1 in the following way (cf. [**PP05**, § 3.1, Corollary 2.1, p. 58]).

PROPOSITION 5.1. *Let $A_\bullet$ and $B_\bullet$ be two quadratic algebras over a field $\mathbb{F}$.*

(i) *The Koszul dual of the direct sum is the free product of the Koszul duals, i.e.*

$$(A_\bullet \sqcap B_\bullet)^! = A^!_\bullet \sqcup B^!_\bullet \quad \textit{and} \quad (A_\bullet \sqcup B_\bullet)^! = A^!_\bullet \sqcap B^!_\bullet.$$

(ii) *The Koszul dual of the symmetric tensor product is the skew-commutative tensor product of the Koszul duals, i.e.*

$$\left(A_\bullet \otimes^1 B_\bullet\right)^! = A^!_\bullet \otimes^{-1} B^!_\bullet \quad \textit{and} \quad \left(A_\bullet \otimes^{-1} B_\bullet\right)^! = A^!_\bullet \otimes^1 B^!_\bullet.$$

The $\mathbb{F}_p$-cohomology ring of a Bloch-Kato pro-p group G is a quadratic algebra over $\mathbb{F}_p$: thus, it is worth asking what is the Koszul dual of such algebra. Also, other important graded algebras for a pro-p group G are the restricted Lie algebra $L_\bullet(G)$ and the algebra $\mathrm{gr}_\bullet(G)$, which are related by Theorem 1.14 – and they happen to be quadratic in some important cases, such as Demushkin groups and θ-abelian groups. The following definition relates $H^\bullet(G, \mathbb{F}_p)$ and $\mathrm{gr}_\bullet(G)$.

DEFINITION 18. Let G be a Bloch-Kato pro-p group. Then G is said to be a **Koszul duality** group if the algebra $\mathrm{gr}_\bullet(G)$ is the Koszul dual of the algebra $H^\bullet(G, \mathbb{F}_p)$, i.e.,

$$H^\bullet(G, \mathbb{F}_p)^! \simeq \mathrm{gr}_\bullet(G).$$

It follows that if G is a Koszul duality pro-p group, then $\mathrm{gr}_\bullet(G)$ is a quadratic $\mathbb{F}_p$-algebra. In particular, let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1 \tag{5.2}$$

be a minimal presentation of G, with R generated by $\{r_1, \dots, r_{r(G)}\}$ as normal subgroup of F. If G is a Koszul duality pro-p group, one has that the initial forms of the relations r_i's have degree 2 in $L_\bullet(G)$, i.e.,

$$r_i \in D_2(F) \smallsetminus D_3(G)(G) \quad \text{for every } i = 1, \dots, r(G). \tag{5.3}$$

Thus, we say that a pro-p group G is **$\mathcal{U}$-quadratic** if it has a presentation (5.2) such that (5.3) holds.

We are to see in the following that the basic blocks of the ETC – i.e., free pro-p groups, Demushkin groups and groups obtained via cyclotomic fibre products and free pro-p products – are Koszul duality groups.

Remark 5.2. Note that for a vector space V over $\mathbb{F}_p$, the Pontryagin dual and the $\mathbb{F}_p$-dual are the same, i.e., $V^* = V^\vee$.

2. Koszul duality and the ETC

2.1. Free pro-p groups and Demushkin groups. Let F be a free pro-p group. (recall that by Remark 2.10 every orientation is cyclotomic for F.) Then F has cohomological dimension 1, and the cohomology ring $H^\bullet(F, \mathbb{F}_p)$ is concentrated in degree 0 and 1. In particular, one has

$$H^\bullet(F, \mathbb{F}_p) = \frac{\mathcal{T}^\bullet\left(F/\Phi(F)^\vee\right)}{\mathcal{R}}, \quad \text{with } \mathcal{R}_1 = \left(F/\Phi(F)^\vee\right)^{\otimes 2}.$$

Therefore, by Example 5 the Koszul dual of $H^\bullet(F, \mathbb{F}_p)$ is the tensor algebra $\mathcal{T}^\bullet(F/\Phi(F))$.

Consider now the restricted Lie algebra induced by the Zassenhaus filtration of F. By Theorem 1.16 the algebra $L_\bullet(F)$ is a free restricted Lie algebra over $\mathbb{F}_p$, and by Proposition 1.13 the universal envelope a free non-commutative $\mathbb{F}_p$-algebra, i.e.,

$$\mathrm{gr}_\bullet(F) \simeq \mathcal{U}_p(L_\bullet(F)) \simeq \mathbb{F}_p\langle\mathcal{X}\rangle = \mathcal{T}^\bullet\left(F/\Phi(F)^\vee\right), \tag{5.4}$$

with $\mathcal{X}$ a minimal generating system of F, where $\mathbb{F}_p\langle\mathcal{X}\rangle$ is to be considered a graded algebra with the grading induced by the degrees of the monomials. Therefore, one has the following.

PROPOSITION 5.3. *Let F be a finitely generated free pro-p group. Then the graded $\mathbb{F}_p$-algebra $\mathrm{gr}_\bullet(F)$ is the Koszul dual of the cohomology ring $H^\bullet(F,\mathbb{F}_p)$, i.e.,*

$$H^\bullet(F,\mathbb{F}_p)^! \simeq \mathrm{gr}_\bullet(F).$$

Now let G be a Demushkin group, with $q_G \neq 2$. Let $\mathcal{X} = \{x_1,\dots,x_d\}$ be a minimal generating system for G as in Theorem 2.22, and for each $i = 1,\dots,d$, let $\chi_i \in H^1(G,\mathbb{F}_p)$ be the dual of x_i. Then, one may write

$$H^\bullet(G,\mathbb{F}_p) = \frac{\mathcal{T}^\bullet\left(H^1(G,\mathbb{F}_p)\right)}{\langle \mathcal{R}_1\rangle},$$

with $\mathcal{R}_1 \leq H^1(G,\mathbb{F}_p)^{\otimes 2}$.

Since the element $\chi_{2i-1}\cup\chi_{2i} = -\chi_{2i}\cup\chi_{2i-1}$ generates $H^2(G,\mathbb{F}_p)$, with $i = 1,\dots,d/2$, one has that $\mathcal{R}_1^\perp \simeq H^2(G,\mathbb{F}_p)^*$ is generated by the element

$$\rho = \chi_1^*\otimes\chi_2^* - \chi_2^*\otimes\chi_1^* + \chi_3^*\otimes\chi_4^* - \ldots + \chi_{d-1}^*\otimes\chi_d^* - \chi_d^*\otimes\chi_{d-1}^*,$$

thus

$$H^\bullet(G,\mathbb{F}_p)^! = \frac{\mathcal{T}^\bullet\left(H^1(G,\mathbb{F}_p)^*\right)}{\langle\rho\rangle} \simeq \frac{\mathbb{F}_p\langle X_1,\dots,X_d\rangle}{\langle [X_1,X_2]+\ldots+[X_{d-1},X_d]\rangle},$$

where $\mathcal{X} = \{X_1\dots,X_d\}$ a set of non-commutative indeterminates and $[X_i,X_j] = X_iX_j - X_jX_i$, with the grading induced by the degrees. Therefore, by (2.19), one has the following.

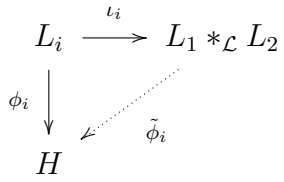
PROPOSITION 5.4. *Let G be a finitely generated Demushkin group with $q_G \neq 2$. Then the $\mathbb{F}_p$-cohomology ring $H^\bullet(G,\mathbb{F}_p)$ is the Koszul dual of the graded $\mathbb{F}_p$-algebra $\mathrm{gr}_\bullet(G)$, i.e.,*

$$H^\bullet(G,\mathbb{F}_p)^! \simeq \mathrm{gr}_\bullet(G).$$

2.2. Free products and cyclo-fibre products. In order to deal with the restricted Lie algebra of a free pro-p product of pro-p groups, we have to define the free product for restricted Lie algebras.

Let L_1 and L_2 be two restricted Lie algebras. The *free product* of restricted Lie algebras of L_1 and L_2 is the restricted Lie algebra $L = L_1 *_{\mathcal{L}} L_2$, equipped with two embeddings $\iota_i\colon L_i \to L$, $i = 1,2$ such

that for every morphism of restricted Lie algebras $\phi_i\colon L_i \to H$ there exists a unique morphism $\tilde{\phi}_i\colon L \to H$ such that the diagram



commutes for both i's (cf. [**Li80**, Remark 1]).

PROPOSITION 5.5. *Let G_1 and G_2 be two finitely generated pro-p groups, and set G to be the free pro-p product $G_1 *_{\hat{p}} G_2$. Then the restricted Lie algebra $L_\bullet(G)$ is the free product of restricted Lie algebras $L_\bullet(G_1) *_{\mathcal{L}} L_\bullet(G_2)$. Moreover, its universal envelope is the free product*

$$\mathcal{U}_p\left(L_\bullet(G)\right) = \mathcal{U}_p\left(L_\bullet(G_1)\right) \sqcup \mathcal{U}_p\left(L_\bullet(G_2)\right). \tag{5.5}$$

PROOF. Let G^{abs} be the *abstract* free product $G_1 * G_2$. Since both G_1 and G_2 are finitely generated, (2.21) implies that the free pro-p product $G = G_1 *_{\hat{p}} G_2$ is the pro-p completion of G^{abs}. By [**Li80**, Theorem 2] one has

$$L_\bullet(G^{abs}) = L_\bullet(G_1) *_{\mathcal{L}} L_\bullet(G_2). \tag{5.6}$$

Since G is finitely generated, every element of the Zassenhaus filtration $D_i(G)$ is open in G, and thus every $D_i(G^{abs})$ has finite index in G^{abs}. Therefore $D_i(G)/D_{i+1}(G) \simeq D_i(G^{abs})/D_{i+1}(G^{abs})$ for every $i \geq 1$, and one has the isomorphism of restricted Lie algebras $L_\bullet(G) \simeq L_\bullet(G^{abs})$.

Equality (5.5) follows directly from [**Li80**, Theorem 1] and Theorem 1.14. □

Thus, Proposition 5.5 and Proposition 5.1 imply the following.

PROPOSITION 5.6. *Let (G_1, θ) and (G_2, θ) be two finitely generated cyclo-oriented pro-p groups, and assume that both are Koszul duality pro-p groups. Then also the free pro-p product $G_1 *_{\hat{p}} G_2$ is a Koszul duality pro-p group.*

PROOF. By [**NSW**, Theorem 4.1.4], one has

$$H^\bullet(G_1 *_{\hat{p}} G_2, \mathbb{F}_p) = H^\bullet(G_1, \mathbb{F}_p) \sqcap H^\bullet(G_2, \mathbb{F}_p) \tag{5.7}$$

(direct product of quadratic $\mathbb{F}_p$-algebras). Therefore,

$$\begin{aligned} H^\bullet\left(G_1 *_{\hat{p}} G_2, \mathbb{F}_p\right)^! &= \left(H^\bullet(G_1, \mathbb{F}_p) \sqcap H^\bullet(G_2, \mathbb{F}_p)\right)^! \\ &= H^\bullet(G_1, \mathbb{F}_p)^! \sqcup H^\bullet(G_2, \mathbb{F}_p)^! \\ &\simeq \mathrm{gr}_\bullet(G_1) \sqcup \mathrm{gr}_\bullet(G_2) \\ &= \mathrm{gr}_\bullet\left(G_1 *_{\hat{p}} G_2\right), \end{aligned}$$

and the statement holds. □

Now let (G, θ) be a finitely generated θ-abelian pro-p group, with $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ if $p = 2$. Then by Theorem 3.12 the $\mathbb{F}_p$-cohomology ring of G is the exterior algebra

$$H^\bullet(G, \mathbb{F}_p) \simeq \bigwedge_{i=0}^{d(G)} H^1(G, \mathbb{F}_p).$$

Therefore, by Example 5, the Koszul dual of $H^\bullet(G, \mathbb{F}_p)$ is the symmetric algebra $S^\bullet(G/\Phi(G))$. Note that such symmetric algebra is isomorphic to the commutative polynomial algebra $\mathbb{F}_p[X_1, \ldots, X_{d(G)}]$, where $\{X_1, \ldots, X_{d(G)}\}$ is a set of commutative indeterminates, equipped with the grading induced by the degrees of the monomials. Thus, by (3.21) one has

$$\mathrm{gr}_\bullet(G) \simeq \mathcal{U}_p(L_\bullet(G)) \simeq H^\bullet(G, \mathbb{F}_p)^!.$$

We are in a similar situation with (G, θ) a finitely generated cyclo-oriented pro-p group, with non-trivial θ-centre and with $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ if $p = 2$. Indeed, Theorem 4.15 and Proposition 5.1 imply the following.

PROPOSITION 5.7. *Let (G, θ) be a finitely generated cyclo-oriented pro-p group with non-trivial θ-centre, and assume $\mathrm{im}(\theta) \simeq \mathbb{Z}_2$ for $p = 2$. Moreover, assume that $G_\circ$ is a Koszul duality group, with $G_\circ$ as in Theorem 4.13. Then the $\mathbb{F}_p$-cohomology ring $H^\bullet(G, \mathbb{F}_p)$ is the Koszul dual of the graded $\mathbb{F}_p$-algebra $\mathrm{gr}_\bullet(G)$.*

PROOF. Set $W = H^1(\mathrm{Z}_\theta(G), \mathbb{F}_p)$. Then by Remark 4.16, Proposition 4.14 and Example 5, one has

$$\begin{aligned} H^\bullet(G,\mathbb{F}_p)^! &= \left(H^\bullet(G_\circ,\mathbb{F}_p) \otimes^{-1} \left(\bigwedge W\right)\right)^! \\ &= H^\bullet(G_\circ,\mathbb{F}_p)^! \otimes^1 \left(\bigwedge W\right)^! \\ &\simeq \mathrm{gr}_\bullet(G_\circ) \otimes^1 \mathbb{F}_p[Y_1,\ldots,Y_d] \\ &= \mathrm{gr}_\bullet(G), \end{aligned}$$

with $d = d(\mathrm{Z}_\theta(G))$. □

EXAMPLE 2. Let G be the cyclotomic fibre product as in Example 1. Recall that the $\mathbb{F}_p$-vector space $H^2(G,\mathbb{F}_p)$ is generated by the elements

$$\chi_1 \cup \chi_2 = \ldots = \chi_{d-1} \cup \chi_d \quad \text{and} \quad \chi_i \cup \psi \text{ for } i = 1,\ldots,d.$$

Let $H^1(G,\mathbb{F}_p)^* = \mathrm{Span}_{\mathbb{F}_p}\{X_1,\ldots,X_d,Y\}$. Then, one has $\mathcal{R}_1^\perp = \mathcal{R}_D \oplus \mathcal{R}_S$, with

$$\begin{aligned} \mathcal{R}_D &= \langle [X_1,X_2] + [X_3,X_4] + \ldots + [X_{d-1},X_d] \rangle, \\ \mathcal{R}_S &= \langle X_1Y - YX_1, \ldots, X_dY - YX_d \rangle. \end{aligned}$$

Therefore,

$$H^\bullet(G,\mathbb{F}_p)^! \simeq \frac{\mathbb{F}_p\langle X_1,\ldots,X_d\rangle}{\langle [X_1,X_2] + \ldots + [X_{d-1},X_d]\rangle} \otimes^1 \mathbb{F}_p[Y],$$

with the grading induced by the degrees of the monomials.

Altogether, the class of Koszul duality pro-p groups is closed under free pro-p products and cyclotomic fibre products, which are the basci operations of the ETC. Also, the fundamental blocks of the ETC (free pro-p groups and Demushkin groups) satisfy Koszul duality as well. Thus, we may summarize the above results in the following theorem.

THEOREM 5.8. *Every pro-p group of elementary type (i.e., every finitely generated pro-p group lying in $\mathcal{ET}_p$) is a Koszul duality group.*

3. Koszul duality for cyclo-oriented pro-p groups

Let G be a pro-p group, and let (5.2) be a minimal presentation for G. Then (5.2) induces a short exact sequence of restricted Lie algebras

$$0 \longrightarrow \mathfrak{R}_\bullet \longrightarrow L_\bullet(F) \longrightarrow L_\bullet(G) \longrightarrow 0 \ . \tag{5.8}$$

In particular, $\mathfrak{R}_\bullet$ is the restricted Lie algebra induced by the filtration $R \cap D_i(F)$, i.e.,

$$\mathfrak{R}_{i-1} = \frac{R \cap D_i(F)}{R \cap D_{i+1}(F)} \quad \text{for every } i \geq 2. \tag{5.9}$$

Since (5.2) is minimal, one has that $R \subseteq D_2(F)$. Thus, one has $\mathfrak{R}_1 = R/R \cap D_3(F) \simeq RD_3(F)/D_3(F)$. Also, by Proposition 1.12 the subgroup $R^p[R,F]$ is contained in $D_3(F)$, and one may define a morphism $\phi\colon R/R^p[R,F] \to D_2(G)/D_3(G)$.

Moreover, $H^2(F,\mathbb{F}_p) = 0$, thus by the five term exact sequence the transgression map $\mathrm{tg}_{F,R}$ is an isomorphism. Hence, the map $\mathrm{tg}_{F,R}$ and the isomorphism $(R/R^p[R,F])^* \simeq H^1(R,\mathbb{F}_p)^F$ induce a natural perfect pairing

$$R/R^p[R,F] \times H^2(G,\mathbb{F}_p) \xrightarrow{(\_,\_)} \mathbb{F}_p \tag{5.10}$$

given by $(\bar{r},\psi) \mapsto \mathrm{tg}^{-1}_{F,R}(\psi).\bar{r}$, with $\psi \in H^2(G,\mathbb{F}_p)$ and $r \in R$. Now let G be a Bloch-Kato pro-p group. Then [**CEM**, Theorem 8.4] implies the following.

Proposition 5.9. *Let G be a Bloch-Kato pro-p group, and let* (5.2) *be a minimal presentationfor G. Then $R^p[R,F] = R \cap D_3(F)$.*

Remark 5.10. Note that all the results produced in [**CEM**] for maximal pro-p Galois groups can be generalized to Bloch-Kato pro-p groups, as they are all developed starting from the characteristics of the $\mathbb{F}_p$-cohomology of such groups, depending on the Bloch-Kato conjecture.

Thus, by Proposition 5.9 one has the isomorphism $R/R^p[R,F] = R/R \cap D_3(F) \simeq RD_3(F)/D_3(F)$, so that (5.10) induces the perfect pairing

$$RD_3(F)/D_3(F) \times H^2(G,\mathbb{F}_p) \xrightarrow{(\_,\_)} \mathbb{F}_p \ . \tag{5.11}$$

The quotient $RD_3(F)/D_3(F)$ is a subspace of $D_2(F)/D_3(F) = L_2(F)$. Recall from Remark 1.17 that the universal envelope $\mathcal{U}_p(L_\bullet(F))$ is the free $\mathbb{F}_p$-algebra $\mathbb{F}_p\langle\mathcal{X}\rangle$, with $\mathcal{X} = \{X_1, \dots, X_d\}$ a set of (non-commutative) indeterminates, with $d = d(F) = d(G)$. We may identify $\mathbb{F}_p\langle\mathcal{X}\rangle$ with the tensor algebra $\mathcal{T}^\bullet(V^*)$, with

$$V = H^1(F, \mathbb{F}_p) = F/\Phi(F)^\vee \simeq G/\Phi(G)^\vee.$$

Then the embedding ψ_L, defined as in (1.8), together with (5.1), induces a monomorphism

$$\frac{RD_3(F)}{D_3(F)} \overset{\psi_2}{\hookrightarrow} L_2(F) \hookrightarrow (V \otimes V)^* \ .$$

PROPOSITION 5.11. *Let G be a finitely generated Bloch-Kato pro-p group. Then the diagram of perfect pairings*

$$\begin{array}{ccc} (V \otimes V)^* \times (V \otimes V) & \longrightarrow & \mathbb{F}_p \\ {\scriptstyle\psi_2}\uparrow \quad \cup\downarrow & & \| \\ \dfrac{RD_3(F)}{D_3(F)} \times H^2(G, \mathbb{F}_p) & \longrightarrow & \mathbb{F}_p \end{array} \tag{5.12}$$

commutes, i.e., $tg^{-1}(\chi_1 \cup \chi_2).\bar{r} = \psi_2(\bar{r})(\chi_1 \otimes \chi_2)$ for every

$$\chi_1, \chi_2 \in V = H^1(F, \mathbb{F}_p) \quad \textit{and} \quad \bar{r} \in RD_3(F)/D_3(F).$$

PROOF. Set $d = d(F)$, and let $\{x_1, \dots, x_d\} \subset F$ be a minimal generating set and $\{\chi_1, \dots, \chi_d\} \subset V$ the dual basis. Then, the set $\{\chi_i \otimes \chi_j, 1 \le i, j \le d\}$ is a basis for $V \otimes V$, and it is enough to verify

$$\mathrm{tg}^{-1}(\chi_i \cup \chi_j).\bar{r} = \psi_2(\bar{r})(\chi_i \otimes \chi_j) \tag{5.13}$$

for every $i, j \in \{1, \dots, d\}$.

By [**NSW**, Prop. 3.9.13] every element $r \in R$ may be uniquely written as

$$\bar{r} \equiv \begin{cases} \displaystyle\prod_{h=1}^{d} x_i^{2a_h} \prod_{h<k} [x_h, x_k]^{a_{hk}} \mod D_3(F), \text{ if } p = 2, \\ \displaystyle\prod_{h<k} [x_i, x_j]^{a_{kh}} \mod D_3(F), \text{ if } p \neq 2, \end{cases}$$

with $0 \leq a_i, a_{ij} \leq p-1$. Recall that $\mathrm{gr}_\bullet(F) \simeq \mathbb{F}_p\langle X_1, \dots, X_d\rangle$. Thus, for every $i = 1, \dots, d$, we may consider X_i to be the dual of χ_i in V^*. Then one has

$$\psi_L\left(x_h^2\right) = X_h \otimes X_h \quad \text{and} \quad \psi_L([x_h, x_k]) = X_h \otimes X_k - X_k \otimes X_h.$$

Therefore

$$\psi_2(\bar{r})(\chi_i \otimes \chi_j) = \begin{cases} a_{ij} \bmod p & \text{if } i < j \\ -a_{ij} \bmod p & \text{if } i > j \\ -\binom{p}{2} a_i \bmod p & \text{if } i = j \end{cases}$$

Again by [**NSW**, Prop. 3.9.13], the above result is the same we get for $\mathrm{tg}^{-1}(\chi_i \cup \chi_j).\bar{r}$, so that equality (5.13) holds. □

Proposition 5.11 implies the following.

THEOREM 5.12. *Let G be a finitely generated Bloch-Kato pro-p group with a minimal presentation* (5.2)*, and let $\mathfrak{r}$ be the ideal of the restricted Lie algebra $L_\bullet(F)$ generated by the elements*

$$\rho_i \in L_2(F), \quad \rho_i \equiv r_i \mod D_3(F),$$

with $i = 1, \dots, r(G)$. Then $\mathcal{U}_p(L_\bullet(F)/\mathfrak{r}) \simeq H^\bullet(G, \mathbb{F}_p)^!$. In particular, if G is quadratically defined,[1] *then G is a Koszul duality pro-p group, i.e.,*

$$\mathrm{gr}_\bullet(G) \simeq H^\bullet(G, \mathbb{F}_p)^!.$$

PROOF. Let $\mathcal{R}_1 \leq V \otimes V$ be the generating relations of the $\mathbb{F}_p$-cohomology ring $H^\bullet(G, \mathbb{F}_p)$. Since (5.12) commutes (and both the horizontal lines are perfect pairings), one has that $\psi_2(\bar{r}) \in \mathcal{R}_1^\perp$ for every $\bar{r}$, i.e., the quotient $RD_3(F)/D_3(F)$ embeds in $\mathcal{R}_1^\perp$ via ψ_2. Moreover, one has

$$\dim_{\mathbb{F}_p}\left(\frac{RD_3(F)}{D_3(F)}\right) = \dim_{\mathbb{F}_p}\left(\frac{R}{R^p[R,F]}\right) = r(G),$$

[1] I.e., G is $\mathcal{U}$-quadratic and $\mathfrak{r} = \mathfrak{R}_\bullet$, with $\mathfrak{R}_\bullet$ as in (5.9).

and, on the other hand,

$$\begin{aligned}\dim_{\mathbb{F}_p}\left(\mathcal{R}_1^{\perp}\right) &= \dim_{\mathbb{F}_p}(V\otimes V) - \dim_{\mathbb{F}_p}\left(\mathcal{R}_1\right)\\ &= \dim_{\mathbb{F}_p}\left(H^2(G,\mathbb{F}_p)\right)\\ &= r(G).\end{aligned}$$

Therefore, $RD_3(F)/D_3(F)$ and $\mathcal{R}_1^{\perp}$ are isomorphic.

Since $RD_3(F)/D_3(F)$ generates $\mathfrak{r}$ as ideal of $L_\bullet(F)$ and $\mathcal{R}^{\perp}$ as ideal of $\mathcal{T}^\bullet(V^*)$, the statement holds by Proposition 1.18. □

COROLLARY 5.13. *A finitely-generated Bloch-Kato pro-p group is $\mathcal{U}$-quadratic.*

Note that in general for a Bloch-Kato pro-p group G the ideal $\mathfrak{r}$ of $L_\bullet(G)$ as defined in Theorem 5.12 is smaller than the ideal $\mathfrak{R}_\bullet$ as in (5.9). Namely, one has

$$\mathfrak{r}\cap L_i(F)\subseteq \frac{R\cap D_i(F)}{R\cap D_{i+1}(F)} \quad \text{for every } i\geq 2,$$

and the initial forms of a set $\{r_1,\dots,r_{r(G)}\}$ of generators of R as normal subgroup of F may be not enough to generate the whole ideal $\mathfrak{R}_\bullet$.

COROLLARY 5.14. *Let G be a finitely generated Bloch-Kato pro-p group, and assume that G is quadratically defined. Then G is a Koszul duality group.*

The material developed in Section 5.3 is partially motivated and inspired by J. Labute's work [**La06**]. In this paper, Labute proves many properties of *mild groups* (i.e., pro-p groups with a *strongly free* presentation). In particular, he shows that if G is a mild group, then one has $\mathfrak{r}=\mathfrak{R}_\bullet$ (cf. [**La06**, Theorem 5.1]). Yet, in general mild groups are very different to Bloch-Kato pro-p groups.

4. Koszul algebras and Koszul pro-p groups

DEFINITION 19. (i) A quadratic[2] algebra $A_\bullet$ over a field $\mathbb{F}$ is said to be a **Koszul algebra** over $\mathbb{F}$ if the homology groups

$$H_{ij}(A_\bullet)=\mathrm{Tor}_{ij}^{A_\bullet}(\mathbb{F},\mathbb{F})$$

[2]In fact this definition holds for all positively graded algebras. Indeed, a Koszul algebra is necessarily quadratic.

(where the first grading i is the cohomological grading and the second grading j is the internal grading induced from the grading of $A_\bullet$) are concentrated on the diagonal, i.e., $H^{ij}(A_\bullet) = 0$ for $i \neq j$ (cf. [**PP05**, § 2.1], [**Ps05**] and [**Ps14**]).

(ii) A Bloch-Kato pro-p group is said to be a H-**Koszul** pro-p group if the $\mathbb{F}_p$-cohomology ring $H^\bullet(G, \mathbb{F}_p)$ is Koszul, and a $\mathcal{U}$-**Koszul** pro-p group if the graded algebra $\mathrm{gr}_\bullet(G) \simeq \mathcal{U}_p(L_\bullet(G))$ is Koszul.

Note that the conditions on $H_{ij}(A_\bullet)$ for $i = 1, 2$ imply that $A_\bullet$ is necessarily quadratic. In particular, a $\mathcal{U}$-Koszul pro-p group is necessarily $\mathcal{U}$-quadratic. The definition of a Koszul algebra was introduced first in the early '70s by S. Priddy, and later associated to Galois theory and group cohomology.

In fact, Koszul algebras are strongly related to Galois cohomology, as they provide an alternative approach to the Bloch-Kato conjecture, see, e.g., [**Ps14**, § 0.1 and § 0.2]. Indeed, one has the following (cf. [**Ps05**, Theorem 1.3]).

THEOREM 5.15. *Let K be a field containing a primitive p-th root of unity, and assume that:*

(i) *the Galois symbol of degree n $\mathcal{K}_n^M(K)/p \to H^n(G_K, \mu_p^{\otimes n})$ is an isomorphism for $n = 2$ and a monomorphism for $n = 3$;*

(ii) *the Milnor $\mathcal{K}$-ring $\mathcal{K}_\bullet^M(K)/p$ is a Koszul $\mathbb{F}_p$-algebra.*

Then the Galois symbol h_K is an isomorphism, i.e., the Bloch-Kato conjecture holds.

Koszul algebras have the following property.

PROPOSITION 5.16. *A quadratic algebra $A_\bullet$ is Koszul if, and only if, the Koszul dual $A_\bullet^!$ is Koszul. In particular, if $A_\bullet$ is Koszul, then one has the isomorphism $A_\bullet^! \simeq H^{\bullet\bullet}(A_\bullet)$.*

EXAMPLE 3. The symmetric algebra $S^\bullet(V)$ and the exterior algebra $\bigwedge_\bullet(V)$ of a vector space V over $\mathbb{F}$ are Koszul (cf. [**PP05**, p. 20]).

COROLLARY 5.17. *Let G be a Bloch-Kato pro-p group, and assume that G is also a Koszul duality group. Then G is H-Koszul if, and only if, G is $\mathcal{U}$-Koszul.*

Let $A_\bullet$ be a (positively) graded algebra over a field $\mathbb{F}$. The *Hilbert series* of $A_\bullet$ is the formal power series defined by

$$h_{A_\bullet}(t) = \sum_{n \geq 0} \dim_{\mathbb{F}}(A_n) t^n.$$

For a quadratic algebra one has the following (cf. [**PP05**, Corollary 2.4]).

LEMMA 5.18. *Let $A_\bullet$ be a quadratic $\mathbb{F}$-algebra, and assume that either $A_3 = 0$ or $A_3^! = 0$. If $h_{A_\bullet}(t)h_{A_\bullet^!}(-t) = 1$, then $A_\bullet$ (and thus also $A_\bullet^!$) is Koszul.*

4.1. H-Koszulity, $\mathcal{U}$-Koszulity and the ETC. It is natural to ask about the behavior of the fundamental blocks of the ETC with respect to H-Koszulity and $\mathcal{U}$-Koszulity. So far, the following result should not be very surprising.

PROPOSITION 5.19. *Let G be a free pro-p group or a Demushkin group. Then G is H-Koszul and $\mathcal{U}$-Koszul.*

PROOF. Assume first that $G = F$ is a free pro-p group. Then $H^\bullet(F, \mathbb{F}_p) = \mathbb{F}_p \oplus H^1(F, \mathbb{F}_p)$ and $\mathrm{gr}_\bullet(F) \simeq \mathbb{F}_p\langle X_1, \ldots, X_d\rangle$, with $d = d(F)$, and we may computer their Hilbert series:

$$\begin{aligned} h_{H^\bullet(F,\mathbb{F}_p)}(t) &= 1 + dt, \\ h_{\mathrm{gr}_\bullet(F)}(t) &= 1 + dt + d^2t^2 + d^3t^3 + \ldots \end{aligned}$$

Thus, we may apply Lemma 5.18, and we obtain

$$h_{H^\bullet(F,\mathbb{F}_p)}(-t) \cdot h_{\mathrm{gr}_\bullet(F)}(t) = (1 - dt)(1 + dt + d^2t^2 + d^3t^3 + \ldots),$$

so that $H^\bullet(F, \mathbb{F}_p)$ and $\mathrm{gr}_\bullet(F)$ are Koszul algebras.

Assume now that G is a Demushkin group. Then one has

$$h_{H^\bullet(G,\mathbb{F}_p)}(t) = 1 + dt + t^2.$$

Moreover, since the canonical presentation of a Demushkin group is strongly free, [**La06**, Theorem 5.1] implies that the Hilbert series of $\mathrm{gr}_\bullet(G)$ is

$$h_{\mathrm{gr}_\bullet(F)}(t) = \frac{1}{1 - (t + t + \ldots + t) + t^2} = \frac{1}{1 - dt + t^2}.$$

Therefore, $h_{H^\bullet(G,\mathbb{F}_p)}(t) \cdot h_{\mathrm{gr}_\bullet(G)}(-t) = 1$, and Lemma 5.18 yields the claim. □

Moreover, the classes of H-Koszul pro-p groups and of $\mathcal{U}$-Koszul pro-p groups is closed under free pro-p products and cyclotomic fibre products.

PROPOSITION 5.20. *Let G, G_1 and G_2 be finitely generated Bloch-Kato pro-p groups.*

(i) *The free pro-p product $G_1 *_{\hat{p}} G_2$ is a H-Koszul pro-p group, resp. a $\mathcal{U}$-Koszul pro-p group, if, and only if, G_1 and G_2 are both H-Koszul, resp. $\mathcal{U}$-Koszul.*

(ii) *Assume that (G, θ) is cyclo-oriented. Then the cyclotomic fibre product $G \ltimes_\theta Z$, with $Z \simeq \mathbb{Z}_p$, is again a H-Koszul pro-p group, resp. a $\mathcal{U}$-Koszul pro-p group, if, and only if, G is H-Koszul, resp. $\mathcal{U}$-Koszul.*

PROOF. The first statement follows from (5.7) and (5.5) and from [**PP05**, Ch. 2, Corollary 1.2]. The second statement follows from Proposition 5.7, Example 3 and again [**PP05**, Ch. 2, Corollary 1.2]. □

THEOREM 5.21. *Every pro-p group of elementary type (i.e., every finitely generated pro-p group lying in $\mathcal{ET}_p$) is a H-Koszul group and a $\mathcal{U}$-Koszul group.*

QUESTION 4. *Let K be a field containing a primitive p-th root of unity such that the maximal pro-p Galois group $G_K(p)$ is finitely generated.*

(i) *Is $G_K(p)$ a Koszul duality group?*

(ii) *Is $G_K(p)$ H-Koszul and/or $\mathcal{U}$-Koszul?*

Note that if (i) holds and $G_K(p)$ is H-Koszul, resp. $\mathcal{U}$-Koszul, then by Proposition 5.16 the group $G_K(p)$ is also $\mathcal{U}$-Koszul, resp. H-Koszul.

Bibliography

[AEJ] J.K. Arason, R. Elman and B. Jacob. Rigid elements, valuations, and realizations of Witt rings. *J. Algebra* 110 (1987), 449-467.

[ABW] S. Arias-de-Reyna, L. Bary-Soroker and G. Wiese (eds.). *Special issue: Proceedings of the Winter School on Galois theory, Universtiy of Luxembourg, February 2012. Vol. I.* Travaux Mathématiques 22, University of Luxembourg, Luxembourg, 2013.

[BK86] S. Bloch and K. Kato. p-adic étale cohomology. *Publ. Math. IHES* 63 (1986), 107-152.

[BCMS] D. Benson, S.K. Chebolu, J. Mináč and J. Swallow. Bloch-Kato pro-p groups and a refinement of the Bloch-Kato conjecture. Preprint (2007).

[BT12] F. Bogomolov and Y. Tschinkel. Introduction to birational anabelian geometry. In: *Current developments in algebraic geometry*, MSRI Publications vol. 59, Cambridge University Press (2012), 17-63.

[Br66] A. Brumer. Pseudocompact algebras, profinite groups and class formations. *J. Algebra* 4 (1966), 442-470.

[CEM] S.K. Chebolu, I. Efrat and J. Mináč. Quotients of absolute Galois groups which determine the entire Galois cohomology. *Math. Ann.* 352 (2012), 205-221.

[CM08] S.K. Chebolu and J. Mináč. Absolute Galois groups viewed from small quotients and the Bloch-Kato conjecture. In: *New topological contexts for Galois theory and algebraic geometry (BIRS 2008)*, Geom. Topol. Monogr. vol. 16, Geom. Topol. Publ. (2009), 31-47.

[CMQ] S.K. Chebolu, J. Mináč and C. Quadrelli. Detecting fast solvability of equations via small powerful Galois groups. *Trans. Amer. Math. Soc.*, to appear.

[DdSMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal. *Analytic Pro-p Groups, Second edition.* Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, Cambridge, 1999.

[DL83] D. Dummit and J. Labute. On a new characterization of Demushkin groups. *Invent. Math.* 73 (1983), 413-418.

[Ef97a] I. Efrat. Free pro-p product decompositions of Galois groups. *Math. Z.* 225 (1997), 245-261.

[Ef97b] I. Efrat. Pro-p Galois groups of algebraic extensions of $\mathbb{Q}$. *J. Num. Th.* 64 (1997), 84-99.

[Ef06] I. Efrat. *Valuation, orderings and Milnor K-theory.* Mathematical surveys and monographs 124, American Mathematical Society, Providence RI, 2006.

[Ef14] I. Efrat. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Adv. Math.* 263 (2014), 389-411.

[EM11] I. Efrat, J. Mináč. On the descending central sequence of absolute Galois groups. *Amer. J. Math.* 133 (2011), 1503-1532.

[En04] A.J. Engler. A recursive description of pro-p Galois groups. *J. Algebra* 274 (2004), no. 2, 511-522.

[EK98] A.J. Engler and J. Koenigsmann. Abelian subgroups of pro-p Galois groups. *Trans. Amer. Math. Soc.* 350 (1998), 2473-2485.

[EN94] A.J. Engler and J.B. Nogueira. Maximal abelian normal subgroups of Galois pro-2 groups. *J. Algebra* 166 (1994), 481-505.

[Er01] Y.L. Ershov. On free products of absolute Galois groups II. *Comm. Algebra* 29 (2001), no. 9, 3773-3779.

[FJ08] M.D. Fried and M. Jarden. *Field arithmetic. Third edition.* Ergebnisse der Mathematik un ihrer Grenzgebiete 3. Springer, Berlin, 2008.

[Gä11] J. Gärtner. *Mild pro-p-groups with trivial cup-product.* PhD thesis at Heidelberg Universität, Heidelberg, 2011.

[Ge13] W.-D. Geyer. Field Theory. In: *Special issue: Proceedings of the Winter School on Galois theory, Universtiy of Luxembourg, February 2012. Vol. I.* Travaux Mathématiques 22, University of Luxembourg, Luxembourg, 2013.

[HJK] D. Haran M. Jarden and J. Koenigsmann. Free product of absolute Galois groups. Preprint (200?), available at `arXiv:math/0005311v1`.

[HJ95] Y.S. Hwang and B. Jacob. Brauer group analogues of results relating the Witt ring to valuations and Galois theory. *Canad. J. Math.* 47 (1995), no. 3 527-543.

[JW89] B. Jacob and R. Ware. A recursive description of the maximal pro-2 Galois group via Witt rings. *Math. Z.* 200 (1989), 379-396.

[JW91] B. Jacob and R. Ware. Realizing dyadic factors of elementary type Witt rings and pro-2 Galois groups. *Math. Z.* 208 (1991), 193-208.

[KS11] B. Klopsch and I. Snopce. Pro-p groups with constant generating number of open subgroups. *J. Algebra* 331 (2011), 263-270.

[KZ05] D.H. Kochloukova and P.A. Zalesskiĭ. Free-by-Demushkin pro-p groups. *Math. Z.* 249 (2005), 731-739.

[Ko05] J. Koenigsmann. Products of absolute Galois groups. *Int. Math. Res. Not.* (2005), no. 24, 1465-1486.

[La67] J.P. Labute. Classification of Demushkin groups. *Canad. J. Math.* 19 (1967), 106-132.

[La70] J.P. Labute. On the descending central series of groups with a single defining relation. *J. Algebra* 14 (1970) 16-23.

[La85] J.P. Labute. The determination of the Lie algebra associated to the lower central series of a group. *Trans. Amer. Math. Soc.* 288 (1985), no. 1, 51-57.

[La06] J.P. Labute. Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$. *J. reine angew. Math.* 596 (2006), 155-182.

[Ld05] A. Ledet. *Brauer type embedding problems.* Volume 21 of *Fields Institute Monographs.* American Mathematical Society, Providence, RI, 2005.

[LS02] D.B. Leep and T.L. Smith. Multiquadratic extensions, rigid fields and pythagorean fields. *Bull. London Math. Soc.* 34 (2002), 140-148.

[Le55] H. Leptin. Ein Darstellungssatz für kompakte, total unzusammenhängende Gruppen. *Arch. Math.* 6 (1955), 371-373 .

[Li80] A.I. Lichtman. On Lie algebras of free products of groups. *J. Pure Appl. Algebra* 18 (1980), 67-74.

[MS82] A.S. Merkur'ev and A.A. Suslin. K-cohomology of Brauer-Severi varieties and the norm residue isomorphism. *Izv. Akad. Nauk SSSR*, Ser. Mat. 46 (1982), 1132-1146 (Russian).

[MS90] A.S. Merkur'ev and A.A. Suslin. The norm residue symbol of degree 3. *Izv. Akad. Nauk SSSR*, Ser. Mat. 54 (1990), (339-356) (Russian).

[MQRTW] J. Mináč, C. Quadrelli, D.M. Riley, N.D. Tan and Th. Weigel. Koszul dual in Galois cohomology of a field. In preparation (2014).

[MSp90] J. Mináč and M. Spira. Formally real fields, pythagorean fields, C-fields and W-groups. *Math. Z.* 205 (1990), no. 4, 519-530.

[MSp96] J. Mináč and M. Spira. Witt rings and Galois groups. *Ann. of Math. (2)* 144 (1996), no. 1, 35-60.

[MT14] J. Mináč and N.D. Tân. Triple Massey products and Galois theory. *J. Eur. Math. Soc.*, to appear.

[Ne99] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften, Vol. 322, Springer, Berlin Heidelberg, 1999.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg. *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften, Vol. 323, Springer, Berlin Heidelberg, 2000.

[PP05] A. Polishchuck and L. Positselski. *Quadratic algebras*. University lecture series 37, American Mathematical Society, Providence RI, 2005.

[Po94] F. Pop. On Grothendieck's conjecture of birational anabelian geometry. *Ann. of Math.* 139 (1994), no. 2, 145-182.

[Ps05] L. Positselski. Koszul property and Bogomolov's conjecture. *Int. Math. Research Not.* 31 (2005), 1901-1936.

[Ps14] L. Positselski. Galois cohomology of a number field is Koszul. Preprint (2014), available at `arXiv:1008.0095`.

[Qu14] C. Quadrelli. Bloch-Kato pro-p groups and locally powerful groups. *Forum Math.* 26 (2014), no. 3, 793-814.

[QW1] C. Quadrelli and Th. Weigel. Diederichsen's theorem for cohomological Mackey functors and finitely generated free pro-p groups. Preprint (2014).

[QW2] C. Quadrelli and Th. Weigel. Profinite groups with cyclotomic p-orientations. Preprint (2014).

[Ri13] L. Ribes. Introduction to profinite groups. In: *Special issue: Proceedings of the Winter School on Galois theory, Universtiy of Luxembourg, February 2012. Vol. I.* Travaux Mathématiques 22, University of Luxembourg, Luxembourg, 2013.

[RZ10] L. Ribes and P. Zalesskiĭ. *Profinite groups, 2nd edition*. Ergebnisse der Mathematik und ihrer Grenzgebiete 40, Springer, Heidelberg, 2010.

[SW00] P. Symonds and Th. Weigel. Cohomology of p-adic analytic groups. In: *New horizons in pro-p groups*, Progress in Mathematics 184, Birkhäuser Boston, Boston, MA, (2000), 349-410.

[Sz77] K. Szymiczek. Quadratic forms over fields. *Dissertationes Math. (Rozprawy Mat.)* 152 (1977).

[Ta76] J. Tate. Relations between K_2 and Galois cohomology. *Invent. Math.* 36 (1976), 257-274.

[Vo03] V. Voevodsky. Motivic cohomology with $\mathbb{Z}/2$-coefficients. *Publ. Math. IEHS* 98 (2003), 59-104.

[Vo11] V. Voevodsky. On motivic cohomology with $\mathbb{Z}/l$-coefficients. *Ann. of Math.* (2) 174 (2011), no. 1, 401-438.

[Wr81] R. Ware. Valuation rings and rigid elements in fields. it Canad. J. Math. 33 (1981), no. 6, 1338-1355.

[Wr92] R. Ware, Galois groups of maximal p-extensions. *Trans. Amer. Math. Soc.* 33 (1992), no. 2, 721-728.

[We08] C. Weibel. The proof of the Bloch-Kato Conjecture. ICTP Lecture Notes Series 23 (2008), 1-28.

[We09] C. Weibel. The norm residue isomorphism theorem. *J. Topol.* 2 (2009), no. 2, 346-372.

[Wg13] Th. Weigel. The projective dimension of profinite modules for pro-p groups. Preprint (2013), available at `arXiv:1303.5872v1`.

[WZ13] Th. Weigel and P.A. Zalesskiĭ. Stallings' decomposition theorem for finitely generated pro-p groups. Preprint (2013), available at `arXiv:1305.4887`.

[Wn13] K. Wingberg. On the theory of ends of a pro-p group. Preprint (2013), available at `arXiv:1305.0634`.

[Wü85] T. Würfel. A remark on the structure of absolute Galois groups. *Proc. Amer. Math. Soc.* 95 (1985), no. 3, 353-356.

Curriculum Vitæ et Studiorum

Name: Claudio Quadrelli

Post-secondary education and degrees:

- B.Sc., Mathematics, 10/2005-7/2008
  Università degli Studi di Milano-Bicocca, Milano, Italia
- M.Sc., Mathematics, 10/2008-10/2010
  Università degli Studi di Milano-Bicocca, Milano, Italia
- Ph.D., Mathematics, 01/2011-12/2014
  Western University, London ON, Canada, and
  Università degli Studi di Milano-Bicocca, Milano, Italia

Honours and awards:

- Grant INdAM for B.Sc students in Math, 2005-2008
  Istituto Nazionale di Alta Matematica "F. Severi", Rome, Italy
- Prize *Francesco Severi* for M.Sc students in Math, 2009
  Istituto Nazionale di Alta Matematica "F. Severi", Rome, Italy
- Graduate Thesis Research Award, 2013
  Faculty of Science, Western University, London ON, Canada

Related work experience: Teaching assistant, Università degli Studi di Milano-Bicocca, 2009-2014.

Publications:

- Bloch-Kato pro-p groups and locally powerful groups. *Forum Math.* 26 (2014), no. 3, 793-814.
- Detecting fast solvability of equations via small powerful Galois groups, with S.K. Chebolu and J. Mináč. *Trans. Amer. Math. Soc.*, to appear.
- Finite quotients of Galois pro-p groups. Submitted to *Ann. Math. Québec.*