Association for Women in Mathematics Series

Alina Bucur
Wei Ho
Renate Scheidler *Editors*

Research Directions in Number Theory

Women in Numbers V

AWM
ASSOCIATION FOR WOMEN IN MATHEMATICS

Springer

Association for Women in Mathematics Series

Volume 33

Focusing on the groundbreaking work of women in mathematics past, present, and future, Springer's Association for Women in Mathematics Series presents the latest research and proceedings of conferences worldwide organized by the Association for Women in Mathematics (AWM). All works are peer-reviewed to meet the highest standards of scientific literature, while presenting topics at the cutting edge of pure and applied mathematics, as well as in the areas of mathematical education and history. Since its inception in 1971, The Association for Women in Mathematics has been a non-profit organization designed to help encourage women and girls to study and pursue active careers in mathematics and the mathematical sciences and to promote equal opportunity and equal treatment of women and girls in the mathematical sciences. Currently, the organization represents more than 3000 members and 200 institutions constituting a broad spectrum of the mathematical community in the United States and around the world.

Titles from this series are indexed by Scopus.

Alina Bucur • Wei Ho • Renate Scheidler
Editors

Research Directions in Number Theory

Women in Numbers V

Springer

AWM
ASSOCIATION FOR WOMEN IN MATHEMATICS

Editors
Alina Bucur
Department of Mathematics
University of California, San Diego
La Jolla, CA, USA

Wei Ho
Department of Mathematics
Princeton University
Princeton, NJ, USA

Renate Scheidler
Department of Mathematics and Statistics
University of Calgary
Calgary, AB, Canada

ISSN 2364-5733 ISSN 2364-5741 (electronic)
Association for Women in Mathematics Series
ISBN 978-3-031-51676-4 ISBN 978-3-031-51677-1 (eBook)
https://doi.org/10.1007/978-3-031-51677-1

Mathematics Subject Classification: 05C25, 14G50, 11G20

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Preface

This volume is a compilation of research and survey papers in number theory, written by members of the *Women in Numbers* (WIN) network and their colleagues, principally by the collaborative research groups formed for the fifth Women in Numbers workshop. *Women in Numbers* 5 (WIN5), organized by Alina Bucur (University of California San Diego), Wei Ho (Institute for Advanced Study, Princeton University, and University of Michigan), and Renate Scheidler (University of Calgary), was to take place on November 15–20, 2020 at the Banff International Research Station in Banff, Alberta, Canada. To our great regret, the event could not take place in-person on site at BIRS as planned due to the COVID-19 pandemic.

The WIN network (womeninnumbertheory.org) was created for the purpose of increasing the number of active female researchers in number theory. The WIN conference series began in 2008 as the main mechanism for effecting this goal. It introduced a novel research mentorship model where women at all career stages, from graduate students to senior members of the community, joined forces to work in focused research groups on cutting-edge projects designed and led by experienced researchers. This model has proven so successful that to date there are over 25 research networks for women in mathematics, each of which holds *Research Collaboration Conferences for Women* as well as other conferences, workshops, special sessions, and symposia. The Association for Women in Mathematics, funded by the National Science Foundation ADVANCE program, is supporting this highly effective research mentorship model (awm-math.org/programs/advance-research-communities).

The goals for WIN5 were to generate research in significant topics in number theory, to broaden the research programs of women working in number theory (especially pre-tenure), to train graduate students and postdocs in number theory by providing experience with collaborative research and the publication process, to extend and strengthen a research network of potential collaborators in number theory and related fields, to enable faculty at small colleges to participate actively in research activities including the mentorship of graduate students and postdocs, and to highlight research activities of women in number theory.

The typical working model for WIN conferences consists of three phases. Prior to the event, participants are organized into project groups by research interest and asked to acquire the necessary background for their project topics. At the workshop, the groups collaborate on their projects and generally achieve significant progress during that time. Following the conference, the groups continue their collaborations remotely, carrying on with their research and eventually writing up their results for publication. The workshop is arguably the highlight of the WIN experience as it offers everyone the opportunity to get to know the participants outside their group, network with women in their field, and immerse themselves in intense collaborative research. The WIN5 project groups were formed prior to the outbreak of the COVID-19 pandemic. Sadly, the pandemic precluded an in-person event, thus depriving participants of this enriching experience. By necessity, the format of WIN5 was adapted and changed to fit the online world. To their great credit, almost all the groups chose to nevertheless proceed with their collaborations. After consulting with group leaders and experienced organizers of online conferences, the WIN5 organizers elected to decline BIRS's kind offer to host an online version of WIN5 during the originally scheduled dates. Instead, we felt that a sequence of more spread-out events would be more beneficial in supporting the collaborations academically, professionally, and socially. On June 30, 2020, we began with a virtual kick-off meet-and-greet plus Q&A for all WIN5 participants. This was followed by two panels on professional life in the virtual world and on grant writing, respectively. We held two online mini workshops in December 2020 and August 2021, where WIN5 groups gave talks to report on their progress. And throughout the period of pandemic-induced social distancing and forced working-from-home, we offered a weekly Wednesday evening virtual Happy Hour where WIN5 participants could voluntarily drop in and chat, usually over a non-virtual beverage of their choice.

For this volume, the editors solicited contributions from the WIN5 collaboration groups and sought additional articles through the Women in Numbers Network mailing list and other platforms. The ten articles collected here span algebraic, geometric, and computational aspects of number theory, including topics in algebraic and algorithmic number theory, algebraic and arithmetic geometry, arithmetic dynamics, Diophantine equations, modular forms, and additive number theory. Several papers in this volume stem from collaborations between authors with different mathematical backgrounds, allowing the group to tackle a problem using multiple perspectives and tools. All submissions were sent to anonymous referees for rigorous peer review.

Acknowledgments

We are grateful to the National Science Foundation (grant DMS-2012061), the Clay Mathematics Institute, the Number Theory Foundation, and Elsevier Publishers for the support they offered us. We are indebted to BIRS for offering to host the originally planned workshop and subsequently offering to host a virtual version.

We owe a big thank you to all WIN5 group leaders for going ahead with their projects despite not having an actual conference, and to all WIN5 participants for staying productive within the confines of solely online collaboration and persevering through the COVID-19 pandemic. The careful and dedicated work of all our anonymous referees, crucial in assuring the quality of this publication, is much appreciated. Lastly, we thank all our authors for contributing to this volume, Springer for publishing these contributions, and our readers for their interest.

The WIN5 Organizers and Editors:

- Alina Bucur (University of California San Diego)
- Wei Ho (Institute for Advanced Study, Princeton University, and University of Michigan)
- Renate Scheidler (University of Calgary)

November 2023

Contents

From Fontaine–Mazur Conjecture to Analytic Pro-p-groups: A Survey

Ramla Abdellatif, Supriya Pisolkar, Marine Rougnant, and Lara Thomas

1 Introduction

The Fontaine–Mazur Conjecture is a core statement in modern arithmetic geometry. Several formulations of this conjecture were given since its original statement (as appeared in [10]), and various angles have been adopted by numerous authors to try to tackle it. To state the original Fontaine–Mazur Conjecture (FMC), we need to introduce some definitions and notations. Let K be a number field, $\overline{K}$ be a fixed separable closure of K and $G_K := \mathrm{Gal}(\overline{K}/K)$ be the corresponding absolute Galois group. Given a prime number p, a finite extension F of the field $\mathbb{Q}_p$ of p-adic numbers and a profinite group G, an *F-representation of G* is a finite-dimensional vector space over F equipped with a continuous and linear action of G. When $F = \mathbb{Q}_p$, we call it a *p-adic representation of G*. A p-adic representation ρ of G_K is called *geometric* if it ramifies only at a finite number of places of K and if, for each place v of K above p, the restriction of ρ to G_v is potentially semi-stable, as defined

R. Abdellatif (✉)
Laboratoire Amiénois de Mathématique Fondamentale et Appliquée (LAMFA)—Université de Picardie Jules Verne, Amiens, France
e-mail: ramla.abdellatif@math.cnrs.fr

S. Pisolkar
Indian Institute of Science, Education and Research (IISER), Pune, India
e-mail: supriya@iiserpune.ac.in

M. Rougnant
Laboratoire de Mathématiques de Besançon, UFR Sciences et techniques, Besançon, France
e-mail: marine.rougnant@univ-fcomte.fr

L. Thomas
Département de Mathématiques, Faculté des Sciences et Techniques de Saint-Etienne, Université Jean Monnet, 23, rue du Docteur Michelon, Saint-Etienne, France
e-mail: lthomas@math.cnrs.fr

A. Bucur et al. (eds.), *Research Directions in Number Theory*, Association for Women in Mathematics Series 33, https://doi.org/10.1007/978-3-031-51677-1_1

by Fontaine in [11, Section 1.8]. Finally, for any integer r, we let $\mathbb{Q}_p(r)$ denote the r-th Tate twist of $\mathbb{Q}_p$, as defined in [27, §3].

Conjecture 1.1 (Fontaine, Mazur) An irreducible p-adic representation of G_K is geometric if, and only if, it is isomorphic to a subquotient of an étale cohomology group with coefficients in $\mathbb{Q}_p(r)$, for some $r \in \mathbb{Z}$, of a (projective, smooth) algebraic variety over K.

In short, the Fontaine–Mazur Conjecture predicts that p-adic representations of global Galois groups that are potentially semi-stable at primes dividing p and unramified outside finitely many places all come from algebraic geometry.

In the recent years, substantial progress has been made using p-adic representations and deformation theory, allowing, for instance, Kisin [17] to prove the original conjecture for families of two-dimensional representations when $K = \mathbb{Q}$. In this special case, the conjecture asserts that potentially semi-stable representations with odd determinant come from modular forms.

Conjecture 1.2 (Fontaine–Mazur Conjecture for $n = 2$) Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_p)$ be an odd, irreducible representation that is unramified outside finitely many primes and whose restriction to the decomposition group at p is potentially semi-stable with distinct Hodge–Tate weights. Then ρ is the twist of a Galois representation associated with a modular form of weight $k \geq 2$.

Kisin's proof relies on an intimate connection between modularity lifting theorems, the Breuil–Mézard conjecture [2], and Breuil's p-adic local Langlands correspondence for GL_2 [3, 4]. In the same direction (meaning using local–global compatibility results and deformation theory), but using different tools (such as completed cohomology), Emerton proved further cases of this conjecture for two-dimensional representations and $K = \mathbb{Q}$ (see [9, Theorem 7.1.1]).

In this chapter, we are interested in a different approach, which can be motivated as follows. First note that Conjecture 1.1 implies the following conjecture, which is elementary to state but completely out of reach for now (see [7] for instance).

Conjecture 1.3 (Weak Fontaine–Mazur Conjecture) Every unramified pro-p-extension of K whose Galois group is p-adic analytic is finite.

Now recall that in [12], Golod and Shafarevich proved the existence of a number field K and a prime p such that K admits an everywhere unramified infinite pro-p-extension L. (Note that they actually provide a way to obtain infinitely many such number fields.) Conjecture 1.3 then claims that the Galois group of such an extension L/K cannot be an infinite analytic pro-p-group (i.e., isomorphic to a closed subgroup of $GL_n(\mathbb{Z}_p)$ for some positive integer n). Hence the idea is that a counter-example to Conjecture 1.3 would produce an everywhere unramified Galois representation with an infinite image, which cannot "come from algebraic geometry" in the sense of Conjecture 1.1.

From Lazard's seminal work on p-adic analytic groups [19, III, 3.4.3], we know that any finite-dimensional p-adic analytic group contains a finite index open uniform subgroup. We can thus reformulate Conjecture 1.3 as follows.

Conjecture 1.4 (Uniform Fontaine–Mazur Conjecture (UFMC)) There is no number field K for which there exists an infinite everywhere unramified Galois pro-p-extension L such that $\mathrm{Gal}(L/K)$ is uniform.

A major advantage in considering uniform groups is that they have a simple characterisation in terms of filtration by their subgroups, which does not hold for arbitrary analytic pro-p-groups. (Recall that a finitely generated pro-p-group is analytic if, and only if, it contains a uniform subgroup of finite index.)

The first evidence in favour of Conjecture 1.4 was given by N. Boston in [5, 6], using purely group-theoretic methods based on the connections between powerful and uniform pro-p-groups instead of representation-theoretic tools. This chapter provides an introduction to these purely group-theoretic tools and methods, which are not so well known among (young) arithmetic geometers, and a review of some of the main results they bring about various conjectures related to Conjectures 1.1 and 1.4. We also present some related questions on which are based recent, current and future works of the authors. We think that this survey paper may be of interest to anyone looking for a different viewpoint on the Fontaine–Mazur Conjecture, which does not require advanced knowledge in p-adic representation theory and highlights the number-theoretic nature of the problem.

This chapter is organised as follows. Section 2 gathers the definitions and basic results we need about (uniform) pro-p-groups. Section 3 is devoted to study the proofs of the main result of [5], which is the following special case of Conjecture 1.4, and of its generalisation to cyclic extensions of degree prime to p, which is the main result of [6].

Theorem 1.5 (Boston) *Given a prime number p and a number field F, let K be a normal extension of F of prime degree $\ell \neq p$ and such that p does not divide $h(F)$, the class number of F. Then there is no infinite, everywhere unramified pro-p-extension L of K such that L/F is Galois and* $\mathrm{Gal}(L/K)$ *is uniform.*

The main ingredient of the group-theoretic methods used to prove these results is the cyclic action on $\mathrm{Gal}(L/K)$ of a generator σ of $\mathrm{Gal}(K/F)$. This works quite well when the action of σ on $\mathrm{Gal}(L/K)$ has no non-trivial fixed point. The study of such actions also appears in the work of Hajir and Maire [14], in their attempt to extend Boston's strategy to (tamely) ramified extensions L/K. The challenge here is to understand the behaviour of the fixed points introduced by the ramification and the resulting constraints on the arithmetic of L/K.

This work of Hajir and Maire motivates our interest in the two following Fontaine–Mazur-style conjectures, where we consider finitely and tamely ramified p-adic representations. These conjectures are known, respectively, as the *Tame Fontaine–Mazur Conjecture* (TFMC) [10, 5a] and the *Uniform Tame Fontaine–Mazur Conjecture* (UTFMC).

Conjecture 1.6 (Tame Fontaine–Mazur Conjecture) Let K be a number field and S be a finite set of places of K that are prime to p. Set $G_S := \mathrm{Gal}(K_S/K)$, where K_S denotes the maximal pro-p-extension of K that is unramified outside S. Then any p-adic representation of G_S has finite image.

The idea behind this statement is that the eigenvalues of a Frobenius element must become roots of unity under the action of a finitely tamely ramified p-adic representation. In this case, the image of such a representation is solvable, hence finite by class field theory. Class field theory also helps to prove that the conjecture holds for one-dimensional representations, as we show in Sect. 4.2. For higher dimensional representations, Conjecture 1.6 seems for now out of reach in general.

Conjecture 1.7 (Uniform Tame Fontaine–Mazur Conjecture) Let K be a number field and Γ be a uniform pro-p-group of dimension $d > 2$ (hence infinite). Then there does not exist a finitely and tamely ramified Galois extension L/K whose Galois group $\mathrm{Gal}(L/K)$ is isomorphic to Γ.

We elaborate on how these statements connect in Sect. 4 and on how the assumptions made matter. In Sect. 5, we expose some connected questions that are of interest to us, as well as recent results proven in this direction by some of the authors.

General Notations From now on, we fix a prime integer p. We let $\mathbb{Q}_p$ be the field of p-adic numbers and $\mathbb{Z}_p$ be its ring of integers. Since the ring $\mathbb{Z}_p$ is isomorphic to the projective limit $\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}$, there exists, for any integer $k \geq 1$, a natural ring isomorphism $\psi_k : \mathbb{Z}_p/p^k\mathbb{Z}_p \simeq \mathbb{Z}/p^k\mathbb{Z}$. These ring isomorphisms allow us to define *principal congruence subgroups* in this p-adic setting as follows. Given any integer $n \geq 2$, we consider the special linear group $\mathrm{SL}_n(\mathbb{Z}_p)$, which is a maximal open compact subgroup of $\mathrm{SL}_n(\mathbb{Q}_p)$. For any integer $k \geq 1$, we can then define the k-th-*principal congruence subgroup* of $\mathrm{SL}_n(\mathbb{Z}_p)$ as $\Gamma_{n,k} := \ker\left(\mathrm{SL}_n(\mathbb{Z}_p) \twoheadrightarrow \mathrm{SL}_n(\mathbb{Z}/p^k\mathbb{Z})\right)$. Note that we choose to use this $\Gamma_{n,k}$ notation instead of the classical $K_n(k)$ notation to highlight the connection with the Galois context.

Assume that we are given a group G. For any subsets X and Y of G and any positive integer n, we write X^n for the subgroup of G generated by $\{x^n, x \in X\}$ and $[X, Y]$ for the subgroup of G generated by $\{[x, y] := x^{-1}y^{-1}xy,\ (x, y) \in X \times Y\}$. As usual, for any subgroup H of G, we let $[G : H]$ denote the index of H in G.

Finally, if Γ is a topological space and if Ω is a subset of Γ, then $\overline{\Omega}$ denotes the closure of Ω in Γ. If Γ is moreover a topological group, a closed subgroup of Γ is called *topologically characteristic* when it is stable under all **continuous** group automorphisms of Γ.

2 Preliminaries on Uniform Pro-p-groups

Our main reference for this section is [8]. The goal here is to recollect all the information we need on uniform pro-p-groups to understand how they connect to the Fontaine–Mazur Conjecture via Boston's method. The reader who is already familiar with uniform pro-p-groups can skip this section and go directly to Sect. 3.

2.1 Some Basic Definitions Related to Profinite Groups

We start by recalling some basic definitions, coming from [8, Chapter 1], which are fundamental for our purpose. The first definition we make is exactly [8, Definition 1.1].

Definition 2.1 A *profinite group* is a compact Hausdorff topological group whose open subgroups form a basis of neighbourhoods of the identity.

According to [8, Proposition 1.3], this is equivalent to the usual definition of profinite groups as inverse limits of finite groups.

Definition 2.2 A profinite group G is *finitely generated* if it contains a finite subset X such that X topologically generates G, i.e., such that the subgroup of G generated by X is dense in G.

Given a profinite group, we define its Frattini subgroup, which is a key tool in the forthcoming study of uniform pro-p-groups, as follows (see [8, Definition 1.8]).

Definition 2.3 Let G be a profinite group. The *Frattini subgroup of* G is defined as $\Phi(G) := \bigcap M$, where the intersection runs over all maximal proper open subgroups of G.

2.2 Pro-p-groups: Definition and Basic Properties

Among all profinite groups, we will mainly focus on those arising as projective limits of p-groups. Such groups are called pro-p-groups and are usually defined as follows (see [8, Definition 1.10]).

Definition 2.4 A *pro-p-group* is a profinite group in which every open normal subgroup has finite index equal to a power of p.

By [8, Proposition 1.12], we know that a group is a pro-p-group if, and only if, it is isomorphic to an inverse limit of p-groups. (Recall that a *p-group* is just a finite group of p-power order.)

Finitely generated pro-p-groups are nicely characterised (among pro-p-groups) by the topology of their Frattini subgroups, as proven in [8, Proposition 1.14].

Proposition 2.5 *A pro-p-group G is finitely generated if, and only if, its Frattini subgroup $\Phi(G)$ is open in G.*

Also note that for pro-p-groups, we can fruitfully go beyond Frattini subgroups via the notion of lower p-series, defined as follows (see [8, Definition 1.15]).

Definition 2.6 The *lower p-series* of a pro-p-group G is the series $(P_i(G))_{i\geq 1}$ of topologically characteristic subgroups of G defined by $P_1(G)=G$ and: $\forall\, i\geq 1,\ P_{i+1}(G) := \overline{P_i(G)^p[P_i(G), G]}$.

The next key proposition shows that the Frattini subgroup of a pro-p-group G is actually encoded in the lower p-series of G [8, Proposition 1.13].

Proposition 2.7 *For any pro-p-group G, we have $\Phi(G) = P_2(G) = \overline{G^p[G, G]}$.*

If G is a finitely generated pro-p-group, then [8, Proposition 3.7] ensures that the quotient $G/\Phi(G)$ is a finite-dimensional $\mathbb{F}_p$-vector space. We can hence consider the following integer.

Definition 2.8 For any finitely generated pro-p-group G, we let $d(G)$ be the dimension of $G/\Phi(G)$ as $\mathbb{F}_p$-vector space:

$$d(G) := \dim_{\mathbb{F}_p} G/\Phi(G)\ .$$

According to [8, Proposition 3.7], this integer is also equal to the minimal cardinality of a (topological) generating set for G. We will see later that, in good cases, $d(G)$ is also equal to the dimension of G as a p-adic analytic group, provided that such a structure exists on G.

2.3 The (Uniform) Power of Pro-p-groups

Following [8, Definition 2.1], we introduce now the following notion of powerfulness for (pro-)p-groups.

Definition 2.9 We say that a p-group G is *powerful* when one of the following holds:

- Either p is odd, and G/G^p is an abelian group
  or
- $p = 2$, and G/G^4 is an abelian group.

We say that a pro-p-group G is *powerful* when the analogous alternative, with G^p and G^4, replaced, respectively by their closure $\overline{G^p}$ or $\overline{G^4}$ in G, holds.

According to [8, Corollary 3.3], powerful pro-p-groups can equivalently be defined as inverse limits of powerful p-groups in which all transition maps are surjective.

We are now ready to follow [8, Definition 4.1] and define our first key notion.

Definition 2.10 A *uniformly powerful pro-p-group* G (or *uniform pro-p-group*) is a powerful, finitely generated pro-p-group G such that: $\forall\ i \geq 1,\ [P_i(G)\colon P_{i+1}(G)] = [G\colon P_2(G)]$.

The assumptions in Definition 2.10 ensure in particular that $P_2(G) = \Phi(G)$ is open in G. Another exciting feature of uniform pro-p-groups is that they are automatically endowed with a structure of p-adic analytic group. The reader interested in the general framework of p-adic analytic groups should refer to Lazard's seminal paper [19], which remains to our knowledge the best reference so far on this topic. For now, we only need the following existence result (see [8, Theorem 8.32]).

Theorem 2.11 *A topological group has a structure of p-adic analytic group if, and only if, it contains an open subgroup which is a uniform pro-p-group.*

In particular, this theorem ensures that uniform pro-p-groups are always endowed with a structure of p-adic analytic group. According to [8, Theorem 8.36], their dimension as analytic groups is then equal to the integer $d(G)$ introduced in Definition 2.8.

2.4 A Key Example: Principal Congruence Subgroups that are Uniform Pro-p-groups

The goal of this subsection is to prove the following result [8, Theorem 5.2], where the principal congruence subgroups $\Gamma_{n,k}$ are those we defined at the end of Sect. 1.

Theorem 2.12 *Let $n \geq 2$ be an integer.*

(1) *If p is odd, then the first principal congruence subgroup $\Gamma_{n,1} \subset \mathrm{SL}_n(\mathbb{Z}_p)$ is a uniform pro-p-group of dimension $n^2 - 1$.*
(2) *If $p = 2$, then the second principal congruence subgroup $\Gamma_{n,2} \subset \mathrm{SL}_n(\mathbb{Z}_2)$ is a uniform pro-p-group of dimension $n^2 - 1$.*

Looking, for instance, at the case $n = 2$, we obtain that:

- For any odd prime p, $\Gamma_1 := \ker\left(\mathrm{SL}_2(\mathbb{Z}_p) \twoheadrightarrow \mathrm{SL}_2(\mathbb{F}_p)\right)$ is a uniform pro-p-group of dimension 3.
- For $p = 2$, $\Gamma_2 := \ker\left(\mathrm{SL}_2(\mathbb{Z}_2) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})\right)$ is a uniform pro-2-group of dimension 3.

Let us point out that for $n = 1$, $\Gamma_{1,m}$ is the trivial group for any integer $m \geq 1$ and any prime p. This explains why we assume $n \geq 2$ in Theorem 2.12.

Though the proof of this result is essentially given in [8, Theorem 5.2], we collect here the relevant facts and definitions it is based on to ease later reference. For convenience, once n is fixed, we write Γ_m instead of $\Gamma_{n,m}$ to avoid this cumbersome notation as often as possible. Said differently, we now fix an integer $n \geq 2$ as well as a prime p and we set:

$$\forall\, m \geq 1,\ \Gamma_m := \ker(\mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(\mathbb{Z}/p^m\mathbb{Z}))\ .$$

Lemma 2.13 *For every $m \geq 1$, the group Γ_m is a pro-p-group. More precisely, we have*

$$\Gamma_m \cong \varprojlim_{r\geq 1} \Gamma_m/\,\Gamma_{m+r},$$

with each $\Gamma_m/\,\Gamma_{m+r}$ being a finite p-group. Moreover, $\Gamma_m/\,\Gamma_{m+1}$ is isomorphic to the additive group $\mathfrak{sl}_n(\mathbb{F}_p)$ of matrices in $M_n(\mathbb{F}_p)$ with trace 0.

Proof Let m be a positive integer. The obvious projection map $\Gamma_m \to \varprojlim_{r\geq 1} \Gamma_m/\,\Gamma_{m+r}$ is injective since we have $\bigcap_{r\geq 1} \Gamma_{m+r} = \{I_n\}$. Conversely, any compatible sequence in $\varprojlim_{r\geq 1} \Gamma_m/\,\Gamma_{m+r}$ provides an element of $M_n(\mathbb{Z}_p)$ that is congruent to I_n modulo p^m. The continuity of the determinant map ensures that such an element must be of determinant 1; hence, we have the desired isomorphism.

We now show that each $\Gamma_m/\,\Gamma_{m+r}$ is a (finite) p-group. By induction on r, it suffices to prove that $\Gamma_m/\,\Gamma_{m+1}$ is a (finite) p-group. To do this, we consider the map $\varphi_m : \Gamma_m \to M_n(\mathbb{Z}_p)$ defined by $\varphi_m(x) := p^{-m}\,(x - I_n)$. One directly checks that $\varphi_m(\Gamma_{m+1})$ is contained in $M_n(p\mathbb{Z}_p)$, and thus we get a well-defined function $\overline{\varphi_m} : \Gamma_m/\,\Gamma_{m+1} \longrightarrow M_n(\mathbb{Z}_p)/M_n(p\mathbb{Z}_p) \simeq M_n(\mathbb{F}_p)$. We claim that $\overline{\varphi_m}$ is a group homomorphism for the usual additive group structure on $M_n(\mathbb{F}_p)$. Indeed, let $I_n + p^m a$ and $I_n + p^m b$ be elements of Γ_m. As $(I_n + p^m a)(I_n + p^m b) = I_n + p^m(a + b) + p^{2m}ab$, we have

$$\varphi_m\left((I_n + p^m a)(I_n + p^m b)\right) = \varphi_m(I_n + p^m(a + b) + p^{2m}ab) = a + b + p^m ab\ .$$

Since $a + b + p^m ab \equiv a + b \bmod p$, we obtain as expected that

$$\overline{\varphi_m}\left((I_n + p^m a)(I_n + p^m b)\right) = a + b \bmod p = \overline{\varphi_m}\left(I_n + p^m a\right) + \overline{\varphi_m}\left(I_n + p^m b\right)\ .$$

Now assume that $[I_n + p^m a] \in \Gamma_m/\,\Gamma_{m+1}$ lies in $\ker \overline{\varphi_m}$. This means that a is in $M_n(p\mathbb{Z}_p)$, hence that $I_n + p^m a$ belongs to Γ_{m+1}, i.e., that $[I_n + p^m a] \in \Gamma_m/\,\Gamma_{m+1}$ is trivial. All this proves that $\overline{\varphi_m}$ is injective. Since $M_n(\mathbb{F}_p)$ is a finite-dimensional $\mathbb{F}_p$-vector space, we obtain that $\Gamma_m/\,\Gamma_{m+1} \simeq \mathrm{Im}\ \overline{\varphi_m}$ is a finite p-group.

To conclude, we are left to check that the image of $\overline{\varphi_m}$ is isomorphic to $\mathfrak{sl}_n(\mathbb{F}_p)$. Given an element $I_n + p^m a$ of Γ_m, let $f_a(X) = \sum_{k=0}^{n} \alpha_k X^k \in \mathbb{Z}_p[X]$ be the characteristic polynomial of a. Then the characteristic polynomial of $-p^m a$ is equal to $f_{-p^m a}(X) = \sum_{k=0}^{n} \alpha_k (-p^m)^k X^k$. By evaluating it at 1, we get that $1 =$

$\det(I_n + p^m a) = f_{-p^m a}(1) = \sum_{k=0}^{n} \alpha_k (-p^m)^k$. Reducing this equality mod p^m shows that $\alpha_0 - 1 \in p^m \mathbb{Z}_p$, hence subtracting 1 from it and dividing the result by p^m give that

$$-\alpha_1 + \sum_{k=2}^{n} \alpha_k (-p^m)^{k-1} = 0 \,.$$

This implies in particular that $-\alpha_1 = \mathrm{tr}(a)$ is in $p^m \mathbb{Z}_p$, hence that $\mathrm{tr}(a) \equiv 0 \bmod p$, which proves that $\overline{\varphi_m}(I_n + p^m a)$ lies in $\mathfrak{sl}_n(\mathbb{F}_p)$, as required. Conversely, let us check that the image of $\overline{\varphi_m}$ is equal to $\mathfrak{sl}_n(\mathbb{F}_p)$. First recall that, since $\overline{\varphi_m}$ is injective, it is also a homomorphism of $\mathbb{F}_p$-vector spaces. We are hence left to prove that a basis of $\mathfrak{sl}_n(\mathbb{F}_p)$ is contained in $\mathrm{Im}\,\overline{\varphi_m}$. For $1 \le i, j \le n$, let e_{ij} be the matrix whose (i, j)-th entry is 1, and all other entries are 0. For $1 \le i \le n-1$, set $d_i := e_{ii} - e_{nn}$. Then an $\mathbb{F}_p$-basis for $\mathfrak{sl}_n(\mathbb{F}_p)$ is given by

$$\left\{e_{ij} : 1 \le i \ne j \le n\right\} \sqcup \{d_i : 1 \le i \le n-1\} \,.$$

As $\varphi_m(I_n + p^m e_{ij}) = e_{ij}$ for all $1 \le i \ne j \le n$ while $\varphi_m(I_n + p^m d_i) = d_i$ for all $1 \le i \le n-1$, we obtain that $\varphi_m(\Gamma_m / \Gamma_{m+1}) = \mathfrak{sl}_n(\mathbb{F}_p)$, as claimed. □

Until the end of this section, we essentially follow [8, Section 5.1], making the changes required to pass from GL_n to SL_n and filling in some missing details. First note that, for all $x \in \Gamma_m$ with $m \ge 1$, we have $x^p \in \Gamma_{m+1}$. Indeed, write $x = I_n + p^m a$ for some $a \in M_n(\mathbb{Z}_p)$. Since a and I_n commute, we have

$$x^p = (I_n + p^m a)^p = I_n + \sum_{k=1}^{p} \binom{p}{k} p^{mk} a^k \,.$$

As p divides $\binom{p}{k}$ for all $1 \le k \le p-1$, we obtain that $x^p \equiv I_n \mod p^{m+1}$, as claimed.

Following [8, Lemma 5.1], we will now see that, unless $(p, m) = (2, 1)$, the p-th power map induces a surjection $\Gamma_m \to \Gamma_{m+1}$.

Lemma 2.14 *Let p be a prime and m be a positive integer. Assume that p is odd or that $m \ge 2$. Then every element of Γ_{m+1} is the p-th power of an element of Γ_m.*

Proof Let $a \in M_n(\mathbb{Z}_p)$ be such that $\det(I_n + p^{m+1} a) = 1$. The goal is to find some $b \in M_n(\mathbb{Z}_p)$ such that $\det(I_n + p^m b) = 1$ and $(I_n + p^m b)^p = I_n + p^{m+1} a$. We will find it by successive approximations, which means that we will produce a sequence $(x_k)_{k \ge 1}$ of elements of $M_n(\mathbb{Z}_p)$ such that

$$\forall\, k \ge 1,\ \det(I_n + p^m x_k) \equiv 1 \bmod p^{m+1+k} \quad \text{and}$$

$$(I_n + p^m x_k)^p \equiv I_n + p^m a \bmod p^{m+1+k} .$$

Then $b := \lim_{k\to\infty} x_k$ will be as expected. First, assume that $I_n + p^{m+1}a \equiv (I_n + p^m x_r)^p \bmod p^{m+r+1}$. Since we have $\det(I_n + p^{m+1}a) = 1$, we already obtain that $\det(I_n + p^m x_r)^p \equiv 1 \bmod p^{m+r+1}$. Now, as we know that $\det(I_n+p^m a) \in 1+p^m\mathbb{Z}_p$, it actually follows that $\det(I_n+p^m x_r) \equiv 1 \bmod p^{m+r+1}$. This shows that we do not need to check at each step whether the determinant congruence holds when constructing the sequence $(x_k)_{k\geq 1}$ as it will automatically be true.

Let us first construct x_1. Note that, as long as m is in the supposed range, we have

$$(I_n + p^m a)^p = I_n + p^{m+1}a + \sum_{k=2}^{p} \binom{p}{k} (p^m a)^k ,$$

which is congruent to $I_n + p^{m+1}a \bmod p^{m+2}$, so we can set $x_1 := a$.

Now suppose that there exists some integer $r \geq 1$ for which we built some $x_r \in M_n(\mathbb{Z}_p)$ satisfying $I_n + p^{m+1}a \equiv (I_n + p^m x_r)^p \bmod p^{m+r+1}$. Then there exists some $c \in M_n(\mathbb{Z}_p)$ such that

$$(I_n + p^m x_r)^p = I_n + p^{m+1}a + p^{m+r+1}c .$$

Note that expanding the left-hand side of this equality provides a $\mathbb{Z}$-linear combination of powers of x_r, which shows that both a and c can be expressed as a $\mathbb{Q}_p$-linear combination of powers of x_r. In particular, this implies that any two among a, c, and x_r commute. Let us thus set

$$z := (I_n + p^m x_r)^{-(p-1)} c \text{ and } x_{r+1} := x_r - p^r z .$$

Then x_{r+1} satisfies the desired congruence. Indeed, we have

$$\begin{aligned}
(I_n + p^m x_{r+1})^p &= ((I_n + p^m x_r) - p^{m+r} z)^p \\
&= \sum_{k=0}^{p} \binom{p}{k} (I_n + p^m x_r)^{p-k} (-p^{m+r} z)^k \\
&= (I_n + p^m x_r)^p + \sum_{k=1}^{p} (-1)^k \binom{p}{k} (I_n + p^m x_r)^{p-k} p^{(m+r)k} z^k \\
&= I_n + p^{m+1}a + p^{m+r+1}c \\
&\quad + \sum_{k=1}^{p} (-1)^k \binom{p}{k} (I_n + p^m x_r)^{p-k} p^{(m+r)k} z^k ,
\end{aligned}$$

which implies that

$$(I_n + p^m x_{r+1})^p \equiv I_n + p^{m+1}a + p^{m+r+1}c - p(I_n + p^m x_r)^{p-1} p^{m+r} z \mod p^{m+r+2},$$

$$\text{i.e., } (I_n + p^m x_{r+1})^p \equiv I_n + p^{m+1}a \mod p^{m+r+2}.$$

By construction, we have $x_{r+1} - x_r = -p^r z$, and thus $b := \lim_{r\to\infty} x_r$ is well defined, which ends the proof. □

The next two results come from [8, Theorem 5.2].

Corollary 2.15 *Let p be a prime integer.*

- *If p is odd, then $P_i(\Gamma_1) = \Gamma_i$ for all $i \geq 1$.*
- *If $p = 2$, then $P_i(\Gamma_2) = \Gamma_{i+1}$ for all $i \geq 1$.*

Proof Set $\varepsilon = 0$ if p is odd and $\varepsilon = 1$ if $p = 2$. We show by induction on $i \geq 1$ that $P_i(\Gamma_{1+\varepsilon}) = \Gamma_{i+\varepsilon}$. When $i = 1$, this follows from the definition of P_1, so we can suppose that $P_i(\Gamma_{1+\varepsilon}) = \Gamma_{i+\varepsilon}$ for some $i \geq 1$. Then Lemma 2.14 ensures that $P_i(\Gamma_{1+\varepsilon})^p = \Gamma_{i+\varepsilon}^p = \Gamma_{i+1+\varepsilon}$.

We now claim that $[P_i(\Gamma_{1+\varepsilon}), \Gamma_{1+\varepsilon}] = [\Gamma_{i+\varepsilon}, \Gamma_{1+\varepsilon}] \subseteq \Gamma_{i+1+\varepsilon}$. Indeed, let $I_n + p^{i+\varepsilon}a \in \Gamma_{i+\varepsilon}$ and $I_n + p^{1+\varepsilon}b \in \Gamma_{1+\varepsilon}$. First, we have

$$(I_n + p^{i+\varepsilon}a)^{-1} = I_n + \sum_{k=1}^{\infty} (-1)^k p^{(i+\varepsilon)k} a^k \ ,$$

which is congruent to $I_n - p^{i+\varepsilon}a \mod p^{i+1+\varepsilon}$. This directly implies that

$$[I_n + p^{i+\varepsilon}a, I_n + p^{i+\varepsilon}b] \equiv I_n \mod p^{i+1+\varepsilon}$$

and hence that $[P_i(\Gamma_{1+\varepsilon}), \Gamma_{1+\varepsilon}] \subseteq \Gamma_{i+1+\varepsilon}$. Thus we have $P_i(\Gamma_{1+\varepsilon})^p [P_i(\Gamma_{1+\varepsilon}), \Gamma_{1+\varepsilon}] \subseteq \Gamma_{i+1+\varepsilon} = P_i(\Gamma_{1+\varepsilon})^p$, so the first inclusion must be an equality. As $\Gamma_{i+1+\varepsilon}$ is open (hence closed) in $\Gamma_{1+\varepsilon}$, it follows that we actually have $P_{i+1}(\Gamma_{1+\varepsilon}) = \Gamma_{i+1+\varepsilon}$, as expected. By induction on $i \geq 1$, this ends the proof. □

Theorem 2.16 *Let p be a prime integer.*

- *If p is odd, then Γ_1 is a uniform pro-p-group of dimension $n^2 - 1$.*
- *If $p = 2$, then Γ_2 is a uniform pro-2-group of dimension $n^2 - 1$.*

Proof As in the proof of Corollary 2.15, we give a uniform proof by setting $\varepsilon = 0$ if p is odd and $\varepsilon = 1$ if $p = 2$. According to Lemma 2.13, $\Gamma_{1+\varepsilon}$ is a pro-p-group; hence, Propositions 2.5 and 2.7 ensure that $\Gamma_{1+\varepsilon}$ is finitely generated if, and only if, $P_2(\Gamma_{1+\varepsilon})$ is open in $\Gamma_{1+\varepsilon}$. But we know from Corollary 2.15 that $P_2(\Gamma_{1+\varepsilon}) = \Gamma_{2+\varepsilon}$, which is open in $\Gamma_{1+\varepsilon}$, so the finite type condition is satisfied.

Now, recall that Lemma 2.14 gives $\Gamma_{1+\varepsilon}^{p} = \Gamma_{2+\varepsilon}$, while Lemma 2.13 shows that $\Gamma_{1+\varepsilon}/\Gamma_{2+\varepsilon} \cong \mathfrak{sl}_n(\mathbb{F}_p)$ is abelian: thus $\Gamma_{1+\varepsilon}$ is powerful. Similarly, Corollary 2.15 gives that $P_i(\Gamma_{1+\varepsilon}) = \Gamma_{i+\varepsilon}$, while Lemma 2.13 shows that $\Gamma_i/\Gamma_{i+1} \cong \mathfrak{sl}_n(\mathbb{F}_p)$; hence, the index condition from Definition 2.10 is satisfied by $P_i(\Gamma_{1+\varepsilon})$ for any $i \geq 1$. All this shows that $\Gamma_{1+\varepsilon}$ is uniform.

Finally, we compute the dimension using Lemma 2.13, Corollary 2.15 and Definition 2.10 as follows. From these statements, we have that $\Gamma_{1+\varepsilon}/\Phi(\Gamma_{1+\varepsilon}) = \Gamma_{1+\varepsilon}/P_2(\Gamma_{1+\varepsilon}) = \Gamma_{1+\varepsilon}/\Gamma_{2+\varepsilon} \cong \mathfrak{sl}_n(\mathbb{F}_p)$. Since $\dim_{\mathbb{F}_p} \mathfrak{sl}_n(\mathbb{F}_p) = n^2 - 1$, we are done. □

We end this section with a well-known result that will be used in Sect. 4. Its proof is as outlined in [20, Page 1271]. Let G be a finitely generated pro-p-group. For any $i \geq 1$, set $H^i(G) := H^i(G, \mathbb{F}_p)$, and let $d_p(G) := \dim_{\mathbb{F}_p} H^1(G)$ be the p-rank of G. Note that in this setting, we have $d(G) = d_p(G)$.

Theorem 2.17 *Any uniform group of dimension 1 or 2 has a quotient isomorphic to $\mathbb{Z}_p$.*

Proving this theorem requires the following result of Lazard [19, V, Proposition (2.5.7.1)].

Theorem 2.18 *Let G be a uniform group of positive dimension d. Then, for all $i \geq 1$, we have*

$$H^i(G) \cong \bigwedge^i (H^1(G)) ,$$

where the exterior product is induced by the cup product.

Proof of Theorem 2.17 Let G be a uniform pro-p-group of dimension $d \in \{1, 2\}$.

If $d = 1$, then G is isomorphic to $\mathbb{Z}_p$ so we are done.

If $d = 2$, then Theorem 2.18 implies that $\dim_{\mathbb{F}_p} H^2(G) = \dim_{\mathbb{F}_p} \bigwedge^2 H^1(G) = 1$, which means that $H^2(G)$ is actually isomorphic to $\mathbb{F}_p$. Now recall that $H^1(G) = H^1(G^{ab})$, where G^{ab} is a finitely generated $\mathbb{Z}_p$-module; hence, it can be written as

$$G^{ab} \simeq \mathbb{Z}_p^r \times \prod_{s=1}^{n} \mathbb{Z}/p^{i_s}\mathbb{Z} \tag{2.1}$$

for some nonnegative integers $r, n, i_1, \ldots, i_n$. Also recall that the short exact sequence

$$1 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\times p} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 1$$

leads to the following long exact sequence of cohomology:

$$\begin{aligned} 0 \longrightarrow H^1(G^{ab}, \mathbb{F}_p) \longrightarrow H^1(G^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\times p} H^1(G^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \\ \longrightarrow H^2(G^{ab}, \mathbb{F}_p) \longrightarrow \ldots \end{aligned}$$

If we let K and C denote, respectively, the kernel and the cokernel of $\times p$, and $d_p(K)$ and $d_p(C)$ denote their respective dimensions as $\mathbb{F}_p$-vector spaces, then what we said above directly shows that

$$d_p(C) \leq \dim_{\mathbb{F}_p}(H^2(G)) \text{ and } d_p(K) \geq d_p(G) .$$

This implies that $d_p(K) - d_p(C) \geq d_p(G) - \dim_{\mathbb{F}_p}(H^2(G)) = 1$. But (2.1) ensures that we also have $d_p(K) - d_p(C) = r = \mathrm{rk}_{\mathbb{Z}_p} G^{ab}$; thus, we obtain that $\mathrm{rk}_{\mathbb{Z}_p}(G^{ab}) \geq 1$, and G^{ab} surjects onto $\mathbb{Z}_p$. □

3 Boston's Proof of a Special Case of Fontaine–Mazur Conjecture

In this section, we study the proof of Theorem 1.5 as given by Boston in [5, 6]. It heavily relies on Lazard's extensive study of p-adic analytic Lie groups, as given in [19]. Recall in particular that Lazard defined the notion of p-saturated groups [19, IV.3.3.1] and used it to give an algebraic characterisation of p-adic analytic groups as topological groups containing a (topologically) finitely generated, open, p-saturated pro-p-group with an integer-valued filtration [19, III.3.2.2]. In [8], the notion of uniform pro-p-groups is used to transfer Lazard's work in a group-theoretic manner and to obtain an analogue characterisation of p-adic analytic groups for odd p, where uniform pro-p-groups play the same role as p-saturated pro-p-groups with integer-valued filtration do in Lazard's statement [8, Page 81]. Note that in [5], Boston used Lazard's terminology (*p-saturated with integer values*, as defined in [19, II.1.2.10 and III.3.3.1]) instead of the *uniform group* one. We will stick to the uniform group formulation in the sequel, but let us recall here the main statement of [5] (namely Theorem 1), as originally stated.

Theorem 3.1 (Boston) *Let K be a normal extension of prime degree $\ell \neq p$ of a number field F such that $p \nmid h(F)$, the class number of F. Then there is no infinite everywhere unramified Galois pro-p-extension L of K such that L is Galois over F and* $\mathrm{Gal}(L/K)$ *is p-saturated with integer values.*

This result gives some evidence for Conjecture 1.3 in a special case. Using the strength of fixed-point-free automorphisms, Boston generalised this result to the case of cyclic extensions L/K, where $[L : K]$ is not necessarily a prime, see [6, Theorem 1]. To do this, he introduced the class of *self-similar* groups (as defined below), which contains the class of uniform groups, and he showed that, under some condition $H(G, n)$ related to fixed-point-free automorphisms (which is conjectured to always hold), Theorem 3.1 carries over for finite cyclic extensions of degree co-prime to p, with 'uniform' replaced by 'self-similar'. Let us define the new notions aforementioned.

Definition 3.2 A pro-p-group G is *self-similar* when there exists a filtration by open, characteristic subgroups $G = G_1 \supseteq G_2 \supseteq \cdots$ such that G_i/G_{i+1} is abelian for all $i \geq 1$ and $\bigcap G_i = \{1\}$, together with a family of group isomorphisms

$$\phi_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$$

which commute with every continuous automorphism of G.

Note that the commutativity of all quotients G_i/G_{i+1} ensures that the second condition must only be checked for outer automorphisms of G. Also note that Definition 3.2 implies that a non-trivial self-similar group is always infinite, since $\lim_{i\to\infty} |G/G_i| = \lim_{i\to\infty} |G/G_2|^{i-1} = \infty$.

The next proposition justifies the relevance of this notion in Boston's work.

Proposition 3.3 *Any uniform group is a self-similar group.*

Proof Let G be a uniform pro-p-group. For any $i \geq 1$, set $G_i := P_i$, where P_i is as in Definition 2.6. Then $(G_i)_{i\geq 1}$ is a filtration as in Definition 3.2 and the map $[x \mapsto x^p]$ induces group isomorphisms $\varphi_i : G_{i-1}/G_i \to G_i/G_{i+1}$ that commute with any continuous automorphism of G; hence, G is indeed a self-similar group. □

We now make explicit the aforementioned condition $H(G, n)$ defined by Boston in [6, Definition 2].

Definition 3.4 Let G be a pro-p-group and n be a positive integer. We say that $H(G, n)$ *holds* when there is a function of n that is an upper bound for the derived length of every finite quotient of G that admits a fixed-point-free automorphism of order n.

We already mentioned above that $H(G, n)$ is conjectured to hold for any pro-p-group G and any integer $n \geq 1$. It is known for uniform groups thanks to [8, p. 52] and [26], as well as in few other cases (see Shalev's work [26] for a description of such cases). This means in particular that for a uniform group G, there is a (uniform) bound on the derived length of the quotients G/P_i for $i \geq 1$.

We can now state the generalisation of Theorem 3.1 as proven in [6, Theorem 1].

Theorem 3.5 (Boston) *Let F be a number field such that p does not divide the class number of F. Let K be a cyclic extension of F of degree $n \geq 2$ co-prime to p. Then there is no infinite, everywhere unramified, Galois pro-p-extension L of K such that L is Galois over F and $\mathrm{Gal}(L/K)$ is self-similar and satisfies the property $H(\mathrm{Gal}(L/K), n)$ as stated in Definition 3.4.*

Before proving this theorem, we recall a classical result of Schur and Zassenhaus [23, Chapter 4].

Theorem 3.6 (Schur–Zassenhaus) *Let $1 \to \Gamma \to \mathcal{G} \to \mathcal{G}/\Gamma \to 1$ be a short exact sequence of profinite groups, with Γ a finitely generated pro-p-group and $\mathcal{G}/\Gamma$ of finite order co-prime to p. Then $\mathcal{G}$ contains a subgroup Δ_0 isomorphic to*

the quotient $\Delta := \mathcal{G}/\Gamma$*, and* Δ_0 *is unique up to conjugation in* $\mathcal{G}$*. In particular,* $\mathcal{G}$ *is isomorphic to a semi-direct product of* Δ *and* Γ*:* $\mathcal{G} = \Gamma \rtimes \Delta_0 \cong \Gamma \rtimes \Delta$.

Proof of Theorem 3.5 To make things more comfortable to the reader, we address here the case of uniform groups: let us mention that the general case of self-similar groups can be proven along the same lines, as done in [6]. Suppose by contradiction that there exists an infinite, everywhere unramified, Galois pro-p-extension L of K such that L/F is Galois and $G := \mathrm{Gal}(L/K)$ is uniform and satisfies condition $H(G, n)$, where $n := [K : F]$. By the Schur–Zassenhaus theorem, the following extension splits:

$$1 \longrightarrow G \to \mathrm{Gal}(L/F) \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1\ .$$

Let us pick an element σ of $\mathrm{Gal}(L/F)$ that lifts a generator of the cyclic group $\mathrm{Gal}(K/F)$ under the splitting above. As G is a normal subgroup of $\mathrm{Gal}(L/F)$, σ induces an action by conjugation on G. Now, since G is a uniform group, we can consider its filtration by the characteristic subgroups P_i given in Definition 2.6. Each P_i is preserved under the action of σ (as it is a characteristic subgroup of G); hence, we get an action by conjugation of σ on each quotient G/P_i.

Suppose that, for all $i \geq 1$, σ has no non-trivial fixed point in G/P_i. As G satisfies $H(G, n)$, there is a uniform bound on the derived length of each of the quotients G/P_i as i goes to ∞. Such a bound cannot exist since a repeated use of the finiteness of class number shows that the maximal unramified pro-p-extension of any fixed derived length must be a finite extension.

This shows that there exists a positive integer i such that the action of σ on G/P_i has a non-trivial fixed point. Assume that i is minimal for this property and let τ be a non-trivial fixed point of σ in G/P_i. By minimality of i, τ must map to the identity element in G/P_{i-1}, i.e., lives in P_{i-1}/P_i, since the action of σ is compatible with $P_{i-1} \supseteq P_i$ and $G/P_i \twoheadrightarrow G/P_{i-1}$. Now recall that Proposition 3.3 ensures that the isomorphism $\phi_{i-1} : P_{i-2}/P_{i-1} \to P_{i-1}/P_i$ is σ-equivariant; hence, $\phi_{i-1}^{-1}(\tau)$ should define a non-trivial fixed point for σ in P_{i-2}/P_{i-1}, which contradicts the minimality of i if $i \geq 3$.

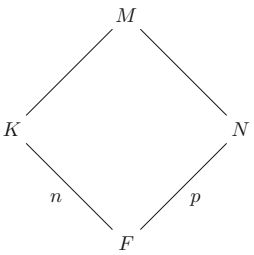
If $i = 2$, then our assumption is that the action by conjugation of σ on G/P_2 has a non-trivial fixed point. By definition, we have $P_2 = \overline{G^p[G, G]}$; hence, G/P_2 is naturally an $\mathbb{F}_p$-vector space. Said differently, it defines a representation over a field of characteristic p of the group $\langle\sigma\rangle$ generated by σ. As this group is, by definition of σ, of cardinality n, which is co-prime to p, we can apply Maschke's theorem to decompose G/P_2 as a direct sum of irreducible representations of $\langle\sigma\rangle$ over $\mathbb{F}_p$. As τ is fixed under the action of σ, this decomposition can be written as $G/P_2 = \mathbb{F}_p\tau \oplus W$ for some representation W of $\langle\sigma\rangle$ over $\mathbb{F}_p$.

The direct sum decomposition ensures that W also defines a subgroup and a quotient of G/P_2. Hence, we can define an extension M of K such that $\mathrm{Gal}(M/K) = \langle\tau\rangle$: we just let M be the fixed field (in L) of W over K. The field extension M/K is then an abelian extension of prime degree p, and we have a tower of fields of the form $F \subset K \subset M$.

We claim that there exists a cyclic extension of degree p over F that is contained in M. Indeed, $\mathrm{Gal}(K/F) \simeq \langle\sigma\rangle$ acts on $\mathrm{Gal}(M/K)$ by conjugation. Since K/F is assumed to be a normal extension, $\mathrm{Gal}(M/K)$ must be a normal subgroup of $\mathrm{Gal}(M/F)$. We can hence apply the Schur–Zassenhaus theorem to write $\mathrm{Gal}(M/F)$ as a semi-direct product of the following form:

$$\mathrm{Gal}(M/F) \simeq \mathrm{Gal}(M/K) \rtimes \mathrm{Gal}(K/F)\,. \tag{3.1}$$

Since τ is fixed under σ, the action of σ on $\mathrm{Gal}(M/K) = \langle\tau\rangle$ is trivial; hence, $\mathrm{Gal}(K/F)$ is also normal in $\mathrm{Gal}(M/F)$, which turns (3.1) into a direct product of the two groups appearing on the right-hand side. As $\mathrm{Gal}(M/K)$ is of order p while $\mathrm{Gal}(K/F)$ is of order n, with n and p being co-prime, we can conclude that there exists a Galois extension N of F of degree p (hence cyclic) in M.



As M/K is unramified, so is N/F, which contradicts the fact that p is co-prime to $h(F)$. In all cases ($i \geq 3$ or $i = 2$), we have a contradiction: this proves that there exists no pro-p-extension L/K that is everywhere unramified and has for Galois group a uniform group. □

4 Some Results on the Tame Fontaine–Mazur Conjecture and Its Uniform Version

For this section, we will mostly refer to [13, 14, 22]. The goal here is to present some results attached to the Tame Fontaine–Mazur Conjecture (TFMC for short) and its Uniform version (TFMC-U for short), as well as related questions on which some of the authors are currently working.

4.1 Motivation and Background

We start by recalling some statements at the core of this section, namely the two versions of the Fontaine–Mazur Conjecture mentioned above, which will be proven to be equivalent to each other (see Sect. 4.3 below).

As explained in Sect. 1, TFMC is an analogue of Conjecture 1.3 for finitely and tamely ramified p-adic representations. Since tame representations are automatically potentially semi-stable (thanks to a theorem of Grothendieck [25, Appendix]), the Fontaine–Mazur Conjecture must imply (under some standard conjectures in algebraic geometry, see [18] for further details) that the following statement holds [10, Conjecture 5a].

Conjecture 4.1 (Tame Fontaine–Mazur Conjecture) Let p be a prime integer and K be a number field. Let S be a finite set of places of K that are all co-prime to p and let K_S be the maximal pro-p-extension of K that is unramified outside S. Set $G_S := \mathrm{Gal}(K_S/K)$. Then, for any positive integer n, any continuous Galois representation $\rho : G_S \to GL_n(\mathbb{Q}_p)$ has finite image.

In Sect. 4.2, we will see that TFMC for $n = 1$ comes from class field theory. When $n > 1$, this conjecture appears so far completely out of reach in general, though some preliminary evidence exists, as those given in [6, 13, 28]. When $K = \mathbb{Q}$ and $n = 2$, we already pointed out in Sect. 1 that the main contributions for now are due to Kisin [17] and Emerton [9], both using different methods from those developed in this chapter.

Recall that Theorem 2.11 claims that any finitely generated p-adic analytic group contains a uniform open subgroup. Moreover, Theorem 2.17 asserts that any uniform group of dimension 1 or 2 admits a quotient isomorphic to $\mathbb{Z}_p$. We can hence rephrase TFMC as follows.

Conjecture 4.2 (Tame Fontaine–Mazur Conjecture—uniform version for (K, d)) Let K be a number field and Γ be a uniform pro-p-group of dimension $d > 2$ (hence infinite). Then there is no finitely and tamely ramified Galois extension of K whose Galois group is isomorphic to Γ.

In the light of Conjectures 1.6 and 1.7 for $n = 2$, we would like to highlight the major contribution of Hajir and Maire in [14] before we go further. Among several key results, they proved an analogue of Theorem 1.5 for odd p, using purely group-theoretic and arithmetic methods such as the effect of a semi-simple cyclic action with fixed points on the group structure, the rigidity of uniform groups, the existence of Minkowski units, some arithmetic properties of Galois groups, etc.

To precise this, we need to introduce some notation and definitions, following [14, 1.2]. We keep the notations of Conjecture 4.1 and we let T be an auxiliary finite set of places of K such that $T \cap S = \emptyset$. Define K_S^T as the maximal pro-p-extension of K that is unramified outside S and in which any place in T splits completely, and let $G_S^T := \mathrm{Gal}(K_S^T/K)$ be the corresponding Galois group. Note that K_S^T is a subfield of K_S while G_S^T is a quotient of G_S and that $K_S^\emptyset = K_S$.

We can now state one of the main results of Hajir–Maire [14, Section 1.2, Theorem], which is also a special case of more general statements proven in [14, Section 2].

Theorem 4.3 (Hajir-Maire) *Let K/k be a quadratic extension with Galois group $\langle\sigma\rangle$. Assume that the odd prime p does not divide the class number of k. Suppose*

that for any finite set Σ of places of k all co-prime to p, there is no continuous Galois representation $G_\Sigma(k) \twoheadrightarrow \Gamma_{2,1}$. Then there exist infinitely many disjoint finite sets S and T of primes of K such that any place of S is prime to p, $|S|$ is arbitrarily large and

(1) *G_S^T is infinite.*
(2) *$G_S^T/\Phi(G_S^T)$ has $|S|$ independent fixed points under the action of σ.*
(3) *There is no continuous Galois representation $\rho : G_S^T \twoheadrightarrow \Gamma_{2,1}$ with $\left(K_S^T\right)^{\ker\rho}$ Galois over k.*

Note that the last assertion is actually a strengthened notion of uniformness (called σ-uniformness) that gives further conditions on the action of σ on G_S^T, see [14, Definition 1.1]. Let us also mention that, although it is not obvious at first sight, this result is actually tightly connected to the Fontaine-Mazur Conjecture for uniform groups of constant type for order 2 automorphisms. The reader interested in more details on this topic should read [14, Corollary 2.6].

4.2 Class Field Theory Implies Tame Fontaine-Mazur Conjecture for $n = 1$

The goal of this section is to prove the tame Fontaine-Mazur Conjecture (Conjecture 1.6) for $n = 1$. This is certainly known to experts in the field, but beginners will find it useful to have a reference where this claim is fully proven; hence, we now give a detailed proof of the following statement. Note that it holds when $\mathbb{Q}_p$ is replaced by any p-adic field L, but we chose to stick to the case of p-adic representations to stay in the framework we used so far.

Theorem 4.4 (TFMC for $n = 1$) *Let K be a number field and p be a rational prime. Let S be a finite set of places of K in which no place has residue characteristic p. Let K_S denote the maximal pro-p-extension of K that is unramified outside S and let $G_S := \mathrm{Gal}(K_S/K)$ be its Galois group. Then every continuous group homomorphism*

$$\chi : G_S \to \mathrm{GL}_1(\mathbb{Q}_p) = \mathbb{Q}_p^\times$$

has finite image.

Proof Since G_S is a compact group (as it is a pro-p-group), its image under the continuous map χ must be a compact subgroup of $\mathbb{Q}_p^\times$; hence, it lands into $\mathbb{Z}_p^\times$. Also note that, since $\mathbb{Q}_p^\times$ is an abelian group, χ must factor through the abelianisation G_S^{ab} of G_S, which motivates the connection with class field theory. The latter provides indeed a canonical group homomorphism with dense image (called Artin reciprocity law)

$$\rho : \mathbb{A}_K^\times / K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} ,$$

which becomes an isomorphism when $\mathbb{A}_K^\times / K^\times$ is replaced by its profinite completion. We are hence reduced to show that the composite group homomorphism $\tilde{\chi} := \chi \circ \rho : \mathbb{A}_K^\times / K^\times \to \mathbb{Z}_p^\times$ has finite image.

Saying that χ is unramified outside S means that χ is trivial on inertia groups for places outside S; hence, it also holds for $\tilde{\chi}$. Now let v be a place in S. We need to distinguish between the finite and Archimedean cases as follows.

If v is a finite place, then the inertia group at v corresponds to the subgroup of $\mathbb{A}_K^\times$ that is trivial at all places outside of v and equal to the subgroup $\mathcal{O}_{K_v}^\times$ of $K_v^\times$ at v. As all places in S are co-prime to p, the group of 1-units in $\mathcal{O}_{K_v}^\times$ is a pro-ℓ-group for some rational prime $\ell \neq p$. But the 1-units of $\mathbb{Z}_p^\times$ form a pro-p-group, and any continuous group homomorphism from a pro-ℓ-group into a pro-p-group is necessarily trivial: the image by $\tilde{\chi}$ of $\mathcal{O}_{K_v}^\times$ must hence be finite. Letting S^∞ denote the subset of finite places in S, we have proven that $\tilde{\chi}\left(\prod_{v\in S^\infty} \mathcal{O}_{K_v}^\times\right)$ is finite.

Let us now study what happens on $\prod_{v\in S^\infty} \varpi_v^{\mathbb{Z}}$, where ϖ_v denotes a uniformising element of $\mathcal{O}_v$. First note that the product is actually a restricted product, which means only finitely many places are such that ϖ_v has a non-trivial image in $\mathbb{Z}_p^\times$. Also recall that any element $x = (\varpi_v^{e_v})_{v\in S^\infty}$ of $\prod_{v\in S^\infty} \varpi_v^{\mathbb{Z}}$ defines a fractional ideal $\mathfrak{a}_x = \prod_v \mathfrak{p}_v^{e_v}$ of K, where $\mathfrak{p}_v$ denotes the prime ideal of $\mathcal{O}_K$ that corresponds to v. (This is well defined as only finitely many e_v can be non-zero.) Let h denote the class number of K: then $\mathfrak{a}_x^h$ is a non-zero principal ideal of $\mathcal{O}_K$ (by the definition of h), So $x \mod K^\times$ must have finite order dividing h. This shows that the quotient of $\prod_{v\in S^\infty} \varpi_v^{\mathbb{Z}}$ by the diagonal copy of $K^\times$ (in $\mathbb{A}_K^\times / K^\times$) has finite exponent dividing h; hence, its image by $\tilde{\chi}$ must satisfy the same condition in $\mathbb{Q}_p^\times$. As $\mathbb{Q}_p^\times$ contains finitely many elements of order dividing h, we can conclude that this image by $\tilde{\chi}$ is finite.

Finally, assume that v is an Archimedean place in S. Since $\mathbb{Z}_p^\times$ is a totally disconnected space, the identity component of $K_v^\times$ (which is either $\mathbb{R}_{>0}$ if v is real, or $\mathbb{C}^\times$ is v is complex) has trivial image under the continuous group homomorphism $\tilde{\chi}$. Letting S_∞ denote the set of Archimedean places in S, we are left to see that $\prod_{v\in S_\infty \text{ real}} \mathbb{R}^\times/\mathbb{R}_{>0}$ has finite image under $\tilde{\chi}$, which is straightforward as S and $\mathbb{R}^\times/\mathbb{R}_{>0} \simeq \mathbb{Z}/2\mathbb{Z}$ are finite sets, so the proof is complete. □