Iwasawa algebras for p-adic Lie groups and Galois groups

Jishnu Ray

NNT : 2018SACLS189

THÈSE DE DOCTORAT

de

L'Université Paris-Saclay

École doctorale de mathématiques Hadamard (EDMH, ED 574)

Établissement d'inscription : Université Paris-Sud

Établissement d'accueil : Université Paris-Sud

Laboratoire d'accueil : Laboratoire de mathématiques d'Orsay, UMR 8628 CNRS

Spécialité de doctorat : Mathématiques fondamentales

Thèse présentée et soutenue à Cachan, le 02 Juillet 2018, par

Jishnu RAY

Iwasawa algebras of p-adic Lie groups and Galois groups

Après avis des rapporteurs : Ralph Greenberg (University of Washington Seattle)
Peter Schneider (Universität Münster)

Jury de soutenance :

Laurent CLOZEL	(Université Paris-Sud) Directeur de thèse
Ariane Mézard	(Sorbonne Université) Directrice de thèse
Christophe Breuil	(Université Paris-Sud) Examinateur
Gabriel Dospinescu	(Ecole Normale Supérieure de Lyon) Examinateur
Christine Huyghe	(Université de Strasbourg) Examinateur
Peter Schneider	(Universität Münster) Rapporteur

This thesis is dedicated to ...
still searching.

université PARIS-SACLAY | École doctorale de mathématiques Hadamard (EDMH)

Titre : Algèbres d'Iwasawa pour les groupes de Lie p-adiques et les groupes de Galois.

Mots Clefs : Algèbre d'Iwasawa, représentations p-adiques, représentations galoisiennes, corps de nombres p-rationnels.

Résumé : Un outil clé dans la théorie des représentations p-adiques est l'algèbre d'Iwasawa, construit par Iwasawa pour étudier les nombres de classes d'une tour de corps de nombres. Pour un nombre premier p, l'algèbre d'Iwasawa d'un groupe de Lie p-adique G, est l'algèbre de groupe G complétée non-commutative. C'est aussi l'algèbre des mesures p-adiques sur G. Les objets provenant de groupes semi-simples, simplement connectés ont des présentations explicites comme la présentation par Serre des algèbres semi-simples et la présentation de groupe de Chevalley par Steinberg. Dans la partie I, nous donnons une description explicite des certaines algèbres d'Iwasawa. Nous trouvons une présentation explicite (par générateurs et relations) de l'algèbre d'Iwasawa pour le sous-groupe de congruence principal de tout groupe de Chevalley semi-simple, scindé et simplement connexe sur $\mathbb{Z}_p$. Nous étendons également la méthode pour l'algèbre d'Iwasawa du sous-groupe pro-p Iwahori de $GL(n, \mathbb{Z}_p)$. Motivé par le changement de base entre les algèbres d'Iwasawa sur une extension de $\mathbb{Q}_p$ nous étudions les représentations p-adique globalement analytiques au sens d'Emerton. Nous fournissons également des résultats concernant la représentation de série principale globalement analytique sous l'action du sous-groupe pro-p Iwahori de $GL(n, \mathbb{Z}_p)$ et déterminons la condition d'irréductibilité. Dans la partie II, nous faisons des expériences numériques en utilisant SAGE pour confirmer heuristiquement la conjecture de Greenberg sur la p-rationalité affirmant l'existence de corps de nombres "p-rationnels" ayant des groupes de Galois $(\mathbb{Z}/2\mathbb{Z})^t$. Les corps p-rationnels sont des corps de nombres algébriques dont la cohomologie galoisienne est particulièrement simple. Ils sont utilisés pour construire des représentations galoisiennes ayant des images ouvertes. En généralisant le travail de Greenberg, nous construisons de nouvelles représentations galoisiennes du groupe de Galois absolu de $\mathbb{Q}$ ayant des images ouvertes dans des groupes réductifs sur $\mathbb{Z}_p$ (ex $GL(n, \mathbb{Z}_p), SL(n, \mathbb{Z}_p), SO(n, \mathbb{Z}_p), Sp(2n, \mathbb{Z}_p)$). Nous prouvons des résultats qui montrent l'existence d'extensions de Lie p-adiques de $\mathbb{Q}$ où le groupe de Galois correspond à une certaine algèbre de Lie p-adique (par exemple $\mathfrak{sl}(n), \mathfrak{so}(n), \mathfrak{sp}(2n)$). Cela répond au problème classique de Galois inverse pour l'algèbre de Lie simple p-adique.

Title : Iwasawa algebras of p-adic Lie groups and Galois groups.

Keys words : Iwasawa algebras, p-adic representations, Galois representations, p-rational fields.

Abstract : A key tool in p-adic representation theory is the Iwasawa algebra, originally constructed by Iwasawa in 1960's to study the class groups of number fields. Since then, it appeared in varied settings such as Lazard's work on p-adic Lie groups and Fontaine's work on local Galois representations. For a prime p, the Iwasawa algebra of a p-adic Lie group G, is a non-commutative completed group algebra of G which is also the algebra of p-adic measures on G. It is a general principle that objects coming from semi-simple, simply connected (split) groups have explicit presentations like Serre's presentation of semi-simple algebras and Steinberg's presentation of Chevalley groups. In Part I, we lay the foundation by giving an explicit description of certain Iwasawa algebras. We first find an explicit presentation (by generators and relations) of the Iwasawa algebra for the principal congruence subgroup of any semi-simple, simply connected Chevalley group over $\mathbb{Z}_p$. Furthermore, we extend the method to give a set of generators and relations for the Iwasawa algebra of the pro-p Iwahori subgroup of $GL(n, \mathbb{Z}_p)$. The base change map between the Iwasawa algebras over an extension of $\mathbb{Q}_p$ motivates us to study the globally analytic p-adic representations following Emerton's work. We also provide results concerning the globally analytic induced principal series representation under the action of the pro-p Iwahori subgroup of $GL(n, \mathbb{Z}_p)$ and determine its condition of irreducibility. In Part II, we do numerical experiments using a computer algebra system SAGE which give heuristic support to Greenberg's p-rationality conjecture affirming the existence of "p-rational" number fields with Galois groups $(\mathbb{Z}/2\mathbb{Z})^t$. The p-rational fields are algebraic number fields whose Galois cohomology is particularly simple and they offer ways of constructing Galois representations with big open images. We go beyond Greenberg's work and construct new Galois representations of the absolute Galois group of $\mathbb{Q}$ with big open images in reductive groups over $\mathbb{Z}_p$ (ex. $GL(n, \mathbb{Z}_p), SL(n, \mathbb{Z}_p), SO(n, \mathbb{Z}_p), Sp(2n, \mathbb{Z}_p)$). We are proving results which show the existence of p-adic Lie extensions of $\mathbb{Q}$ where the Galois group corresponds to a certain specific p-adic Lie algebra (ex. $\mathfrak{sl}(n), \mathfrak{so}(n), \mathfrak{sp}(2n)$). This relates our work with a more general and classical inverse Galois problem for p-adic Lie extensions.

Acknowledgements

I express the deepest gratitude to my PhD thesis supervisors Laurent Clozel and Ariane Mézard. I am indebted to Clozel not only for his time and extreme patience but also for his intellectual contributions in developing my research. I thank him for investing his valuable time in going through my proofs very carefully and suggesting several possible developments. Essentially under his strong guidance I am able to learn mathematics and progress in my research during the doctoral years.

I am very grateful to Ariane Mézard for her constant encouragement and emotional support during challenging times of my thesis. Without her expertise and co-ordination in organizing study groups, Part II of this thesis would not have existed. I also wish to sincerely thank her for providing me the opportunity to meet her every week and discuss about the progress of my research and my thesis. She also organized possible collaborations with me, Christophe Cornut and Razvan Barbulescu which culminated in generalizing Ralph Greenberg's work on p-rational fields.

I thank Ralph Greenberg for visiting Institut de Mathématiques de Jussieu - Paris Rive Gauche, for providing his valuable insights on p-rational fields and also for being one of the reporters of my thesis. I sincerely thank George Gras, Christian Maire, A. Chazad Movahhedi, Bill Allombert for their interest in our joint work with Razvan concerning p-rational fields. Alongside, I also thank my collaborators Cornut and Barbulescu. Thanks are due to Marie-France Vignéras for her discussion with Cornut concerning our joint work. I would like to thank Konstantin Ardakov for appreciating my research and encouraging me to improve in my results in Part I. We had numerous email exchanges and Ardakov took the time of going through my results, answering my questions, and suggesting possible ways of generalizing them.

I thank Christophe Breuil, Gabriel Dospinescu, Christine Huyghe, Peter Schneider (reporter of my thesis) for agreeing to be a part of the jury. My sincere gratefulness goes to Guy Henniart for his constant help and support on several occasions throughout my master and doctoral years at the Université Paris Sud and also for listening to the results of my thesis. Many thanks to Agnès David, Tobias Schmidt, Volker Heiermann, Otmar Venjakob, Bruno Kahn for inviting me to their seminars and providing me the opportunity to speak on the results of my thesis to their department's faculty members. I am deeply grateful to Sarah Zerbes, Minhyong Kim, Ulrike Tillman, Sir Andrew Wiles for listening to the results of my thesis over Skype and for asking several questions. I am also grateful to Matthias Strauch for a discussion on the topic of section 3 of my thesis and giving me references. To Sujatha Ramdorai, Lior Silberman, many thanks for their interest in my work and providing me future possibilities to carry on my research at the University of British Columbia. Thanks also to Fred Diamond, Toby Gee and Florian Herzig for supporting my research.

Thanks to all the department members of the Université Paris Sud, in particular, to Gaëtan Chenevier and Olivier Fouquet for their advanced master 2 courses. I also acknowledge the financial support from Ecole Doctorale de Mathématique Hadamard (EDMH) throughout my thesis work. Many thanks to Frédéric Paulin for his guidance and monitoring the progress of my research. I express my gratitude to B. Sury for his good wishes, encouragement and guidance since my Bachelor studies at the Indian Statistical Institute (ISI). I wish to thank all the faculty members of Indian Statistical Institute, Tata Institute of Fundamental Research, University of Padova, in particular to Siva Atreya, Najmuddin Fakhruddin (my VSRP advisor at Tata Institute), T.N. Venkataramana, M. A. Garuti (my mentor at the University of Padova) for their support. During my ALGANT International master first year at the University of Padova under the Erasmus Mundus European program, Garuti encouraged me to pursue the field of my interest at the University of Paris-Sud in the second year and I am truly grateful to him for arranging it. I also thank Nirupam Kar for teaching me mathematics during my 11-th and 12-th grade and preparing me for the ISI entrance exam.

Thanks to my seniors Jyoti Prakash Saha, Sourav Ghosh, Santosh Nadimpalli and to my friends Ammar Yasir Kiliç, Mai Tien Long, Jinbo Ren for all the discussions we had. I am also grateful to late Jacques Gallay (Université Paris-Sud) for teaching me basic French and for the wonderful moments that we spent together during his last few years. I also thank Jacques' wife Ines Gallay (CNRS and Université Paris-Sud) for her care, support and for providing accommodation to me and my mother during the entire period of my thesis. Finally, but not least, I want to thank my

parents. My father kindled mathematical interest in me during my early school years with number theoretic problems and puzzles. I am also indebted to my mother for her love and affection. Thank you both for your constant support through the ups and downs of my academic career. Your confidence in me has enhanced my ability to get through them all and succeed in the end.

Table of Contents

Introduction (in French)

Dans cette section, je présente les résultats de ma thèse en géométrie arithmétique, théorie d'Iwasawa, théorie des représentations galoisiennes, dans le cadre du programme de Langlands p-adique. La partie I de ma thèse contient des résultats du côté théorie des représentations du programme de Langlands tandis que la partie II contient des résultats du côté Galois. Les résultats peuvent être divisés en cinq sections (0.1 - 0.5).

0.1 Présentation explicite de l'algèbre d'Iwasawa pour le premier noyau de congruence

Soit p un nombre premier. La première branche de ma recherche se concentre sur la description explicite de l'algèbre d'Iwasawa d'un groupe de Lie p-adique G sur $\mathbb{Z}_p$. La théorie d'Iwasawa trouve son origine dans le travail révolutionaire d'Iwasawa dans les année 1960 concernant la croissance des nombres de classes des corps de nombres. L'algèbre d'Iwasawa d'un groupe G, notée $\Lambda(G)$ ou $\mathbb{Z}_p[[G]]$, est définie par

$$\Lambda(G) := \varprojlim_{H} \mathbb{Z}_p[G/H]$$

où H décrit les sous-groupes ouverts de G. L'algèbre de Iwasawa joue un rôle dans différentes branches des mathématiques. Par exemple, à l'aide de l'algèbre d'Iwasawa Lazard a étudié les groupes de Lie analytiques p-adiques ([Laz65]). Il y définit la notion de groupes p-saturés et caractérise algébriquement la notion de groupes analytiques p -adiques comme groupes topologiques contenant un groupe p-saturé admettant une filtration entière.

Dans le cadre de la théorie des représentations locales, les algèbres d'Iwasawa interviennent via les modules de Fontaine. Fontaine ([Fon90]), décrit une équivalence de catégories entre la catégorie des représentations $\mathbb{Q}_p$-linéaires du groupe de Galois absolu de $\mathbb{Q}$ et la catégorie des (φ, Γ) - modules étales sur un anneau. Cette équivalence de catégories est utilisée en autre par Colmez et d'autres pour prouver la correspondance de Langlands p-adique pour $GL_2(\mathbb{Q}_p)$ [CDP14].

Les algèbres d'Iwasawa jouent également un rôle essentiel en théorie p -adique des représentations de $G(\mathbb{Q}_p)$, les $\mathbb{Q}_p$-points d'un groupe réductif G sur $\mathbb{Q}_p$, initialement étudiée par Schneider/Teitelbaum et Emerton. Schneider et Teitelbaum ont traduit l'étude de la théorie des représentations d'un espace de Banach p -adique (sur une extension finie K de $\mathbb{Q}_p$) en l'étude de modules sur les algèbres d'Iwasawa.

Enfin, du point de vue de la théorie d'Iwasawa, il est crucial d'en comprendre la structure. Il a semblé que la description explicite, par générateurs et relations, de ces algèbres était jusqu'à présent inaccessible. Cependant, la présentation de Serre des algèbres semi-simples et la présentation de Steinberg des groupes de Chevalley [Ser87], [Ste67] nous font croire que les objets provenant de groupes déployés semi-simples ont une présentation explicite.

Le résultat principal de la section 1 est de donner une présentation explicite, par générateurs et relations, de l'algèbre d'Iwasawa pour le sous-groupe $G(1) := \ker(G(\mathbb{Z}_p) \to G(\mathbb{F}_p))$ de tout groupe de Chevalley G semi-simple, scindé, simplement connexe sur $\mathbb{Z}_p$ (Théorème 0.1, 0.2). Cela généralise un travail précédent de Clozel pour $G = SL_2(\mathbb{Z}_p)$ (cf. [Clo11]).

Soit p un nombre premier impair. Lazard définit, pour un groupe H localement $\mathbb{Q}_p$-analytique, une fonction, appelée p-valuation, $\omega : H - \{1\} \to (\frac{1}{p-1}, \infty) \subset \mathbb{R}$ satisfaisant certaines propriétés (cf. [Laz65] III. 2.1.2). Soit d la dimension de H (en tant que variété analytique locale). Lazard définit également une base ordonnée de H par rapport à la p-valuation ω. Il s'agit d'une séquence ordonnée d'éléments $h_1, ..., h_d \in H - \{1\}$ tels que les conditions suivantes soient satisfaites :

1. $\psi : \mathbb{Z}_p \xrightarrow{\sim} H, (x_1, ..., x_d) \longmapsto h_1^{x_1} \cdots h_d^{x_d}$,

2. $\omega(h_1^{x_1} \cdots h_d^{x_d}) = \min_{1 \leq i \leq d}(\omega(h_i) + val_p(x_i))$,

où l'application ψ est un homéomorphisme.

Soit G un groupe réductif déployé sur $\mathbb{Z}_p$, T un tore maximal déployé en G, $M = X^*(T)$ son groupe de caractères,

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \oplus_{\alpha\in\Phi}\mathfrak{g}_\alpha$$

la décomposition en poids pour l'action de T sur $\mathfrak{g} = \mathrm{Lie}(G)$. Nous notons $\Pi \subset \Phi$ une base du système de racines $\Phi \subset M$, Φ^- (Φ^+) l'ensemble des racines négatives (resp. positives) et pour chaque $\delta \in \Pi$, X_δ une $\mathbb{Z}_p$-base de $\mathfrak{g}_\delta$. Nous développons $(X_\delta)_{\delta\in\Pi}$ en un système de Chevalley $(X_\alpha)_{\alpha\in\Phi}$ de G [GP11, XXIII 6.2]. La p-valuation ω sur $G(1)$ est $\omega(x) = k$ si x est dans le k-ème noyau de congruence mais pas dans le $(k+1)$ -ème.

Ainsi, nous trouvons une base ordonnée de $G(1)$.

Théorème 0.1 (voir Théorème 1.9 de la section 1)**.** *Une base ordonnée pour le premier noyau de congruence $G(1)$ est donnée par*

$$\{x_\beta(p), h_\delta(1+p), x_\alpha(p); \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\},$$

l'ordre étant compatible avec la fonction de hauteur croissante sur les racines.

Ici, pour $\alpha \in \Phi$, nous notant par $U_\alpha \subset G$ le groupe unipotent correspondant, et $x_\alpha : G_{a,\mathbb{Z}_p} \to U_\alpha$ l'isomorphisme donné par $x_\alpha(t) = \exp(tX_\alpha)$. Pour $\lambda \in \mathbb{Q}_p^*, \alpha \in \Phi$, nous définissons $h_\alpha(\lambda) := w_\alpha(\lambda)w_\alpha(1)^{-1}$ où $w_\alpha(\lambda) := x_\alpha(\lambda)x_{-\alpha}(-\lambda^{-1})x_\alpha(\lambda)$.

Le groupe $\langle h_\delta(u), \delta \in \Pi, u \in 1+p\mathbb{Z}_p\rangle$ engendre le tore de $G(1)$. Réciproquement tout élément g du tore de $G(1)$ peut être écrit de façon unique comme $g = \prod_{\delta\in\Pi} h_\delta(1+v_\delta)$ où $v_\delta \in p\mathbb{Z}_p$ (voir Corollaire du lemme 28 p. 44 de [Ste67]).

Soit $\Lambda(G(1))$ l'algèbre d'Iwasawa de $G(1)$ sur $\mathbb{Z}_p$,

$$\Lambda(G(1)) = \varprojlim_H \mathbb{Z}_p[G(1)/H].$$

Cette algèbre d'Iwasawa peut également être vue comme le dual des fonctions continues de $G(1)$ à $\mathbb{Z}_p$, ie $\Lambda(G(1)) = \mathrm{Hom}_{\mathbb{Z}_p}(C(G(1)), \mathbb{Z}_p)$ (voir le lemme 22.1 de [Sch11]).

Considérons $\mathcal{A} = \mathbb{Z}_p\{\{V_\alpha, W_\delta, \alpha \in \Phi, \delta \in \Pi\}\}$, l'algèbre des séries entières non-commutatives sur $\mathbb{Z}_p$ en plusieurs variables V_α et W_δ, où α décrit les racines et δ décrit les racines simples. L'ordre des variables est donné par la fonction hauteur sur les racines, comme dans le Théorème 0.1. Soit $\mathcal{R}$ l'idéal bilatère (à gauche et à droite) fermé engendré dans $\mathcal{A}$ par les relations

1. $(1+W_\delta)(1+V_\alpha) = (1+V_\alpha)^{(1+p)^{\langle\alpha,\delta\rangle}}(1+W_\delta)$,
2. $(1+V_{\alpha_1})(1+V_{\alpha_2}) = (1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1+\alpha_2 \notin \Phi)$,
3. $(1+V_{\alpha_1})(1+V_{\alpha_2}) = \Big(\prod_{i,j>0}(1+V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}}\Big)(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1+\alpha_2 \in \Phi)$,
4. $(1+V_{\alpha_3})(1+V_{-\alpha_3}) = (1+V_{-\alpha_3})^Q\Big(\prod_{i=1}^l(1+W_{\delta_i})^{n_iP}\Big)(1+V_{\alpha_3})^Q$,

Notre théorème principal dans la section 1 est

Théorème 0.2 (voir Théorème 1.22 de la section 1)**.** *Pour $p > 2$, l'algèbre d'Iwasawa $\Lambda(G(1))$ est naturellement isomorphe, comme anneau topologique, à $\mathcal{A}/\mathcal{R}$.*

Enfin, nous étendons nos méthodes pour donner une présentation explicite de l'algèbre d'Iwasawa du pro-p Iwahori sous-groupe de $GL(n, \mathbb{Z}_p)$ sous l'hypothèse supplémentaire $p > n+1$ qui généralise le cas pour $n = 2$ par Clozel [Clo17].

0.2 Présentation explicite de l'algèbre d'Iwasawa pour le pro-p Iwahori

Soit G le pro-p Iwahori de $SL_n(\mathbb{Z}_p)$ i.e. le groupe de matrices dans $SL_n(\mathbb{Z}_p)$ qui sont unipotentes supérieures modulo l'idéal $p\mathbb{Z}_p$. Une base ordonnée de G est donnée par

Théorème 0.3 (voir Théorème 2.5 de la section 2). *Les éléments*

$$\{x_\beta(p), h_\delta(1+p), x_\alpha(1); \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\}$$

forment une base ordonnée pour la p-valuation ω (cf. 2.1) sur G, où l'ordre est le suivant :

(i) prendre d'abord les matrices unipotentes inférieures dans l'ordre donné par la fonction de hauteur (croissante) sur les racines,
(ii) ensuite prendre les éléments diagonaux $h_\delta(1+p)$ pour $\delta \in \Pi$ dans n'importe quel ordre et,
(iii) enfin, prendre les matrices unipotentes supérieures dans l'ordre lexicographique suivant : la matrice $(1+E_{i,j})$ vient avant $(1+E_{k,l})$ si et seulement si $i \geq k$ et $i = k \implies j > l$.

Ici la matrice $E_{i,j}$ est la matrice élémentaire standard.

La présentation de l'algèbre d'Iwasawa $\Lambda(G)$ est donnée par

Théorème 0.4 (voir Théorème 2.4.3 de la section 2). *Pour $p > n+1$, l'algèbre d'Iwasawa $\Lambda(G)$ est isomorphe à $\mathcal{A}/\mathcal{R}$, où $\mathcal{A} = \mathbb{Z}_p\{\{V_\alpha, W_\delta, U_\beta, \alpha \in \Phi^+, \beta \in \Phi^-, \delta \in \Pi\}\}$ avec l'ordre donné dans le théorème 0.3 et $\mathcal{R}$ est l'idéal bilatère fermé de $\mathcal{A}$ engendré par les relations (2.50 − 2.64).*

Nous obtenons le corollaire suivant :

Corollaire 0.1 (voir le corollaire 2.15 de la section 2). *L'algèbre d'Iwasawa du sous-groupe pro-p Iwahori de $GL_n(\mathbb{Z}_p)$ est un quotient $\mathcal{A}'/\mathcal{R}$, avec*

$$\mathcal{A}' = \mathbb{Z}_p\{\{Z, V_\alpha, U_\beta, W_\delta, \alpha \in \Phi^+, \beta \in \Phi^-, \delta \in \Pi\}\},$$

$\mathcal{R}$ défini par les relations (2.50 − 2.64) et Z commute avec $U_\beta, V_\alpha, W_\delta$ pour tous α, β, δ.

Cette présentation explicite des algèbres d'Iwasawa est utilisée par Clozel pour étudier les propriétés du centre de l'algèbre d'Iwasawa pour le premier noyau de congruence principal de $SL(2, \mathbb{Z}_p)$. Avec L une extension finie non-ramifiée de $\mathbb{Q}_p$, la présentation explicite peut aussi être utilisée pour définir "changement de base formel" [Clo17] des algèbres d'Iwasawa

$$\Lambda_L \to \Lambda_{\mathbb{Q}_p}$$

où Λ_L et $\Lambda_{\mathbb{Q}_p}$ sont les algèbres d'Iwasawa des sous-groupes pro-p Iwahori sur L et $\mathbb{Q}_p$ respectivement. Le changement de base formel est donné par des séries formelles qui convergent uniquement vers des distributions analytiques globales qui sont les duaux continus des fonctions analytiques rigides sur le pro-p Iwahori considéré comme un espace analytique rigide ([Clo17]). Cela motive également l'étude des vecteurs analytiques globaux des représentations p-adiques discutée dans la section suivante.

En plus des implications de notre présentation explicite de l'algèbre d'Iwasawa, Dong Han et Feng Wei notent que nos résultats pourraient fournir des moyens de répondre à la question ouverte d'existence d'éléments normaux non triviaux dans Ω_G, réduction modulo p de l'algèbre d'Iwasawa de G (voir Introduction et section 5 de [HW18]). Un élément $r \in \Omega_G$ est normal si $r\Omega_G = \Omega_G r$. La question sur les éléments normaux apparait dans [BW13], et a été reformulée dans [HW18] qui ont traité les cas de $SL(2, \mathbb{Z}_p)$ et $SL(3, \mathbb{Z}_p)$. Comme noté dans [HW18], les éléments normaux aident à construire des idéaux réflexifs dans l'algèbre d'Iwasawa. La question principale de Han et Wei est de trouver un mécanisme pour construire des idéaux d'algèbres de groupes complets sans utiliser d'éléments centraux ou de sous-groupes normaux fermés. Ainsi ils obtiendraient des moyens naturels de construire des idéaux dans l'algèbre Iwasawa (*loc.cit*).

Questions futures. Le sous-groupe pro-p Iwahori de $GL(n, \mathbb{Z}_p)$, pour $p > n+1$ est un groupe p-saturé au sens de Lazard. Cela pose la question naturelle de savoir si l'on peut généraliser le Corollaire 0.1 pour obtenir une présentation explicite de l'algèbre Iwasawa pour tout groupe p-saturé.

0.3 Série principale globalement analytique

La deuxième branche de ma recherche concerne les vecteurs analytiquement globaux, au sens d'Emerton [Eme17], de représentations p-adiques de $GL_n(\mathbb{Q}_p)$ sous l'action du sous-groupe pro-p Iwahori G de $GL_n(\mathbb{Q}_p)$. Ici, nous notons G (resp. B) le pro-p Iwahori (resp. le sous-groupe d'Iwahori) égal au sous-groupe des matrices dans $GL_n(\mathbb{Z}_p)$ qui sont inférieures unipotentes (respectivement triangulaires inférieures) modulo $p\mathbb{Z}_p$. D'après les travaux d'Emerton [Eme17], il est clair qu'il est possible de généraliser le travail effectué par Schneider et Teitelbaum aux représentations localement analytiques [ST02b], et de construire une théorie des représentations de séries principales globalement analytiques sous l'action du pro-p Iwahori. Nous montrons que le sous-espace de l'algèbre de Tate des fonctions analytiques rigides de la série principale localement analytique est une représentation globalement analytique de G (Théorème 0.5). De plus, nous déterminons la condition d'irréductibilité de telles séries principales globalement analytiques (Théorème 0.6).

Soit K une extension finie de $\mathbb{Q}_p$. Rappelons la définition d'une représentation globalement analytique. Soit $\mathbb{G}$ le groupe rigide-analytique dont les $\mathbb{Z}_p$-points coincident avec le groupe G. On note $\mathcal{A}(\mathbb{G}, K)$ l'algèbre de Tate des fonctions globalement analytiques sur $\mathbb{G}$ [Bos14], c'est-à-dire des fonctions qui peuvent être écrites globalement sur $\mathbb{G}$ comme série entière avec les coordonnées de $\mathbb{G}$ ayant des coefficients (en K) qui tendent vers 0. Soit V un espace K-Banach de norme $||\cdot||$. Si $g \to \pi(g)$ est une représentation de G sur V, on dit que π (ou V) est une représentation globalement analytique si l'application

$$O_v := g \longmapsto g \cdot v = \pi(g)v$$

est une fonction globalement analytique de $\mathbb{G}$ à V. Ainsi, dans les coordonnées $(x_1, ..., x_d)$ de $\mathbb{G}$, nous avons :

$$g \cdot v = \sum_{m \in \mathbb{N}^d} \underline{x}^m v_m$$

où $v_m \in V$ et $||v_m|| \to 0$ quand $|m| = m_1 + \cdots + m_d \to 0$. Ici, $m = (m_1, ..., m_d)$ et $\underline{x}^m = x_1^{m_1} \cdots x_d^{m_d}$, $m_i \in \mathbb{N}$. (Pour les propriétés des représentations globalement analytiques, voir [Eme17].) Cette définition peut être généralisée à n'importe quel groupe analytique rigide sur $\mathbb{Q}_p$, et pas seulement au pro-p Iwahori.

Notons $\mathbb{P}$ le sous-groupe de Borel des matrices triangulaires supérieures dans $GL_n(\mathbb{Q}_p)$, $\mathbb{T}$ le tore maximal de $GL_n(\mathbb{Q}_p)$, P^+ le sous-groupe de Borel des matrices triangulaires supérieures dans $GL_n(\mathbb{Z}_p)$, W le groupe Weyl de $GL_n(\mathbb{Q}_p)$ par rapport à $\mathbb{T}$, $P_w^+ = B \cap wP^+w^{-1}$, où B est le sous-groupe de matrices dans $GL_n(\mathbb{Z}_p)$ qui sont des triangles inférieures modulo $p\mathbb{Z}_p$.

Soit χ un caractère localement analytique du tore T_0 de B à $K^\times$, c'est-à-dire $\chi : T_0 \to K^\times$ avec $\chi(t_1, ..., t_n) = \chi_1(t_1) \cdots \chi_n(t_n)$, et $\chi_i(t) = t^{c_i}$ où $c_i = \frac{d}{dt}\chi_i(t)|_{t=1}$ pour t suffisamment proche de 1, $c_i \in K$, $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}}$ l'induction localement analytique, c'est-à-dire :

$$\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}} := \{f \in \mathcal{A}_{\mathrm{loc}}(GL_n(\mathbb{Q}_p), K) : f(gb) = \chi(b^{-1})f(g), g \in GL_n(\mathbb{Q}_p), b \in \mathbb{P}\},$$

où $\mathcal{A}_{\mathrm{loc}}$ désigne l'ensemble des fonctions localement analytiques .

Localement analytique signifie que dans un voisinage d'un point, les fonctions peuvent être écrites comme des séries. Nous avons les décompositions B-equivariantes

$$\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}} \cong \mathrm{ind}_{P^+}^{GL_n(\mathbb{Z}_p)}(\chi)_{\mathrm{loc}} \cong \oplus_{w \in W} \mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$$

où l'action de χ^w est donnée par $\chi^w(h) = \chi(w^{-1}hw)$. Le premier isomorphisme est dû à la décomposition d'Iwasawa [OS10, sec. 3.2.2] et le second est dû à la décomposition de Bruhat (*loc.cit.* et [Car79, section 3.5]).

L'espace vectoriel sous-jacent à $\mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$ est isomorphe aux fonctions localement analytiques $\mathbb{Z}_p^m \to K$ pour une dimension appropriée m. Soit $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ l'algèbre de Tate des fonctions globalement analytiques de $\mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$, c'est-à-dire des fonctions qui peuvent être écrites comme séries de puissances sur l'espace analytique rigide $\mathbb{Z}_p^m$ avec des coefficients dans K qui tendent vers 0.

De même, notons $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi) := \oplus_{w\in W}\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ le sous-espace des vecteurs globalement analytiques de $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}}$. Supposons que le caractère χ est analytique c'est-à-dire $v_p(c_i) > \frac{e}{p-1} - 1$ où e est l'indice de ramification de K. Rappelons que G est le groupe de matrices dans $GL_n(\mathbb{Z}_p)$ qui sont unipotentes inférieurs modulo $p\mathbb{Z}_p$, i.e. G est le sous-groupe pro-p Iwahori.

En généralisant le travail de Clozel pour $n = 2$ [Clo16], nous démontrons le théorème suivant :

Théorème 0.5 (Théorème 3.21 de section 3)**.** *Si $p > n+1$ et χ est analytique, alors la représentation $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ est une représentation globalement analytique admissible de G. Ceci implique que $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)$ est aussi une représentation globalement analytique de G.*

L'admissibilité des représentations globalement analytiques a été définie par Emerton [Eme17]. Pour l'analyticité globale, nous calculons explicitement l'action de G sur l'algèbre de Tate des fonctions analytiques globales de $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ et montrons que l'action est une fonction globalement analytique sur G vu comme un espace rigide-analytique.

De plus, nous déterminons la condition d'irréductibilité de la série principale globalement analytique $\mathrm{ind}_{P^+}^{B}(\chi)$ où $w = Id$. Soit μ la forme linéaire de l'algèbre de Lie du tore T_0 à K donnée par

$$\mu = (-c_1, ..., -c_n) : Diag(t_1, ..., t_n) \mapsto \sum_{i=1}^{n} -c_i t_i$$

où $t = (t_i) \in \mathrm{Lie}(T_0)$. Pour la racine négative $\alpha = (i, j) \in \Phi^-, i > j$, soit $H_{(i,j)} = E_{i,i} - E_{j,j}$ où $E_{i,i}$ est la matrice élémentaire standard.

Théorème 0.6 (Théorème 3.9 de section 3)**.** *Supposons $p > n+1$ et χ analytique. La représentation globalement analytique $\mathrm{ind}_{P^+}^{B}(\chi)$ de G est topologiquement irréductible si et seulement si pour tout $\alpha = (i, j) \in \Phi^-$, $-\mu(H_{\alpha=(i,j)}) + i - j \notin \{1, 2, 3, ...\}$.*

Notons que pour les représentations localement analytiques $\mathrm{ind}_{P^+}^{B}(\chi)_{\mathrm{loc}}$ ce résultat d'irréductibilité a été prouvé par Orlik et Strauch [OS10] en généralisant les travaux originaux de Schneider et Teitelbaum [ST02b] pour $n = 2$. Pour l'irréductibilité des séries globalement analytiques, nous utilisons d'abord l'action de l'algèbre de Lie de G pour montrer que tout sous-espace G-invariant fermé de $\mathrm{ind}_{P^+}^{B}(\chi)$ contient la fonction constante 1. La partie restante de l'argument de la preuve de l'irréductibilité utilise la notion de modules de Verma et sa condition d'irréductibilité. Pour assurer l'irréductibilité de ce module Verma, nous avons besoin de la condition $-\mu(H_{\alpha=(i,j)}) + i - j \notin \{1, 2, 3, ...\}$ d'après un résultat dû à Bernstein-Gelfand. (Voir Théorème 7.6.24 de [Dix77]).

Nous passons ensuite au changement de base local de Langlands des représentations irréductibles de $GL_n(\mathbb{Q}_p)$ à $GL_n(L)$ où L est une extension cyclique non-ramifiée de degré N. Il y a 2 situations différentes ; d'abord, les représentations complexes et ensuite les représentations p-adiques. Nous présentons brièvement le cas connu du changement de base pour les représentations complexes. Le cas complexe, étudié par Arthur et Clozel [AC89], associe à chaque représentation irréductible admissible de $GL_n(\mathbb{Q}_p)$, une représentation admissible π_L de $GL_n(L)$, qui est stable sous l'action de $\mathrm{Gal}(L/\mathbb{Q}_p)$. De nombreuses propriétés de relèvement local peuvent être prouvées par des moyens globaux, à savoir la formule des traces. Ce changement de base est naturellement associé à un homomorphisme d'algèbres de Hecke [AC89, Chapter 1, section 4],

$$b : \mathcal{H}_L \to \mathcal{H}_{\mathbb{Q}_p}$$

où $\mathcal{H}_L$, (resp. $\mathcal{H}_{\mathbb{Q}_p}$) sont les algèbres de Hecke non-ramifiées de fonctions à support compact invariant par $GL_n(\mathcal{O}_L)$, (resp. $GL_n(\mathbb{Z}_p)$).

Un exemple important et bien connu de changement de base pour la représentation complexe est donné par des séries principales non-ramifiées. Soit

$$\pi = \mathrm{ind}_{P(\mathbb{Q}_p)}^{GL_n(\mathbb{Q}_p)}(\chi_1, ..., \chi_n)$$

l'induction unitaire du sous-groupe Borel $P(\mathbb{Q}_p)$ de $GL_n(\mathbb{Q}_p)$, où les χ_i sont des caractères unitaires non-ramifiés de $\mathbb{Q}_p^\times$. Alors π est irréductible et le changement de base de π est donné par

$$\pi_L = \mathrm{ind}_{P(L)}^{GL_n(L)}(\eta_1, ..., \eta_n)$$

où $\eta_i = \chi_i \circ N_{L/\mathbb{Q}_p}$, ($N_{L/\mathbb{Q}_p}$ est la norme). Par la conjecture locale de Langlands pour les représentations complexes ([HT01], [Hen00]), on sait que π est associée à une représentation R de degré n du groupe Weil-Deligne $WD_{\mathbb{Q}_p}$. Ensuite, le changement de base de base π_L de π est associé à la restriction de R à WD_L, notée R_L, c'est-à-dire

$$R \leftrightsquigarrow \pi \text{ et } R_L \leftrightsquigarrow \pi_L.$$

Une question naturelle est de construire un changement de base local, compatible avec la fonctorialité de Langlands, pour les représentations p-adiques. Clozel dans [Clo16] a proposé d'utiliser le théorème du produit tensoriel de Steinberg. Si π est une représentation p-adique de $GL_n(\mathbb{Q}_p)$, alors un candidat possible pour le changement de base π_L de π est le produit tensoriel complété de π^σ pour tout $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$, c'est-à-dire

$$\pi_L = \widehat{\otimes}_\sigma \pi^\sigma.$$

Ce travail est effectué dans la section 3 pour les séries principales. Plus précisément, après avoir déterminé les vecteurs globalement analytiques de la série principale induite par le Borel, sous l'action du sous-groupe pro-p Iwahori G sur $\mathbb{Q}_p$, nous utilisons le théorème du produit tensoriel de Steinberg et nous obtenons une représentation de $G(L)$ invariante par l'action de $\mathrm{Gal}(L/\mathbb{Q}_p)$ (comparer avec [Clo16, section 3.2]). Pour chaque $w \in W$, nous considèrons la représentation globalement analytique admissible $I_{w,\mathbb{Q}_p}(\chi) := \mathrm{ind}_{P_w^+}^B(\chi^w)$ de $G(\mathbb{Q}_p)$. La représentation $\mathrm{ind}_{P_w^+}^B(\chi^w)$ s'étend naturellement à une représentation admissible globalement analytique de $G(L)$ appelée "changement de base holomorphe" que nous notons $I_{w,L}(\chi)$.

Le changement de base de Langlands de cette série principale globalement analytique donné par le théorème du produit tensoriel de Steinberg satisfait alors le théorème suivant :

Théorème 0.7 (Théorème 3.22 de section 3)**.** *Par le changement de base de Langlands, la représentation* $\oplus_{w\in W}(\widehat{\otimes}_\sigma I_{w,L}(\chi^w)^\sigma)$ *est une représentation globalement analytique admissible de* $G(L)$ *où* $\sigma \in \Sigma = \mathrm{Gal}(L/\mathbb{Q}_p)$.

L'analogue de l'homomorphisme de transfert du changement de base entre les algèbres de Hecke $b : \mathcal{H}_L \to \mathcal{H}_{\mathbb{Q}_p}$, dans le cas p-adique, peut être vu à partir d'une application "formelle" entre les algèbres d'Iwasawa qui n'a de sens que pour des distributions globalement analytiques sur le groupe, considérées comme espace analytique-rigide. Plus précisément, en utilisant la présentation explicite de l'algèbre Iwasawa du sous-groupe pro-p Iwahori, on peut définir un homomorphisme formel

$$b : \Lambda_L \to \Lambda_{\mathbb{Q}_p}$$

similaire à la situation classique entre les algèbres de Hecke non-ramifiées. Ici Λ_L et $\Lambda_{\mathbb{Q}_p}$ sont les algèbres d'Iwasawa du pro-p Iwahori de $GL_n(L)$ et $GL_n(\mathbb{Q}_p)$ respectivement. Clozel l'a construit pour $GL(2)$ [Clo17] et nous croyons que sa construction s'étendra à $GL(n)$, grâce aux résultats de la section 2.

Questions futures. Il semble intéressant de déterminer les vecteurs globalement analytiques des représentations p-adiques plus générales de $GL(2, \mathbb{Q}_p)$, par exemple la représentation "trianguline" de Colmez [Col08] (voir aussi [Col14]), qui correspond à un quotient de la série principale. On peut aussi explorer le lien entre les vecteurs globalement analytiques des représentations p-adiques (sous le pro-p Iwahori ou un sous-groupe rigide-analytique approprié de $GL(2)$) et les (φ, Γ)-modules [Col10]. Il s'agit d'obtenir un résultat similaire à la correspondance existante pour les représentations localement analytiques [CD14, Sec VI.3].

0.4 Construire des représentations galoisiennes ayant une image ouverte

Dans la deuxième partie de la thèse, nous nous intéressons aux corps de nombres dits «p-rationnels». Ces extensions de $\mathbb{Q}$ qui jouent un rôle majeur dans la théorie classique d'Iwasawa et l'étude des représentations galoisiennes. Afin de les motiver et de les relier à notre travail sur les algèbres Iwasawa dans la première partie, il est nécessaire d 'introduire un problème bien connu en théorie d'Iwasawa sur lequel K. Iwasawa travaillait dans les années 1950's.

Soit maintenant K une extension finie de $\mathbb{Q}$, K_∞ est la $\mathbb{Z}_p$- extension cyclotomique de K de groupe Galois $\Gamma = \mathrm{Gal}(K_\infty/K)$. Nous définissons $K_m = K_\infty^{\Gamma_m}$ où Γ/Γ_m est cyclique d'ordre p^m. L'objet principal de la théorie d'Iwasawa est l'étude des nombres de classe de la tour de corps de nombres,

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \subset \cdots$$

où K_m/K est l'extension cyclique de degré p^m et $K_\infty = \cup_m K_m$. Iwasawa a remarqué que si p^{e_m} est la plus grande puissance de p divisant le nombre de classes de K_m, alors il existe des entiers λ, μ, ν tels que

$$e_m = \lambda m + \mu p^m + \nu$$

pour tous les m suffisamment grand. L'ingrédient principal de la preuve est basé sur l'étude du groupe de Galois $X = \mathrm{Gal}(F_\infty/K_\infty)$, où $F_\infty = \cup_m F_m$ et F_m est la plus grande p-extension abélienne de K_m non ramifiée en dehors de p et voir X comme un module sur l'algèbre d'Iwasawa $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$.

Ceci nous amène à regarder les corps de nombres K tels que le groupe de Galois $\mathrm{Gal}(L/K)$ où L est l'extension maximale non-ramifiée en dehors de p est un pro-p groupe libre. Autrement dit, en notant M^{ab} l'extension abélienne maximale non-ramifiée en dehors de p, nous avons

1. $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(M^{ab}/K)) = r_2 + 1$ (c'est la conjecture de Leopoldt pour K et p),

2. $\mathrm{Gal}(M^{ab}/K)$ est un $\mathbb{Z}_p$-module sans torsion,

où (r_1, r_2) est la signature de K. Les corps vérifiant (1) et (2) sont appelés "p-rationnels" et ont plusieurs applications en théorie des représentations [JNQD93], [Mov88a], [Gre16]. L'exemple le plus simple de corps p-rationnel est $\mathbb{Q}$, où M est l'extension cyclotomique $\mathbb{Z}_p$. D'autres exemples de corps p-rationnels sont donné par $\mathbb{Q}(\mu_p)$, où μ_p est une racine primitive p-ième racine de l'unité et p est un nombre premier régulier.

Une application théorique importante des représentations galoisiennes de ces corps a été réalisée par R. Greenberg en 2016 ([Gre16]). Il a construit des représentations galoisiennes d'image ouverte dans $GL_n(\mathbb{Z}_p)$. Plus précisément, Greenberg a montré que si $p \geq 4[\frac{n}{2}] + 1$ et p est régulier et $K = \mathbb{Q}(\mu_p)$, alors il existe une représentation continue

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to GL_n(\mathbb{Z}_p)$$

ayant une image ouverte. Le résultat de Greenberg est particulièrement remarquable puisque la source standard de représentations galoisiennes est la géométrie algébrique (par exemple les variétés abéliennes, les formes automorphes, etc.), alors que la construction de Greenberg n'est pas géométrique. Cela pose une question naturelle de savoir si l'on peut construire une telle représentation ayant une grande image ouverte pour tout groupe réductif.

En collaboration avec Christophe Cornut [CR18], nous construisons des représentations galoisiennes du groupe galoisien absolu de $\mathbb{Q}$ avec de grandes images ouvertes dans $\mathbf{G}(\mathbb{Z}_p)$, où $\mathbf{G}$ est un groupe réductif adjoint simple sur $\mathbb{Z}_p$. Nous prouvons un résultat qui montre l'existence d'extensions de Lie p-adique de $\mathbb{Q}$ où le groupe de Galois correspond à une certaine algèbre de Lie spécifique p-adique. En généralisant la construction par Greenberg pour $GL(n)$ [Gre16], on obtient le résultat suivant.

Théorème 0.8 (Corollaire 4.22 de section 4)**.** *Soit $\mathbf{G}$ un groupe réductif adjoint simple sur $\mathbb{Z}_p$ de sous-groupe Iwahori noté I et de sous-groupe pro-p Iwahori noté $I(1)$. Soit K le corps cyclotomique $\mathbb{Q}(\mu_p)$ et M l'extension maximale de K, non ramifiée en dehors des places de K au dessus de p.*

Alors, il existe une constante c dépendant uniquement du type de $\mathbf{G}$ telle que si $p > c$ est un nombre premier régulier, nous avons un morphisme continu

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to I$$

avec $\rho(\mathrm{Gal}(M/K)) = I(1)$.

Le sous-groupe pro-p Iwahori $I(1)$ est d'indice fini dans $\mathbf{G}(\mathbb{Z}_p)$. Le théorème 0.8 construit une représentation galoisienne dont image contient $I(1)$. La façon de prouver le théorème 0.8 est de trouver un ensemble minimal de générateurs topologiques de $I(1)$. Pour un nombre premier régulier p, $K = \mathbb{Q}(\mu_p)$, $\mathrm{Gal}(M/K)$ est un groupe pro-p libre. Ensuite, nous avons construit un homomorphisme continu de $\mathrm{Gal}(M/K)$ à $I(1)$, en envoyant des générateurs de $\mathrm{Gal}(M/K)$ sur les générateurs topologiques de $I(1)$ de façon à ce que l'homomorphisme s'étende à $\mathrm{Gal}(M/\mathbb{Q})$. Dans le théorème suivant, nous trouvons un ensemble minimal de générateurs topologiques du sous-groupe pro-p Iwahori de tout groupe réductif $\mathbf{G}$ (pas nécessairement adjoint) sur $\mathbb{Z}_p$ de tore $\mathbf{T}$.

Théorème 0.9 (Théorème 4.1 de section 4)**.** *Les éléments suivants forment un ensemble minimal de générateurs topologiques du sous-groupe p-Iwahori $I(1)$ de $G = \mathbf{G}(\mathbb{Z}_p)$:*

1. *les éléments semi-simples $\{s(1+p) : s \in \mathcal{S}\}$ de $T(1)$,*
2. *pour chaque $c \in \mathcal{C}$, les éléments unipotents $\{x_\alpha(1) : \alpha \in \Pi_c\}$,*
3. *pour chaque $c \in \mathcal{C}$, l'élément unipotent $x_{-\alpha_{c,max}}(p)$,*
4. *si $p = 3$, pour chaque $d \in \mathcal{D}$, l'élément unipotent $x_{\delta_d}(1)$.*

Ici, $T(1)$ est le tore maximal de $I(1)$, $\mathcal{C}$ est le nombre de composantes irréductibles des racines Φ (ainsi $\Phi = \coprod_{c\in\mathcal{C}} \Phi_c$ et $\Pi = \coprod_{c\in\mathcal{C}} \Pi_c$), $\alpha_{c,max}$ est la racine positive de grande hauteur dans la composante racine Φ_c, $\mathcal{D} \subset \mathcal{C}$ est l'ensemble des composants irréductibles de type G_2. Pour $d \in \mathcal{D}$, $\delta_d \in \Phi_{d,+}$ (les racines positives de Φ_d) est la somme des deux racines simples dans Π_d et nous fixons un ensemble de représentants $\mathcal{S} \subset M^\vee = X_*(\mathbf{T})$ (co-caractères de $\mathbf{T}$) qui forment $\mathbb{F}_p$ - base de $(M^\vee/\mathbb{Z}\Phi^\vee)\otimes\mathbb{F}_p = \oplus_{s\in\mathcal{S}}\mathbb{F}_p\cdot s\otimes 1$. Pour $t \in \mathbb{Z}_p$, $x_\alpha(t) = exp(tX_\alpha)$ est le sous-groupe unipotent de $\mathbf{G}(\mathbb{Z}_p)$ correspondant à la racine $\alpha \in \Phi$. La famille $(X_\alpha)_{\alpha\in\Phi}$ est un système Chevalley de l'algèbre de Lie de G. Par exemple, si $G = GL(n, \mathbb{Z}_p)$ et $\alpha = (i, j)$, alors $x_\alpha(t) = 1 + tE_{i,j}$ pour la matrice élémentaire $E_{i,j}$.

Nos constructions donnent une extension galoisenne M sur $\mathbb{Q}$ telle que $\mathrm{Gal}(M^{\ker(\rho)}/\mathbb{Q})$ est un groupe de Lie p-adique qui contient le sous-groupe Iwahori d'un groupe adjoint, simple comme sous-groupe d'indice fini. Cela répond au problème classique de Galois inverse pour l'algèbre de Lie simple p-adique: si L est une algèbre de Lie de dimension finie sur $\mathbb{Q}_p$, alors il existe une extension de Galois sur $\mathbb{Q}$ telle que le groupe de Galois est un groupe de Lie p-adique dont l'algèbre de Lie est isomorphe à L. Notez que notre construction impose l'hypothèse de p-rationalité du corps K.

Les corps p-rationnels totalement réels satisfont la conjecture λ et μ invariante de Greenberg: pour un corps de nombres totalement réel k, les invariants d'Iwasawa $\lambda = \lambda_p(k)$ et $\mu = \mu_p(k)$ associés à la classe idéaux de la $\mathbb{Z}_p$-extension cyclotomique k_∞/k sont nuls (cf. [Gra16a], [Gre76], voir aussi [Was97] pour le fait que $\mu = 0$ quand k est abélien). Ces corps sont également utiles pour développer des approches p-adiques pour résoudre la conjecture λ et μ invariante de Greenberg (cf. [Gra16a], [JNQD93]).

Questions futures. Il y a une liste de questions ouvertes, initialement posées par Greenberg, concernant la construction de représentations de Galois à image ouverte qui sont géométriques. On peut trouver une discussion dans [Gre16, Remarque 6.4]. On pourra aussi comparer cette approche aux résultats de [Kat17].

0.5 Expériences numériques et heuristiques sur la conjecture de la p-rationnalité de Greenberg

La construction de la section 0.4 impose l'hypothèse de p-rationalité du corps de base. C'est pourquoi, nous concentrons notre attention sur l'étude des corps p-rationnels d'un point de vue calculatoire dans la section 5.

La section 5 (en collaboration avec Razvan Barbulescu) a été initiée par une conjecture de Greenberg [Gre16, Conjecture 4.8], d'existence d'un corps p-rationnel K tel que $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$ pour tout p et t. En d'autres termes, on peut construire des corps p-rationnels comme composé d'extensions quadratiques. Greenberg donne quelques exemples ($p = 3, 5$ et $t = 5, 6$, cf. [Gre16]) de corps p-rationnels satisfaisant sa conjecture. La conjecture permet notamment de généraliser sa construction pour produire des représentations galoisiennes ayant une grande image ouverte.

Nous cherchons donc à trouver de nouvelles techniques algorithmiques pour déterminer des corps p-rationnels d'une manière rapide et efficace et d'étudier la densité des corps p-rationnels. Ceci nous conduit également généraliser la conjecture de Greenberg aux groupes de Galois $(\mathbb{Z}/q\mathbb{Z})^t$ où q est un premier différent de p. Pour fixer des idées, pour un groupe fini G, nous disons que $\mathrm{GC}_\infty(G, p)$ (c'est-à-dire la conjecture de Greenberg pour G et p) est vraie s'il existe un nombre infini de corps p-rationnel K ayant G pour groupe de Galois. Il s'agit donc d'un raffinement du problème inverse de Galois pour les corps de nombres avec la condition de relions p-rationalité. Nous avons obtenus des exemples des corps p-rationnels pour $G = (\mathbb{Z}/2\mathbb{Z})^t, (\mathbb{Z}/3\mathbb{Z}), \mathbb{Z}/4\mathbb{Z}, V_4, D_4, A_4, S_4$ quand $5 \leq p < 100$ ([BR17b]).

Tout d'abord, dans la section 5, nous relions la notion de corps p-rationnels à celle de régulateur p-adique et de nombre de classes, ce qui suffit à prouver $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ et à donner des exemples de corps satisfaisant la conjecture de Greenberg ayant pour le groupe de Galois $(\mathbb{Z}/2\mathbb{Z})^t$ pour $t \in [7, 11]$ et $p \in [5, 97]$. Nous rappelons ensuite les conjectures existantes ([CM90], [CL84b], [CL84a], [CM87], [HZ16]) sur la divisibilité par p du nombre de classes et du régulateur p-adique normalisé. Ces conjectures sont dues à Cohen-Lenstra-Martinet (pour le nombre de classes) et Hofmann-Zhang (pour le régulateur p-adique).

Cohen-Lenstra-Martinet en 1989 ont testé leur conjecture et ont écrit "nous croyons que le mauvais accord [avec les tables] est dû au fait que les discriminants ne sont pas assez grands". Perplexes par cette affirmation, nous avons repris leurs calculs et fait des statistiques sur les corps de conducteur inférieur à 8000, c'est-à-dire de discriminant inférieur à 64×10^6, (par exemple [Gra75] a considéré les corps de conducteur inférieur à 4000). Depuis, les capacités des ordinateurs ont augmenté de plus d'un facteur 1000. Ainsi nous avons pu calculer les statistiques pour les corps de conducteur inférieur à 10^7, c'est-à-dire de discriminant inférieur à 10^{14}. Il nous a fallu environ un mois utilisant en parallèle 30 cores soit environ 2,5 années CPU.

En regardant les données du tableau 4 nous avons pu réinterprété les résultats préalablement obtenus : la vitesse de convergence vers la densité moyenne est très lente et les statistiques à 8000 ont une erreur relative entre 19% et 100%. Ce n'a donc pas permis à Cohen et Martinet de conclure. Cependant les statistiques à 10^7 ont seulement une erreur relative entre 0.2% et 15.5%, donc nous pouvons conclure. Les données numériques confirment leur conjecture. Notez que les algorithmes connus pour calculer explicitement le nombre de classes sont lents. L'astuce que nous avons utilisée est un algorithme qui teste la divisibilité par p du nombre de classes de corps cycliques cubiques de discriminant inférieur à 10^14 sans calculer leur nombre de classes. Il s'agit d'un algorithme dû à N.-M. Gras [Gra75], utilisant la notion d'unités cyclotomiques.

Nous donnons également un nouvel algorithme pour produire des unités dans des corps cycliques cubiques qui est utilisé pour tester la valuation dans p du régulateur p-adique, qui est plus rapide que le calcul d'un système d'unités fondamentales. Un algorithme [PV15] de Pitoun et Varescon nous permet aussi de donner des exemples de corps p-rationnels avec des groupes de Galois non-abéliens.

Ainsi, nous obtenons une famille de corps cycliques cubiques qui contient un nombre infini de

corps 5-rationnels sous une liste d'hypothèses arithmétiques (section 5.11). Cela réduit le problème de fournir des exemples de corps 5-rationnels cycliques cubiques au problème de tester juste une liste d'hypothèses arithmétiques réduisant énormément le temps de calcul.

Sur la base des résultats conjecturaux existants et de nos calculs numériques vérifiant ces conjectures sur la divisibilité par p du nombre de classes et du régulateur p-adique normalisé, nous montrons que pour $q = 2$ ou 3 et $p > 5q^t$ alors pour tout entier t, $\mathrm{GC}_\infty((\mathbb{Z}/q\mathbb{Z})^t, p)$ est vrai.

Théorème 0.10 (Théorème 5.6 de section 5)**.** *Soit p un premier impair. Alors*

1. *il existe un nombre infini de corps p-rationnels quadratiques.*
2. *Supposons qu'il existe une infinité d'entiers impairs $a \not\equiv 21, 23 (mod\ 25)$ tels que $m = \frac{1}{4}(a^2 + 27)$ est premier et satisfait les conditions arithmétiques de Hypothesis 5.35. Alors $GC(\mathbb{Z}/3\mathbb{Z}, 5)$ est vrai.*
3. *Sous des conjectures basées sur des heuristiques et des expériences numériques (Conjecture 5.41 et Conjecture 5.39), quand $q = 2$ ou 3, pour tout premier p et tout entier t tels que $p > 5q^t$, il existe un nombre infini de corps p-rationnels de groupe Galois $(\mathbb{Z}/q\mathbb{Z})^t$.*

La conjecture 5.39 donne la probabilité que le nombre de classe h_K d'un corps K soit premier à p et $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$ ou $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^t$. Cette conjecture est une reformulation de l'heuristique de Cohen-Martinet [CM90], [CL84b] et de la formule du nombre de classes de Kuroda [Kur50], [Lem94]. Nous avons également vérifié numériquement cette conjecture pour les corps K de groupe Galois $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et de conducteur $\leq 10^6$. (voir tableau 5). Nous avons aussi testé conjecture 5.39 pour les corps de nombres cycliques cubiques de conducteur $\leq 10^7$ (voir le tableau 4).

Enfin la conjecture 5.41 est une reformulation de la conjecture de Hofmann et Zhang qui donne la densité des corps de nombres totalement réels de groupe de Galois $(\mathbb{Z}/q\mathbb{Z})^t$ (où $q = 2$ ou 3) dont le régulateur p-adique normalisé est divisible par p pour au moins un de ses sous-corps cycliques.

Les algorithmes peuvent être trouvés en ligne à l'adresse suivante:
`https://webusers.imj-prg.fr/ razvan.barbaud/pRational/pRational.html`

Questions futures. En résumé, la conjecture de Greenberg est résolue dans le cas particulier de $G = \mathbb{Z}/2\mathbb{Z}$ et est comforme aux heuristiques et aux calculs numériques pour $G = (\mathbb{Z}/q\mathbb{Z})^t$ quand $q = 2$ ou 3 . Dans le cas général des groupes de Galois non-abéliens, nos résultats sont positifs mais se limitent à une liste d'exemples.

Le problème soulève de nouvelles questions sur l'indépendance des nombres de classes et des régulateurs p-adiques, qui pourraient être abordées par des techniques de théorie analytique des nombres développes pour obtenir des progrès recents sur l'heuristique de Cohen-Lenstra-Martinet. Il est intéressant de créer de nouveaux algorithmes pour tester la divisibilité par p du regulateur et du nombre de classes avec une meilleure complexité que les algorithmes qui calculent un système d'unités fondamentales ou les nombre de classes.

Summary of results

In this section I present a broad overview of the results of my thesis in the domain of Arithmetic Geometry, Iwasawa theory, Galois representations and p-adic Langlands program. Part I of my thesis contains results in the representation theoretic side of the Langlands program while Part II contains results pertaining to the Galois side. The results can be divided into five sections (1-5) including a computational aspect discussed in section 5. The results appeared in the papers [Ray16], [Ray17], [Ray18], [CR18] and [BR17b].

0.6 An explicit presentation of the Iwasawa algebra for the first congruence kernel of Chevalley groups

Let p be a prime. The first branch of my research focuses on finding an explicit presentation of the Iwasawa algebra of a compact p-adic Lie group G over $\mathbb{Z}_p$. Iwasawa theory had its origins in Iwasawa's ground breaking work in the 1950's on the growth of class numbers in infinite $\mathbb{Z}_p$-extension of number fields. For a prime p, the Iwasawa algebra of a p-adic Lie group G, denoted by $\Lambda(G)$ or $\mathbb{Z}_p[[G]]$, is a non-commutative completed group algebra of G. It is defined by

$$\Lambda(G) := \varprojlim_N \mathbb{Z}_p[G/N]$$

where N varies over all the open normal subgroups of G. This algebra has many applications in different branches of mathematics. For example, Lazard provides an extensive study of p-adic analytic Lie groups in *Groupes analytiques p-adiques* [Laz65]. He defines the notion of p-saturated groups and characterized algebraically the notion of p-adic analytic groups as topological groups containing a topologically finitely generated open p-saturated pro-p group with an integer valued filtration.

In the theory of local Galois representations, Iwasawa algebras come in through Fontaine modules. Fontaine in [Fon90] describes an equivalence between the category of finite dimensional $\mathbb{Q}_p$-linear representations of the absolute Galois group of $\mathbb{Q}$ and the category of the so called étale (φ, Γ)-modules over a suitable ring. This equivalence of categories is used by Colmez and others to prove the p-adic Langlands correspondence for $GL_2(\mathbb{Q}_p)$ [CDP14].

The Iwasawa algebras also play a vital role in the study of p-adic representation theory of $G(\mathbb{Q}_p)$, the $\mathbb{Q}_p$-points of a reductive group G over $\mathbb{Q}_p$, initially studied by Emerton and Schneider/Teitelbaum. Schneider and Teitelbaum manage to translate the study of p-adic Banach space representation theory (over a finite extension K of $\mathbb{Q}_p$) to the study of modules over the Iwasawa algebra [ST02a].

From the view point of Iwasawa theory, it is crucial to understand structural results about these Iwasawa algebras. By Serre's presentation of semi-simple algebras and Steinberg's presentation of Chevalley groups [Ser87], [Ste67], we believe that objects coming from semi-simple split groups have explicit presentations.

The main result in section 1 is to give an explicit presentation, by generators and relations, of the Iwasawa algebra for the subgroup $G(1) := \ker(G(\mathbb{Z}_p) \to G(\mathbb{F}_p))$ of any semi-simple, simply connected, split Chevalley group G over $\mathbb{Z}_p$ (Theorem 0.2, 0.3). This generalizes a previous work of my advisor Clozel for $G = SL_2(\mathbb{Z}_p)$ (cf. [Clo11]).

Recall that Lazard defines, for any compact locally $\mathbb{Q}_p$-analytic group H, a function, said to be a p-valuation, $\omega : H - \{1\} \to (\frac{1}{p-1}, \infty) \subset \mathbb{R}$ satisfying certain properties (cf. [Laz65] III.2.1.2). Let d be the dimension of H (as a locally analytic manifold). Lazard also defines an ordered basis of H with respect to the p-valuation ω. This is an ordered sequence of elements $h_1, ..., h_d \in H - \{1\}$ such that the following conditions hold:

1. $\psi : \mathbb{Z}_p^d \xrightarrow{\sim} H, (x_1, ..., x_d) \longmapsto h_1^{x_1} \cdots h_d^{x_d}$,

2. $\omega(h_1^{x_1} \cdots h_d^{x_d}) = \min_{1 \leq i \leq d}(\omega(h_i) + val_p(x_i))$,

where the map ψ is a homeomorphism.

Fix a pinning of G [GP11, XXIII 1] $(T, M, \Phi, \Pi, (X_\delta)_{\delta\in\Pi})$. Thus T is a split maximal torus in G, $M = X^*(T)$ is its group of characters,

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \oplus_{\alpha\in\Phi}\mathfrak{g}_\alpha$$

is the weight decomposition for the action of T on $\mathfrak{g} = \mathrm{Lie}(G)$, $\Pi \subset \Phi$ is a basis of the root system $\Phi \subset M$, Φ^- and Φ^+ be the set of negative and positive roots and for each $\delta \in \Pi$, X_δ is a $\mathbb{Z}_p$-basis of $\mathfrak{g}_\delta$. We expand $(X_\delta)_{\delta\in\Pi}$ to a Chevalley system $(X_\alpha)_{\alpha\in\Phi}$ of G [GP11, XXIII 6.2]. The p-valuation ω on $G(1)$ is $\omega(x) = k$ if x is in the k-th congruence kernel but not in the $(k+1)$-th congruence kernel.

In the following, we find an ordered basis of $G(1)$.

Theorem 0.2 (see Theorem 1.9 of section 1)**.** *An ordered basis for the first congruence kernel $G(1)$ is given by*

$$\{x_\beta(p), h_\delta(1+p), x_\alpha(p); \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\}.$$

Here we can choose any order compatible with increasing height function on the roots and fix the ordering once for all.

Here, for $\alpha \in \Phi$, we denote by $U_\alpha \subset G$ the corresponding unipotent group, by $x_\alpha : G_{a,\mathbb{Z}_p} \to U_\alpha$ the isomorphism given by $x_\alpha(t) = \exp(tX_\alpha)$. For $\lambda \in \mathbb{Q}_p^*, \alpha \in \Phi$, we define $h_\alpha(\lambda) := w_\alpha(\lambda)w_\alpha(1)^{-1}$ where $w_\alpha(\lambda) := x_\alpha(\lambda)x_{-\alpha}(-\lambda^{-1})x_\alpha(\lambda)$.

The group $\langle h_\delta(u), \delta \in \Pi, u \in 1+p\mathbb{Z}_p\rangle$ generates the torus of $G(1)$ and conversely any element g in the torus of $G(1)$ can be written uniquely as $g = \prod_{\delta\in\Pi} h_\delta(1+v_\delta)$ where $v_\delta \in p\mathbb{Z}_p$ (cf. Corollary of lemma 28 p. 44 of [Ste67]).

Now, let $\Lambda(G(1))$ be the Iwasawa algebra of $G(1)$ over $\mathbb{Z}_p$, i.e.

$$\Lambda(G(1)) = \varprojlim_N \mathbb{Z}_p[G(1)/N],$$

where the inverse limit is taken over all the open normal subgroup N of $G(1)$. This Iwasawa algebra can also be viewed as the dual of continuous functions from $G(1)$ to $\mathbb{Z}_p$, i.e. $\Lambda(G(1)) = \mathrm{Hom}_{\mathbb{Z}_p}(C(G(1)), \mathbb{Z}_p)$ (cf. Lemma 22.1 of [Sch11]).

Consider $\mathcal{A} = \mathbb{Z}_p\{\{V_\alpha, W_\delta, \alpha \in \Phi, \delta \in \Pi\}\}$, the non-commutative power series over $\mathbb{Z}_p$ in several variables V_α and W_δ, where α varies over the roots and δ varies over the simple roots and the ordering of the variables is given by the height function on the roots, as in Theorem 0.2. The topology of $\mathcal{A}$ is given by the powers of the maximal ideal $\mathcal{M}_\mathcal{A} = (p, V_\alpha, W_\delta, \alpha \in \Phi, \delta \in \Pi)$. Let $\mathcal{R}$ be the closed two-sided ideal generated in $\mathcal{A}$ by the following relations:

1. $(1+W_\delta)(1+V_\alpha) = (1+V_\alpha)^{(1+p)^{\langle\alpha,\delta\rangle}}(1+W_\delta)$,
2. $(1+V_{\alpha_1})(1+V_{\alpha_2}) = (1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1+\alpha_2 \notin \Phi)$,
3. $(1+V_{\alpha_1})(1+V_{\alpha_2}) = \Big(\prod_{i,j>0}(1+V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}}\Big)(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1+\alpha_2 \in \Phi)$,
4. $(1+V_{\alpha_3})(1+V_{-\alpha_3}) = (1+V_{-\alpha_3})^Q\Big(\prod_{i=1}^l(1+W_{\delta_i})^{n_iP}\Big)(1+V_{\alpha_3})^Q$,

where $P = \frac{log(1+p^2)}{log(1+p)}, Q = (1+p^2)^{-1}, c_{i,j} \in \mathbb{Z}$ and the Cartan integer [Ste67, p. 30] $\langle\alpha,\delta\rangle \in \mathbb{Z}$. Then, our main theorem in section 1 is the following.

Theorem 0.3 (see Theorem 1.22 of section 1)**.** *For $p > 2$, the Iwasawa algebra $\Lambda(G(1))$ is naturally isomorphic as a topological ring to $\mathcal{A}/\mathcal{R}$.*

Applications of such an explicit presentation include results concerning the center of the Iwasawa algebra [Clo11]. Furthermore, we extend our methods to give an explicit presentation of the Iwasawa algebra of the pro-p Iwahori subgroup of $GL_n(\mathbb{Z}_p)$ with an additional hypothesis $p > n+1$ which generalizes the case for $n = 2$ by Clozel [Clo17].

0.7 An explicit presentation of the Iwasawa algebra for the pro-p Iwahori subgroup of $GL(n, \mathbb{Z}_p)$

Let here G be the pro-p Iwahori subgroup of $SL_n(\mathbb{Z}_p)$, that is, the group of matrices in $SL_n(\mathbb{Z}_p)$ which are upper unipotent modulo the ideal $p\mathbb{Z}_p$. Then the ordered basis is given by

Theorem 0.4 (see Theorem 2.5 of section 2). *The elements*

$$\{x_\beta(p), h_\delta(1+p), x_\alpha(1); \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\}$$

form an ordered basis for the p-valuation ω (definition 2.1) on G, where the ordering is as follows:

(i) first take the lower unipotent matrices in the order given by the (increasing) height function on the roots,
(ii) then take the diagonal elements $h_\delta(1+p)$ for $\delta \in \Pi$ starting from the top left extreme to the low right extreme and,
(iii) finally, take the upper unipotent matrices in the following lexicographic order:
The matrix $(1+E_{i,j})$ comes before $(1+E_{k,l})$ if and only if $i \geq k$ and $i = k \implies j > l$.

That is, for the upper unipotent matrices we start with the low and right extreme and then fill the lines from the right, going up, the matrix $E_{i,j}$ being the standard elementary matrix at $(i,j)^{th}$ place.

The presentation of the Iwasawa algebra $\Lambda(G)$ is given by the following theorem.

Theorem 0.5 (see Theorem 2.4.3 of section 2). *For $p > n+1$, the Iwasawa algebra $\Lambda(G)$ is isomorphic to $\mathcal{A}/\mathcal{R}$, where $\mathcal{A} = \mathbb{Z}_p\{\{V_\alpha, W_\delta, U_\beta, \alpha \in \Phi^+, \beta \in \Phi^-, \delta \in \Pi\}\}$ with the ordering on the variables $V_\alpha, W_\delta, U_\beta$ according to the roots as in theorem 0.4 and $\mathcal{R}$ is the closed two-sided ideal of $\mathcal{A}$ generated by the relations (2.50 − 2.64).*

This gives us the following corollary.

Corollary 0.6 (see corollary 2.15 of section 2). *The Iwasawa algebra of the pro-p Iwahori subgroup of $GL_n(\mathbb{Z}_p)$ is a quotient $\mathcal{A}'/\mathcal{R}$, with $\mathcal{A}' = \mathbb{Z}_p\{\{Z, V_\alpha, U_\beta, W_\delta, \alpha \in \Phi^+, \beta \in \Phi^-, \delta \in \Pi\}\}$ and $\mathcal{R}$ is defined by the relations (2.50 − 2.64) and*
(Comm) Z commutes with $U_\beta, V_\alpha, W_\delta$ for all α, β, δ.

With L a finite unramified extension of $\mathbb{Q}_p$, the explicit presentation can be used to define a "formal base change map" [Clo17] of the Iwasawa algebras

$$\Lambda_L \to \Lambda_{\mathbb{Q}_p}$$

where Λ_L and $\Lambda_{\mathbb{Q}_p}$ are the Iwasawa algebras of the pro-p Iwahori subgroups over L and $\mathbb{Q}_p$ respectively. Such a formal base change map is given by power series which only converge for globally analytic distributions which are continuous dual of the rigid-analytic functions on the pro-p Iwahori seen as a rigid-analytic space ([Clo17]). This leads us also to the study of the globally analytic vectors of p-adic representations discussed in the next section.

Apart from the above implications of our explicit presentation of the Iwasawa algebra, Dong Han and Feng Wei note that our results may provide possible ways to answer the open question on the existence of non-trivial normal elements in $\Omega_G := \Lambda(G) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ (cf. introduction and section 5 of [HW18]). An element $r \in \Omega_G$ is normal if $r\Omega_G = \Omega_G r$. The question on the normal elements was originally posed in [BW13], later reformulated in [HW18], having dealt with the case for $SL(2, \mathbb{Z}_p)$ and $SL(3, \mathbb{Z}_p)$. As noted in [HW18], the normal elements help in constructing reflexive ideals in the Iwasawa algebra. The main question of Han and Wei is to find a mechanism for constructing ideals of completed group algebras without using central elements or closed normal subgroups which provide natural ways to construct ideals in the Iwasawa algebra (*loc.cit*).

Future Questions. The pro-p Iwahori subgroup of $GL(n, \mathbb{Z}_p)$ is a p-saturated group in the sense of Lazard for $p > n+1$. This raises the natural question of whether one can generalize corollary 0.6 in order to obtain an explicit presentation of the Iwasawa algebra for any p-saturated group.

0.8 Globally analytic principal series representation and base change

The second branch of my research focuses on finding the globally analytic vectors, in the sense of Emerton [Eme17], of p-adic representations of $GL_n(\mathbb{Q}_p)$ under the action of the pro-p Iwahori subgroup G of $GL_n(\mathbb{Q}_p)$. We also construct a p-adic base change of the globally analytic principal series to a finite extension of $\mathbb{Q}_p$ satisfying Langlands correspondence. Here we take the pro-p Iwahori (resp. Iwahori) subgroup G (resp. B) to be the subgroup of matrices in $GL_n(\mathbb{Z}_p)$ which are lower unipotent (resp. lower triangular) modulo $p\mathbb{Z}_p$. After the works by Emerton [Eme17], it became clear that generalizing the work done by Schneider and Teitelbaum for the locally analytic representations [ST02b], it is possible to build a corresponding theory for the globally analytic principal series representation under the action of the pro-p Iwahori. We show that the Tate algebra of rigid-analytic functions within the locally analytic principal series is a globally analytic representation of G (theorem 0.7). Furthermore, we determine the condition of irreducibility of the globally analytic principal series (theorem 0.8).

Let K be a finite extension of $\mathbb{Q}_p$. Let us recall the definition of a globally analytic representation. Let $\mathbb{G}$ be the rigid-analytic group whose $\mathbb{Z}_p$-points is the pro-p Iwahori group G, $\mathcal{A}(\mathbb{G}, K)$ be the Tate algebra of globally analytic functions on $\mathbb{G}$ [Bos14], i.e. functions which can be written globally on $\mathbb{G}$ as power series with coordinates of $\mathbb{G}$ having coefficients (in K) going to 0. Let V be a K-Banach space with norm $||\cdot||$. If $g \to \pi(g)$ is a representation of G on V, we say that π (or V) is a globally analytic representation if the map

$$O_v := g \longmapsto g \cdot v = \pi(g)v$$

is a globally analytic function from $\mathbb{G}$ to V. Thus, in coordinates $(x_1, ..., x_d)$ of $\mathbb{G}$, we have:

$$g \cdot v = \sum_{m \in \mathbb{N}^d} \underline{x}^m v_m$$

where $v_m \in V$ and $||v_m|| \to 0$ as $|m| = m_1 + \cdots + m_d \to 0$. Here, $m = (m_1, ..., m_d)$ and $\underline{x}^m = x_1^{m_1} \cdots x_d^{m_d}$, $m_i \in \mathbb{N}$. For the basic properties of the globally analytic representations, see [Eme17]. This definition can be generalized to any rigid-analytic group over $\mathbb{Q}_p$, not just the pro-p Iwahori.

Denote by $\mathbb{P}$ the Borel subgroup of the upper triangular matrices in $GL_n(\mathbb{Q}_p)$, $\mathbb{T}$ the maximal torus of $GL_n(\mathbb{Q}_p)$, P^+ the Borel subgroup of the upper triangular matrices in $GL_n(\mathbb{Z}_p)$, W the ordinary Weyl group of $GL_n(\mathbb{Q}_p)$ with respect to $\mathbb{T}$, $P_w^+ = B \cap wP^+w^{-1}$.

Let χ be a locally analytic character from the torus T_0 of B to $K^\times$, that is, $\chi : T_0 \to K^\times$ with $\chi(t_1, ..., t_n) = \chi_1(t_1) \cdots \chi_n(t_n)$, and $\chi_i(t) = t^{c_i}$ where $c_i = \frac{d}{dt}\chi_i(t)|_{t=1}$ for t sufficiently close to 1, $c_i \in K$, $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}}$ be the locally analytic induction, that is:

$$\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}} := \{f \in \mathcal{A}_{\mathrm{loc}}(GL_n(\mathbb{Q}_p), K) : f(gb) = \chi(b^{-1})f(g), g \in GL_n(\mathbb{Q}_p), b \in \mathbb{P}\},$$

where $\mathcal{A}_{\mathrm{loc}}$ denotes the set of locally analytic functions.

A locally analytic function means that around a neighborhood of a point the function can be written as a power series. We have the B-equivariant decompositions

$$\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}} \cong \mathrm{ind}_{P^+}^{GL_n(\mathbb{Z}_p)}(\chi)_{\mathrm{loc}} \cong \oplus_{w \in W} \mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$$

where the action of χ^w is given by $\chi^w(h) = \chi(w^{-1}hw)$. The first isomorphism is due to Iwasawa decomposition [OS10, sec. 3.2.2] and the second one is due to Bruhat decomposition (*loc. cit.* and [Car79, sec. 3.5]).

The vector space of $\mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$ is isomorphic to the locally analytic functions $\mathbb{Z}_p^m \to K$ for an appropriate dimension m. Let $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ be the Tate algebra of globally analytic functions inside $\mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$, that is, any element of $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ can be written as a power series on the rigid-analytic space $\mathbb{Z}_p^m$ with coefficients in K going to 0.

Similarly define $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi) := \oplus_{w\in W}\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ to be the subspace of globally analytic vectors of $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}}$. Further, assume that χ is analytic i.e. $v_p(c_i) > \frac{e}{p-1} - 1$ where e is the ramification index of K (cf. [Clo16, eq. 3.4]). Recall that G is the group of matrices in $GL_n(\mathbb{Z}_p)$ which are lower unipotent modulo $p\mathbb{Z}_p$, that is, the pro-p Iwahori subgroup.

Generalizing the work of my advisor Clozel for $n = 2$ [Clo16], we prove the following theorem:

Theorem 0.7 (see theorem 3.21 of section 3)**.** *If $p > n+1$ and χ is analytic, then the representation $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ is an admissible globally analytic representation of G. This implies that $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)$ is also a globally analytic representation of G.*

(admissibility is in the sense of Emerton [Eme17]). We need to take $p > n + 1$, so that the pro-p Iwahori subgroup of $GL(n)$ is p-saturated in the sense of Lazard [Laz65, III, 3.2.7.5] and is isomorphic rigid-analytically to the product $\mathbb{Z}_p^d$ [Laz65, III, 3.3.2] (for some d, here $\mathbb{Z}_p$ is seen as a rigid-analytic closed ball of radius 1). For global analyticity, we compute explicitly the action of G on the Tate algebra of globally analytic functions f of $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ and show that the action map $g \to g \cdot f$ is a globally analytic function on $\mathbb{G}$.

Furthermore, we determine the condition of irreducibility of the globally analytic principal series $\mathrm{ind}_{P_0}^{B}(\chi)$ where $P_0 = P_w^+$ with $w = Id$. Let μ be the linear form from the Lie algebra of the torus T_0 to K given by

$$\mu = (-c_1, ..., -c_n) : Diag(t_1, ..., t_n) \mapsto \sum_{i=1}^{n} -c_i t_i$$

where $t = (t_i) \in \mathrm{Lie}(T_0)$. For any negative root $\alpha = (i, j) \in \Phi^-, i > j$, let $H_{(i,j)} = E_{i,i} - E_{j,j}$, where $E_{i,i}$ is the standard elementary matrix.

Theorem 0.8 (see theorem 3.9 of section 3)**.** *Suppose $p > n + 1$ and χ analytic. The globally analytic representation $\mathrm{ind}_{P_0}^{B}(\chi)$ of G is topologically irreducible if and only if for all $\alpha = (i, j) \in \Phi^-$, $-\mu(H_{\alpha=(i,j)}) + i - j \notin \{1, 2, 3, ...\}$.*

Note that for the locally analytic representation $\mathrm{ind}_{P_0}^{B}(\chi)_{\mathrm{loc}}$, this irreducibility result was proved by Orlik and Strauch [OS10] generalizing the original works of Schneider and Teitelbaum [ST02b] for $n = 2$. For the irreducibility of the globally analytic principal series, we first use the action of the Lie algebra of G to show that any non-zero closed G-invariant subspace of $\mathrm{ind}_{P_0}^{B}(\chi)$ contains the constant function 1. The remaining part of the argument for the proof of irreducibility uses the notion of Verma modules and its condition of irreducibility. To ensure the irreducibility of this Verma module we need the condition $-\mu(H_{\alpha=(i,j)}) + i - j \notin \{1, 2, 3, ...\}$ which is a result due to Bernstein-Gelfand in Dixmier (cf. Theorem 7.6.24 of [Dix77]).

Next we proceed to Langlands local base change of irreducible representations of $GL_n(\mathbb{Q}_p)$ to $GL_n(L)$ where L is an unramified cyclic extension of degree N. There are 2 branches; first, the complex representations and second, the p-adic representations. We briefly present the known case of base change for the complex representations. The complex case, studied extensively by Arthur and Clozel [AC89], associates to each admissible irreducible representation of $GL_n(\mathbb{Q}_p)$, an admissible representation π_L of $GL_n(L)$, which is stable under the action of $\mathrm{Gal}(L/\mathbb{Q}_p)$. Many of the properties of the local lifting can be proved by global means, namely the trace formula. This base change map is naturally associated to a homomorphism of the Hecke algebras [AC89, Chapter 1, section 4],

$$b : \mathcal{H}_L \to \mathcal{H}_{\mathbb{Q}_p}$$

where $\mathcal{H}_L, \mathcal{H}_{\mathbb{Q}_p}$ are the unramified Hecke algebras of compactly supported functions invariant by $GL_n(\mathcal{O}_L), GL_n(\mathbb{Z}_p)$.

An important well known example of base change for the complex representations is given by the unramified principal series. Let

$$\pi = \mathrm{ind}_{\mathbb{P}(\mathbb{Q}_p)}^{GL_n(\mathbb{Q}_p)}(\chi_1, ..., \chi_n)$$

be the unitary induction from the Borel subgroup $\mathbb{P}(\mathbb{Q}_p)$ of $GL_n(\mathbb{Q}_p)$, and χ_i are the complex unramified unitary characters of $\mathbb{Q}_p^\times$. Then π is irreducible and the base change of π is given by

$$\pi_L = \mathrm{ind}_{\mathbb{P}(L)}^{GL_n(L)}(\eta_1, ..., \eta_n)$$

where $\eta_i = \chi_i \circ N_{L/\mathbb{Q}_p}$, ($N_{F/\mathbb{Q}_p}$ being the norm map). By the local Langlands conjecture for complex representations ([HT01],[Hen00]), we know that π is associated to a representation R of degree n of the Weil-Deligne group $WD_{\mathbb{Q}_p}$. Then the base change π_L of π is associated to the restriction of R to WD_L, denoted by R_L, i.e.

$$R \leftrightsquigarrow \pi \text{ and } R_L \leftrightsquigarrow \pi_L.$$

A natural question is to construct a local base change, compatible with Langlands functoriality, for the p-adic representations. Very little is know in this p-adic case. Clozel in [Clo16] proposed to use the Steinberg's tensor product theorem. Namely, if π is a p-adic representation of $GL_n(\mathbb{Q}_p)$, then a possible candidate for the base change π_L of π is the completed tensor product of π^σ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$, that is,

$$\pi_L = \widehat{\otimes}_\sigma \pi^\sigma.$$

This is carried out in section 3 for the globally analytic principal series representation. More precisely, having found out the globally analytic vectors of the principal series induced from the Borel, under the action of the pro-p Iwahori subgroup G over $\mathbb{Q}_p$, we apply the Steinberg tensor product theorem and we obtain a representation of $G(L)$ (compare also [Clo16, section 3.2]). For each $w \in W$, consider the globally analytic admissible representation $I_{w,\mathbb{Q}_p}(\chi) := \mathrm{ind}_{P_w^+}^B(\chi^w)$ of $G(\mathbb{Q}_p)$. The globally analytic representation $\mathrm{ind}_{P_w^+}^B(\chi^w)$ extends naturally to a globally analytic admissible representation of $G(L)$, called the "holomorphic base change" (3.2.2), which we denote by $I_{w,L}(\chi)$.

The Langlands base change (3.2.2) of this globally analytic principal series, given by the Steinberg tensor product theorem, then satisfies the following theorem:

Theorem 0.9 (see theorem 3.22 of section 3)**.** *Assume $p > n+1$ and χ analytic. The Langlands base change $\oplus_{w\in W}(\widehat{\otimes}_\sigma\, I_{w,L}(\chi^w)^\sigma)$ is a globally analytic admissible representation of $G(L)$ where $\sigma \in \Sigma = \mathrm{Gal}(L/\mathbb{Q}_p)$.*

The analogue of the base change transfer homomorphism between the unramified Hecke algebras $b : \mathcal{H}_L \to \mathcal{H}_{\mathbb{Q}_p}$, in the p-adic case, can be seen from a "formal" map between the Iwasawa algebras which makes sense (or is well-defined) only for the globally analytic distributions on the group, seen as a rigid-analytic space. More precisely, as we already mentioned before, using the explicit presentation of the Iwasawa algebra of the pro-p Iwahori subgroup of $GL(n)$, one can define a formal homomorphism

$$b : \Lambda_L \to \Lambda_{\mathbb{Q}_p}$$

exactly similar as in the classical situation between unramified Hecke algebras, where Λ_L and $\Lambda_{\mathbb{Q}_p}$ are the Iwasawa algebras of the pro-p Iwahori of $GL_n(L)$ and $GL_n(\mathbb{Q}_p)$ respectively. Clozel constructed it for $GL(2)$ [Clo17] and we believe, by our results of section 2, that his construction easily extends to $GL(n)$.

Future Questions. It is an interesting future project to determine the globally analytic vectors of more general p-adic representations of $GL(2, \mathbb{Q}_p)$, for example, the "trianguline" representation of Colmez [Col08] (see also [Col14]), which corresponds to a quotient of the principal series. Also, one can explore the connection with the globally analytic vectors of p-adic representations (under the pro-p Iwahori or a suitable rigid-analytic subgroup of $GL(2)$) and (φ, Γ)-modules [Col10], similar to the existing correspondence for the locally analytic representations [CD14, Sec VI.3].

0.9 Constructing Galois representations with big open images

In the second part of the thesis we are concerned with number fields which are called "p-rational" extensions of $\mathbb{Q}$ which play a major role in the classical Iwasawa theory and Galois representations. In order to give a motivation for them and relate it with our work concerning Iwasawa algebras in Part I, it is necessary to introduce a well known problem in Iwasawa theory on which K. Iwasawa worked in the 1950's.

Let now K be a finite extension of $\mathbb{Q}$, K_∞ is a $\mathbb{Z}_p$-extension of K with Galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$. Set $K_m = K_\infty^{\Gamma_m}$ where Γ/Γ_m is cyclic of order p^m. Then the main object of Iwasawa theory began by studying the class numbers of the following tower of number fields,

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \subset \cdots$$

where K_m/K is a cyclic extension of degree p^m and $K_\infty = \cup_m K_m$. Iwasawa noticed that if p^{e_m} is the highest power of p dividing the class number of K_m, then there exists integers λ, μ, ν such that

$$e_m = \lambda m + \mu p^m + \nu$$

for all sufficiently large m. The main ingredient in the proof is based on considering the Galois group $\mathrm{Gal}(F_\infty/K_\infty)$ (here $F_\infty = \cup_m F_m$ and F_m is the maximal abelian p-extension of K_m which is unramified at all primes of K_m) and viewing this Galois group as a module over the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$.

This motivates us to look at number fields K such that the Galois group of the maximal pro-p extension M unramified outside p is a free pro-p group. That is, with M^{ab} the maximal abelian pro-p extension of K unramified outside p, we have

1. $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(M^{ab}/K)) = r_2 + 1$ (Leopoldt's conjecture for K and p),

2. $\mathrm{Gal}(M^{ab}/K)$ is torsion free as a $\mathbb{Z}_p$-module,

here (r_1, r_2) is the signature of K. Such fields verifying (1) and (2) above are called "p-rational" and have several applications in representation theory [JNQD93], [Mov88b], [Gre16]. The simplest example of p-rational field is $\mathbb{Q}$, where M is the cyclotomic $\mathbb{Z}_p$-extension. Other examples of p-rational fields are $\mathbb{Q}(\mu_p)$, where μ_p is a primitive p-th root of unity and p is a regular prime.

One important representation theoretic application of such fields was carried out by R. Greenberg in 2016 [Gre16], where he constructed Galois representations with open image in $GL_n(\mathbb{Z}_p)$. More precisely, Greenberg has shown that if $p \geq 4[\frac{n}{2}] + 1$ and p is regular and $K = \mathbb{Q}(\mu_p)$, then there exists a continuous representation

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to GL_n(\mathbb{Z}_p)$$

with open image. Greenberg's result is particularly noteworthy since the standard source of Galois representation is algebraic geometry (e.g. abelian varieties, automorphic forms etc.), whereas the construction by Greenberg is not geometric. This raises a natural question of whether one can construct such representation with big open image for any reductive group.

In collaboration with Christophe Cornut [CR18], we construct Galois representations of the absolute Galois group of $\mathbb{Q}$ with big open images in $\mathbf{G}(\mathbb{Z}_p)$, where $\mathbf{G}$ is an adjoint simple split reductive group over $\mathbb{Z}_p$. We are proving a result which shows the existence of a p-adic Lie extension of $\mathbb{Q}$ where the Galois group corresponds to a certain specific p-adic Lie algebra. Generalizing the construction by Greenberg for $GL(n)$ [Gre16], we obtain the following result.

Theorem 0.10 (Corollary 4.22 of section 4)**.** *Let $\mathbf{G}$ be an adjoint simple split reductive group over $\mathbb{Z}_p$ with the Iwahori subgroup I and the pro-p Iwahori subgroup $I(1)$. Let K be the cyclotomic field $\mathbb{Q}(\mu_p)$ and M be the maximal pro-p extension of K, unramified outside the places of K above p. Then, there is a constant c depending only upon the type of $\mathbf{G}$ such that if $p > c$ is a regular prime, there is a continuous morphism*

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to I$$

with $\rho(\mathrm{Gal}(M/K)) = I(1)$.

The pro-p Iwahori subgroup $I(1)$ is of finite index in $\mathbf{G}(\mathbb{Z}_p)$. Theorem 0.10 constructs Galois representation with image containing $I(1)$. Thus the representations of theorem 0.10 have large open images. The way of proving theorem 0.10 is by finding a minimal set of topological generators of $I(1)$. For a regular prime p, $K = \mathbb{Q}(\mu_p)$, a result of Shafarevich gives that $\mathrm{Gal}(M/K)$ is a free pro-p group showing that $\mathbb{Q}(\mu_p)$ is p-rational. Then we construct a continuous homomorphism from $\mathrm{Gal}(M/K)$ to $I(1)$, by sending generators of $\mathrm{Gal}(M/K)$ to the topological generators of $I(1)$, such that the homomorphism extends to $\mathrm{Gal}(M/\mathbb{Q})$. In the following theorem, we find a minimal set of topological generators of the pro-p Iwahori subgroup of any split reductive group $\mathbf{G}$ (not necessarily adjoint) over $\mathbb{Z}_p$ with torus $\mathbf{T}$.

Theorem 0.11 (Theorem 4.1 of section 4)**.** *The following elements form a minimal set of topological generators of the pro-p-Iwahori subgroup $I(1)$ of $G = \mathbf{G}(\mathbb{Z}_p)$:*

1. *the semi-simple elements $\{s(1+p) : s \in \mathcal{S}\}$ of $T(1)$,*

2. *for each* $c \in \mathcal{C}$, *the unipotent elements* $\{x_\alpha(1) : \alpha \in \Pi_c\}$,

3. *for each* $c \in \mathcal{C}$, *the unipotent element* $x_{-\alpha_{c,max}}(p)$,

4. *if* $p = 3$, *for each* $d \in \mathcal{D}$, *the unipotent element* $x_{\delta_d}(1)$.

Here, $T(1)$ is the maximal split torus of $I(1)$, $\mathcal{C}$ is the number of irreducible components of the roots Φ (that is, $\Phi = \coprod_{c\in\mathcal{C}} \Phi_c$ and the simple roots $\Pi = \coprod_{c\in\mathcal{C}} \Pi_c$), $\alpha_{c,max}$ the highest positive root in the root component Φ_c, $\mathcal{D} \subset \mathcal{C}$ is the set of irreducible components of type G_2. For $d \in \mathcal{D}$, $\delta_d \in \Phi_{d,+}$ (the positive roots of Φ_d) is the sum of the two simple roots in Π_d and we fix a set of representatives $\mathcal{S} \subset M^\vee = X_*(\mathbf{T})$ (co-characters of $\mathbf{T}$) which form a $\mathbb{F}_p$-basis of $(M^\vee/\mathbb{Z}\Phi^\vee) \otimes \mathbb{F}_p = \oplus_{s\in\mathcal{S}}\mathbb{F}_p \cdot s \otimes 1$. For $t \in \mathbb{Z}_p$, recall that $x_\alpha(t) = exp(tX_\alpha)$ is the one dimensional unipotent subgroup of $\mathbf{G}(\mathbb{Z}_p)$ corresponding to the root $\alpha \in \Phi$. Here $(X_\alpha)_{\alpha\in\Phi}$ is a Chevalley system of the Lie algebra of G. For example, if $G = GL(n, \mathbb{Z}_p)$ and $\alpha = (i, j)$, then $x_\alpha(t) = 1 + tE_{i,j}$ for the standard elementary matrix $E_{i,j}$.

Our constructions give the Galois extension M over $\mathbb{Q}$ such that $\mathrm{Gal}(M^{\ker(\rho)}/\mathbb{Q})$ is a p-adic Lie group which contains the pro-p Iwahori subgroup of an adjoint, split, simple group as a subgroup of finite index. This proves the classical inverse Galois problem for simple p-adic Lie algebras: if L is any finite dimensional simple Lie algebra over $\mathbb{Q}_p$, then there exists a Galois extension over $\mathbb{Q}$ such that the Galois group is a p-adic Lie group whose Lie algebra is isomorphic to L. Note that our construction works only under the assumption of p-rationality.

The p-rational totally real fields satisfy Greenberg's λ and μ invariant conjecture which says that, for a totally real number field k, the Iwasawa $\lambda = \lambda_p(k)$ and $\mu = \mu_p(k)$ invariants associated to the ideal class of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k are 0 (cf. [Gra16a], [Gre76], see also [Was97] for the fact that $\mu = 0$ when k is abelian). These fields are also useful for developing p-adic approaches to solve the above Greenberg's λ and μ invariant conjecture (cf. [Gra16a],[JNQD93]).

Future Questions. There are a list of open questions, originally asked by Greenberg, concerning the construction of Galois representations with open image which are geometric and have nice arithmetic properties at p. In particular, one can wonder to construct the representation ρ so that the restriction of ρ to a decomposition subgroup is crystalline or Hodge-Tate. Also, one may ask the question of the existence of representations of the local absolute Galois group $\mathrm{Gal}(K_\mathfrak{p})$ with open image having good arithmetic properties. Here $K_\mathfrak{p}$ is the completion of a p-rational field K at a prime $\mathfrak{p}$ above p. One can find more discussion on the open questions in [Gre16, Remark 6.4]. Compare also the recent results of [Kat17].

0.10 Numerical experiments and heuristics on Greenberg's p-rationality conjecture

Note that our construction in section 0.9 works only under the assumption of p-rationality. Therefore, we focus our attention to the study of p-rational fields from a computational point of view in section 5.

Section 5 (in collaboration with Razvan Barbulescu) grew out of a conjecture of Greenberg [Gre16, Conjecture 4.8], namely, for any p and t, there exists a p-rational field K with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$. In other words, one can construct a p-rational field as a compositum of quadratic extensions. However, Greenberg gives examples ($p = 3, 5$ and $t = 5, 6$, cf. [Gre16]) of p-rational fields satisfying his conjecture. Greenberg was interested in this conjecture because it allowed him to generalize his construction to produce more examples of Galois representations with big open image assuming the existence of such p-rational fields.

This proposes us to find new algorithmic techniques to determine p-rationality of a number field in a computationally fast and efficient way and to study the density of p-rational fields. One can also generalize Greenberg's conjecture for any field with Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ where q is a prime different from p. To fix ideas, for a finite group G, we say that $\mathrm{GC}_\infty(G, p)$ (i.e. Greenberg's conjecture for G and p) holds if there exists infinitely many number fields of Galois group G which are p-rational. This can be thought of a refinement of the inverse Galois problem for number fields with the condition that now we want p-rational fields. We have examples of p-rational fields for

$G = (\mathbb{Z}/2\mathbb{Z})^t, (\mathbb{Z}/3\mathbb{Z}), \mathbb{Z}/4\mathbb{Z}, V_4, D_4, A_4, S_4$ when $p \in [5, 97]$ and $t \in [7, 11]$ (section 5.11, example 5.34 and table 1 of section 5).

First, in section 5, we relate the notion of p-rationality to that of the class number and the p-adic regulator, which is enough to prove $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ and to give examples of Greenberg's p-rationality conjecture with Galois group $(\mathbb{Z}/2\mathbb{Z})^t$ for $t \in [7, 11]$ and $p \in [5, 97]$. We then recall existing conjectures ([CM90], [CL84b], [CL84a], [CM87], [HZ16]) on the divisibility of the class number and the normalized p-adic regulator by a prime p due to Cohen-Lenstra-Martinet (for the class number) and Hofmann-Zhang (for the p-adic regulator).

Cohen-Lenstra-Martinet in 1989 tested their conjecture and wrote that "we believe that the poor agreement [with the tables] is due to the fact that the discriminants are not sufficiently large". Puzzled by this assertion we repeated their computations and made statistics on the fields of conductor less than 8000, i.e. discriminant less than 64×10^6, which was the bound for the computations of that time (e.g. [Gra75] considered the fields of conductor less than 4000). Since then computers' capabilities have increased by more than a factor 1000 so that we could compute the statistics for fields of conductor less than 10^7, i.e. discriminant less than 10^{14}, in roughly one calendar month, in parallel on several 30 cores and summed up to roughly 2.5 CPU years.

Looking at the data in Table 4 we understand what happened: the convergence speed to the mean density is very slow and the statistics to 8000 have a relative error between 19% and 100% which didn't allow Cohen and Martinet to conclude. However, statistics to 10^7 have only a relative error between 0.2% and 15.5%, so we can conclude that the numerical data confirms their conjecture. Note that the best known algorithms to actually compute the class number of a number field are slow and so the trick we used is an algorithm to test the divisibility by p of the class number of cyclic cubic fields of discriminant less that 10^{14} without computing the class number, due to N.-M. Gras [Gra75], using the notion of cyclotomic units (section 5.8).

Moreover, we give a new algorithm to produce units in cyclic cubic fields which is used to test the valuation in p of the p-adic regulator, which is faster than computing a system of fundamental units (section 5.9). An algorithm [PV15] of Pitoun and Varescon to test p-rationality for arbitrary number fields, allows us to give examples of p-rational number fields of non-abelian Galois groups (example 5.34 of section 5).

Furthermore, we find a family of cyclic cubic number fields which contains infinitely many 5-rational fields under a list of arithmetic assumptions (section 5.11). The reduces the problem of providing examples of 5-rational cubic cyclic fields to the problem of testing just a list of arithmetic assumptions reducing vastly the computational time.

Based on existing conjectural results and our numerical computations verifying those conjectures on the divisibility of the class number and the normalized p-adic regulator by a prime p we show that for $q = 2$ or 3 and $p > 5q^t$ then for any integer t, $\mathrm{GC}_\infty((\mathbb{Z}/q\mathbb{Z})^t, p)$ holds.

Let Φ_m denote the cyclotomic polynomial associated to m and $\varphi(m)$ its degree. Joint with Barbulescu Razvan, our main theorem is

Theorem 0.12 (Theorem 5.6 of section 5)**.** *Let p be an odd prime. Then*

1. *there exists infinitely many quadratic p-rational number fields.*
2. *Assume there exist infinitely many odd integers a such that $m = \frac{1}{4}(a^2+27)$ is prime and such that the arithmetic conditions in Hypothesis 5.35 are satisfied. Then $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, 5)$ holds.*
3. *Under conjectures based on heuristics and numerical experiments (Conjecture 5.41 and Conjecture 5.39), when $q = 2$ or 3, for any prime p and any integer t such that $p > 5q^t$, $\mathrm{GC}_\infty((\mathbb{Z}/q\mathbb{Z})^t, p)$ holds.*

Here, conjecture 5.39 of section 5 gives the probability of the class number h_K of a number field K to be coprime to p with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$ or $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^t$. This conjecture is a reformulation of Cohen-Martinet heuristics [CM90], [CL84b] and Kuroda's class number formula [Kur50], [Lem94]. We have also verified this conjecture numerically for number fields K with Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ with conductor $\leq 10^6$ and primes in $[5 - 19]$ (see table 5). Moreover, we have also tested for cyclic cubic number fields with conductor $\leq 10^7$ and primes in $[5 - 19]$ (see table 4). As we already mentioned, since we have computed cyclic cubic number fields with large discriminants our computations, in particular, matches with Cohen-Lenstra-Martinet heuristics with a relative error of 0.2% to 15.5%.

Also, conjecture 5.41 of section 5 is a reformulation of the Hofmann and Zhang's conjecture which gives the density of totally real number fields with Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ (where $q = 2$ or 3)

for which the normalized p-adic regulator is divisible by p for at least one of its cyclic subfields. We have also supported conjecture 5.4 with numerical evidence where the sample consists of all number fields $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ with $d_1, d_2 \in [2, 300]$ squarefree and distinct, and $p = 5, 7, 11$ (cf. table 6).

The algorithms can be found in the online complement [BR17a].

Future Questions. To sum up, Greenberg's conjecture is solved in the particular case of $G = \mathbb{Z}/2\mathbb{Z}$ and it is well supported by heuristics and numerical experiments for $G = (\mathbb{Z}/q\mathbb{Z})^t$ when $q = 2$ or 3. In the general case of non-abelian Galois groups however our results are limited to a list of examples.

The problem raises new questions about the independence of class numbers and of p-adic regulators, which could be tackled by techniques of analytic number theory, similar to the recent progress on the Cohen-Lenstra-Martinet heuristic. It is interesting to create new algorithms to test divisibility of p-regulator and of the class number by p with a better complexity than computing a system of fundamental units and respectively the class number.

Part I
Algebras of functions and distributions on p-adic groups and p-adic representation theory

Table of Contents

1 Iwasawa algebras for the first congruence kernel of Chevalley groups

1.1 Introduction

Lazard, in his seminal work [Laz65], II.2.2 studied non-commutative Iwasawa algebras for pro-p groups. They are completed group algebras

$$\Lambda(P) = \varprojlim_{N \in \mathcal{N}(P)} \mathbb{Z}_p[P/N]$$

where $\mathcal{N}(P)$ is the set of open normal subgroups of P. For any odd prime p, Clozel in his paper [Clo11] gives an explicit presentation of the Iwasawa algebra of the subgroup of level 1 of $SL_2(\mathbb{Z}_p)$, which is $\Gamma_1(SL_2(\mathbb{Z}_p)) = \ker(SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p))$. Notice that as $\Gamma_1(SL_2(\mathbb{Z}_p)) \cong \mathbb{Z}_p^3$, its (non-commutative) Iwasawa algebra is isomorphic (as a topological $\mathbb{Z}_p$-*module*) to the ring of power series in three variables. The key ingredient in Clozel's proof was to compute the relations between those variables viewing them as elements of the Iwasawa algebra. The case $p = 2$ has to be omitted because then $\Gamma_1(SL_2(\mathbb{Z}_p))$ will have p-torsion and thus its Iwasawa algebra is not an integral domain which prevents one from using deep results of Lazard.

Our main result is to give an explicit presentation, by generators and relations, of the Iwasawa algebra for the subgroup of level 1 of a semi-simple, simply connected, split Chevalley group over $\mathbb{Z}_p$. Let G be a semi-simple, simply connected Chevalley group over $\mathbb{Z}_p$ with a split maximal torus T, Φ be the root system of the Lie algebra of G with respect to the Lie algebra of T, Π be a set

of simple roots of Φ. Under a faithful representation of group schemes $G \hookrightarrow GL_n$ over $\mathbb{Z}$, consider $G(1)$-the pullback of the congruence kernel at level 1 of $GL_n(\mathbb{Z}_p)$. The natural filtration of $G(1)$ by deeper congruence subgroups enables us to define a p-valuation ω on $G(1)$ (sec. 1.4).

Let us now present a brief overview of the results obtained in this section.

- The first result is to find an ordered basis of $G(1)$, in the sense of Lazard, with respect to its p-valuation (sec. 1.3). Such an ordered basis is constructed in theorem 1.9. For the proof we have used the triangular decomposition of $G(1)$ and the assumption that our group G is simply connected.

- The second result concerns the presentation of the Iwasawa algebra of $G(1)$ in terms of generators and relations. Let $\mathcal{A}$ be the universal non-commutative p-adic algebra over $\mathbb{Z}_p$ in the variables $\{V_\alpha, W_\delta; \alpha \in \Phi, \delta \in \Pi\}$; the ordering being given by the increasing height function on the roots. The algebra $\mathcal{A}$ has a topology given by the filtration by the powers of its unique maximal ideal. The algebra $\mathcal{A}$ is naturally sent to $\Lambda(G(1))$ (cf. 1.6). Computing in $\Lambda(G(1))$, we obtain the relations between the variables in $\mathcal{A}$ precisely given by $(1.15, 1.16, 1.17, 1.18)$ and let $\mathcal{R}$ be the closed two-sided ideal generated by the relations in $\mathcal{A}$. Then our main result is (cf. Theorem 1.22)

  Theorem. *For $p > 2$, the Iwasawa algebra $\Lambda(G(1))$ is naturally isomorphic as a topological ring to $\mathcal{A}/\mathcal{R}$.*

  To compute the relations between the variables in $\mathcal{A}$, we have used the Steinberg's Chevalley relations for simply connected groups ([Ste67]). The advantage of this description of the Iwasawa algebra is not only its simplicity but also the fact that it allows one to do explicit computations about its center. For example, for the group $\Gamma_1(SL_2(\mathbb{Z}_p))$, Clozel used his presentation to show that the center of the Iwasawa algebra of $\Gamma_1(SL_2(\mathbb{Z}_p))$ is composed of the multiple of the Dirac measure at 1, thus giving a different proof of Ardakov's result (cf. [Ard04]).

Hence, the objective is to solve two problems: firstly finding an ordered basis for the p-valuable group $G(1)$, secondly to use it to give an explicit presentation of the Iwasawa algebra of $G(1)$.

Roadmap. In Section 1.2 we go for a quick tour through the notions of p-valuable groups and Chevalley groups that we need. In section 1.3 we construct an ordered basis of $G(1)$ in theorem 1.9, an alternative proof of which is provided in section 1.4 using the theory of uniform pro-p groups (cf. [DSMS03]). Then, in section 1.5, we use Steinberg's relations of Chevalley groups to compute the relations in $\Lambda(G(1))$. Finally, in section 1.6, we first provide an explicit presentation of the Iwasawa algebra of $G(1)$ with coefficients in $\mathbb{F}_p$ (cf. theorem 1.21) and then we lift its coefficients to $\mathbb{Z}_p$ to prove our main result, which is theorem 1.22.

1.2 Recall on p-valued groups and Chevalley groups

Let G be any abstract group. We recall that an application

$$\omega : G \to \mathbb{R}_+^* \cup \{+\infty\}$$

is called a filtration (cf. [Laz65], II.1.1.1) if the following conditions hold for all $x, y \in G$:

1. $\omega(xy^{-1}) \geqslant \min(\omega(x), \omega(y))$,
2. $\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y)$.

If ω is such a filtration, then G is called a filtered group and $\omega(x)$ is called the filtration of the element x.

For any $v \in \mathbb{R}_+^*$, we define the subgroups

$$G_v = \{x \in G | \omega(x) \geqslant v\} \text{ and } G_{v+} = \{x \in G | \omega(x) > v\}.$$

Then the subgroups G_v satisfy the following three relations:

1. $G = \cup_{v>0} G_v$,

2. $[G_v, G_{v'}] \subset G_{v+v'}$ for $v, v' \in \mathbb{R}_+^*$,

3. $G_v = \cap_{v' \leq v} G_{v'}$ for $v \in \mathbb{R}_+^*$,

where $[G_v, G_{v'}]$ is the commutator subgroup of G_v and $G_{v'}$. Conversely, if there exists a family of subgroups G_v satisfying the above three relations then we can define a filtration ω by the formula

$$\omega(x) = \sup v \text{ for } x \in G_v.$$

(Cf. Lazard, [Laz65], II.1.1.2.4). Such a filtration ω is called separated if $\omega(x) = +\infty$ implies $x = 1$. For a prime number p and for all $v \in \mathbb{R}_+$, we define

$$\varphi(v) = \min(v + 1, pv).$$

The filtration ω is called a p-filtration if it verifies the following axiom:

$$\omega(x^p) \geqslant \varphi(\omega(x)) \text{ for } x \in G,$$

that is,

$$\omega(x^p) \geq \min(\omega(x) + 1, p\omega(x)).$$

In that case, G is said to be a p-filtered group with the p-filtration ω.

Definition 1.1. *A filtered group G is p-valued if, for all $x \in G$, ω satisfies the following three axioms:*

$$\omega(x) < \infty, \ x \neq 1,$$
$$\omega(x) > (p-1)^{-1},$$
$$\omega(x^p) = \omega(x) + 1.$$

Such a group G is also called p-valuable, and ω is called a p-valuation on G with the convention $\omega(1) = \infty$. Henceforth, we assume that G is a profinite group and ω is a p-valuation on G which defines the topology of G.

The G_v's form a decreasing filtration of G, so there exists a unique topology on G (the topology defined by the filtration) such that G_v's form a fundamental system of open neighborhoods of identity. It is the topology defined by ω. We put for each $v > 0$,

$$\mathrm{gr}_v G := G_v / G_{v+} \text{ and } \mathrm{gr}(G) := \oplus_{v>0} \mathrm{gr}_v G.$$

The commutator induces a Lie bracket on $\mathrm{gr}(G)$ which gives $\mathrm{gr}(G)$ the structure of a Lie algebra over $\mathbb{F}_p$. The map P defined by

$$P : \mathrm{gr}(G) \to \mathrm{gr}(G), \ P(gG_{v+}) = g^p G_{(v+1)+}$$

is an $\mathbb{F}_p$-linear map on $\mathrm{gr}(G)$, which gives $\mathrm{gr}(G)$ the structure of a graded Lie algebra over $\mathbb{F}_p[P]$ (cf. [Laz65], III.2.1.1).

Definition 1.2. *The pair (G, ω) is called of finite rank if $gr(G)$ is finitely generated over $\mathbb{F}_p[P]$.*

As $\mathrm{gr}(G)$ is a torsion free module over $\mathbb{F}_p[P]$ (cf. [Sch11], remark 25.2), being finitely generated torsion free module over a principal ideal domain $\mathbb{F}_p[P]$, it is free over $\mathbb{F}_p[P]$. We define

$$\mathrm{rank}(G, \omega) := \mathrm{rank}_{\mathbb{F}_p[P]} \mathrm{gr} G.$$

For $g_1, ..., g_d \in G$, we consider the continuous map

$$\mathbb{Z}_p^d \to G, \ (x_1, ..., x_d) \mapsto g_1^{x_1} \cdots g_d^{x_d}. \tag{1.1}$$

The map above depends on the order of $g_1, ..., g_d$ and hence it is not a group homomorphism.

Definition 1.3. *The sequence of elements $(g_1, ..., g_d)$ in G is called an ordered basis of (G, ω) if the map in (1.1) is a bijection (and hence, by compactness, a homeomorphism) and*

$$\omega(g_1^{x_1}, \cdots, g_d^{x_d}) = \min_{1 \leqslant i \leqslant d} (\omega(g_i) + val_p(x_i)) \text{ for } x_i \in \mathbb{Z}_p. \tag{1.2}$$

If (G,ω) is of finite rank, then the rank of gr$G$ over $\mathbb{F}_p[P]$ is finite. Following [Sch11] (proposition 26.5), we can relate the basis of G to the basis of $\mathrm{gr}(G)$ over $\mathbb{F}_p[P]$. In fact, the following lemma holds.

Lemma 1.4. *The sequence $(g_1,...,g_d)$ is an ordered basis of (G,ω) if and only if $\sigma(g_1),...,\sigma(g_d)$ is a basis of the $\mathbb{F}_p[P]$-module $gr(G)$ where for $g\neq 1$, $\sigma(g):=gG_{\omega(g)+}\in gr(G)$.*

In particular a p-valuation ω of G is a p-filtration, separated for which $\mathrm{gr}_v(G)=0$ for $v\leqslant (p-1)^{-1}$, and $\mathrm{gr}(G)$ is torsion free (cf. the discussion after 2.1.2.3, chap III of [Laz65]).

Let G be a p-valued group, complete, with discrete filtration. Let $g_1,...,g_d$ be an ordered basis. Then G is defined to be p-saturated (cf. [Laz65], III.2.2.7) if the valuations $\omega(g_i)$ satisfy the following relation:

$$(p-1)^{-1}<\omega(g_i)\leqslant p(p-1)^{-1},\ i\in[1,d]. \tag{1.3}$$

In the remaining part of this section, we introduce the basic notion of Chevalley groups over $\mathbb{Z}$ (cf. [Che95],[Kos66]) following section 1 of [Abe69] . Steinberg gives the construction in [Ste67].

Let $G_{\mathbb{C}}$ be a connected complex semi-simple Lie group, $T_{\mathbb{C}}$ a maximal torus of $G_{\mathbb{C}}$, $\mathfrak{g}_{\mathbb{C}},\mathfrak{t}_{\mathbb{C}}$ be the Lie algebras of $G_{\mathbb{C}}$ and $T_{\mathbb{C}}$ respectively. Let Φ be the root system of $\mathfrak{g}_{\mathbb{C}}$ with respect to $\mathfrak{t}_{\mathfrak{C}}$, $\Pi=\{\delta_1,...,\delta_l\}$ be a set of simple roots of Φ, $\mathfrak{g}_{\mathbb{Z}}$ be a Chevalley lattice (cf. Theorem 1 of [Ste67]) of $\mathfrak{g}_{\mathbb{C}}$ generated by the Chevalley basis (cf. p.6 of [Ste67]) $\{H_{\delta_1},...,H_{\delta_l},X_\gamma,\gamma\in\Phi\}$. For each $\gamma\in\Phi$, the element $H_\gamma=[X_\gamma,X_{-\gamma}]$ is contained in the submodule $\mathfrak{t}_{\mathbb{Z}}=\mathfrak{g}_{\mathbb{Z}}\cap\mathfrak{t}_{\mathbb{C}}$. We then have, by definition of the Chevalley basis,

(a) $\gamma(H_\gamma)=2,\gamma\in\Phi$,
(b) if γ_1,γ_2 are roots, then $\gamma_2(H_{\gamma_1})=v-u$, where v,u are the non-negative integers such that $\gamma_2+i\gamma_1$ is a root if and only if $-v\leq i\leq u$, or
(c) if γ_1,γ_2 and $\gamma_1+\gamma_2$ are roots, $[X_{\gamma_1},X_{\gamma_2}]=N_{\gamma_1,\gamma_2}X_{\gamma_1+\gamma_2}$, where $N_{\gamma_1\gamma_2}=\pm(v+1)$.

Let ρ be a faithful representation of $G_{\mathbb{C}}$ in an n-dimensional vector space V over $\mathbb{C}$, $d\rho$ the differential of ρ which is a representation of $\mathfrak{g}_{\mathbb{C}}$ in V. Then, there exists (cf. p.17 of [Ste67]) a free n-dimensional, $\mathbb{Z}$-module $V_{\mathbb{Z}}$ generated by $\{v_1,...,v_n\}$ in V which is stable under the action of the universal enveloping algebra $\mathfrak{U}_{\mathbb{Z}}$. We also have

$$d\rho(H_\gamma)v_i=\lambda_i(H_\gamma);1\leq i\leq n,\gamma\in\Phi$$

where λ_i are linear functions on $\mathfrak{t}_{\mathbb{C}}$ with $\lambda_i(H_\gamma)\in\mathbb{Z}$. The base $\{v_1,...,v_n\}$ of $V_{\mathbb{Z}}$ determines the coordinates $x_{ij}(1\leq i,j\leq n)$ on $GL(V)$ and the restrictions of x_{ij} to $G_{\mathbb{C}}$ generate a subring $\mathbb{Z}[G]$ of the affine algebra $\mathbb{C}[G]$ of $G_{\mathbb{C}}$. The ring $\mathbb{Z}[G]$ has a structure of a Hopf algebra (cf. section 1 of [Abe69]) and defines a group scheme G over $\mathbb{Z}$. Namely,

$$R\to G(R)=Hom(\mathbb{Z}[G],R)$$

is a contravariant functor from the category of commutative unitary rings into the category of groups. We call the group G the Chevalley group scheme associated with $G_{\mathbb{C}}$.

Now, for any $t\in\mathbb{C}$, $x_\gamma(t)=exp\ td\rho(X_\gamma),(\gamma\in\Phi)$, is an element of $G_{\mathbb{C}}$ and the coordinates of $x_\gamma(t)$ are polynomial functions on t with coefficients in $\mathbb{Z}$. Let $\mathbb{Z}[\zeta]$ be the algebra over $\mathbb{Z}$ generated by one variable ζ. Then there exists a homomorphism of $\mathbb{Z}[G]$ onto $\mathbb{Z}[\zeta]$ which assigns to each x_{ij} the (i,j)-coordinate of $x_\gamma(\zeta)$. The homomorphism induces an injective homorphism of groups

$$G_\gamma(R)=Hom(\mathbb{Z}[\zeta],R)\to G(R)=Hom(\mathbb{Z}[G],R)$$

We denote also by $x_\gamma(t),t\in R$, the element of $G(R)$ corresponding to an element of $G_\gamma(R)$ such that $\zeta\to t$.

Let P(resp. X,P_r) the additive group generated by the weights of all the representations of G (resp. the weights of ρ, the roots of $\mathfrak{g}_{\mathbb{C}}$). Then these are all free abelian groups of rank l such that $P\supseteq X\supseteq P_r$. The group G is said to be simply connected or universal if $P=X$. Henceforth we fix the ring R to be $\mathbb{Z}_p$, p being an odd prime, and we always work with the simply connected group denoted G, and $G(\mathbb{Z}_p)$ will denote its $\mathbb{Z}_p$-points.

For $\lambda\in\mathbb{Q}_p^*,\gamma\in\Phi$, we define

$$h_\gamma(\lambda):=w_\gamma(\lambda)w_\gamma(1)^{-1}$$

where

$$w_\gamma(\lambda):=x_\gamma(\lambda)x_{-\gamma}(-\lambda^{-1})x_\gamma(\lambda).$$

Given our embedding $\rho:G\hookrightarrow GL_n$, let us define, for $k\in\mathbb{N}$,

$$\Gamma(k) := \ker(GL_n(\mathbb{Z}_p) \to GL_n(\mathbb{Z}_p/p^k\mathbb{Z}_p))$$

(the $\mathbb{Z}$-structure on GL_n being given by $V_{\mathbb{Z}}$) and $G(k) := G(\mathbb{Z}_p) \cap \Gamma(k)$. Then $G(k)$ is called the k^{th} congruence kernel of $G(\mathbb{Z}_p)$ which satisfies a descending filtration $G(1) \supseteq G(2) \supseteq \cdots$.

1.3 Ordered basis of $G(1)$

Let us define ω, a function on the first congruence kernel $G(1)$, by

$$\omega(x) = k \text{ for } x \in G(k)\backslash G(k+1). \tag{1.4}$$

We then show in theorem 1.5 that ω is a p-valuation on $G(1)$. Furthermore, we show in theorem 1.9 that $\{x_\beta(p), h_\delta(1+p), x_\alpha(p);\ \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\}$ forms an ordered basis for $(G(1), \omega)$, where the order is given by the height function on the roots.

Theorem 1.5. *The valuation ω defined in (1.4) is a p-valuation on $G(1)$.*

Proof. First we recall that the function (denoted again by ω) on $\Gamma(1)$, defined as

$$\omega(x) = k \text{ for } x \in \Gamma(k)\backslash\Gamma(k+1)$$

is a p-valuation on $\Gamma(1)$ (cf. p.171 of [Sch11]). Therefore, $\Gamma(k)$ satisfies the following three conditions:

$$\begin{gathered}\Gamma(1) = \cup_{k\geqslant 1}\Gamma(k),\\ [\Gamma(k), \Gamma(k^{'})] \subset \Gamma_{k+k'} \text{ for } k, k^{'} \in \mathbb{N},\\ \Gamma(v) = \cap_{w\leq v}\Gamma(w) \text{ for } v, w \in \mathbb{N}.\end{gathered}$$

By definition of $G(k)$ we have

$$\begin{gathered}G(1) = \cup_{k\geqslant 1}G(k),\\ G(v) = \cap_{w\leq v}G(w) \text{ for } v, w \in \mathbb{N}.\end{gathered}$$

Also,

$$\begin{aligned}[G(k), G(k^{'})] &\subseteq G(\mathbb{Z}_p) \cap [\Gamma(k), \Gamma(k^{'})],\\ &\subseteq G(\mathbb{Z}_p) \cap \Gamma(k+k^{'}),\\ &= G(k+k^{'}).\end{aligned}$$

This shows that (by section 1.2) ω is a filtration on $G(1)$. Obviously, if $x \in G(1)$ then $\omega(x) = +\infty$ implies $x \in \cap_k G(k) \subset \cap_k \Gamma(k) = 1$ which in particular shows that ω is separated. For $x \in G(1), x \neq 1$ we have $\omega(x) < \infty$. The valuation $\omega(g)$ is strictly greater than $(p-1)^{-1}$ for all $g \in G(1)$. To prove that $\omega(g^p) = \omega(g) + 1$, we use the fact that $\Gamma(1)$ is p-valuable.

Suppose $\omega(x) = k$ i.e. $x \in G(k)\backslash G(k+1)$ where $G(k) = \Gamma(k) \cap G(\mathbb{Z}_p)$. Since $\Gamma(1)$ is p-valuable, $x^p \in \Gamma(k+1)\backslash\Gamma(k+2)$. This implies that $x^p \in G(k+1)\backslash G(k+2)$. Hence, we obtain $\omega(x^p) = \omega(x) + 1$. This finishes the proof that ω is a p-valuation on $G(1)$. □

Let h be the height function on the roots $\gamma \in \Phi$ which is given by $h(\gamma) = \sum_{i=1}^{l} m_i$ for $\gamma = \sum_{i=1}^{l} m_i\delta_i$.

Theorem 1.6. *Any element $g \in G(k)$ can be uniquely written as*

$$g = \prod_{\beta\in\Phi^-} x_\beta(u_\beta) \prod_{\delta\in\Pi} h_\delta(1+v_\delta) \prod_{\alpha\in\Phi^+} x_\alpha(w_\alpha),$$

where $u_\beta, w_\alpha, v_\delta \in p^k\mathbb{Z}_p$. The order of the above product is chosen and fixed once for all such that the height function h on the roots increases.

Proof. Let us define

$$\begin{aligned}U(\mathbb{Z}_p, p^k\mathbb{Z}_p) &:= \langle x_\alpha(t); t \in p^k\mathbb{Z}_p, \alpha \in \Phi^+\rangle,\\ V(\mathbb{Z}_p, p^k\mathbb{Z}_p) &:= \langle x_\beta(v); v \in p^k\mathbb{Z}_p, \beta \in \Phi^-\rangle,\\ T(\mathbb{Z}_p, p^k\mathbb{Z}_p) &:= \langle h_\gamma(u); u \in 1 + p^k\mathbb{Z}_p, \gamma \in \Phi\rangle.\end{aligned}$$

From corollary 3.3 and section 3.21 of [Abe69] we have a unique triangular decomposition

$$G(k) = V(\mathbb{Z}_p, p^k\mathbb{Z}_p)T(\mathbb{Z}_p, p^k\mathbb{Z}_p)U(\mathbb{Z}_p, p^k\mathbb{Z}_p). \tag{1.5}$$

Proposition 2.5 (and the discussion following it) of [Abe69] gives that each element of $U(\mathbb{Z}_p, p^k\mathbb{Z}_p)$ can be written uniquely in the form $\prod_{\alpha\in\Phi^+} x_\alpha(t_i), t_i \in p^k\mathbb{Z}_p$, where the product is taken over all the positive roots with the order according to increasing height, the uniqueness criterion follows from p.26-corollary 2 of [Ste67]. Because of symmetry the similar statement will also hold for $V(\mathbb{Z}_p, p^k\mathbb{Z}_p)$.

For $h_\gamma(u) \in T(\mathbb{Z}_p, p^k\mathbb{Z}_p), \gamma \in \Phi$, lemma 28 and the proof of corollary 5, p.44 of [Ste67] give that there exist integers n_i such that

$$h_\gamma(u) = \prod_{i=1}^l h_{\delta_i}(u)^{n_i} = \prod_{i=1}^l h_{\delta_i}(u^{n_i}),$$

where $\delta_1, \cdots, \delta_l$ are the simple roots, l being the cardinality of the set of simple roots. The above expression is unique because our G is simply connected (cf. Corollary of lemma 28 p.44 of [Ste67]). Thus by 1.5, each element $g \in G(k)$ can be uniquely written as

$$g = \prod_{\beta\in\Phi^-} x_\beta(u_\beta) \prod_{\delta\in\Pi} h_\delta(1+v_\delta) \prod_{\alpha\in\Phi^+} x_\alpha(w_\alpha),$$

where $u_\beta, w_\alpha, v_\delta \in p^k\mathbb{Z}_p$. The order of the above product is given by the height function on the roots. □

Remark 1.7. The paper [Abe69] by Abe gives actually the decomposition

$$G(k) = U(\mathbb{Z}_p, p^k\mathbb{Z}_p)T(\mathbb{Z}_p, p^k\mathbb{Z}_p)V(\mathbb{Z}_p, p^k\mathbb{Z}_p).$$

Its proof uses proposition 1 of [Che95] and by just following the proof of corollary 3.3 of [Abe69], one can easily show that there is no harm if we interchange the places of $V(\mathbb{Z}_p, p^k\mathbb{Z}_p)$ and $U(\mathbb{Z}_p, p^k\mathbb{Z}_p)$ in the above decomposition.

Theorem 1.8. *Let $g \in G(k)$. Then using the decomposition given by theorem* 1.6, *if*

$$g = \prod_{\beta\in\Phi^-} x_\beta(u_\beta) \prod_{\delta\in\Pi} h_\delta(1+v_\delta) \prod_{\alpha\in\Phi^+} x_\alpha(w_\alpha),$$

then

$$\omega(g) = \min_{\{\beta\in\Phi^-, \alpha\in\Phi^+, \delta\in\Pi\}} \{val_p(u_\beta), val_p(v_\delta), val_p(w_\alpha)\}.$$

Proof. Let $g \in G(k)\backslash G(k+1)$ so that $\omega(g) = k$. Then any one of the elements of

$$\{u_\beta, v_\delta, w_\alpha; \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\}$$

should belong to $p^k\mathbb{Z}_p$ and not all of them in $p^{k+1}\mathbb{Z}_p$, because if all the elements $u_\beta, v_\delta, w_\alpha \in p^{k+1}\mathbb{Z}_p$, then $g \in G(k+1)$ and this is a contradiction to our assumption. □

For $m_\beta, n_\delta, z_\alpha \in \mathbb{Z}_p$ we have

$$\begin{aligned}
&\omega\Big(\prod_{\beta\in\Phi^-} x_\beta(p)^{m_\beta} \prod_{\delta\in\Pi} h_\delta(1+p)^{n_\delta} \prod_{\alpha\in\Phi^+} x_\alpha(p)^{z_\alpha}\Big) \\
&= \omega\Big(\prod_{\beta\in\Phi^-} x_\beta(pm_\beta) \prod_{\delta\in\Pi} h_\delta((1+p)^{n_\delta}) \prod_{\alpha\in\Phi^+} x_\alpha(pz_\alpha)\Big) \\
&= \min_{\beta,\alpha,\delta}\{1+val_p(m_\beta), 1+val_p(n_\delta), 1+val_p(z_\alpha)\}.
\end{aligned}$$

The first equality follows from p.30, and lemma 28 of [Ste67] and the second equality follows from Theorem 1.8.

Since $\omega(x_\beta(p)) = \omega(x_\alpha(p)) = \omega(h_\delta(1+p)) = 1$ and $p > 2$, $G(1)$ is also p-saturated (cf. 1.3). Hence, with theorem 1.6, it follows that:

Theorem 1.9. *The first congruence kernel $G(1)$ is p-saturated with an ordered basis*

$$\{x_\beta(p), h_\delta(1+p), x_\alpha(p); \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\},$$

the order being given by the height function on the roots.

The group $G(1)$ has a decomposition

$$G(1) = \prod_{\beta\in\Phi^-} N_\beta \prod_{\delta\in\Pi} T_\delta \prod_{\alpha\in\Phi^+} N_\alpha,$$

where

$$\begin{aligned} N_\beta &= \langle x_\beta(u), u \in p\mathbb{Z}_p\rangle, \\ N_\alpha &= \langle x_\alpha(w), w \in p\mathbb{Z}_p\rangle, \\ T_\delta &= \langle h_\delta(1+v), v \in p\mathbb{Z}_p\rangle; \end{aligned}$$

the order of the products is taken according to the height function on the roots.

Let $\Lambda(G(1))$ be the Iwasawa algebra of $\mathbb{Z}_p$-valued measures on $G(1)$. It can also be thought as distributions on $G(1)$ in the sense of [Was97]. The decomposition of $G(1)$ given above yields a decomposition of $\Lambda(G(1))$ as a topological $\mathbb{Z}_p$-module:

$$\Lambda(G(1)) = \Lambda(N_{-\alpha_{max}})\hat{\otimes}\cdots\hat{\otimes}\Lambda(T_\delta)\hat{\otimes}\cdots\hat{\otimes}\Lambda(N_{\alpha_{max}}) \tag{1.6}$$

where α_{max} is the highest root and the order of the product is taken according to the height function on the roots. The factors of (1.6) are the spaces of distributions on the factors of $G(1)$. If f is a function on $G(1)$ and $U_\beta, V_\alpha, W_\delta$ distributions on $N_\beta, T_\delta, N_\alpha$, then

$$< U_{-\alpha_{max}} \otimes\cdots\otimes W_\delta \otimes\cdots\otimes V_{\alpha_{max}}, f > \tag{1.7}$$
$$:=< U_{-\alpha_{max}} \otimes\cdots\otimes W_\delta \otimes\cdots\otimes V_{\alpha_{max}}, f(u_{-\alpha_{max}}\cdots h_\delta\cdots n_{\alpha_{max}}) > \tag{1.8}$$

where $u_\beta \in N_\beta, h_\delta \in T_\delta, n_\alpha \in N_\alpha$ and f is seen as a function on

$$\prod_{\beta\in\Phi^-} N_\beta \prod_{\delta\in\Pi} T_\delta \prod_{\alpha\in\Phi^+} N_\alpha.$$

For each factor, $U = N_\beta, T_\delta$ or N_α of $G(1)$, $\Lambda(U)$ is naturally sent to $\Lambda(G(1))$, by integrating a function $f \in C(G(1), \mathbb{Z}_p)$ against $\mu \in \Lambda(U)$ on the U-factor. This map is compatible with the convolution product as in [Clo11].

1.4 Alternative proof of Lazard's ordered basis

In this section we briefly sketch another proof of theorem 1.9 using group theory. Dixon, Sautoy, Mann and Segal in [DSMS03] describe a subclass of p-saturated groups called uniform pro-p groups. Briefly, if H is a uniform pro-p group then it is p-saturated and conversely if H is p-saturated then H^p is uniform. The Heisenberg group of uni-upper-triangular 3×3 matrices with entries in the ring of p-adic integers, for $p > 2$, gives an example of a p-saturated but non-uniform pro-p group of rank 3. J. Gonzales-Sanches gives a nice characterization of p-saturated groups in [GS07]. This is pointed out to me by Konstantin Ardakov. In this section, without giving the proofs, we use the results of [DSMS03] to provide another proof of theorem 1.9.

Let $p > 2$ be a prime. Let G be a pro-p group which is topologically finitely generated. Then we say that G is powerful if $G/\overline{G^p}$ is abelian. Moreover, if G is torsion-free, then we say that G is uniform. Note that [DSMS03] has a different definition for uniform pro-p group, but Theorem 4.5 of [DSMS03] shows that it is equivalent to the definition given above. For uniform pro-p group G we have the following proposition:

Proposition 1.10. *Let G be a topologically finitely generated uniform pro-p group. Let $G = \overline{\langle a_1, \cdots a_d\rangle}$ such that d is minimum. Then*

$$G = \overline{\langle a_1\rangle}\cdots\overline{\langle a_d\rangle}$$

and the mapping

$$(\lambda_1, ..., \lambda_d) \to a_1^{\lambda_1}\cdots a_d^{\lambda_d}$$

from $\mathbb{Z}_p^d$ to G is a homeomorphism.

Proof. See proposition 3.7 and theorem 4.9 of [DSMS03]. □

Remark 1.11. With the hypothesis as in proposition 1.10, the discussion in section 4.2 of [DSMS03] shows that G has an integrally valued p-valuation ω and an Lazard's ordered basis $a_1, ..., a_d$ with $\omega(a_i) = 1, i \in [1, d]$ (see also the remark after lemma 4.3 of [ST03]).

In section 8.2 of [DSMS03], the authors describe p-adic analytic groups. Without giving the definition, we just like to point out that uniform pro-p groups are p-adic analytic groups (cf. example 5, section 8.17 of [DSMS03]).

In the following we define the notion of standard groups (cf. definition 8.2.2 of [DSMS03]).

Definition 1.12. *Let G be a p-adic analytic group. Then G is a standard group (of dimension d over $\mathbb{Q}_p$) if*

(i) the analytic manifold structure on G is defined by a global atlas of the form $\{(G, \psi, d)\}$ where ψ is a homeomorphism of G onto $(p\mathbb{Z}_p)^d$ with $\psi(1) = 0$,
(ii) for $j = 1, ..., d$, there exists $P_j(X, Y) \in \mathbb{Z}_p[[X, Y]]$ such that

$$\psi_j(xy^{-1}) = P_j(\psi(x), \psi(y))$$

for all $x, y \in G$, where $\psi = (\psi_1, ..., \psi_d)$.

Proposition 1.13. *Let G be a standard group of dimension d over $\mathbb{Q}_p$. Then G is a uniform pro-p group of dimension d.*

Proof. See theorem 8.31 of [DSMS03]. □

Lemma 1.14. *The first congruence kernel $G(1)$ is a $\mathbb{Z}_p$- standard group (of level 1) with dimension $|\Phi| + |\Pi|$.*

Proof. By theorem 1.6 each element $g \in G(1)$ can be uniquely written as $\prod_{\beta\in\Phi^-} x_\beta(u_\beta) \prod_{\delta\in\Pi} h_\delta(1 + v_\delta) \prod_{\alpha\in\Phi^+} x_\alpha(w_\alpha)$ for some $u_\beta, v_\delta, w_\alpha \in p\mathbb{Z}_p$. The proof then follows from theorem 8 of [Ste67] and exercise 11 of chapter 13 of [DSMS03]. □

Alternative proof of Theorem 1.9: Lemma 1.14 gives us that $G(1)$ is a $\mathbb{Z}_p$-standard group of dimension $|\Phi| + |\Pi|$. Then proposition 1.13 gives that $G(1)$ is a uniform pro-p group. But uniform pro-p groups are p-valuable and p-saturated (cf. remark after lemma 4.3 of [ST03].) Now, Theorem 1.6 shows that

$$G(1) = \prod_{\beta\in\Phi^-} \overline{x_\beta(p)} \prod_{\delta\in\Pi} \overline{h_\delta(1+p)} \prod_{\alpha\in\Phi^+} \overline{x_\alpha(p)},$$

where the bars denotes the closure, that is,

$$\begin{aligned}
\overline{x_\beta(p)} &= \{x_\beta(p)^{m_\beta}, \forall m_\beta \in \mathbb{Z}_p\} = \{x_\beta(m_\beta p), \forall m_\beta \in \mathbb{Z}_p\},\\
\overline{x_\alpha(p)} &= \{x_\alpha(p)^{z_\alpha}, \forall z_\alpha \in \mathbb{Z}_p\} = \{x_\alpha(z_\alpha p), \forall z_\alpha \in \mathbb{Z}_p\},\\
\overline{h_\delta(1+p)} &= \{h_\delta(1+p)^{n_\delta}, \forall n_\delta \in \mathbb{Z}_p\} = \{h_\delta((1+p)^{n_\delta}), \forall n_\delta \in \mathbb{Z}_p\}.
\end{aligned}$$

Then remark 1.11 finishes the proof of Theorem 1.9 [Q.E.D].

1.5 Iwasawa algebras and relations

In this section, for $\alpha \in \Phi$ and $\delta \in \Pi$, we identify (as a $\mathbb{Z}_p$-module) the Iwasawa algebra of $G(1)$ with the ring of power series in the variables V_α and W_δ over $\mathbb{Z}_p$ (cf. 1.9). This isomorphism is given by sending $1 + V_\alpha \mapsto x_\alpha(p)$ and $1 + W_\delta \mapsto h_\delta(1+p)$. As the Iwasawa algebra is non-commutative, this identification is obviously not a ring isomorphism. Therefore, the goal of this section is to study the product of the variables in wrong order, viewing them as elements of the Iwasawa algebra, and then find the relations among the variables $(1.15 - 1.18)$.

Theorem 1.9 gives us an ordered basis of $G(1)$ with the p-valuation ω. By definition we have a homeomorphism

$$\begin{aligned}
c : \mathbb{Z}_p^d &\to G(1)\\
(y_1, ..., y_d) &\mapsto g_1^{y_1} \cdots g_d^{y_d}
\end{aligned}$$

where $d = |\Phi| + |\Pi|$ and $(g_1, ..., g_d)$ is the ordered basis of $G(1)$. Let $C(G(1))$ be continuous functions from $G(1)$ to $\mathbb{Z}_p$. The map c induces, by pulling back functions, an isomorphism of $\mathbb{Z}_p$-modules

$$c^* : C(G(1)) \simeq C(\mathbb{Z}_p^d).$$

We may recall that $\Lambda(G(1))$ is the Iwasawa algebra of $G(1)$ over $\mathbb{Z}_p$, that is, $\Lambda(G(1)) := \varprojlim_{N \in \mathcal{N}(G(1))}(G(1)/N)$ where $\mathcal{N}(G(1))$ is the set of open normal subgroups in $G(1)$. Lemma 22.1 of [Sch11] shows that

$$\Lambda(G(1)) = Hom_{\mathbb{Z}_p}(C(G(1)), \mathbb{Z}_p).$$

So dualizing the map c^*, we get an isomorphism of $\mathbb{Z}_p$-modules

$$c_* = \Lambda(\mathbb{Z}_p^d) \cong \Lambda(G(1)).$$

This gives us the following isomorphism of $\mathbb{Z}_p$-modules:

$$\tilde{c} : \mathbb{Z}_p[[V_\alpha, W_\delta; \alpha \in \Phi, \delta \in \Pi]] \cong \Lambda(G(1)) \tag{1.9}$$

$$1 + V_\alpha \mapsto x_\alpha(p) \tag{1.10}$$

$$1 + W_\delta \mapsto h_\delta(1+p). \tag{1.11}$$

This is because the Iwasawa algebra of $\mathbb{Z}_p^d$ can be identified with the ring of power series in d variables (cf. prop 20.1 of [Sch11]). From (1.6), any $\lambda \in \Lambda(G(1))$ can be written uniquely as

$$\lambda = \sum_m \lambda_m V_{-\alpha_{max}}^{m_1} \cdots W_\delta^{m_-} \cdots V_{\alpha_{max}}^{m_d}, \tag{1.12}$$

with $\lambda_m \in \mathbb{Z}_p, m = (m_1, ..., m_d) \in \mathbb{N}^d$. The product of the above variables

$$V_{-\alpha_{max}}^{m_1} \cdots W_\delta^{m_-} \cdots V_{\alpha_{max}}^{m_d} := V_{-\alpha_{max}}^{m_1} \otimes \cdots \otimes W_\delta^{m_-} \otimes \cdots \otimes V_{\alpha_{max}}^{m_d}$$

is taken according to the height function on the roots. We note that we can write unambiguously the variables $V_\alpha^n, W_\delta^n; n \geq 0$ because from the discussion after (1.7) in section 1.3, it follows that the convolution of V_α's (or W_δ's) taken n times equals their tensor product, i.e.

$$V_\alpha^n = V_\alpha \otimes \cdots \otimes V_\alpha = V_\alpha * \cdots * V_\alpha.$$

It immediately follows from (1.7) that the convolution (taken on $G(1)$) of the distributions V_α, W_δ equals their tensor product when they are taken in the order of the height function. We simply write, consistent with our previous notation,

$$V_{-\alpha_{max}}^{m_1} \cdots W_\delta^{m_-} \cdots V_{\alpha_{max}}^{m_d} = V_{-\alpha_{max}}^{m_1} * \cdots * W_\delta^{m_-} * \cdots * V_{\alpha_{max}}^{m_d},$$

where

$$V_\alpha^n = V_\alpha * V_\alpha * \cdots * V_\alpha, (n \geq 0), \tag{1.13}$$

and

$$W_\delta^n = W_\delta * W_\delta * \cdots * W_\delta, (n \geq 0). \tag{1.14}$$

In the following we study the product of the variables in the wrong order.

Let $b_i := g_i - 1$, $(g_1, ..., g_d)$ being the Lazard ordered basis of $G(1)$ and $b^m := b_1^{m_1} \cdots b_d^{m_d}$, for any multi-index $m = (m_1, ..., m_d) \in \mathbb{N}^d$, in $\Lambda(G(1))$. We define a function

$$\tilde{\omega} : \Lambda(G(1)) \backslash \{0\} \to [0, \infty)$$

by

$$\tilde{\omega}\Big(\textstyle\sum_m c_m b^m\Big) := \inf_m \Big(val_p(c_m) + |m|\Big)$$

where $c_m \in \mathbb{Z}_p, |m| := m_1 + \cdots + m_l$, with the convention that $\tilde{\omega}(0) := \infty$.

By the isomorphism $\tilde{c}$, we can identify the variables $V_\alpha, W_\delta; (\alpha \in \Phi, \delta \in \Pi)$ as elements of the Iwasawa algebra of $G(1)$. Our goal is to find the relations among the above variables. For this, we use the Chevalley relations given by Steinberg in [Ste67]. With $x_\alpha(p)$, $h_\delta(1+p)$ as defined in section 1.2, [Ste67] gives

$$h_\delta(1+p) x_\alpha(p) h_\delta(1+p)^{-1} = x_\alpha((1+p)^{\langle \alpha, \delta \rangle} p), (\alpha \in \Phi, \delta \in \Pi)$$

where $\langle \alpha, \delta \rangle = 2(\alpha, \delta)/(\delta, \delta) \in \mathbb{Z}$ (cf. [Ste67], p.30). It follows that the corresponding relation in the Iwasawa algebra of $G(1)$ is

$$(1 + W_\delta)(1 + V_\alpha) = (1 + V_\alpha)^{(1+p)^{\langle \alpha, \delta \rangle}} (1 + W_\delta), (\alpha \in \Phi, \delta \in \Pi). \tag{1.15}$$

Let $\alpha_1, \alpha_2 \in \Phi, \alpha_1 \neq -\alpha_2$ and $\alpha_1 + \alpha_2 \notin \Phi$ then example (a), p.24 of [Ste67] gives

$$x_{\alpha_1}(p)x_{\alpha_2}(p) = x_{\alpha_2}(p)x_{\alpha_1}(p), (\alpha_1, \alpha_2 \in \Phi).$$

Thus, the relation in the Iwasawa algebra is

$$(1 + V_{\alpha_1})(1 + V_{\alpha_2}) = (1 + V_{\alpha_2})(1 + V_{\alpha_1}), (\alpha_1, \alpha_2 \in \Phi). \tag{1.16}$$

If $\alpha_1 \neq -\alpha_2$ and $\alpha_1 + \alpha_2 \in \Phi$ then $x_{\alpha_1}(p)x_{\alpha_2}(p) = [x_{\alpha_1}(p), x_{\alpha_2}(p)]x_{\alpha_2}(p)x_{\alpha_1}(p)$, where $[,]$ is the commutator function. So lemma 15, p.22 of [Ste67] gives

$$x_{\alpha_1}(p)x_{\alpha_2}(p) = \Big(\prod_{i,j>0} x_{i\alpha_1+j\alpha_2}(c_{ij}p^i p^j) \Big) x_{\alpha_2}(p)x_{\alpha_1}(p), (\alpha_1, \alpha_2 \in \Phi),$$

where $c_{ij} \in \mathbb{Z}$ and the order of the product is as prescribed in lemma 15 of [Ste67]. This gives

$$(1 + V_{\alpha_1})(1 + V_{\alpha_2}) = \Big(\prod_{i,j>0} (1 + V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}} \Big) (1 + V_{\alpha_2})(1 + V_{\alpha_1}), (\alpha_1, \alpha_2 \in \Phi). \tag{1.17}$$

If $\alpha_3 \in \Phi^+$, corollary 6, p.46 of [Ste67] gives a homomorphism

$$\varphi_{\alpha_3} : SL_2(\mathbb{Q}_p) \to \langle x_{\alpha_3}(t), x_{-\alpha_3}(t); t \in \mathbb{Q}_p \rangle$$

such that

$$\begin{aligned} \varphi_{\alpha_3}(1 + tE_{12}) &= x_{\alpha_3}(t), \\ \varphi_{\alpha_3}(1 + tE_{21}) &= x_{-\alpha_3}(t), \\ \varphi_{\alpha_3}(tE_{11} + t^{-1}E_{22}) &= h_{\alpha_3}(t), \end{aligned}$$

where E_{ij} is the 2×2 matrix with 1 in the $(i, j)^{th}$ entry and zero elsewhere. We have

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

where $t = 1+p^2, u = p(1+p^2)^{-1}, v = p(1+p^2)^{-1}$. As φ_{α_3} is a homomorphism, we therefore obtain

$$x_{\alpha_3}(p)x_{-\alpha_3}(p) = x_{-\alpha_3}(v)h_{\alpha_3}(t)x_{\alpha_3}(u), (\alpha_3 \in \Phi^+).$$

As before let $\delta_1, ..., \delta_l$ be the simple roots where $l = |\Pi|$. Then, as in the proof of Theorem 1.6, we can uniquely decompose

$$h_{\alpha_3}(t) = \textstyle\prod_{i=1}^{l} h_{\delta_i}(t^{n_i}) \text{ for } n_i \in \mathbb{Z}.$$

Now, let $P = \frac{log(1+p^2)}{log(1+p)} \in \mathbb{Z}_p, 1 + p^2 = (1 + p)^P$ and let $Q = (1 + p^2)^{-1}$ then

$$h_{\alpha_3}(t) = h_{\alpha_3}(1 + p)^P = \prod_{i=1}^{l} h_{\delta_i}(1 + p)^{n_i P}, (\alpha_3 \in \Phi^+, \delta_i \in \Pi).$$

This gives that the corresponding relation in the Iwasawa algebra is

$$(1 + V_{\alpha_3})(1 + V_{-\alpha_3}) = (1 + V_{-\alpha_3})^Q \Big(\prod_{i=1}^{l} (1 + W_{\delta_i})^{n_i P} \Big) (1 + V_{\alpha_3})^Q, (\alpha_3 \in \Phi^+, \delta_i \in \Pi). \tag{1.18}$$

Thus, we have shown

Lemma 1.15. *With the notations as above, we have the following relations in $\Lambda(G(1))$:*

1. $(1 + W_\delta)(1 + V_\alpha) = (1 + V_\alpha)^{(1+p)^{\langle \alpha, \delta \rangle}} (1 + W_\delta)$,

2. $(1 + V_{\alpha_1})(1 + V_{\alpha_2}) = (1 + V_{\alpha_2})(1 + V_{\alpha_1}), (\alpha_1 + \alpha_2 \notin \Phi)$,

3. $(1+V_{\alpha_1})(1+V_{\alpha_2}) = \Big(\prod_{i,j>0}(1+V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}}\Big)(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1+\alpha_2 \in \Phi)$,

4. $(1+V_{\alpha_3})(1+V_{-\alpha_3}) = (1+V_{-\alpha_3})^Q\Big(\prod_{i=1}^{l}(1+W_{\delta_i})^{n_iP}\Big)(1+V_{\alpha_3})^Q$.

Consider $\mathcal{A}$ - the universal non-commutative p-adic algebra in variables V_α and W_δ, where α varies over the roots and δ varies over the simple roots and the ordering of the variables are given by the height function on the roots to which they correspond. Thus, it is composed of all non-commutative series

$$f = \sum_{n\geqslant 0}\sum_i a_i x^i$$

where $a_i \in \mathbb{Z}_p$, $x^i := x_{i(1)}\cdots x_{i(n)}$ and for all $n \geqslant 0$, i runs over all maps $\{1,2,...,n\} \to \{1,2,...,d\}$; the monomials x_i, with i increasing, are assigned to the product of the variables among $\{V_\alpha, W_\delta; \alpha \in \Phi, \delta \in \Pi\}$ corresponding to a fixed order compatible with the partial order given by the height function on the roots. The algebra $\mathcal{A}$, denoted by $\mathbb{Z}_p\{\{x_1,...,x_d\}\}$, has a maximal ideal $\mathcal{M}_\mathcal{A}$ generated by $(p, x_1, ..., x_d)$ and a prime ideal $\mathcal{P}_\mathcal{A}$ generated by $(x_1, ..., x_d)$. The topology on $\mathcal{A}$ is given by the powers of $\mathcal{M}_\mathcal{A}$.

Let $\mathcal{R}$ be the closed two-sided ideal generated in $\mathcal{A}$ by the relations $(1.15 - 1.18)$. Let $\overline{\mathcal{A}}$ be the image of the reduction modulo p map on $\mathcal{A}$; i.e. we consider the non-commutative series with coefficients in $\mathbb{F}_p$ with its natural topology given by its maximal ideal $\mathcal{M}_{\overline{\mathcal{A}}}$.

Lemma 1.16. *Let $\overline{\mathcal{R}}$ be the image of $\mathcal{R}$ in $\overline{\mathcal{A}}$. Then $\overline{\mathcal{R}}$ is the closed two-sided ideal generated in $\overline{\mathcal{A}}$ by the images of the relations* $(1.15, 1.16, 1.17, 1.18)$.

Proof. We follow the proof exactly as in lemma 1.3 of [Clo11]. For completeness we repeat the proof. We denote by $\mathcal{I} \subset \mathcal{A}$ the *ideal* generated by the relations, let $\mathcal{J} \subset \overline{\mathcal{A}}$ be the similar ideal. Then $\mathcal{J}$ is obviously the image of $\mathcal{I}$ in $\overline{\mathcal{A}}$; we denote it by $\overline{\mathcal{I}}$.

Let $\overline{\mathcal{R}}$ be the reduction of $\mathcal{R}$, and consider the closure $cl(\overline{\mathcal{I}})$ of $\overline{\mathcal{I}}$ in $\overline{\mathcal{A}}$. If $f \in \mathcal{R}$, we have $f = \lim_n f_n (f_n \in \mathcal{I})$ for the topology given by $\mathcal{M}_\mathcal{A}^N$. This implies that $\overline{f} = \lim \overline{f_n}$ for the topology given by $\mathcal{M}_{\overline{\mathcal{A}}}^N$ on $\overline{\mathcal{A}}$, thus $\overline{f} \in cl(\overline{\mathcal{I}})$. Conversely, assume $\overline{f} \in \overline{\mathcal{A}}$ can be written $\overline{f} = \lim \overline{f_n}$ with $\overline{f_n} \in \overline{\mathcal{I}}$. Then, $\overline{f_n}$ is the reduction of a series $f_n \in \mathcal{I} \subset \mathcal{R}$. Since $\mathcal{R}$ is closed and $\mathcal{A}$ is compact, we may assume that f_n converges to $g \in \mathcal{R}$. Then, by definition of the topologies, $\overline{f} = \lim \overline{f_n} = \overline{g}$. Thus $cl(\overline{\mathcal{I}}) = \overline{\mathcal{R}}$, which finishes the proof. □

1.6 Presentation of the Iwasawa algebra $\Lambda(G(1))$ for $p > 2$

Our goal in this section is to give an explicit presentation of $\Lambda(G(1))$ (theorem 1.22). The strategy of the proof is to first show the corresponding statement with coefficients in $\mathbb{F}_p$ and then lift the coefficients to $\mathbb{Z}_p$. Let

$$\Omega_{G(1)} = \Lambda(G(1)) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$$

be the Iwasawa algebra with finite coefficients as in [Clo11]. We show in theorem 1.21 that for $p > 2$, the Iwasawa algebra mod p, $\Omega_{G(1)}$, is naturally isomorphic to $\overline{\mathcal{A}}/\overline{\mathcal{R}}$. We first construct a map $\overline{\varphi} : \overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}} \to \Omega_{G(1)}$ (see corollary 1.19), then using the natural grading (see the discussion before proposition 1.20) on $\overline{\mathcal{B}}$, we show that $\dim \mathrm{gr}^n\overline{\mathcal{B}} \leqslant \dim S_n$ (see proposition 1.20), where S_n is the space of homogeneous commutative polynomials in the variables $\{V_\alpha, W_\delta; \alpha \in \Phi, \delta \in \Pi\}$ over $\mathbb{F}_p$ of degree n.

Let us define

$$\mathcal{M}_\Lambda^N := \{\lambda \in \Lambda(G(1)) | \tilde{\omega}(\lambda) \geqslant N\}.$$

It follows from Lazard's results [Laz65] (also Schneider, chapter 6 of [Sch11]) that $\mathcal{M}_\Lambda^N$ is indeed the N^{th} power of the maximal ideal $\mathcal{M}_\Lambda$ of $\Lambda(G(1))$.

We consider the filtration of $\mathcal{A}$ given by the powers of its maximal ideal. Then we can define a valuation $w_\mathcal{A}$ given by:

$$\begin{gathered}\text{let } f = \sum_i a_i x^i, \\ \text{then } w_\mathcal{A}(f) = \inf_i(val_p(a_i) + |i|)\end{gathered}$$

where $|i| = n$ is the degree of i.

The non-commutative polynomial algebra

$$A := \mathbb{Z}_p\{x_1, ..., x_d\}$$

is a dense subalgebra of $\mathcal{A}$.

Lemma 1.17. *Let $\varphi : A \to \Lambda(G(1))$ be the natural map which sends $x_i \in A$ $(1 \leq i \leq d; i$ increasing$)$ to the variable $\{V_\alpha, W_\delta; \alpha \in \Phi, \delta \in \Pi\}$ in the Iwasawa algebra $\Lambda(G(1))$, corresponding to the order compatible with increasing height function on the roots. Then, this map extends continuously to a surjective homomorphism $\mathcal{A} \to \Lambda(G(1))$. Moreover, for $N \geqslant 0$, we have*

$$\varphi(\mathcal{M}_{\mathcal{A}}^N) \subset \mathcal{M}_\Lambda^N.$$

Proof. For continuity we use the fact that the valuation $\tilde{\omega}$ is additive i.e.

$$\tilde{\omega}(\lambda * \mu) = \tilde{\omega}(\lambda) + \tilde{\omega}(\mu); \lambda, \mu \in \Lambda(G(1)).$$

This is a nontrivial fact proved by Lazard (cf. [Laz65], III.2.3.3).

The continuity of the map φ is implied by the stronger property

$$\tilde{\omega}(\varphi(x^i)) = n = |i| \tag{1.19}$$

where n is the degree of the monomial. By induction on n, this follows from the non-trivial fact that $\tilde{\omega}$ is additive. If $f \in \mathcal{M}_{\mathcal{A}}^N$, we have $w_{\mathcal{A}}(f) \geqslant N$ and the continuity follows from 1.19 by $\mathbb{Z}_p$-linearity. The surjectivity follows from $(1.12 - 1.14)$ and the fact that φ is already surjective if $\mathcal{A}$ is replaced by the set of linear combinations of the well-ordered monomials (i increasing). This completes the proof. □

Therefore, we obtain the following two corollaries:

Corollary 1.18. *There is a natural continuous surjection*

$$\mathcal{B} = \mathcal{A}/\mathcal{R} \to \Lambda(G(1)).$$

Corollary 1.19. *There is a continuous surjection*

$$\overline{\varphi} : \overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}} \to \Omega_{G(1)}.$$

This follows from Lemma 1.16.

By Abelian distribution theory, $\Omega_{G(1)}$ is, as a space, isomorphic to the commutative power series ring in the variables V_α and W_δ over $\mathbb{F}_p$ with the compact topology, where α varies over the roots and δ varies over the simple roots. By obvious computation one can show that

$$\mathcal{M}_\Omega^N = \{\lambda \in \Omega_{G(1)} : v_\Omega(\lambda) \geqslant N\},$$

v_Ω being the usual valuation on power series, is the reduction of $\mathcal{M}_\Lambda^N$. It is also a (two-sided) ideal, $\mathcal{M}_\Omega$ being the maximal ideal.

Similarly, in $\mathcal{A}$ we have that the reduction mod p of $\mathcal{M}_{\mathcal{A}}^N$ is the ideal of series

$$\overline{f} = \textstyle\sum_i a_i x^i \text{ with } (a_i \in \mathbb{F}_p)$$

such that $|i| \geqslant N$. We obtain the maximal ideal of $\overline{\mathcal{A}}$ by setting $N = 1$. Furthermore, we have $(\mathcal{M}_{\overline{\mathcal{A}}})^N = \mathcal{M}_{\overline{\mathcal{A}}}^N$.

In the following we study the algebra $\overline{\mathcal{B}}$ using the relations $(1.15, 1.16, 1.17, 1.18)$ which are used to prove Proposition 1.20 below. Then, we will use it to give the proof of Theorem 1.21, which in turn, after lifting coefficients to $\mathbb{Z}_p$, leads to the proof of Theorem 1.22.

Consider the natural filtration of $\overline{\mathcal{A}}$ by the powers of $\mathcal{M}_{\overline{\mathcal{A}}}$, which we denote by $F^n\overline{\mathcal{A}}$ as in [Clo11]. We have $F^n\overline{\mathcal{A}}/F^{n+1}\overline{\mathcal{A}} = \mathrm{gr}^n\overline{\mathcal{A}}$. The filtration F^n induces a filtration on $\overline{\mathcal{B}}$:

$$F^n\overline{\mathcal{B}} = F^n\overline{\mathcal{A}} + \overline{\mathcal{R}}$$

and hence a graduation

$$\mathrm{gr}^n\overline{\mathcal{B}} = F^n\overline{\mathcal{A}} + \overline{\mathcal{R}}/F^{n+1}\overline{\mathcal{A}} + \overline{\mathcal{R}}.$$

Hence, we have

$$\mathrm{gr}^n\overline{\mathcal{B}} = F^n\overline{\mathcal{A}}/F^{n+1}\overline{\mathcal{A}} + (F^n\overline{\mathcal{A}} \cap \overline{\mathcal{R}}).$$

Let S_n be the space of homogeneous commutative polynomials in the variables $\{V_\alpha, W_\delta; \alpha \in \Phi, \delta \in \Pi\}$ over $\mathbb{F}_p$ of degree n. Let Σ_n be the corresponding space of homogeneous non-commutative polynomials of degree n; hence $\Sigma_n \to F^n\overline{\mathcal{A}}/F^{n+1}\overline{\mathcal{A}}$, and therefore $\Sigma_n \to \mathrm{gr}^n\overline{\mathcal{B}}$, is surjective.

Proposition 1.20. *We have* $\dim\, gr^n\overline{\mathcal{B}} \leqslant \dim S_n$.

Proof. The case $n = 1$ is obvious. We first prove the proposition for $n = 2$ by studying the relations defining $\mathcal{R}$ (or rather $\overline{\mathcal{R}}$) and then we use an induction argument to complete the proof.

For $\alpha \in \Phi$, $\delta \in \Pi$, relation 1.15 is

$$(1 + W_\delta)(1 + V_\alpha) = (1 + V_\alpha)^{(1+p)^{\langle \alpha, \delta \rangle}}(1 + W_\delta), (\alpha \in \Phi, \delta \in \Pi).$$

We set $q = (1 + p)^{\langle \alpha, \delta \rangle}$, so that $q \equiv 1[p]$. Expanding the above relation we obtain

$$1 + W_\delta + V_\alpha + W_\delta V_\alpha = \Big(1 + qV_\alpha + \tfrac{q(q-1)}{2}V_\alpha^2 + \cdots\Big)(1 + W_\delta).$$

As $\frac{q(q-1)}{2} \equiv 0[p]$ and $p > 2$,

$$1 + W_\delta + V_\alpha + W_\delta V_\alpha = (1 + qV_\alpha)(1 + W_\delta) + R(V_\alpha)(1 + W_\delta)$$

where $R(V_\alpha)$ has degree $\geqslant 3$. Thus

$$W_\delta V_\alpha = (q - 1)V_\alpha + q(V_\alpha W_\delta) + R_1(V_\alpha, W_\delta)$$

where $R_1(V_\alpha, W_\delta)$ has degree $\geqslant 3$. Since $q \equiv 1[p]$ we deduce

$$W_\delta V_\alpha = V_\alpha W_\delta \text{ in } \mathrm{gr}^2\overline{\mathcal{B}}.$$

Relation 1.16 obviously gives for $\alpha_1, \alpha_2 \in \Phi, \alpha_1 \neq -\alpha_2, \alpha_1 + \alpha_2 \notin \Phi$,

$$V_{\alpha_1}V_{\alpha_2} = V_{\alpha_2}V_{\alpha_1}, (\alpha_1, \alpha_2 \in \Phi).$$

Relation 1.17 is for $\alpha_1, \alpha_2 \in \Phi, \alpha_1 \neq -\alpha_2, \alpha_1 + \alpha_2 \in \Phi$,

$$(1 + V_{\alpha_1})(1 + V_{\alpha_2}) = \Big(\textstyle\prod_{i,j>0}(1 + V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}}\Big)(1 + V_{\alpha_2})(1 + V_{\alpha_1}),$$

where $c_{ij} \in \mathbb{Z}$. Now,

$$(1 + V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}} = 1 + cV_{i\alpha_1+j\alpha_2} + \tfrac{c(c-1)}{2}V^2_{i\alpha_1+j\alpha_2} + \cdots$$

where $c = c_{ij}p^{i+j-1}$. It is easy to see that $p|c$ if $i > 0$ and $j > 0$. As $p > 2$, and 2 is invertible in $\mathbb{Z}_p$ we deduce

$$(1 + V_{i\alpha_1+j\alpha_2})^{c_{ij}p^{i+j-1}} \equiv 1[\mod F^3\overline{\mathcal{B}}].$$

This implies

$$V_{\alpha_1}V_{\alpha_2} = V_{\alpha_2}V_{\alpha_1} \text{ in } \mathrm{gr}^2\overline{\mathcal{B}}.$$

Relation 1.18 for $\alpha_3 \in \Phi^+$ is the following:

$$(1 + V_{\alpha_3})(1 + V_{-\alpha_3}) = (1 + V_{-\alpha_3})^Q\Big(\textstyle\prod_{i=1}^{l}(1 + W_{\delta_i})^{n_iP}\Big)(1 + V_{\alpha_3})^Q, (\alpha_3 \in \Phi^+, \delta_i \in \Pi).$$

The constant $Q = (1+p^2)^{-1} \equiv 1[p^2]$, $\frac{Q(Q-1)}{2} \equiv 0[p]$. As $P = \frac{log(1+p^2)}{log(1+p)} \equiv p[p^2]$, $p > 2$, 2 is invertible in $\mathbb{Z}_p$, we get that

$$(1 + W_{\delta_i})^P \equiv 1[\mod (p, W^3_{\delta_i})], (\delta_i \in \Pi).$$

Hence, modulo $F^3\overline{\mathcal{B}}$, relation 1.18 reduces to

$$(1 + V_{\alpha_3})(1 + V_{-\alpha_3}) = 1 + QV_{-\alpha_3} + QV_{\alpha_3} + Q^2V_{-\alpha_3}V_{\alpha_3}[\mod F^3\overline{\mathcal{B}}], (\alpha_3 \in \Phi^+).$$

Therefore, as $Q \equiv 1[p^2]$ we obtain

$$V_{\alpha_3}V_{-\alpha_3} \equiv V_{-\alpha_3}V_{\alpha_3} \text{ in } \mathrm{gr}^2\overline{\mathcal{B}} \text{ for } \alpha_3 \in \Phi^+.$$

This proves

$$\dim\, \mathrm{gr}^2\overline{\mathcal{B}} \leqslant \dim S_2.$$

Now, consider an arbitrary monomial of degree n,

$$x^i = x_{i_1}...x_{i_n}.$$

As in Lemma 3.2 of [Clo11], we can change x^i into a well-ordered monomial ($b \mapsto i_b$ increasing) by a sequence of transpositions. Consider a move $(b, b+1) \mapsto (b+1, b)$ and assume $i_b > i_{b+1}$. We write

$$x^i = x^f x_{i_b} x_{i_{b+1}} x^e$$

where $\deg(f) = r$, $\deg(e) = s$ and $\deg(i) = n$. Then, from the proof of Proposition 1.20 we have $x_{i_b} x_{i_{b+1}} = x_{i_{b+1}} x_{i_b}[F^3\overline{\mathcal{B}}]$. Hence, we obtain $x^f x_{i_{b+1}} x_{i_b} x^e \equiv x^i[F^{n+1}], n = r+s+2$. This reduces the number of inversions in x^i.

This completes the proof of proposition 1.20. □

In the following we state our main theorems. After proposition 1.20 their proofs directly follow from [Clo11]. But for convenience of the reader we include the proofs.

Theorem 1.21. *For $p > 2$, the Iwasawa algebra mod p, $\Omega_{G(1)}$, is naturally isomorphic to $\overline{\mathcal{A}}/\overline{\mathcal{R}}$.*

Proof. (Cf. [Clo11]). The natural map $\varphi : \mathcal{A} \to \Lambda(G(1))$ sends $\mathcal{M}_{\mathcal{A}}^n$ to $\mathcal{M}_{\Lambda}^n$. As $F^\bullet$ on $\overline{\mathcal{B}}$ is the filtration inherited from the natural filtration on $\overline{\mathcal{A}}$, we see that $\overline{\varphi}$ sends $F^n\overline{\mathcal{B}}$ to $\mathcal{M}_{\Omega}^n$. As $\overline{\varphi}$ is surjective, the natural map

$$\mathrm{gr}\overline{\varphi} : \mathrm{gr}^\bullet\overline{\mathcal{B}} \to \mathrm{gr}^\bullet\Omega_{G(1)}$$

is surjective. Moreover, it is an isomorphism because $\dim \mathrm{gr}^n\overline{\mathcal{B}} \leqslant \dim S_n = \dim \mathrm{gr}^n\Omega_{G(1)}$. (The last equality follows from the discussion after corollary 1.19, see also Theorem 7.24 of [DSMS03]). Since the filtration on $\overline{\mathcal{B}}$ is complete, we deduce that $\overline{\varphi}$ is an isomorphism (cf. Theorem 4 (5), p.31 of [LO96]). We have $\overline{\mathcal{B}}$ complete because $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$, where $\overline{\mathcal{R}}$ is closed and therefore complete for the filtration induced from that of $\overline{\mathcal{A}}$. □

Theorem 1.22. *For $p > 2$, the Iwasawa algebra $\Lambda(G(1))$is naturally isomorphic to $\mathcal{A}/\mathcal{R}$.*

Proof. The reduction of φ is $\overline{\varphi}$. We recall that $\overline{\mathcal{R}}$ is the image of $\mathcal{R}$ in $\overline{\mathcal{A}}$. Let $f \in \mathcal{A}$ satisfies $\varphi(f) = 0$. We then have $\overline{f} \in \overline{\mathcal{R}}$ since $\overline{\mathcal{A}}/\overline{\mathcal{R}} \cong \Omega_{G(1)}$. So $f = r_1 + pf_1, r_1 \in \mathcal{R}, f_1 \in \mathcal{A}$. Then $\varphi(f_1) = 0$. Inductively, we obtain an expression $f = r_n + p^n f_n$ of the same type. Since $p^n f_n \to 0$ in $\mathcal{A}$ and $\mathcal{R}$ is closed, we deduce that $f \in \mathcal{R}$. □

In conclusion for $p > 2$ and G simply connected, we have found a Lazard basis of $G(1)$ with respect to its p-valuation ω (see theorem 1.9). Furthermore, we have used it to construct explicit generators and relations for the Iwasawa algebra $\Omega_{(G(1))}$ with coefficients in $\mathbb{F}_p$ (see theorem 1.21) and then we have lifted the coefficients to $\mathbb{Z}_p$ to construct the generators and relations of $\Lambda(G(1))$ (see theorem 1.22).

2 Iwasawa algebra for the pro-p Iwahori subgroup of $GL(n, \mathbb{Z}_p)$

2.1 Introduction

Let G be the pro-p Iwahori subgroup of $SL_n(\mathbb{Z}_p)$, that is, the group of matrices in $SL_n(\mathbb{Z}_p)$ which are upper unipotent modulo the ideal $p\mathbb{Z}_p$.

Recall from section 1.1, the notion of the Iwasawa algebra of G which is a non-commutative completed group algebra defined by

$$\Lambda(G) := \varprojlim_{N \in \mathcal{N}(G)} (G/N),$$

where $\mathcal{N}(G)$ is the set of open normal subgroups in G. This algebra has many applications in number theory and p-adic representation theory ([Eme17]). It is used by Iwasawa [Iwa59] to study the growth of class numbers in towers of number fields. Schneider and Teitelbaum use the Iwasawa algebra to study the category of $\mathbb{Q}_p$-Banach representations of compact p-adic Lie groups [ST02a]. In section 1, we found an explicit presentation of the Iwasawa algebra for the first principal congruence kernel of a semi-simple, simply connected Chevalley group over $\mathbb{Z}_p$. In this section, our goal is to extend the method to give an explicit presentation of the Iwasawa algebra for the pro-p Iwahori subgroup of $SL(n, \mathbb{Z}_p)$ generalizing the work of Clozel for $n = 2$ [Clo17]. Our main result (see Theorem 2.15) is the following.

Theorem. *For $p > n + 1$, the Iwasawa algebra of the pro-p Iwahori subgroup of $SL(n, \mathbb{Z}_p)$ is naturally isomorphic as a topological ring to $\mathcal{A}/\mathcal{R}$.*

Here $\mathcal{A}$ is a non-commutative power series ring over $\mathbb{Z}_p$ in the variables $V_\alpha, W_\delta, U_\beta$ where α, δ, β varies over the positive, simple and negative roots respectively. The ordering among the variables is given by the ordering on the roots as in Theorem 2.5. The algebra $\mathcal{R}$ is a closed two-sided ideal in $\mathcal{A}$ generated by a set of explicit relations between these variables (2.50-2.64).

We first deduce the explicit presentation for $\Omega_G := \Lambda(G) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$, the Iwasawa algebra modulo p (theorem 2.4.2) and then we lift the coefficients to $\mathbb{Z}_p$. We also extend our proof to the case when G is the pro-p Iwahori of $GL(n, \mathbb{Z}_p)$ (corollary 2.15).

The explicit presentation can be used to define a "formal base change map" [Clo17] of Iwasawa algebras

$$\Lambda_L \to \Lambda_{\mathbb{Q}_p}$$

where Λ_L is the Iwasawa algebra over a finite unramified extension L of $\mathbb{Q}_p$. Such a formal base change map is given by power series which only converge for the globally analytic distributions (continuous dual of the rigid-analytic functions) on the pro-p Iwahori seen as a rigid-analytic space (*loc.cit*). This leads us also to the study of the globally analytic vectors of p-adic representations which will be our object in section 3.

Apart from the above implications of our explicit presentation of the Iwasawa algebra, Dong Han and Feng Wei note that our results may provide possible ways to answer the open question on the existence of non-trivial normal elements in $\Omega_G := \Lambda(G) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ (cf. introduction and section 5 of [HW18]). An element $r \in \Omega_G$ is normal if $r\Omega_G = \Omega_G r$. The question on the normal elements was originally posed in [BW13], later reformulated in [HW18] having dealt with the case for $SL(2, \mathbb{Z}_p)$ and $SL(3, \mathbb{Z}_p)$. As noted in [HW18], the normal elements help in constructing reflexive ideals in the Iwasawa algebra. The main question of Han and Wei is to find a mechanism for constructing ideals of completed group algebras without using central elements or closed normal subgroups which provide natural ways to construct ideals in the Iwasawa algebra (*loc.cit*).

Roadmap. Section 2.2.1 is devoted to preliminary notations. The theorem on ordered basis of the pro-p Iwahori group G with respect to the p-valuation ω (2.1) on G is given in section 2.2.2 (theorem 2.5). In section 2.3.1 we recall the notion of the Iwasawa algebra $\Lambda(G)$ of G, the algebra of p-adic measures on G. By a theorem of Lazard, this algebra is isomorphic as a $\mathbb{Z}_p$-module to a ring of power series in several variables. The relations between the variables inside $\Lambda(G)$ are given in lemma 2.11 in section 2.3.2. The computations for the proof of lemma 2.11 are included in section 2.5. Sections 2.3.1 and 2.4.1 deal with the construction of a continuous surjection $\varphi : \mathcal{A} \to \Lambda(G)$. Let $\overline{\mathcal{B}} := \overline{\mathcal{A}}/\overline{\mathcal{R}}$ be the reduction modulo p of $\mathcal{A}/\mathcal{R}$. The algebra $\overline{\mathcal{B}}$ has a natural grading discussed after Theorem 2.4.1. For integer $m \geq 0$, we provide an upper bound on the dimension of the m-th

graded piece $\mathrm{gr}^m\overline{\mathcal{B}}$ in section 2.4.2 (see lemma 2.14). The computations for the proof of lemma 2.14 is included in section 2.6. Finally, the proof of the explicit presentation of Ω_G and $\Lambda(G)$ is in section 2.4.3.

2.2 Lazard's ordered Basis for the pro-p Iwahori subgroup G

Recall that G is the pro-p Iwahori subgroup of $SL_n(\mathbb{Z}_p)$, i.e. G is the group of matrices in $SL_n(\mathbb{Z}_p)$ which are upper unipotent modulo the maximal ideal $p\mathbb{Z}_p$ of $\mathbb{Z}_p$. The goal of this section is to find an ordered basis in the sense of Lazard [Laz65] for the pro-p Iwahori group G. This will later be used in deducing an explicit presentation of the Iwasawa algebra of G (theorem 2.4.3).

In this section, we first define a function $\omega_{\frac{1}{n}}$ on G which is a p-valuation (2.2) in the sense of Lazard (cf. chapter III, 2.1.2 of [Laz65]). Then, in section 2.2.2, we give an ordered basis for the p-valuation (Theorem 2.5). This means that we find an ordered set of elements $g_1, ..., g_d \in G$ such that

1. The map $\mathbb{Z}_p^d \to G$ sending $(z_1, ..., z_d) \mapsto g_1^{z_1} \cdots g_d^{z_d}$ is a bijection and
2. $\omega_{\frac{1}{n}}(g_1^{z_1} \cdots g_d^{z_d}) = \min_{1\leq i\leq d}(\omega_{\frac{1}{n}}(g_i) + val_p(z_i))$.

(Cf. section 1.2).

2.2.1 p-valuation on G

Let p be a prime number. Fix a pinning [GP11, XXIII 1] of the split reductive group SL_n over $\mathbb{Z}_p$

$$(T_S, M, \Phi, \Pi, (X_\varsigma)_{\varsigma\in\Pi})$$

where T_S is a split maximal torus in SL_n, $M = X^*(T_S)$ is its group of characters,

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \oplus_{\varsigma\in\Phi}\mathfrak{g}_\varsigma$$

is the weight decomposition for the action of T_S on $\mathfrak{g} = \mathrm{Lie}(SL_n)$, $\Pi \subset \Phi$ is a basis of the root system $\Phi \subset M$ and for each $\varsigma \in \Pi$, X_ς is a $\mathbb{Z}_p$-basis of $\mathfrak{g}_\varsigma$.

We denote the positive and negative roots by Φ^+ and Φ^- respectively with respect to the standard Borel subgroup of $SL_n(\mathbb{Z}_p)$. The height function on the roots $h(\varsigma) \in \mathbb{Z}$ of $\varsigma \in \Phi$ is the sum of the coefficients of ς in the basis Π of Φ. We expand $(X_\varsigma)_{\varsigma\in\Pi}$ to a Chevalley system $(X_\varsigma)_{\varsigma\in\Phi}$ of SL_n [GP11, XXIII 6.2]. For $\varsigma \in \Phi$, $t \in \mathbb{Z}_p$, $\lambda \in \mathbb{Z}_p^*$, we denote $x_\varsigma(t) = \exp(tX_\varsigma)$, $h_\varsigma(\lambda) = w_\varsigma(\lambda)w_\varsigma(1)^{-1}$, where $w_\varsigma(\lambda) = x_\varsigma(\lambda)x_{-\varsigma}(-\lambda^{-1})x_\varsigma(\lambda)$.

Henceforth, we assume

$$p > n + 1. \tag{2.1}$$

Thus, G is p-saturated (cf. Lazard, [Laz65], 3.2.7.5, chap. 3).

The following construction can be found in [Sch11, p. 172].

Definition 2.1. *For each real a with $\frac{1}{p-1} < a < \frac{p-2}{(p-1)(n-1)}$, $g \in G, g = (a_{ij})$, a p-valuation ω_a on G is given by*

$$\omega_a(g) := \min\Big(\min_{1\leq i\neq j\leq n}((j-i)a + val_p(a_{ij})), \min_{1\leq i\leq n} val_p(a_{ii} - 1)\Big), \tag{2.2}$$

$$= \min\Big((j-i)a + val_p(a_{ij})_{i\neq j}, val_p(a_{ii} - 1)\Big). \tag{2.3}$$

Setting $a = \frac{1}{n}$, we write simply ω for ω_a. The function ω makes G a p-valuable group in the sense of [Laz65, III.2.1.2]. In fact, for $p > n + 1$, (G, ω) is p-saturated [Laz65, III.3.2.7.5].

The pro-p Iwahori group G has a triangular decomposition

$$G = N^-TN^+$$

(cf p. 317, section 1.6 of [Gar97], also [BT72]), where N^- (resp. N^+) is the subgroup of lower (resp. upper) unipotent matrices of G and T is the subgroup of the diagonal matrices of G. Let α, β, δ be the roots in Φ^+, Φ^-, Π respectively. From 2.2 we deduce that

$$\omega(x_\beta(p)) = \frac{(j-i)}{n} + 1;\ \beta \in \Phi^-, \beta = (i,j), i > j, \tag{2.4}$$

$$\omega(h_\delta(1+p)) = 1;\ \delta \in \Pi, \tag{2.5}$$

$$\omega(x_\alpha(1)) = \frac{(j-i)}{n};\ \alpha \in \Phi^+, \alpha = (i,j), i < j. \tag{2.6}$$

In the next section we are going to use this p-valuation ω on G in order to find an ordered basis of G in the sense of Lazard (cf. Lazard, [Laz65, III, 2.2]).

2.2.2 Ordered basis

In this section we find an ordered basis for the p-valuation on G (theorem 2.5). But before proving theorem 2.5 we need a preparatory lemma 2.2 and a proposition 2.3. Let $E_{i,j}$ be the standard elementary matrix at (i,j)-th place.

Lemma 2.2. *Any element $g \in G$ has a unique expression of the form*

$$g = \prod_{\beta \in \Phi^-} x_\beta(u_\beta) \prod_{\delta \in \Pi} h_\delta(1+v_\delta) \prod_{\alpha \in \Phi^+} x_\alpha(w_\alpha), \tag{2.7}$$

where $u_\beta, v_\delta \in p\mathbb{Z}_p, w_\alpha \in \mathbb{Z}_p$. The order of the products is taken as follows (compare also theorem 2.5):

(i) first take the lower unipotent matrices in the order given by the (increasing) height function on the roots,
(ii) then take the diagonal elements $h_\delta(1+p)$ for $\delta \in \Pi$ starting from the top left extreme to the low right extreme and,
(iii) finally, take the upper unipotent matrices in the following lexicographic order:
The matrix $(1+E_{i,j})$ comes before $(1+E_{k,l})$ if and only if $i \geq k$ and $i = k \implies j > l$.

That is, for the upper unipotent matrices we start with the low and right extreme and then fill the lines from the right, going up.

Proof. • Any element of T can be uniquely written as $\prod_{\delta \in \Pi} h_\delta(1+v_\delta)$ with $v_\delta \in p\mathbb{Z}_p$. (cf. last paragraph of the proof of Theorem 3.2 of [Ray16].) If $\delta = (i, i+1)$, then $h_\delta(1+v_\delta)$ is the diagonal matrix $(1+p)^{v_\delta}E_{i,i} + (1+p)^{-v_\delta}E_{i+1,i+1} + \sum_{j \neq i} E_{j,j}$. So, each element Z of T can be uniquely written as

$$Z = \sum_{k=1}^{n} (1+p)^{x_{k,k} - x_{k-1,k-1}} E_{k,k} \tag{2.8}$$

for unique $x_{k,k} \in \mathbb{Z}_p$ and $x_{0,0} = x_{n,n} = 0$.

• For $x_{i,j} \in \mathbb{Z}_p$, we have

$$\begin{aligned}&(1+px_{n,1}E_{n,1})(1+px_{n-1,1}E_{n-1,1})(1+px_{n,2}E_{n,2}) \cdots (1+px_{n,n-1})E_{n,n-1} \\ &\quad = 1 + px_{n,1}E_{n,1} + px_{n-1,1}E_{n-1,1} + px_{n,2}E_{n,2} + \cdots + px_{n,n-1}E_{n,n-1},\end{aligned}$$

where the order of the product is taken according to the (increasing) height function on the roots. This directly implies that every element X of N^- can be written as

$$X = (1+pE_{n,1})^{x_{n,1}}(1+pE_{n-1,1})^{x_{n-1,1}}(1+pE_{n,2})^{x_{n,2}} \cdots (1+pE_{n,n-1})^{x_{n,n-1}} = I + \sum_{\substack{i \in [2,n] \\ j \in [1,i-1]}} px_{i,j}E_{i,j}, \tag{2.9}$$

with unique $x_{i,j} \in \mathbb{Z}_p$.

Thus, each element of N^- can be uniquely written as a product $\prod_{\beta\in\Phi^-} x_\beta(p)$ with the ordering given by the height function.

• Also, because of our dual lexicographic order on N^+, we have

$(1+x_{n-1,n}E_{n-1,n})(1+x_{n-2,n}E_{n-2,n})(1+x_{n-2,n-1}E_{n-2,n-1})\cdots(1+x_{1,2}E_{1,2})$
$= 1+x_{n-1,n}E_{n-1,n}+x_{n-2,n}E_{n-2,n}+x_{n-2,n-1}E_{n-2,n-1}+\cdots+x_{1,2}E_{1,2}.$

Indeed, for any $b\in\mathbb{N}$, if we take the product of the first b terms in the L.H.S of the above equation, the set of column entries which appears in the subscript of the elementary matrices of the product, is disjoint from the row entry which appears in the subscript of the elementary matrix occurring in the $(b+1)^{th}$ term of the product in the L.H.S. We also use $E_{i,j}E_{k,l}=E_{i,l}$ for $j=k$ and $E_{i,j}E_{k,l}=0$ if $j\neq k$.

So, each element Y of N^+ can be uniquely written as

$$Y=(1+E_{n-1,n})^{x_{n-1,n}}(1+E_{n-2,n})^{x_{n-2,n}}(1+E_{n-2,n-1})^{x_{n-2,n-1}}...(1+E_{1,2})^{x_{1,2}}=I+\sum_{\substack{i\in[1,n-1]\\ j\in[i+1,n]}} x_{i,j}E_{i,,j}, \tag{2.10}$$

with $x_{i,j}\in\mathbb{Z}_p$.

Therefore, from the triangular decomposition $G=N^-TN^+$, we get that each element $g\in G$ has a unique expression of the form

$$g=\prod_{\beta\in\Phi^-} x_\beta(u_\beta)\prod_{\delta\in\Pi} h_\delta(1+v_\delta)\prod_{\alpha\in\Phi^+} x_\alpha(w_\alpha), \tag{2.11}$$

where $u_\beta, v_\delta\in p\mathbb{Z}_p, w_\alpha\in\mathbb{Z}_p$. The order of the products is taken according to Theorem 2.5. This proves lemma 2.2. □

In order to find an ordered basis for the p-valuation on G, we need to compute the p-valuation of the product XZY (the matrices X,Y,Z are defined in the proof of lemma 2.2).

Proposition 2.3. *Let $a_{i,j}$ be the $(i,j)^{th}$ entry of the matrix $XZY=(a_{i,j})$. Then,*

$$a_{1,j}=(1+p)^{x_{1,1}}x_{1,j},\ j\in[2,n] \tag{2.12}$$
$$a_{i,1}=px_{i,1}(1+p)^{x_{1,1}},\ i\in[2,n] \tag{2.13}$$
$$a_{1,1}=(1+p)^{x_{1,1}} \tag{2.14}$$
$$a_{i,j}=(\sum_{k=1}^{m}px_{i,k}x_{k,j}(1+p)^{x_{k,k}-x_{k-1,k-1}})+px_{i,j}(1+p)^{x_{j,j}-x_{j-1,j-1}},\ 2\leq j<i\leq n \tag{2.15}$$
$$a_{i,j}=(\sum_{k=1}^{m}px_{i,k}x_{k,j}(1+p)^{x_{k,k}-x_{k-1,k-1}})+x_{i,j}(1+p)^{x_{i,i}-x_{i-1,i-1}},\ 2\leq i<j\leq n \tag{2.16}$$
$$a_{i,j}=(\sum_{k=1}^{m}px_{i,k}x_{k,j}(1+p)^{x_{k,k}-x_{k-1,k-1}})+(1+p)^{x_{i,i}-x_{i-1,i-1}},\ 2\leq i=j\leq n. \tag{2.17}$$

Proof. Multiplying the matrix X (see equation 2.9) with Z (see equation 2.8) we get

$$XZ=\sum_{k=1}^{n}(1+p)^{x_{k,k}-x_{k-1,k-1}}E_{k,k}+\sum_{\substack{i=2,\ldots,n\\ j=1,\ldots,i-1}} px_{i,j}(1+p)^{x_{j,j}-x_{j-1,j-1}}E_{i,j}. \tag{2.18}$$

So, if we write the $(i,j)^{th}$ coordinate of the matrix XZ by $(XZ)_{i,j}$, then we deduce (from 2.18) that

$$(XZ)_{i,1}=px_{i,1}(1+p)^{x_{1,1}},\ i\in[2,n], \tag{2.19}$$

and

$$(XZ)_{1,1}=(1+p)^{x_{1,1}}, (XZ)_{1,j}=0,\ j\in[2,n]. \tag{2.20}$$

Also, for $i \geq 2$, it is clear from equation 2.18 that the i^{th} row of the matrix XZ is

$$[px_{i,1}(1+p)^{x_{1,1}}, ..., \underbrace{px_{i,i-1}(1+p)^{x_{i-1,i-1}-x_{i-2,i-2}}}_{(XZ)_{i,i-1}}, \underbrace{(1+p)^{x_{i,i}-x_{i-1,i-1}}}_{(XZ)_{i,i}}, 0, 0, ..., 0] \tag{2.21}$$

In order to compute the $(i,j)^{th}$ entry of the matrix $XZY = (a_{i,j})$ we have to multiply the i^{th} row of the matrix XZ given above by the j^{th} column of the matrix Y (the matrix Y is given in 2.10).

Now, as the first row of the matrix Y is $[1, x_{1,2}, x_{1,3}, ..., x_{1,n}]$, from equation 2.20 it is clear that

$$a_{1,j} = (1+p)^{x_{1,1}} x_{1,j},\ j \in [2,n]. \tag{2.22}$$

As the first column of the matrix Y is $[1, 0, ..., 0]^t$ (here 't' denotes the transpose of the row vector), we deduce from equation 2.19 and 2.20 that

$$a_{i,1} = px_{i,1}(1+p)^{x_{1,1}},\ i \in [2,n], \tag{2.23}$$

and

$$a_{1,1} = (1+p)^{x_{1,1}}. \tag{2.24}$$

For $j \geq 2$, the j^{th} column of the matrix Y is

$$[x_{1,j}, x_{2,j}, ..., x_{j-1,j}, 1, 0, ..., 0]^t.$$

Therefore, multiplying the i^{th} row of the matrix XZ given by 2.21 with the j^{th} column of the matrix Y given above, for $i, j \geq 2, m = \min\{i-1, j-1\}$, we get the following three subcases (viz. $i > j, i < j$ and $i = j$):

$$a_{i,j} = (\sum_{k=1}^{m} px_{i,k}x_{k,j}(1+p)^{x_{k,k}-x_{k-1,k-1}}) + px_{i,j}(1+p)^{x_{j,j}-x_{j-1,j-1}},\ 2 \leq j < i \leq n,$$

$$a_{i,j} = (\sum_{k=1}^{m} px_{i,k}x_{k,j}(1+p)^{x_{k,k}-x_{k-1,k-1}}) + x_{i,j}(1+p)^{x_{i,i}-x_{i-1,i-1}},\ 2 \leq i < j \leq n,$$

$$a_{i,j} = (\sum_{k=1}^{m} px_{i,k}x_{k,j}(1+p)^{x_{k,k}-x_{k-1,k-1}}) + (1+p)^{x_{i,i}-x_{i-1,i-1}},\ 2 \leq i = j \leq n.$$

This completes the proof of proposition 2.3. □

Proposition 2.3 gives us the following corollary.

Corollary 2.4. *The valuations of the terms $a_{i,j}$ obtained in equations (2.12 − 2.17) are the following:*

$$val_p(a_{1,j}) = val_p(x_{1,j}),\ j \geq 2, \tag{2.25}$$

$$val_p(a_{i,1}) = val_p(px_{i,1}),\ i \geq 2, \tag{2.26}$$

$$val_p(a_{1,1} - 1) = 1 + val_p(x_{1,1}), \tag{2.27}$$

$$val_p(a_{i,j}) = val_p\Big((\sum_{k=1}^{m} px_{i,k}x_{k,j}) + px_{i,j}\Big),\ i,j \geq 2, i > j, m = j-1, \tag{2.28}$$

$$val_p(a_{i,j}) = val_p\Big((\sum_{k=1}^{m} px_{i,k}x_{k,j}) + x_{i,j}\Big),\ i,j \geq 2, i < j, m = i-1 \tag{2.29}$$

$$val_p(a_{i,i} - 1) = val_p\Big((\sum_{k=1}^{m} px_{i,k}x_{k,i}) + p(x_{i,i} - x_{i-1,i-1})\Big),\ i \geq 2, m = i-1. \tag{2.30}$$

The following theorem gives an ordered basis for the p-valuation ω on G.

Theorem 2.5. *The elements*

$$\{x_\beta(p), h_\delta(1+p), x_\alpha(1); \beta \in \Phi^-, \delta \in \Pi, \alpha \in \Phi^+\}$$

form an ordered basis for the p-valuation ω on G, where the ordering is as follows:

(i) first take the lower unipotent matrices in the order given by the (increasing) height function on the roots,
(ii) then take the diagonal elements $h_\delta(1+p)$ for $\delta \in \Pi$ starting from the top left extreme to the low right extreme and,
(iii) finally, take the upper unipotent matrices in the following lexicographic order:
The matrix $(1+E_{i,j})$ comes before $(1+E_{k,l})$ if and only if $i \geq k$ and $i = k \implies j > l$.

Point (iii) means that for the upper unipotent matrices we start with the low and right extreme and then fill the lines from the right, going up.

Proof. Let $g_1, ..., g_d$ ($d = |\Phi| + |\Pi|$) denote the ordered basis as in the statement of Theorem 2.5. Then, by lemma 2.2, we have a bijective map

$$\mathbb{Z}_p^d \to G$$
$$(x_{n,1}, ..., x_{1,2}) \to g_1^{x_{n,1}} \cdots g_d^{x_{1,2}}.$$

In the following, our objective is to show

$$\omega(g_1^{x_{n,1}} \cdots g_d^{x_{1,2}}) = \omega(XZY)$$
$$= \min\Big(\tfrac{j-i}{n} + val_p(a_{i,j})_{i\neq j}, val_p(a_{i,i}-1)\Big),$$
$$= \min_{\substack{(i_1,j_1)=\beta\in\Phi^-,\ (i_2,j_2)=\alpha\in\Phi^+ \\ (t,t+1)=\delta\in\Pi, t\in[1,n-1]}} \Big\{\omega(x_\beta(p))+val_p(x_{i_1,j_1}), \omega(x_\alpha(1))+val_p(x_{i_2,j_2}), \omega(h_\delta(1+p))+val_p(x_{t,t})\Big\}.$$

Let us define, for $1 \leq i, j \leq n$,

$$v_{i,j} = \frac{j-i}{n} + val_p(a_{i,j}); (i \neq j), \tag{2.31}$$
$$v_{i,i} = val_p(a_{i,i} - 1). \tag{2.32}$$

Then we have to show that

$$\omega(g_1^{x_{n,1}} \cdots g_d^{x_{1,2}}) = \omega(XZY) = \min_{1\leq i,j\leq n}(v_{i,j}) \tag{2.33}$$
$$= \min_{\substack{(i_1,j_1)=\beta\in\Phi^-,\ (i_2,j_2)=\alpha\in\Phi^+ \\ (t,t+1)=\delta\in\Pi}} \Big\{\omega(x_\beta(p)) + val_p(x_{i_1,j_1}), \omega(x_\alpha(1)) + val_p(x_{i_2,j_2}), \omega(h_\delta(1+p)) + val_p(x_{t,t})\Big\}, \tag{2.34}$$

for $i_1 > j_1, i_2 < j_2, t = 1, ..., n-1$. The first two equalities of the above equation are obvious (by definition). To prove the last equality we will rearrange the $v_{i,j}$'s and then use induction. First we order the $v_{i,j}$'s, appearing in equation 2.33 in such a way that the indices are given by:

$$\text{(for all } 1 \leq i, j, i', j' \leq n) \text{ if } \min\{i', j'\} < \min\{i, j\} \text{ then } v_{i',j'} \text{ comes before } v_{i,j}. \tag{2.35}$$

Such an ordering of the $v_{i,j}$'s can be achieved by first taking the $v_{i,j}$'s in the first row and the first column starting from the top left extreme $(v_{1,1}, .., v_{1,n}, v_{2,1}, ..., v_{n,1})$, then the second row and the second column $(v_{2,2}, ..., v_{2,n}, v_{3,2}, ..., v_{n,2})$ and so on.

To compute $\omega(g_1^{x_{n,1}} \cdots g_d^{x_{1,2}}) = \min(v_{i,j})$ we use induction: As the basic step of the induction process (the zero-th step) we compute $S_0 := \min(v_{1,1}, ..., v_{1,n}, v_{2,1}, ..., v_{n,1}) = \min_{2\leq i,j\leq n}(v_{1,1}, v_{1,j}, v_{i,1})$ and then we proceed in stages, adding one $v_{i,j}$ at each stage of induction according to the prescribed order of the $v_{i,j}$, i.e. in the first stage we compute $S_1 := \min\{S_0, v_{2,2}\}$, then in the second stage we compute $S_2 := \min(S_1, v_{2,3})$ and so on until we have completed computing minimum of all the $v_{i,j}$'s. Note that in the last stage, i.e. at the stage $n^2 - n - (n-1)$, $S_{n^2-2n+1} = \min_{1\leq i,j\leq n}\{v_{i,j}\} = \omega(g_1^{x_{n,1}} \cdots g_d^{x_{1,2}})$ (cf. (2.33)).

From the definition of $v_{i,j}$ (see equation 2.31) and equations $(2.25 - 2.27)$ of Corollary 2.4 we get, for $2 \leq i, j \leq n$, that

$\min\limits_{2\leq i,j\leq n}(v_{1,1},v_{1,j},v_{i,1}) = \min\limits_{2\leq i,j\leq n}\Big\{\frac{j-1}{n}+val_p(a_{1,j}),\frac{1-i}{n}+val_p(a_{i,1}),val_p(a_{1,1}-1)\Big\}$
$= \min\limits_{2\leq i,j\leq n}\Big\{\frac{j-1}{n}+val_p(x_{1,j}),\frac{1-i}{n}+1+val_p(x_{i,1}),1+val_p(x_{1,1})\Big\}$
$= \min\limits_{\substack{\alpha=(1,j),\beta=(i,1)\\ \delta=(1,2),2\leq i,j\leq n}}\Big\{\omega(x_\alpha(1))+val_p(x_{1,j}),\omega(x_\beta(p))+val_p(x_{i,1}),\omega(h_\delta(1+p))+val_p(x_{1,1})\Big\}.$

Then, at each stage of the induction, say q^{th} stage, $q\in\mathbb{N}$, of computing the minimum, we compute $S_q=\min(S_{q-1},v_{i,j})$ for some (i,j) with $i,j\geq 2$, where S_{q-1} is the minimum computed in the $(q-1)^{th}$ stage [the subscript q depends on (i,j)].
Henceforth, we fix the coordinate (i,j) appearing in the definition of S_q. Note that S_{q-1} is by definition minimum of all the $v_{i',j'}$ appearing before $v_{i,j}$ in the ordering and by induction hypothesis we can assume that

$$S_{q-1}=\min_H\Big\{\omega(x_\alpha(1))+val_p(x_{i'_2,j'_2}),\omega(x_\beta(p))+val_p(x_{i'_1,j'_1}),\omega(h_\delta(1+p))+val_p(x_{t,t})\Big\},\quad(2.36)$$

where $H=\Big\{\alpha=(i'_2,j'_2)\in\Phi^+,\beta=(i'_1,j'_1)\in\Phi^-,\delta=(t,t+1)\in\Pi$ such that $v_{i'_1,j'_1}<v_{i,j},v_{i'_2,j'_2}<v_{i,j},v_{t,t}<v_{i,j}\Big\}$. (Here, the symbol $<$ denotes the order function and not the ordinary less than symbol, that is, when we write $v_{i'_1,j'_1}<v_{i,j}$ we mean that $v_{i'_1,j'_1}$ comes before $v_{i,j}$ in the order given by equation 2.35). By proposition 2.6 below, we have

$$S_q:=\min\{S_{q-1},v_{i,j}\}=\min\{S_{q-1},V_{i,j}\},\quad(2.37)$$

where

$$V_{i,j}=\omega(x_{\beta_2=(i,j)}(p))+val_p(x_{i,j});(\text{if } i>j)$$
$$V_{i,j}=\omega(x_{\alpha_2=(i,j)}(1))+val_p(x_{i,j});(\text{if } i<j)$$
$$V_{i,j}=\omega(h_{\delta=(i,i+1)}(1+p))+val_p(x_{i,i}-x_{i-1,i-1});(\text{if } i=j).$$

Assume 2.37 for now (for the proof see proposition 2.6 below).

Therefore, in the last stage (i.e when $q=n^2-n-(n-1)$) of our induction process we will obtain

$\omega(g_1^{x_{n,1}}\cdots g_d^{x_{1,2}})$
$=\min\Big(\frac{j-i}{n}+val_p(a_{i,j})_{i\neq j},val_p(a_{i,i}-1)\Big)$,
$=\min_{1\leq i,j\leq n}(v_{i,j})$ (with ordered $v_{i,j}$),
$=S_{q=n^2-2n+1}$,
$=$
$$\min_{\substack{(i_1,j_1)=\beta\in\Phi^-,\ (i_2,j_2)=\alpha\in\Phi^+\\ (t,t+1)=\delta\in\Pi,t\in[1,n-1]}}\Big\{\omega(x_\beta(p))+val_p(x_{i_1,j_1}),\omega(x_\alpha(1))+val_p(x_{i_2,j_2}),\omega(h_\delta(1+p))+val_p(x_{t,t})\Big\}.$$

This complete our proof of Theorem 2.5. □

Proposition 2.6. *With notations as in the proof of Theorem 2.5, we have*

$$S_q:=\min\{S_{q-1},v_{i,j}\}=\min\{S_{q-1},V_{i,j}\},\quad(2.38)$$

where

$$V_{i,j}=\omega(x_{\beta_2=(i,j)}(p))+val_p(x_{i,j});(\textit{if } i>j)$$
$$V_{i,j}=\omega(x_{\alpha_2=(i,j)}(1))+val_p(x_{i,j});(\textit{if } i<j)$$
$$V_{i,j}=\omega(h_{\delta=(i,i+1)}(1+p))+val_p(x_{i,i}-x_{i-1,i-1});(\textit{if } i=j).$$

Proof. To prove equation 2.38, we first note that for all $k=1,...,m=\min\{i-1,j-1\}$, we have $k<i,k<j$, hence (cf. equation 2.35) the terms $\omega(x_{\beta_1=(i,k)}(p))+val_p(x_{i,k})=\frac{k-i}{n}+val_p(px_{i,k})$ and $\omega(x_{\alpha_1=(k,j)}(1))+val_p(x_{k,j})=\frac{j-k}{n}+val_p(x_{k,j})$ belong to R.H.S of equation 2.36 (because since $k<i$ and $k<j$, equation 2.35 gives $v_{i,k}<v_{i,j}$ and $v_{k,j}<v_{i,j}$). Thus, to prove equation 2.38, it suffices to find

$$\min_{k=1,...,m}\Big\{\frac{k-i}{n}+val_p(px_{i,k}),\frac{j-k}{n}+val_p(x_{k,j}),v_{i,j}\Big\}\quad(2.39)$$

and show that

$$\min_{k=1,\dots,m}\Big\{\frac{k-i}{n}+val_p(px_{i,k}),\frac{j-k}{n}+val_p(x_{k,j}),v_{i,j}\Big\}$$
$$=\min_{\substack{\alpha_1=(k,j),\beta_1=(i,k)\\k=1,\dots,m}}\Big\{\omega(x_{\alpha_1=(k,j)}(1))+val_p(x_{k,j}),\omega(x_{\beta_1=(i,k)}(p))+val_p(x_{i,k}),V_{i,j}\Big\}.$$

We divide this problem in three cases, first when $i>j$, second when $i<j$ and third when $i=j$. These three cases are dealt in **(I),(II),(III)** below.

First we consider the case $i,j\geq 2, i>j, m:=\min\{i-1,j-1\}=j-1$. So $m<j<i$. Then

$\min_{k=1,\dots,m}\Big\{\frac{k-i}{n}+val_p(px_{i,k}),\frac{j-k}{n}+val_p(x_{k,j}),v_{i,j}=\frac{j-i}{n}+val_p(a_{i,j})\Big\}$
$=\min_{k=1,\dots,m}\Big\{\frac{k-i}{n}+1+val_p(x_{i,k}),\frac{j-k}{n}+val_p(x_{k,j}),\frac{j-i}{n}+val_p((\sum_{k=1}^m px_{i,k}x_{k,j})+px_{i,j})\Big\}$
$=$
$\min_{\substack{\beta_1=(i,k),\alpha_1=(k,j)\\k=1,\dots m}}\Big\{\omega(x_{\beta_1}(p))+val_p(x_{i,k}),\omega(x_{\alpha_1}(1))+val_p(x_{k,j}),\frac{j-i}{n}+val_p((\sum_{k=1}^m px_{i,k}x_{k,j})+px_{i,j})\Big\}$
$=\min_{\substack{\beta_1=(i,k),\alpha_1=(k,j)\\\beta_2=(i,j),k=1,\dots m}}\Big\{\omega(x_{\beta_1}(p))+val_p(x_{i,k}),\omega(x_{\alpha_1}(1))+val_p(x_{k,j}),\omega(x_{\beta_2}(p))+val_p(x_{i,j})\Big\}$—**(I)**,

where the first equality follows from 2.28 and the second equality follows from $(2.4-2.6)$. To prove the last equality, we notice that if $val_p(px_{i,j})<val_p(\sum_{k=1}^m px_{i,k}x_{k,j})$ then it is obvious. On the other hand, if

$$val_p(px_{i,j})\geq val_p(\sum_{k=1}^m px_{i,k}x_{k,j}) \tag{2.40}$$

then both the terms (L.H.S and R.H.S of the last equality of **I**) equals

$$\min_{\substack{\beta_1=(i,k),\alpha_1=(k,j)\\k=1,\dots m}}\Big\{\omega(x_{\beta_1}(p))+val_p(x_{i,k}),\omega(x_{\alpha_1}(1))+val_p(x_{k,j})\Big\},$$

because

$$\frac{j-i}{n}+val_p((\sum_{k=1}^m px_{i,k}x_{k,j})+px_{i,j})\geq \frac{j-i}{n}+val_p(\sum_{k=1}^m px_{i,k}x_{k,j}) \text{ (using (2.40))} \tag{2.41}$$
$$\geq \frac{j-i}{n}+\min_{k=1,\dots,m}\{val_p(px_{i,k})\} \tag{2.42}$$
$$=\min_{k=1,\dots,m}\Big\{\frac{j-i}{n}+val_p(px_{i,k})\Big\} \tag{2.43}$$
$$\geq \min_{k=1,\dots,m}\Big\{\frac{k-i}{n}+val_p(px_{i,k})\Big\} \text{ (as } k\leq m=j-1<j) \tag{2.44}$$
$$=\min_{k=1,\dots,m}\Big\{\omega(x_{\beta_1=(i,k)}(p))+val_p(x_{i,k})\Big\}. \tag{2.45}$$

and

$$\omega(x_{\beta_2=(i,j)}(p))+val_p(x_{i,j})=\frac{j-i}{n}+val_p(px_{i,j})$$
$$\geq \frac{j-i}{n}+val_p(\sum_{k=1}^m px_{i,k}x_{k,j}) \text{ (using (2.40))}$$
$$\geq \min_{k=1,\dots,m}\Big\{\omega(x_{\beta_1=(i,k)}(p))+val_p(x_{i,k})\Big\} \text{ (using } (2.41-2.45)).$$

The argument for the case $i,j\geq 2, i<j, m=i-1<i<j$ is similar to our previous computation and so we omit it. The result that we obtain in that case is the following:

$$\min_{k=1,\dots,m}\left\{\tfrac{k-i}{n}+val_p(px_{i,k}),\tfrac{j-k}{n}+val_p(x_{k,j}),v_{i,j}=\tfrac{j-i}{n}+val_p(a_{i,j})\right\}$$
$$=$$
$$\min_{\substack{\beta_1=(i,k),\alpha_1=(k,j)\\k=1,\dots m}}\left\{\omega(x_{\beta_1}(p))+val_p(x_{i,k}),\omega(x_{\alpha_1}(1))+val_p(x_{k,j}),\tfrac{j-i}{n}+val_p((\textstyle\sum_{k=1}^m px_{i,k}x_{k,j})+x_{i,j})\right\}$$
$$=\min_{\substack{\beta_1=(i,k),\alpha_1=(k,j)\\\alpha_2=(i,j),k=1,\dots m}}\left\{\omega(x_{\beta_1}(p))+val_p(x_{i,k}),\omega(x_{\alpha_1}(1))+val_p(x_{k,j}),\omega(x_{\alpha_2}(1))+val_p(x_{i,j})\right\}\text{—(II)}.$$

Now, for $i,j\geq 2, i=j, m:=\min\{i-1,j-1\}=i-1=j-1$,

$$\min_{k=1,\dots,m}\left\{\tfrac{k-i}{n}+val_p(px_{i,k}),\tfrac{j-k}{n}+val_p(x_{k,j}),v_{i,i}=val_p(a_{i,i}-1)\right\}$$
$$=\min_{k=1,\dots,m}\left\{\tfrac{k-i}{n}+val_p(px_{i,k}),\tfrac{j-k}{n}+val_p(x_{k,j}),val_p((\textstyle\sum_{k=1}^m px_{i,k}x_{k,i})+p(x_{i,i}-x_{i-1,i-1}))\right\}$$
$$=\min_{k=1,\dots,m}\left\{\tfrac{k-i}{n}+val_p(px_{i,k}),\tfrac{j-k}{n}+val_p(x_{k,j}),1+val_p(x_{i,i}-x_{i-1,i-1})\right\}$$
$$=$$
$$\min_{\substack{\beta_1=(i,k),\alpha_1=(k,j),\\\delta=(i,i+1),k=1,\dots m}}\left\{\omega(x_{\beta_1}(p))+val_p(x_{i,k}),\omega(x_{\alpha_1}(1))+val_p(x_{k,j}),\omega(h_\delta(1+p))+val_p(x_{i,i}-x_{i-1,i-1})\right\},$$

—-(III)

where the first equality follows from 2.30 and the third equality follows from 2.5. To prove the second equality, we notice that if $val_p(p(x_{i,i}-x_{i-1,i-1}))<val_p(\sum_{k=1}^m px_{i,k}x_{k,i})$ then it is obvious. On the contrary, if

$$val_p(p(x_{i,i}-x_{i-1,i-1}))\geq val_p(\sum_{k=1}^m px_{i,k}x_{k,i}) \tag{2.46}$$

then both the terms (L.H.S and R.H.S of the second equality of **III**) equals

$$\min_{k=1,\dots,m}\left\{\tfrac{k-i}{n}+val_p(px_{i,k}),\tfrac{j-k}{n}+val_p(x_{k,j})\right\}$$

as

$$val_p((\sum_{k=1}^m px_{i,k}x_{k,i})+p(x_{i,i}-x_{i-1,i-1}))\geq val_p(\sum_{k=1}^m px_{i,k}x_{k,i})\text{ (using (2.46))} \tag{2.47}$$
$$\geq \min_{k=1,\dots,m}\left\{val_p(px_{i,k})\right\} \tag{2.48}$$
$$>\min_{k=1,\dots,m}\left\{\frac{k-i}{n}+val_p(px_{i,k})\right\}\text{ (as } k<i) \tag{2.49}$$

and

$$1+val_p((x_{i,i}-x_{i-1,i-1}))\geq val_p(\sum_{k=1}^m px_{i,k}x_{k,i})\text{ (using (2.46))}$$
$$>\min_{k=1,\dots,m}\left\{\frac{k-i}{n}+val_p(px_{i,k})\right\}\text{ (using } (2.47-2.49))$$

This completes the demonstration of equation 2.38.

□

Remark 2.7. Note that in theorem 2.5, we have ordered the lower unipotent matrices by the increasing height function on the roots. Theorem 2.5 also holds true (with the same proof) if we order the lower unipotent matrices by the following (lexicographic) order:

the matrix $(1+pE_{i,j})$ comes before $(1+pE_{k,l})$ if and only if $i<k$ and $i=k \implies j<l$,

that is, we start with the top and left extreme and the fill the lines from the left, going down. With $x_{k,1}\in\mathbb{Z}_p$,

$$(1+px_{2,1}E_{2,1})(1+px_{3,1}E_{3,1})(1+px_{3,2}E_{3,2})\cdots(1+px_{n,n-1}E_{n,n-1})=I+\sum_{\substack{i\in[2,n]\\j\in[1,i-1]}}px_{i,j}E_{i,j},$$

(this is X in equation 2.9). Indeed, for any $b\in\mathbb{N}$, if we take the product of the first b terms in the L.H.S of the above equation, the set of column entries which appears in the subscript of the

elementary matrices of the product, is disjoint from the row entry which appears in the subscript of the elementary matrix occurring in the $(b+1)^{th}$ term of the product in the L.H.S. We also use $E_{i,j}E_{k,l} = E_{i,l}$ for $j = k$ and $E_{i,j}E_{k,l} = 0$ if $j \neq k$.

The rest of the proof of Theorem 2.5 goes without any change.

2.3 Relations in the Iwasawa algebra

In this section we first recall the notion of the Iwasawa algebra of G which is naturally isomorphic as a $\mathbb{Z}_p$-module to a commutative ring of power series in several variable over $\mathbb{Z}_p$. Then we find the relations between those variables in order to give a ring theoretic presentation of the Iwasawa algebra (lemma 2.11).

This section is organized as follows. In section 2.3.1, we recall the notion of the Iwasawa algebra of G, and for $\beta \in \Phi^-, \alpha \in \Phi^+, \delta \in \Pi$, we identify (as a $\mathbb{Z}_p$-module) the Iwasawa algebra of G with the ring of power series in the variables $U_\beta, V_\alpha, W_\delta$ over $\mathbb{Z}_p$. This isomorphism is given by sending $1 + V_\alpha \mapsto x_\alpha(1), 1 + W_\delta \mapsto h_\delta(1+p)$ and $1 + U_\beta \mapsto x_\beta(p)$. As the Iwasawa algebra is non-commutative, this isomorphism is obviously not a ring isomorphism. Therefore, in section 2.3.2, we study the products of the variables "in the wrong order", viewing them as elements of the Iwasawa algebra and then we find the relations among them $(2.50 - 2.64)$. Finally, we consider $\mathcal{A}$ to be the non-commutative power series over $\mathbb{Z}_p$ in the variables V_α, W_δ, and U_β corresponding to the order of roots as in Theorem 2.5 and construct a natural map $\varphi : \mathcal{A} \to \Lambda(G)$ which factors through the quotient of $\mathcal{A}$ modulo the relations $(2.50 - 2.64)$.

2.3.1 Iwasawa algebra

After Theorem 2.5, we have a homeomorphism $c : \mathbb{Z}_p^d \to G$. Let $C(G)$ be continuous functions from G to $\mathbb{Z}_p$. The map c induces, by pulling back functions, an isomorphism of $\mathbb{Z}_p$-modules

$$c^* : C(G) \simeq C(\mathbb{Z}_p^d).$$

Definition 2.8. *Let $\Lambda(G)$ be the Iwasawa algebra of G over $\mathbb{Z}_p$, that is,*

$$\Lambda(G) := \varprojlim_{N \in \mathcal{N}(G)} (G/N),$$

where $\mathcal{N}(G)$ is the set of open normal subgroups in G.

Now, lemma 22.1 of [Sch11] shows that

$$\Lambda(G) = \mathrm{Hom}_{\mathbb{Z}_p}(C(G), \mathbb{Z}_p).$$

So, dualizing the map c^*, we get an isomorphism of $\mathbb{Z}_p$-modules

$$c_* = \Lambda(\mathbb{Z}_p^d) \cong \Lambda(G).$$

Lemma 2.9 (Prop. 20.1 of [Sch11])**.** *We have the following isomorphism of $\mathbb{Z}_p$-modules*

$$\begin{gathered}\tilde{c} : \mathbb{Z}_p[[U_\beta, V_\alpha, W_\delta; \beta \in \Phi^-, \alpha \in \Phi^+, \delta \in \Pi]] \cong \Lambda(G) \\ 1 + V_\alpha \longmapsto x_\alpha(1) \\ 1 + W_\delta \longmapsto h_\delta(1+p) \\ 1 + U_\beta \longmapsto x_\beta(p).\end{gathered}$$

We note that for obvious reasons the isomorphism above is not a ring isomorphism. Now, let $b_i := g_i - 1$ and $b^m := b_1^{m_1} \cdots b_d^{m_d}$ for any multi-index $m = (m_1, ..., m_d) \in \mathbb{N}^d$.

Definition 2.10. *We can define a valuation on $\Lambda(G)$*

$$\tilde{\omega} := \tilde{\omega}_{\frac{1}{n}} : \Lambda(G) \backslash \{0\} \to [0, \infty)$$

by

$$\tilde{\omega}\Big(\textstyle\sum_{m \in \mathbb{N}^d} c_m b^m\Big) := \inf_{m \in \mathbb{N}^d} \Big(val_p(c_m) + \sum_{i=1}^d m_i \tilde{\omega}(g_i)\Big)$$

where $c_m \in \mathbb{Z}_p$, with the convention that $\tilde{\omega}(0) := \infty$.

The valuation $\tilde{\omega}$ is the natural valuation on $\Lambda(G)$ (cf. [Sch11, Section 28]).

2.3.2 Relations

The isomorphism $\tilde{c}$ of lemma 2.9, provides an identification of the variables $V_\alpha, W_\delta, U_\beta$ as the elements of the Iwasawa algebra of G. Our objective is to find the relations among the above variables. For this we use the Chevalley relations [Ste67] and sometimes also direct computation.

Lemma 2.11. *In the Iwasawa algebra $\Lambda(G)$, the variables $V_\alpha, W_\delta, U_\beta$ satisfy the following relations.*

$$(1+W_\delta)(1+U_\beta) = (1+U_\beta)^q(1+W_\delta), (\beta \in \Phi^-), q = (1+p)^{\langle \beta, \delta \rangle} \tag{2.50}$$

$$(1+W_\delta)(1+V_\alpha) = (1+V_\alpha)^{q'}(1+W_\delta), (\alpha \in \Phi^+), q' = (1+p)^{\langle \alpha, \delta \rangle} \tag{2.51}$$

$$V_\alpha U_\beta = U_\beta V_\alpha, (\alpha \in \Phi^+, \beta \in \Phi^-, \alpha \neq -\beta, \alpha+\beta \notin \Phi) \tag{2.52}$$

$$(1+V_\alpha)(1+U_\beta) = (1+V_{(i,k)})^p(1+U_\beta)(1+V_\alpha), i<k, (\alpha=(i,j) \in \Phi^+, \beta=(j,k) \in \Phi^-) \tag{2.53}$$

$$(1+V_\alpha)(1+U_\beta) = (1+U_{(i,k)})(1+U_\beta)(1+V_\alpha), i>k, (\alpha=(i,j) \in \Phi^+, \beta=(j,k) \in \Phi^-) \tag{2.54}$$

$$(1+V_\alpha)(1+U_\beta) = (1+V_{(k,j)})^{-p}(1+U_\beta)(1+V_\alpha), k<j, (\alpha=(i,j) \in \Phi^+, \beta=(k,i) \in \Phi^-) \tag{2.55}$$

$$(1+V_\alpha)(1+U_\beta) = (1+U_{(k,j)})^{-1}(1+U_\beta)(1+V_\alpha), k>j, (\alpha=(i,j) \in \Phi^+, \beta=(k,i) \in \Phi^-) \tag{2.56}$$

$$(1+V_\alpha)(1+U_{-\alpha}) = (1+U_{-\alpha})^{(1+p)^{-1}}(1+W_{(i,i+1)})\cdots(1+W_{(j-1,j)})(1+V_\alpha)^{(1+p)^{-1}}, (\alpha=(i,j) \in \Phi^+) \tag{2.57}$$

$$U_{\beta_1}U_{\beta_2} = U_{\beta_2}U_{\beta_1}, (\beta_1, \beta_2 \in \Phi^-, \beta_1+\beta_2 \notin \Phi) \tag{2.58}$$

$$(1+U_{\beta_1})(1+U_{\beta_2}) = (1+U_{(i,k)})^p(1+U_{\beta_2})(1+U_{\beta_1}), (\beta_1=(i,j), \beta_2=(j,k) \in \Phi^-) \tag{2.59}$$

$$(1+U_{\beta_1})(1+U_{\beta_2}) = (1+U_{(k,j)})^{-p}(1+U_{\beta_2})(1+U_{\beta_1}), (\beta_1=(i,j), \beta_2=(k,i) \in \Phi^-) \tag{2.60}$$

$$W_{\delta_1}W_{\delta_2} = W_{\delta_2}W_{\delta_1}, (\delta_1, \delta_2 \in \Pi, \delta_1 \neq \delta_2) \tag{2.61}$$

$$V_{\alpha_1}V_{\alpha_2} = V_{\alpha_2}V_{\alpha_1}, (\alpha_1, \alpha_2 \in \Phi^+, \alpha_1+\alpha_2 \notin \Phi) \tag{2.62}$$

$$(1+V_{\alpha_1})(1+V_{\alpha_2}) = (1+V_{(i,k)})(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1=(i,j), \alpha_2=(j,k) \in \Phi^+) \tag{2.63}$$

$$(1+V_{\alpha_2})(1+V_{\alpha_1}) = (1+V_{(k,j)})(1+V_{\alpha_1})(1+V_{\alpha_2}), (\alpha_1=(i,j), \alpha_2=(k,i) \in \Phi^+). \tag{2.64}$$

Proof. We use the Steinberg's relations in the group G and then translate them in $\mathcal{A}$ in order to deduce the relations in lemma 2.11. For example, recalling the notations $h_\delta(1+p)$ and $x_\beta(p)$ in section 2.2.2, Steinberg [Ste67] gives

$$h_\delta(1+p)x_\beta(p)h_\delta(1+p)^{-1} = x_\beta((1+p)^{\langle \beta, \delta \rangle}p), (\beta \in \Phi^-, \delta \in \Pi),$$

where $\langle \beta, \delta \rangle \in \mathbb{Z}$ (cf. p. 30 of [Ste67]). So the corresponding relation in the Iwasawa algebra is

$$(1+W_\delta)(1+U_\beta) = (1+U_\beta)^q(1+W_\delta), (\beta \in \Phi^-), \tag{2.65}$$

where $q = (1+p)^{\langle \beta, \delta \rangle}$. This is relation 2.50

By similar means we compute the other relations of lemma 2.11. One can find the computation in section 2.5. □

We consider $\mathcal{A}$ - the universal p-adic algebra of non-commutative power series in the variables V_α, W_δ, and U_β where α varies over the positive roots, δ varies over the simple roots and β varies over the negative roots. We denote $\mathcal{A} = \mathbb{Z}_p\{\{V_\alpha, W_\delta, U_\beta, \alpha \in \Phi^+, \delta \in \Pi, \beta \in \Phi^-\}\}$. Thus, it is composed of all non-commutative series

$$f = \textstyle\sum_{k \geqslant 0} \sum_i a_i x^i$$

where $a_i \in \mathbb{Z}_p$ and, for all $k \geqslant 0$, i runs over all maps $\{1,2,...,k\} \to \{1,2,...,d\}$, $(d = |\Phi| + |\Pi|)$; we set $x_1 = U_{(n,1)}, x_2 = U_{(n-1,1)}, x_3 = U_{(n,2)}, \ldots, x_{\frac{n(n-1)}{2}+1} = W_{(1,2)}, \ldots, x_{\frac{n^2+n-2}{2}} = W_{(n-1,n)}, x_{\frac{n^2+n}{2}} = V_{(n-1,n)}, \ldots, x_d = V_{(1,2)}$, i.e. x_i's (with i increasing) are assigned to the variables among $\{V_\alpha, W_\delta, U_\beta\}$ corresponding to the order as prescribed in Theorem 2.5. We set $x^i = x_{i(1)}x_{i(2)}\cdots x_{i(k)}$.

Let $\mathcal{R} \subset \mathcal{A}$ be the closed (two-sided) ideal generated by the relations (2.50-2.64) and $\overline{\mathcal{A}}$ be the reduction modulo p of $\mathcal{A}$. After lemma 1.16, we obtain

Corollary 2.12. *Let $\overline{\mathcal{R}}$ be the image of $\mathcal{R}$ in $\overline{\mathcal{A}}$. Then $\overline{\mathcal{R}}$ is the closed two-sided ideal in $\overline{\mathcal{A}}$ generated by the relations (2.50-2.64).*

2.4 Presentation of the Iwasawa algebra $\Lambda(G)$ for $p > n+1$

Our goal in this section is to give an explicit presentation of $\Lambda(G)$. The strategy of the proof is to show the corresponding statement for

$$\Omega_G := \Lambda_G \otimes_{\mathbb{Z}_p} \mathbb{F}_p,$$

which is the Iwasawa algebra with finite coefficients. We show in Theorem 2.4.2 that for $p > n+1$, the Iwasawa algebra Ω_G is naturally isomorphic to $\overline{\mathcal{A}}/\overline{\mathcal{R}}$. In section 2.4.1, we construct a continuous surjective map $\varphi : \mathcal{A} \to \Lambda(G)$. Thus, we get a natural continuous surjection $\mathcal{B} := \mathcal{A}/\mathcal{R} \to \Lambda(G)$. Therefore, by lemma 2.12, we obtain a surjection $\overline{\varphi} : \overline{\mathcal{B}} := \overline{\mathcal{A}}/\overline{\mathcal{R}} \to \Omega_G$. In section 2.4.2, using the natural grading on $\overline{\mathcal{B}}$, we show that $\dim \mathrm{gr}^m \overline{\mathcal{B}} \leqslant \dim_{\mathbb{F}_p} \mathrm{gr}^m \Omega_G$ (cf. Proposition 2.14). Finally, in section 2.4.3, we give the proof of an explicit presentation of $\Lambda(G)$ and Ω_G (cf. Theorems 2.4.2 and 2.4.3). Later in corollary 2.15 we extend our result to obtain an explicit presentation of the Iwasawa algebra for the pro-p Iwahori of $GL(n, \mathbb{Z}_p)$.

2.4.1 Iwasawa algebra with finite coefficients

We first construct a natural surjective, continuous map $\varphi : \mathcal{A} \to \Lambda(G)$.

The non-commutative polynomial algebra

$$A := \mathbb{Z}_p\{x_1, ..., x_d\}$$

is a dense subalgebra of $\mathcal{A}$.

Lemma 2.13. *Let us define a natural map $\varphi : A \to \Lambda(G)$ mapping $x_i \in A$ (with i increasing) to the corresponding variable among $\{V_\alpha, W_\delta, U_\beta\}$ in the Iwasawa algebra $\Lambda(G)$, according to the order as prescribed in Theorem 2.5. Then, this map extends continuously to a surjective homomorphism $\mathcal{A} \to \Lambda(G)$.*

Proof. It suffices to show that if a sequence in $\mathcal{A}$ converges to 0 in the topology of $\mathcal{A}$, the image converges to 0 in $\Lambda(G)$.
The topology of $\mathcal{A}$ is given by the valuation $v_{\mathcal{A}}$; we write

$$F = \sum a_i x^i$$
$$v_{\mathcal{A}}(F) = \inf_i (val_p(a_i) + |i|).$$

Lazard (cf. 2.3, chap.3 of [Laz65]) shows that ω is an additive valuation, $\omega(\eta\nu) = \omega(\nu) + \omega(\eta)$ for $\nu, \eta \in \Lambda(G)$. For $F \in \mathcal{A}$, with image $\mu \in \Lambda(G)$, we have

$$\begin{aligned}
\omega(\mu) = \omega(\sum a_i x^i) & \\
&\geqslant \inf_i \{val_p(a_i) + \sum_{i=1}^{d} m_i \omega(g_i)\} \text{ (for some } m_i \in \mathbb{N}) \\
&\geqslant \frac{1}{n} v_{\mathcal{A}}(F).
\end{aligned}$$

The third inequality follows because
$\omega(W_{(i',i'+1)}) = 1 > \frac{1}{n}$, $\omega(U_{(i,j)}) = \frac{n-i+j}{n} \geqslant \frac{1}{n}$ and $\omega(V_{(i'',j'')}) = \frac{j''-i''}{n} \geqslant \frac{1}{n}$, where $(i,j) \in \Phi^-, i' = 1, ..., n-1, (i'', j'') \in \Phi^+$.

Hence, the map $\varphi : \mathcal{A} \to \Lambda(G)$ is continuous.

The surjectivity follows from the fact that φ is already surjective if $\mathcal{A}$ is replaced by the set of linear combinations of well-ordered monomials (i increasing).

□

The Iwasawa algebra $\Lambda(G)$ is filtered by $\frac{1}{n}\mathbb{N}$. The filtration of $\Lambda(G)$ defines a filtration on $\Omega_G := \Lambda_G \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ given by $F^v\Omega_G = F^v\Lambda_G \otimes \mathbb{F}_p$. Reduction modulo p gives is a natural map $\overline{\mathcal{A}} \to \Omega_G$ whose kernel contains $\overline{\mathcal{R}}$.

As an $\mathbb{F}_p$-vector space, $\mathrm{gr}^v\Lambda_G$ is generated by the independent elements

$$p^d \prod_{(i,j)\in\Phi^-} U_{(i,j)}^{p_{ij}} \prod_{i'=1}^{n-1} W_{(i',i'+1)}^{m_{i',i'+1}} \prod_{(i'',j'')\in\Phi^+} V_{(i'',j'')}^{n_{i'',j''}} \text{ such that}$$
$$d + \sum_{(i,j)\in\Phi^-} [\tfrac{j-i}{n} + 1]p_{ij} + \sum_{i'=1}^{n-1} m_{i',i'+1} + \sum_{(i'',j'')\in\Phi^+} (\tfrac{j''-i''}{n}) n_{i'',j''} = v.$$

(Cf. p.199 of [Sch11]). Then $\mathrm{gr}^v\Omega_G$ is generated by the elements

$$\prod_{(i,j)\in\Phi^-} U_{(i,j)}^{p_{ij}} \prod_{i'=1}^{n-1} W_{(i',i'+1)}^{m_{i',i'+1}} \prod_{(i'',j'')\in\Phi^+} V_{(i'',j'')}^{n_{i'',j''}} \text{ such that}$$
$$\sum_{(i,j)\in\Phi^-} [\tfrac{j-i}{n} + 1]p_{ij} + \sum_{i'=1}^{n-1} m_{i',i'+1} + \sum_{(i'',j'')\in\Phi^+} (\tfrac{j''-i''}{n}) n_{i'',j''} = v,$$

and these elements are linearly independent. We do not change the filtration replacing $v \in \frac{1}{n}\mathbb{N}$ by $m = nv \in \mathbb{N}$, the valuations of the variables $(U_{(i,j)}, W_{(i',i'+1)}, V_{(i'',j'')})$ being now $(n-i+j, n, j''-i'')$ where $(i,j) \in \Phi^-, i' = 1, ..., n-1, (i'', j'') \in \Phi^+$.

In particular we have for $m \in \mathbb{N}$:

Theorem 2.4.1. *(Lazard) The dimension d_m of $gr^m\Omega_G$ over $\mathbb{F}_p$ is equal to the dimension of the space of homogeneous symmetric polynomials of degree m in the variables $\{U_{(i,j)}, W_{(i',i'+1)}, V_{(i'',j'')}\}$ having degrees corresponding to their valuations $(n - i + j, n, j'' - i'')$ where $(i,j) \in \Phi^-, i' \in [1, n-1], (i'', j'') \in \Phi^+$.*

We must now consider on $\overline{\mathcal{A}}$, the filtration of $\overline{\mathcal{A}}$ obtained by assigning the degrees $(n-i+j, n, j''-i'')$ to the formal variables $(U_{(i,j)}, W_{(i',i'+1)}, V_{(i'',j'')})$. Then $\mathrm{gr}^m\overline{\mathcal{A}}$ is isomorphic to the space of non-commutative polynomials of degree m. We endow $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$ with the induced filtration, so

$$\mathrm{gr}^m\overline{\mathcal{B}} = Fil^m\overline{\mathcal{A}}/(Fil^{m+1}\overline{\mathcal{A}} + Fil^m\overline{\mathcal{A}} \cap \overline{\mathcal{R}}).$$

By construction the map $\mathrm{gr}^m\overline{\mathcal{B}} \to \mathrm{gr}^m\Omega_G$ is surjective.

2.4.2 Bound on the dimension of the graded pieces of $\mathcal{B}$

The following proposition gives an upper bound for $\dim \mathrm{gr}^m\overline{\mathcal{B}}$ generalizing the case for the pro-p Iwahori of $SL(2, \mathbb{Z}_p)$ by Clozel ([Clo17, lemma 2.11]).

Proposition 2.14. *For $m \geqslant 0$, we have $\dim\, gr^m\overline{\mathcal{B}} \leqslant d_m = \dim_{\mathbb{F}_p} gr^m\Omega_G$.*

Proof. The Lemma is true for $m = 0$. For $m = 1$, $\mathrm{gr}^1\overline{\mathcal{B}}$ is a quotient of the space $Fil^1\overline{\mathcal{A}}/Fil^2\overline{\mathcal{A}}$ with basis $U_{(n,1)}$ and $V_{(i_1,i_1+1)}$ for $i_1 = 1, 2, ..., n-1$. So, $\dim \mathrm{gr}^1\overline{\mathcal{B}} \leqslant n = d_1$.

To show the general case we will consider each relation and then apply induction argument to show that we decrease the number of inversions.

First consider relation 2.50

$$(1 + W_\delta)(1 + U_\beta) = (1 + U_\beta)^q(1 + W_\delta), (\delta \in \Pi, \beta \in \Phi^-),$$

where $q = (1+p)^{\langle\beta,\delta\rangle} \equiv 1[p]$. We have

$$(1 + U_\beta)^q = 1 + qU_\beta + \tfrac{q(q-1)}{2}U_\beta^2 + \cdots$$

where $\frac{q(q-1)}{2} \equiv 0[p]$. By the Lazard condition $p > n + 1$, we can show that

$$(1 + W_\delta)(1 + U_\beta) = (1 + U_\beta)(1 + W_\delta)(\text{ mod } Fil^{n+s+1}),$$

where $s =$ degree of U_β. This is because, for any natural number $m \geq 2$, U_β^m has degree ms. So, we need to show that

$$ms \leq n + s \text{ implies } \tbinom{q}{m} \equiv 0 \pmod{p},$$

i.e. $$(m-1)s \leq n \text{ implies } \binom{q}{m} \equiv 0 \pmod{p}.$$

Now, $(m-1) \leq (m-1)s$. Therefore, it suffices to show that

$$m-1 \leq n \implies \binom{q}{m} \equiv 0 \pmod{p}. \tag{2.66}$$

But by the Lazard condition we get $m-1 \leq n < p-1$. So, $m < p$ and then trivially $val_p(m!) = 0$. Hence, $\binom{q}{m} \equiv 0 \pmod{p}$which gives

$$W_\delta U_\beta = U_\beta W_\delta \text{ in } Fil^{n+s+1}, (\delta \in \Pi, \beta \in \Phi^-).$$

Consider a non-commutative monomial

$$x^i = x_{i_1} x_{i_2} \cdots x_{i_w}.$$

To avoid confusion we will write x^i as x^{i^*} because we will be using i, j, k for the roots. Assume the homogeneous degree of x^{i^*} is equal to t. We can change x^{i^*} into a well-ordered monomial ($b \to i_b$ increasing) by a sequence of transpositions (Lemma 3.2 of [Clo11]). Consider a move $(b, b+1) \to (b+1, b)$ and assume $i_b > i_{b+1}$. We write

$$x^{i^*} = x^f x_b x_{b+1} x^e$$

where $\deg(f) = r^{'}$, $\deg(e) = s^{'}$, $\deg(i^*) = t$. Henceforth, we fix the notations $r^{'}, s^{'}, t$ to be the degrees of f, e, i^* respectively. If

$$(x_b, x_{b+1}) = (W_\delta, U_\beta),$$

then $x^f U_\beta W_\delta x^e \equiv x^{i^*} \pmod{Fil^{t+1}}$, $t = r^{'} + n + s + s^{'}$. This reduces the number of inversions in x^{i^*}.

We do the same argument for the other relations (2.51-2.64), i.e. we consider each of the relations and show that we reduce the number of inversions in each case. The computations can be found in section 2.6. This completes the proof Proposition 2.14, because note that, inside $gr^m\overline{\mathcal{B}}$, we can arrange the variables in the wrong order by a sequence of transposition to put them in the right order (the right order as in the algebra $\mathcal{A}$). This shows that dim $gr^m\overline{\mathcal{B}} \leq$ dim $gr^m\Omega_G$ since, by theorem 2.4.1, $\mathrm{gr}^m\Omega_G$ contains homogeneous *symmetric* polynomials.

□

2.4.3 Explicit presentations of the Iwasawa algebras $\Lambda(G)$ and Ω_G

In this section we give our main theorem constructing an explicit presentation of the Iwasawa algebras $\Lambda(G)$ and Ω_G. In corollary 2.15, we extend our result to include the case of the pro-p Iwahori of $GL(n, \mathbb{Z}_p)$.

Theorem 2.4.2. *The map $\overline{\mathcal{A}} \to \Omega_G$ gives an isomorphism $\overline{\mathcal{B}} := \overline{\mathcal{A}}/\overline{\mathcal{R}} \cong \Omega_G$.*

Proof. (Cf. [Clo11] and [Clo17]). The natural map $\varphi : \mathcal{A} \to \Lambda(G)$ respects the filtration and reduces modulo p to $\overline{\varphi} : \overline{\mathcal{B}} \to \Omega_G$. As $\overline{\varphi}$ is surjective, the natural map of graded algebras

$$\mathrm{gr}\overline{\varphi} : \mathrm{gr}^\bullet\overline{\mathcal{B}} \to \mathrm{gr}^\bullet\Omega_G$$

is surjective. Moreover, it is an isomorphism because dim $\mathrm{gr}^m\overline{\mathcal{B}} \leqslant$ dim $\mathrm{gr}^m\Omega_G$ (proposition 2.14). Since the filtration on $\overline{\mathcal{B}}$ is complete, we deduce that $\overline{\varphi}$ is an isomorphism (cf. Theorem 4 (5), p.31 of [LO96]). We have $\overline{\mathcal{B}}$ complete because $\overline{\mathcal{B}} = \overline{\mathcal{A}}/\overline{\mathcal{R}}$, where $\overline{\mathcal{R}}$ is closed and therefore complete for the filtration induced from that of $\overline{\mathcal{A}}$. □

Theorem 2.4.3. *The map $\mathcal{A} \to \Lambda(G)$ gives, by passing to the quotient, an isomorphism $\mathcal{B} = \mathcal{A}/\mathcal{R} \cong \Lambda(G)$.*

Proof. We need the argument of [Clo11]. The reduction of φ is $\overline{\varphi}$. We recall that $\overline{\mathcal{R}}$ is the image of $\mathcal{R}$ in $\overline{\mathcal{A}}$. Let $f \in \mathcal{A}$ satisfies $\varphi(f) = 0$. We then have $\overline{f} \in \overline{\mathcal{R}}$ since $\overline{\mathcal{A}}/\overline{\mathcal{R}} \cong \Omega_G$. So $f = r_1 + pf_1, r_1 \in \mathcal{R}, f_1 \in \mathcal{A}$. Then $\varphi(f_1) = 0$. Inductively, we obtain an expression $f = r_n + p^n f_n$ of the same type. Since $p^n f_n \to 0$ in $\mathcal{A}$ and $\mathcal{R}$ is closed, we deduce that $f \in \mathcal{R}$. □

This gives us the following corollary:

Corollary 2.15. *The Iwasawa algebra of the pro-p Iwahori subgroup of $GL_n(\mathbb{Z}_p)$ is a quotient $\mathcal{A}'/\mathcal{R}$, with $\mathcal{A}' = \mathbb{Z}_p\{\{Z, V_\alpha, U_\beta, W_\delta, \alpha \in \Phi^+, \beta \in \Phi^-, \delta \in \Pi\}\}$ and $\mathcal{R}$ is defined by the relations $(2.50 - 2.64)$ and*
(Comm) Z commutes with $U_\beta, V_\alpha, W_\delta$ for all α, β, δ.

Here the variable Z corresponds to the element $(1+p)I_n \in GL_n(\mathbb{Z}_p)$.

In conclusion, for $p > n+1$, we have found a Lazard basis of G with respect to its p-valuation ω (see theorem 2.5). Furthermore, we have obtained the relations inside the Iwasawa algebra of G, thus giving us an explicit presentation of $\Lambda(G)$ (see theorem 2.4.3) by controlling the dimension of $\mathrm{gr}^m\overline{\mathcal{B}}$ (Proposition 2.14). This readily gives the presentation of the Iwasawa algebra of the pro-p Iwahori subgroup of $GL_n(\mathbb{Z}_p)$ (corollary 2.15).

2.5 Computations for the proof of Lemma 2.11

In this section we complete the computations needed for Lemma 2.11. We quote lemma 2.11.

***Lemma* 2.11** *In the Iwasawa algebra $\Lambda(G)$, the variables $V_\alpha, W_\delta, U_\beta$ satisfy the following relations.*

$$
\begin{aligned}
(1+W_\delta)(1+U_\beta) &= (1+U_\beta)^q(1+W_\delta), (\beta \in \Phi^-), q = (1+p)^{\langle \beta, \delta \rangle} \\
(1+W_\delta)(1+V_\alpha) &= (1+V_\alpha)^{q'}(1+W_\delta), (\alpha \in \Phi^+), q' = (1+p)^{\langle \alpha, \delta \rangle} \\
V_\alpha U_\beta &= U_\beta V_\alpha, (\alpha \in \Phi^+, \beta \in \Phi^-, \alpha \neq -\beta, \alpha+\beta \notin \Phi) \\
(1+V_\alpha)(1+U_\beta) &= (1+V_{(i,k)})^p(1+U_\beta)(1+V_\alpha), i<k, (\alpha=(i,j) \in \Phi^+, \beta=(j,k) \in \Phi^-) \\
(1+V_\alpha)(1+U_\beta) &= (1+U_{(i,k)})(1+U_\beta)(1+V_\alpha), i>k, (\alpha=(i,j) \in \Phi^+, \beta=(j,k) \in \Phi^-) \\
(1+V_\alpha)(1+U_\beta) &= (1+V_{(k,j)})^{-p}(1+U_\beta)(1+V_\alpha), k<j, (\alpha=(i,j) \in \Phi^+, \beta=(k,i) \in \Phi^-) \\
(1+V_\alpha)(1+U_\beta) &= (1+U_{(k,j)})^{-1}(1+U_\beta)(1+V_\alpha), k>j, (\alpha=(i,j) \in \Phi^+, \beta=(k,i) \in \Phi^-) \\
(1+V_\alpha)(1+U_{-\alpha}) &= (1+U_{-\alpha})^{(1+p)^{-1}}(1+W_{(i,i+1)})\cdots(1+W_{(j-1,j)})(1+V_\alpha)^{(1+p)^{-1}}, (\alpha=(i,j) \in \Phi^+) \\
U_{\beta_1}U_{\beta_2} &= U_{\beta_2}U_{\beta_1}, (\beta_1, \beta_2 \in \Phi^-, \beta_1+\beta_2 \notin \Phi) \\
(1+U_{\beta_1})(1+U_{\beta_2}) &= (1+U_{(i,k)})^p(1+U_{\beta_2})(1+U_{\beta_1}), (\beta_1=(i,j), \beta_2=(j,k) \in \Phi^-) \\
(1+U_{\beta_1})(1+U_{\beta_2}) &= (1+U_{(k,j)})^{-p}(1+U_{\beta_2})(1+U_{\beta_1}), (\beta_1=(i,j), \beta_2=(k,i) \in \Phi^-) \\
W_{\delta_1}W_{\delta_2} &= W_{\delta_2}W_{\delta_1}, (\delta_1, \delta_2 \in \Pi, \delta_1 \neq \delta_2) \\
V_{\alpha_1}V_{\alpha_2} &= V_{\alpha_2}V_{\alpha_1}, (\alpha_1, \alpha_2 \in \Phi^+, \alpha_1+\alpha_2 \notin \Phi) \\
(1+V_{\alpha_1})(1+V_{\alpha_2}) &= (1+V_{(i,k)})(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1=(i,j), \alpha_2=(j,k) \in \Phi^+) \\
(1+V_{\alpha_2})(1+V_{\alpha_1}) &= (1+V_{(k,j)})(1+V_{\alpha_1})(1+V_{\alpha_2}), (\alpha_1=(i,j), \alpha_2=(k,i) \in \Phi^+).
\end{aligned}
$$

Proof. Recalling the notations $h_\delta(1+p)$ and $x_\beta(p)$ in section 2.2.2, Steinberg [Ste67] gives

$$h_\delta(1+p)x_\beta(p)h_\delta(1+p)^{-1} = x_\beta((1+p)^{\langle \beta, \delta \rangle}p), \ (\beta \in \Phi^-, \delta \in \Pi),$$

where $\langle \beta, \delta \rangle \in \mathbb{Z}$ (cf. p. 30 of [Ste67]). So the corresponding relation in the Iwasawa algebra is

$$(1+W_\delta)(1+U_\beta) = (1+U_\beta)^q(1+W_\delta), (\beta \in \Phi^-), \tag{2.67}$$

where $q = (1+p)^{\langle \beta, \delta \rangle}$.

We also have

$$h_\delta(1+p)x_\alpha(1)h_\delta(1+p)^{-1} = x_\alpha((1+p)^{\langle \alpha, \delta \rangle}), (\alpha \in \Phi^+).$$

So the corresponding relation in the Iwasawa algebra is

$$(1+W_\delta)(1+V_\alpha) = (1+V_\alpha)^{q'}(1+W_\delta), (\alpha \in \Phi^+), \tag{2.68}$$

where $q' = (1+p)^{\langle \alpha, \delta \rangle}$.

If $\alpha \neq -\beta$ and $\alpha+\beta \notin \Phi$, then by example (a), p.24 of [Ste67] we have

$$x_\alpha(1)x_\beta(p) = x_\beta(p)x_\alpha(1), (\alpha \in \Phi^+, \beta \in \Phi^-).$$

So in this case, we have the following relation in the Iwasawa algebra:

$$V_\alpha U_\beta = U_\beta V_\alpha, (\alpha \in \Phi^+, \beta \in \Phi^-). \tag{2.69}$$

If on the contrary, $\alpha \neq -\beta$ and $\alpha+\beta \in \Phi$, then we have two subcases:

Subcase 1. $\alpha=(i,j), \beta=(j,k)$ then we have by direct computation (writing $x_{(i,j)}(1) = 1+E_{i,j}$)

$$
\begin{aligned}
x_\alpha(1)x_\beta(p) &= [x_\alpha(1), x_\beta(p)]x_\beta(p)x_\alpha(1). \\
x_\alpha(1)x_\beta(p) &= x_{(i,k)}(p)x_\beta(p)x_\alpha(1), ((i,k) = \alpha+\beta).
\end{aligned}
$$

Now, in the Iwasawa algebra, $x_{(i,k)}(p)$ corresponds to $(1+V_{(i,k)})$ if $i<k$ and to $(1+U_{(i,k)})$ if $i>k$.

Thus, we get the following two relations in the Iwasawa algebra:

$$(1+V_\alpha)(1+U_\beta)=(1+V_{(i,k)})^p(1+U_\beta)(1+V_\alpha), i<k, (\alpha\in\Phi^+,\beta\in\Phi^-), \tag{2.70}$$

$$(1+V_\alpha)(1+U_\beta)=(1+U_{(i,k)})(1+U_\beta)(1+V_\alpha), i>k, (\alpha\in\Phi^+,\beta\in\Phi^-), \tag{2.71}$$

where $(i,k)=\alpha+\beta=(i,j)+(j,k)$.

Subcase 2. $\alpha=(i,j),\beta=(k,i)$, then we have

$$x_\alpha(1)x_\beta(p)=[x_\alpha(1),x_\beta(p)]x_\beta(p)x_\alpha(1),$$
$$x_\alpha(1)x_\beta(p)=x_{(k,j)}(-p)x_\beta(p)x_\alpha(1),(\alpha+\beta=(k,j)).$$

So, as before, we get the following two relations in the Iwasawa algebra:

$$(1+V_\alpha)(1+U_\beta)=(1+V_{(k,j)})^{-p}(1+U_\beta)(1+V_\alpha), k<j, (\alpha\in\Phi^+,\beta\in\Phi^-), \tag{2.72}$$

$$(1+V_\alpha)(1+U_\beta)=(1+U_{(k,j)})^{-1}(1+U_\beta)(1+V_\alpha), k>j, (\alpha\in\Phi^+,\beta\in\Phi^-), \tag{2.73}$$

where $(k,j)=\beta+\alpha=(k,i)+(i,j)$.

If we have $\alpha=-\beta$, let $\alpha=(i,j)[i<j]$, then just by computation one can show that

$$x_\alpha(1)x_\beta(p)=x_\beta(p(1+p)^{-1})Hx_\alpha((1+p)^{-1}),$$

where H is the diagonal matrix with $(1+p)$ in the $(i,i)^{th}$ place and $(1+p)^{-1}$ in the $(j,j)^{th}$ place and 1 in the other diagonal positions. The above relation, in $SL_2(\mathbb{Z}_p)$, can be realized by the following matrix equation:

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\p&1\end{pmatrix}=\begin{pmatrix}1&0\\p(1+p)^{-1}&1\end{pmatrix}\begin{pmatrix}(1+p)&0\\0&(1+p)^{-1}\end{pmatrix}\begin{pmatrix}1&(1+p)^{-1}\\0&1\end{pmatrix}.$$

So we obtain

$$x_\alpha(1)x_\beta(p)=x_\beta(p(1+p)^{-1})h_{(i,i+1)}(1+p)\cdots h_{(j-1,j)}(1+p)x_\alpha((1+p)^{-1}).$$

Hence, the corresponding relation in the Iwasawa algebra is

$$(1+V_\alpha)(1+U_{-\alpha})=(1+U_{-\alpha})^{(1+p)^{-1}}(1+W_{(i,i+1)})\cdots(1+W_{(j-1,j)})(1+V_\alpha)^{(1+p)^{-1}},(\alpha\in\Phi^+). \tag{2.74}$$

In the following, we give relations among the variables corresponding to the lower unipotent subgroup.

Let $\beta_1,\beta_2\in\Phi^-,\beta_1+\beta_2\notin\Phi$, then $x_{\beta_1}(p)x_{\beta_2}(p)=x_{\beta_2}(p)x_{\beta_1}(p)$. So the corresponding relation in the Iwasawa algebra is

$$U_{\beta_1}U_{\beta_2}=U_{\beta_2}U_{\beta_1},(\beta_1,\beta_2\in\Phi^-). \tag{2.75}$$

On the other hand, if $\beta_1+\beta_2\in\Phi$, then we have the following two cases, computations of which actually take place in $GL(3)$:

Case 1. Let $\beta_1=(i,j),\beta_2=(j,k)[i>j>k]$. Then,

$$x_{\beta_1}(p)x_{\beta_2}(p)=x_{(i,k)}(p^2)x_{\beta_2}(p)x_{\beta_1}(p),(\beta_1+\beta_2=(i,k)).$$

The corresponding relation in the Iwasawa algebra is

$$(1+U_{\beta_1})(1+U_{\beta_2})=(1+U_{(i,k)})^p(1+U_{\beta_2})(1+U_{\beta_1}),(\beta_1,\beta_2\in\Phi^-,(i,k)=\beta_1+\beta_2), \tag{2.76}$$

since $x_{(i,k)}(p)$ corresponds to $(1+U_{(i,k)})$.

Case 2. Let $\beta_1=(i,j),\beta_2=(k,i),[k>i>j]$. We have

$$x_{\beta_1}(p)x_{\beta_2}(p)=x_{(k,j)}(-p^2)x_{\beta_2}(p)x_{\beta_1}(p),(\beta_1+\beta_2=(k,j)).$$

The corresponding relation in the Iwasawa algebra is

$$(1+U_{\beta_1})(1+U_{\beta_2}) = (1+U_{(k,j)})^{-p}(1+U_{\beta_2})(1+U_{\beta_1}), (\beta_1, \beta_2 \in \Phi^-, (k,j) = \beta_1 + \beta_2). \quad (2.77)$$

As the diagonal elements commute, we have for $\delta_1, \delta_2 \in \Pi, \delta_1 \neq \delta_2$,

$$W_{\delta_1} W_{\delta_2} = W_{\delta_2} W_{\delta_1}, (\delta_1, \delta_2 \in \Pi). \quad (2.78)$$

Now, we give the relations among the variables corresponding to the upper unipotent subgroup of G.

If $\alpha_1, \alpha_2 \in \Phi^+, \alpha_1 + \alpha_2 \notin \Phi$, then $x_{\alpha_1}(1)x_{\alpha_2}(1) = x_{\alpha_2}(1)x_{\alpha_1}(1)$. So the corresponding relation in the Iwasawa algebra is

$$V_{\alpha_1} V_{\alpha_2} = V_{\alpha_2} V_{\alpha_1}, (\alpha_1, \alpha_2 \in \Phi^+). \quad (2.79)$$

On the other hand, if $\alpha_1 + \alpha_2 \in \Phi$, then we have the following two subparts:

Subpart 1. Let $\alpha_1 = (i,j), \alpha_2 = (j,k)[i < j < k]$. Then,

$$x_{\alpha_1}(1)x_{\alpha_2}(1) = x_{(i,k)}(1)x_{\alpha_2}(1)x_{\alpha_1}(1), (\alpha_1 + \alpha_2 = (i,k)).$$

The corresponding relation in the Iwasawa algebra is

$$(1+V_{\alpha_1})(1+V_{\alpha_2}) = (1+V_{(i,k)})(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1, \alpha_2 \in \Phi^+, \alpha_1 + \alpha_2 = (i,k)). \quad (2.80)$$

Subpart 2. Let $\alpha_1 = (i,j), \alpha_2 = (k,i), [k < i < j]$. We have the relation

$$x_{\alpha_1}(1)x_{\alpha_2}(1) = x_{(k,j)}(-1)x_{\alpha_2}(1)x_{\alpha_1}(1), (\alpha_1 + \alpha_2 = (k,j)).$$

The corresponding relation in the Iwasawa algebra is

$$(1+V_{\alpha_1})(1+V_{\alpha_2}) = (1+V_{(k,j)})^{-1}(1+V_{\alpha_2})(1+V_{\alpha_1}).$$

which is the same as

$$(1+V_{\alpha_2})(1+V_{\alpha_1}) = (1+V_{(k,j)})(1+V_{\alpha_1})(1+V_{\alpha_2}), (\alpha_1, \alpha_2 \in \Phi^+, \alpha_1 + \alpha_2 = (k,j)). \quad (2.81)$$

2.6 Computations for the proof of Proposition 2.14

In this section we give the computations necessary to prove proposition 2.14. We quote proposition 2.14.

Proposition 2.14 *For $m \geqslant 0$, we have* $\dim\, gr^m\overline{\mathcal{B}} \leqslant d_m = \dim_{\mathbb{F}_p} \mathrm{gr}^m\Omega_G$.

Proof We provide the remaining computations for the proof as indicated in the last paragraph of section 2.4.2. There we have already explained the strategy of the proof and dealt with relation 2.50. Consider relation 2.51. The argument of this exactly follows the case of relation 2.50 already treated, for which we have shown that we can reduce the number of inversions and so we omit it. Relation 2.52 is also obvious to deal with, hence we consider 2.53. It reduces to

$$V_\alpha U_\beta = U_\beta V_\alpha \ (\mathrm{mod}\ Fil^{r+s+1}), (\alpha \in \Phi^+, \beta \in \Phi^-),$$

where $r = \deg\,(V_\alpha)$ and $s = \deg\,(U_\beta)$.

In this case, we have $\alpha = (i,j),\ \beta = (j,k),\ r = j-i,\ s = n-j+k$ and $k-i = \deg(V_{(i,k)=\alpha+\beta})$. So, we need to show that

$$(1+V_{(i,k)})^p \equiv 1 (\mathrm{mod}\ Fil^{n-i+k+1}).$$

That is, for any natural number $m \geq 2$, we have to show that

$$(k-i)m \leq n-i+k \implies \tbinom{p}{m} \equiv 0 \ (\mathrm{mod}\ p),$$

i.e. we have to show that

$$(k-i)(m-1) \leq n \implies \tbinom{p}{m} \equiv 0 \ (\mathrm{mod}\ p).$$

But since $k > i$ (see relation 2.53), we only have to show that

$$(m-1) \leq n \implies \tbinom{p}{m} \equiv 0 \ (\mathrm{mod}\ p),$$

which we checked in 2.66.

So, if $(x_b, x_{b+1}) = (V_\alpha, U_\beta)$, then $x^{i^*} \equiv x^f U_\beta V_\alpha x^e (Fil^{t+1})$, $t = r' + s' + r + s$.

Consider relation 2.54. It is

$$(1+V_\alpha)(1+U_\beta) = (1+U_{(i,k)})(1+U_\beta)(1+V_\alpha), i > k, (\alpha \in \Phi^+, \beta \in \Phi^-, (i,k) = \alpha+\beta)$$

where $\alpha = (i,j), \beta = (j,k), j > i > k$.

Now, $\deg(V_{(i,j)}) = j-i$, $\deg(U_{(j,k)}) = n-j+k$, $\deg(V_\alpha U_\beta) = n+k-i = \deg(U_{(i,k)})$. Therefore, $\deg(U_{(i,k)}V_\alpha)$ and $\deg(U_{(i,k)}U_\beta)$ are greater than $\deg(V_\alpha U_\beta)$. This gives

$$V_\alpha U_\beta = U_{(i,k)} + U_\beta V_\alpha (Fil^{r+s+1}),$$

where $r = \deg(V_\alpha)$, $s = \deg(U_\beta)$. If

$$(x_b, x_{b+1}) = (V_\alpha, U_\beta),$$

then after replacing $V_\alpha U_\beta$ by $U_\beta V_\alpha + U_{(i,k)}$, we have to show that we reduce the number of inversions. For any set S, let $|S|$ denote its cardinality. In the following, the notation $|_{i_\zeta > i\mu}^{\zeta<\mu,}|$ will denote $\sum\limits_{\substack{\zeta<\mu \\ i_\zeta > i\mu}} 1$. Similarly, $2|_{i_\zeta > i\mu}^{\zeta<\mu,}| := \sum\limits_{\substack{\zeta<\mu \\ i_\zeta > i\mu}} 2$. The number of inversions in x^{i^*} was originally as follows, where ζ, μ denotes indices $\neq b, b+1$ in the product x^{i^*}:

$$inv = \\ |_{i_\zeta > i\mu}^{\zeta<\mu,}| + |_{i_\mu \in [index(U_\beta), index(V_\alpha)|}^{\mu>b+1,}| + 2|_{i_\mu < index(U_\beta)}^{\mu>b+1,}| + |_{i_\zeta \in]index(U_\beta), index(V_\alpha)]}^{\zeta<b,}| + 2|_{i_\zeta > index(V_\alpha)}^{\zeta<b,}| \quad + 1.$$

Here, the cardinality symbols have natural meanings as explained above in the case for $|^{\zeta<\mu,}_{i_\zeta>i\mu}|$. For example, the term $2|^{\mu>b+1,}_{i_\mu<index(U_\beta)}|$ is by definition $\sum_{\substack{\mu>b+1,\\ i_\mu<index(U_\beta)}} 2$. The notation $]index(U_\beta), index(V_\alpha)]$ denotes the half open interval and by $index(U_-)$ we mean that if U_- corresponds to x_c for some $c \in 1, ..., d$ (variable in $\mathcal{A}$, cf. first paragraph of section 2.2), then $index(U_-) = c$. Thus, $index(U_\beta) < index(V_\alpha)$. Now, $V_\alpha U_\beta \to U_\beta V_\alpha$ clearly decreases the number of inversions and after changing $V_\alpha U_\beta$ into $U_{(i,k)}$, we have

$$inv' = |^{\zeta<\mu,}_{i_\zeta>i\mu}| + |^{\mu>b+1,}_{i_\mu<index(U_{(i,k)})}| + |^{\zeta<b,}_{i_\zeta>index(U_{(i,k)})}|.$$

As $index(U_{(i,k)}) < index(V_\alpha)$, we have

$$\begin{aligned}|^{\mu>b+1,}_{i_\mu<index(U_{(i,k)})}| \leq |^{\mu>b+1,}_{i_\mu<index(V_\alpha)}| &= |^{\mu>b+1,}_{i_\mu\in[index(U_\beta),index(V_\alpha)[}| + |^{\mu>b+1,}_{i_\mu<index(U_\beta)}| \\ &\leq |^{\mu>b+1,}_{i_\mu\in[index(U_\beta),index(V_\alpha)[}| + 2|^{\mu>b+1,}_{i_\mu<index(U_\beta)}|.\end{aligned}$$

Also, $index(U_\beta) = index(U_{(j,k)}) < indexU_{(i,k)}$ because $j > i$ and our chosen order of the Lazard's basis for G. Therefore,

$$\begin{aligned}|^{\zeta<b,}_{i_\zeta>index(U_{(i,k)})}| \leq |^{\zeta<b,}_{i_\zeta>index(U_\beta)}| &= |^{\zeta<b,}_{i_\zeta\in]index(U_\beta),index(V_\alpha)]}| + |^{\zeta<b,}_{i_\zeta>index(V_\alpha)}| \\ &\leq |^{\zeta<b,}_{i_\zeta\in]index(U_\beta),index(V_\alpha)]}| + 2|^{\zeta<b,}_{i_\zeta>index(V_\alpha)}|.\end{aligned}$$

Hence, $inv' < inv$.

Now, we consider the relation 2.55. With similar argument as in the case while dealing with the relation 2.53, using the condition $p > n + 1$, it will reduce to

$$U_\beta V_\alpha = V_\alpha U_\beta (Fil^{r+s+1}), (\alpha \in \Phi^+, \beta \in \Phi^-),$$

where $r = \deg(U_\beta)$ and $s = \deg(V_\alpha)$. So, $V_\alpha U_\beta \to U_\beta V_\alpha$ will obviously reduce the number of inversions.

Let us consider relation 2.56 which is

$$(1 + U_\beta)(1 + V_\alpha) = (1 + U_{(k,j)})(1 + V_\alpha)(1 + U_\beta), k > j, (k, j) = \beta + \alpha,$$

where $\alpha = (i, j), \beta = (k, i), i < j < k$. Expanding, we obtain

$$V_\alpha U_\beta = U_\beta V_\alpha - U_{(k,j)} - U_{(k,j)} V_\alpha - U_{(k,j)} U_\beta (Fil^{r+s+1}),$$

where $r = \deg(U_\beta)$ and $s = \deg(V_\alpha)$. Now, $\deg(V_\alpha U_\beta) = j - i + n - k + i = n + j - k = \deg(U_{(k,j)})$. So, $\deg(U_{(k,j)} V_\alpha)$ and $\deg(U_{(k,j)} U_\beta)$ are greater than $\deg(V_\alpha U_\beta)$. Thus,

$$V_\alpha U_\beta = -U_{(k,j)} + U_\beta V_\alpha (Fil^{r+s+1}).$$

Let $(x_b, x_{b+1}) = (V_\alpha, U_\beta)$. The number of inversions in x^{i^*} was originally as follows, where ζ, μ denotes indices $\neq b, b + 1$ in the product x^{i^*}:

$$\begin{aligned}&inv = \\ &|^{\zeta<\mu,}_{i_\zeta>i\mu}| + |^{\mu>b+1,}_{i_\mu\in[index(U_\beta),index(V_\alpha)[}| + 2|^{\mu>b+1,}_{i_\mu<index(U_\beta)}| + |^{\zeta<b,}_{i_\zeta\in]index(U_\beta),index(V_\alpha)]}| + 2|^{\zeta<b,}_{i_\zeta>index(V_\alpha)}| \quad + 1.\end{aligned}$$

As $index(U_\beta) < index(V_\alpha)$, the transition $V_\alpha U_\beta \to U_\beta V_\alpha$ clearly reduces the number of inversions and by changing $V_\alpha U_\beta$ into $-U_{(k,j)}$ we get

$$inv' = |^{\zeta<\mu,}_{i_\zeta>i\mu}| + |^{\mu>b+1,}_{i_\mu<index(U_{(k,j)})}| + |^{\zeta<b,}_{i_\zeta>index(U_{(k,j)})}|.$$

Now, as $index(U_{(k,j)}) < index(V_\alpha)$ we have

$$\begin{aligned}|^{\mu>b+1,}_{i_\mu<index(U_{(k,j)})}| \leq |^{\mu>b+1,}_{i_\mu<index(V_\alpha)})| &= |^{\mu>b+1,}_{i_\mu\in[index(U_\beta),index(V_\alpha)[}| + |^{\mu>b+1,}_{i_\mu<index(U_\beta)}| \\ &\leq |^{\mu>b+1,}_{i_\mu\in[index(U_\beta),index(V_\alpha)[}| + 2|^{\mu>b+1,}_{i_\mu<index(U_\beta)}|.\end{aligned}$$

Also, $index(U_\beta) = index(U_{(k,i)}) < indexU_{(k,j)}$ because $i < j$ and our chosen order of the Lazard's basis for G. Therefore,

$$\begin{aligned}|_{i_\zeta > index(U_{(k,j)})}^{\zeta<b,}| \leq |_{i_\zeta > index(U_\beta)}^{\zeta<b,}| = |_{i_\zeta \in]index(U_\beta), index(V_\alpha)]}^{\zeta<b,}| + |_{i_\zeta > index(V_\alpha)}^{\zeta<b,}| \\ \leq |_{i_\zeta \in]index(U_\beta), index(V_\alpha)]}^{\zeta<b,}| + 2|_{i_\zeta > index(V_\alpha)}^{\zeta<b,}|.\end{aligned}$$

Hence, $inv^{'} < inv$.

Consider relation 2.57. It is

$$(1+V_\alpha)(1+U_{-\alpha}) = (1+U_{-\alpha})^{(1+p)^{-1}}(1+W_{(i,i+1)})\cdots(1+W_{(j-1,j)})(1+V_\alpha)^{(1+p)^{-1}}, (\alpha \in \Phi^+),$$

where $\alpha = (i,j)[i<j]$. Let $q = (1+p)^{-1}$. Expanding $(1+U_{-\alpha})^q$, we get that

$$(1+U_{-\alpha})^q = 1 + qU_{-\alpha} + \tfrac{q(q-1)}{2}U_{-\alpha}^2 \cdots$$

If r =deg$(U_{-\alpha})$, then for any positive integer $m \geq 2$ we have $rm \leq n \implies \binom{q}{m} \equiv 0 \pmod p$ because $m \leq rm \leq n < p-1$ trivially implies $\binom{q}{m} \equiv 0 \pmod p$ for $m \geq 2$.

We have $n = \deg(V_\alpha U_{-\alpha})$. Expanding the relation above and looking modulo Fil^{n+1} we deduce

$$V_\alpha U_{-\alpha} = W_{(i,i+1)} + \cdots + W_{(j-1,j)} + U_{-\alpha}V_\alpha (Fil^{n+1}),$$

since all other product terms will be of the form $W_- D$ for some nontrivial variable D and hence have degree strictly greater than n =deg(W_-).

Let $(x_b, x_{b+1}) = (V_\alpha, U_{-\alpha})$, then if we replace $V_\alpha U_{-\alpha}$ by $U_{-\alpha}V_\alpha$ then we reduce the inversions. If we replace $V_\alpha U_{-\alpha}$ by $W_{(k,k+1)}$ then we show that we reduce the number of inversions.
The number of inversions inv in x^{i^*} in the beginning was

$$|_{i_\zeta > i_\mu}^{\zeta<\mu,}| + |_{i_\mu \in [index(U_{-\alpha}), index(V_\alpha)[}^{\mu>b+1,}| + 2|_{i_\mu < index(U_{-\alpha})}^{\mu>b+1,}| + |_{i_\zeta \in]index(U_{-\alpha}), index(V_\alpha)]}^{\zeta<b,}| + 2|_{i_\zeta > index(V_\alpha)}^{\zeta<b,}| \quad +1.$$

After changing $V_\alpha U_{-\alpha}$ into $W_{k,k+1}$, for some $k \in [i, j-1]$, we count the number of inversions:

$$inv^{'} = |_{i_\zeta > i_\mu}^{\zeta<\mu,}| + |_{i_\mu < index(W_{k,k+1}) = \frac{n(n-1)}{2}+k}^{\mu>b+1,}| + |_{i_\zeta > index(W_{k,k+1}) = \frac{n(n-1)}{2}+k}^{\zeta<b,}|.$$

As $index(W_{k,k+1}) < index(V_\alpha)$, we have

$$\begin{aligned}|_{i_\mu < index(W_{k,k+1})}^{\mu>b+1,}| \leq |_{i_\mu < index(V_\alpha)}^{\mu>b+1,}| = |_{i_\mu \in [index(U_{-\alpha}), index(V_\alpha)[}^{\mu>b+1,}| + |_{i_\mu < index(U_{-\alpha})}^{\mu>b+1,}| \\ \leq |_{i_\mu \in [index(U_{-\alpha}), index(V_\alpha)[}^{\mu>b+1,}| + 2|_{i_\mu < index(U_{-\alpha})}^{\mu>b+1,}|.\end{aligned}$$

Also, as $index(U_{-\alpha}) < index(W_{k,k+1})$, we have

$$\begin{aligned}|_{i_\zeta > index(W_{k,k+1})}^{\zeta<b,}| \leq |_{i_\zeta > index(U_{-\alpha})}^{\zeta<b,}| = |_{i_\zeta \in]index(U_{-\alpha}), index(V_\alpha)]}^{\zeta<b,}| + |_{i_\zeta > index(V_\alpha)}^{\zeta<b,}| \\ \leq |_{i_\zeta \in]index(U_{-\alpha}), index(V_\alpha)]}^{\zeta<b,}| + 2|_{i_\zeta > index(V_\alpha)}^{\zeta<b,}|.\end{aligned}$$

Hence, we obtain $inv^{'} < inv$.

Consider relation 2.58 which is

$$U_{\beta_1}U_{\beta_2} = U_{\beta_2}U_{\beta_1}, (\beta_1, \beta_2 \in \Phi^-).$$

So U_{β_1}, U_{β_2} commute and we can reduce the number of inversions. Similarly, the relations 2.59 and 2.60 will reduce to $U_{\beta_1}U_{\beta_2} = U_{\beta_2}U_{\beta_1}(Fil^{r+s+1})$ where $r = \deg(U_{\beta_1})$ and $s = \deg(U_{\beta_2})$. (For this use the Lazard condition $p > n+1$ and the computation on degrees as we have already done in 2.66; example: for 2.59 we have for all natural number $m \geq 2$, $m-1 \leq \deg(U_{i,k})(m-1) \leq n \implies \binom{p}{m} \equiv 0 \pmod p$). So, if we start with the wrong order, that is, suppose $index(U_{\beta_1}) > index(U_{\beta_2})$, then $U_{\beta_1}U_{\beta_2} \to U_{\beta_2}U_{\beta_1}$ reduces the number of inversions.

Relation 2.61 is

$$W_{\delta_1}W_{\delta_2} = W_{\delta_2}W_{\delta_1}(Fil^{2n+1}),(\delta_1,\delta_2 \in \Pi).$$

So, if we start with the wrong order, that is, suppose $index(W_{\delta_1}) > index(W_{\delta_2})$, then $W_{\delta_1}W_{\delta_2} \to W_{\delta_2}W_{\delta_1}$ reduces the number of inversions. Relation 2.62 is similar and so we omit it. We need to struggle with relation 2.63 and 2.64.

First we consider relation 2.63. We have

$$(1+V_{\alpha_1})(1+V_{\alpha_2}) = (1+V_{(i,k)})(1+V_{\alpha_2})(1+V_{\alpha_1}), (\alpha_1,\alpha_2 \in \Phi^+, \alpha_1+\alpha_2 = (i,k)),$$

where $\alpha_1 = (i,j), \alpha_2 = (j,k), i < j < k$. So we have

$$V_{\alpha_1}V_{\alpha_2} = V_{(i,k)} + V_{(i,k)}V_{\alpha_1} + V_{\alpha_2}V_{\alpha_1}(Fil^{r+s+1}),$$

where $r := j - i = \deg(V_{\alpha_1})$ and $s := k - j = \deg(V_{\alpha_2})$. So, the degree of $V_{\alpha_1}V_{\alpha_2}$ is $k-i$ which is the same as the degree of $V_{(i,k)}$. Therefore, we have

$$V_{\alpha_1}V_{\alpha_2} = V_{(i,k)} + V_{\alpha_2}V_{\alpha_1}(Fil^{r+s+1}).$$

We note that $V_{\alpha_1} = V_{(i,j)}$ and $V_{\alpha_2} = V_{(j,k)}$ and $i < j < k$. So, the wrong order is $V_{\alpha_1}V_{\alpha_2}$ and not $V_{\alpha_2}V_{\alpha_1}$, i.e. $index(V_{\alpha_1}) > index(V_{\alpha_2})$. If $(x_b, x_{b+1}) = (V_{\alpha_1}, V_{\alpha_2})$, the number of inversions in x^{i^*} was originally as follows, where ζ, μ denotes indices $\neq b, b+1$ in the product x^{i^*}:

$$inv = |^{\zeta<\mu,}_{i_\zeta>i\mu}| + |_{i_\mu\in[index(V_{\alpha_2}),index(V_{\alpha_1})[}^{\mu>b+1,}| + 2|^{\mu>b+1,}_{i_\mu<index(V_{\alpha_2})}| + |^{\zeta<b,}_{i_\zeta\in]index(V_{\alpha_2}),index(V_{\alpha_1})]}| + 2|^{\zeta<b,}_{i_\zeta>index(V_{\alpha_1})}| \quad +1.$$

The map $V_{\alpha_1}V_{\alpha_2} \to V_{\alpha_2}V_{\alpha_1}$ obviously reduces the number of inversions and by changing $(x_b, x_{b+1}) \to V_{(i,k)}$ we have

$$inv' = |^{\zeta<\mu,}_{i_\zeta>i\mu}| + |^{\mu>b+1,}_{i_\mu<index(V_{(i,k)})}| + |^{\zeta<b,}_{i_\zeta>index(V_{(i,k)})}|.$$

Now, $index(V_{(i,k)}) < index(V_{(i,j)}) = index(V_{\alpha_1})$ and $index(V_{\alpha_2}) = index(V_{(j,k)}) < index(V_{(i,k)})$ as $k > j > i$, because of our lexicographic choice of the ordering of the Lazard's basis for N^+. So we have

$$\begin{aligned}|^{\mu>b+1,}_{i_\mu<index(V_{(i,k)})}| \le |^{\mu>b+1,}_{i_\mu<index(V_{\alpha_1})}| &= |_{i_\mu\in[index(V_{\alpha_2}),index(V_{\alpha_1})[}^{\mu>b+1,}| + |^{\mu>b+1,}_{i_\mu<index(V_{\alpha_2})}| \\ &\le |_{i_\mu\in[index(V_{\alpha_2}),index(V_{\alpha_1})[}^{\mu>b+1,}| + 2|^{\mu>b+1,}_{i_\mu<index(V_{\alpha_2})}|,\end{aligned}$$

and

$$\begin{aligned}|^{\zeta<b,}_{i_\zeta>index(V_{(i,k)})}| \le |^{\zeta<b,}_{i_\zeta>index(V_{\alpha_2})}| &= |^{\zeta<b,}_{i_\zeta\in]index(V_{\alpha_2}),index(V_{\alpha_1})]}| + |^{\zeta<b,}_{i_\zeta>index(V_{\alpha_1})}| \\ &\le |^{\zeta<b,}_{i_\zeta\in]index(V_{\alpha_2}),index(V_{\alpha_1})]}| + 2|^{\zeta<b,}_{i_\zeta>index(V_{\alpha_1})}|.\end{aligned}$$

Hence, we obtain $inv' < inv$.

Consider relation 2.64. It is

$$(1+V_{\alpha_2})(1+V_{\alpha_1}) = (1+V_{(k,j)})(1+V_{\alpha_1})(1+V_{\alpha_2}), (\alpha_1,\alpha_2 \in \Phi^+, \alpha_1+\alpha_2 = (k,j)),$$

where $\alpha_2 = (k,i), \alpha_1 = (i,j), k < i < j$. Like the previous relation it is evident that the wrong order is $V_{\alpha_2}V_{\alpha_1}$ i.e. $index(V_{\alpha_2}) > index(V_{\alpha_1})$ and we have

$$V_{\alpha_2}V_{\alpha_1} = V_{(k,j)} + V_{\alpha_1}V_{\alpha_2}(Fil^{r+s+1}),$$

where $r = \deg(V_{\alpha_2})$ and $s = \deg(V_{\alpha_1})$. Let $(x_b, x_{b+1}) = (V_{\alpha_2}, V_{\alpha_1})$. We count the number of inversions like we did in our previous relation.

$$inv = |^{\zeta<\mu,}_{i_\zeta>i\mu}| + |_{i_\mu\in[index(V_{\alpha_1}),index(V_{\alpha_2})[}^{\mu>b+1,}| + 2|^{\mu>b+1,}_{i_\mu<index(V_{\alpha_1})}| + |^{\zeta<b,}_{i_\zeta\in]index(V_{\alpha_1}),index(V_{\alpha_2})]}| + 2|^{\zeta<b,}_{i_\zeta>index(V_{\alpha_2})}| \quad +1.$$

The map $V_{\alpha_2}V_{\alpha_1} \to V_{\alpha_1}V_{\alpha_2}$ reduces the number of inversions as $index(V_{\alpha_2}) > index(V_{\alpha_1})$ and after changing $(x_b, x_{b+1}) \to V_{(k,j)}$, we have

$$inv' = |_{i_\zeta > i_\mu}^{\zeta<\mu,}| + |_{i_\mu < index(V_{(k,j)})}^{\mu>b+1,}| + |_{i_\zeta > index(V_{(k,j)})}^{\zeta<b,}|.$$

Here, $index(V_{(k,j)}) < index(V_{(k,i)}) = index(V_{\alpha_2})$ and $index(V_{\alpha_1}) = index(V_{(i,j)}) < index(V_{(k,j)})$ because $k < i < j$ and because of our lexicographic choice of the ordering of the Lazard's basis of N^+. Therefore,

$$\begin{aligned} |_{i_\mu < index(V_{(k,j)})}^{\mu>b+1,}| \leq |_{i_\mu < index(V_{\alpha_2})}^{\mu>b+1,}| &= |_{i_\mu \in [index(V_{\alpha_1}), index(V_{\alpha_2})[}^{\mu>b+1,}| + |_{i_\mu < index(V_{\alpha_1})}^{\mu>b+1,}| \\ &\leq |_{i_\mu \in [index(V_{\alpha_1}), index(V_{\alpha_2})[}^{\mu>b+1,}| + 2|_{i_\mu < index(V_{\alpha_1})}^{\mu>b+1,}|, \end{aligned}$$

and

$$\begin{aligned} |_{i_\zeta > index(V_{(k,j)})}^{\zeta<b,}| \leq |_{i_\zeta > index(V_{\alpha_1})}^{\zeta<b,}| &= |_{i_\zeta \in]index(V_{\alpha_1}), index(V_{\alpha_2})]}^{\zeta<b,}| + \sum_{|} |_{i_\zeta > index(V_{\alpha_2})}^{\zeta<b,}| \\ &\leq |_{i_\zeta \in]index(V_{\alpha_1}), index(V_{\alpha_2})]}^{\zeta<b,}| + 2|_{i_\zeta > index(V_{\alpha_2})}^{\zeta<b,}|. \end{aligned}$$

Hence, we deduce $inv' < inv$. So we have completed the proof of our Proposition 2.14.

---

3 Globally analytic principal series representation and base change

3.1 Introduction

The paper [Clo16] deals with the construction of base change of globally analytic distributions on the pro-p Iwahori groups (seen as rigid-analytic spaces) which is compatible with the p-adic Langlands correspondence in the case of principal series of $GL(2)$, and this is what we will extend to $GL(n)$ in this section. Of course, we need to take $p > n+1$, so that the pro-p Iwahori subgroup of $GL(n)$ is p-saturated in the sense of Lazard [Laz65, III, 3.2.7.5] and isomorphic analytically to the product $\mathbb{Z}_p^d$ [Laz65, III, 3.3.2] (for some d, here $\mathbb{Z}_p$ is seen as a rigid-analytic closed ball of radius 1).

In section 3.2.1, for a finite unramified extension L over $\mathbb{Q}_p$, we briefly recall the notion of restriction of scalars functor in the context of rigid-analytic spaces. In section 3.2.2, we give the basic definitions of holomorphic and Langlands base change maps following [Clo16]. Section 3.3.1 treats the case of principal series of $GL(n)$. Specifically, denote by G the pro-p Iwahori subgroup of $GL_n(\mathbb{Z}_p)$ (the group of matrices in $GL_n(\mathbb{Z}_p)$ that are lower unipotent modulo $p\mathbb{Z}_p$), B the subgroup of matrices in $GL_n(\mathbb{Z}_p)$ which are lower triangular modulo $p\mathbb{Z}_p$, $P_0 \supset T_0$ the set of upper triangular (resp. diagonal) matrices in B, $Q_0 = P_0 \cap G$, P^+ the Borel subgroup of upper triangular matrices in $GL_n(\mathbb{Z}_p)$, W the Weyl group (isomorphic to S_n) of $GL_n(\mathbb{Q}_p)$ with respect to its maximal torus, $P_w^+ = B \cap wP^+w^{-1}, w \in W$, $\chi : T_0 \to K^\times$ a locally analytic character with $\chi(t_1, ..., t_n) = \chi_1(t_1) \cdots \chi_n(t_n)$, and $\chi_i(t) = t^{c_i}$, where $c_i = \frac{d}{dt}\chi_i(t)|_{t=1}$, for t sufficiently close to 1, I_{loc} be the locally analytic functions

$$I_{\mathrm{loc}} = \{f \in \mathcal{A}_{\mathrm{loc}}(G, K) : f(gb) = \chi(b^{-1})f(g), b \in Q_0, g \in G\},$$

where $\mathcal{A}_{\mathrm{loc}}(G, K)$ is the space of the locally analytic functions on G having values in an extension K over $\mathbb{Q}_p$. Note that the vector space of locally analytic principal series $\mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}}$ is isomorphic to the space I_{loc}, which are the locally analytic functions from $\mathbb{Z}_p^d \to K$ for an appropriate dimension d (cf. section 3.3.1). "Locally analytic function" mean that locally around a neighborhood of a point, the function can be written in the form of a power series with coefficients in K.

Then, we show in lemmas 3.2, 3.3, 3.7 that the action of G on the *globally analytic vectors* of I_{loc}, given by $h \cdot f(g) \longmapsto f(h^{-1}g)$ $(h \in G)$, is a globally analytic action in the sense of Emerton [Eme17]. Here the globally analytic vectors of I_{loc} are the Tate algebra of functions from $\mathbb{Z}_p^d \to K$ which can be written as power series on the affinoid rigid-analytic space $\mathbb{Z}_p^d$ with coefficients in K going to 0 (section 3.3.1) . For a detailed discussion on globally analytic representation see [Eme17].

The requisite condition of analyticity of χ is treated in 3.16. Let μ be the linear form from the Lie algebra of the torus T_0 to K given by

$$\mu = (-c_1, ..., -c_n) : Diag(t_1, ..., t_n) \mapsto \sum_{i=1}^{n} -c_i t_i$$

where $t = (t_i) \in \mathrm{Lie}(T_0)$. For negative root $\alpha = (i, j), i > j$, let $H_{(i,j)} = E_{i,i} - E_{j,j}$ where $E_{i,i}$ is the standard elementary matrix.

Then, we show that (see theorem 3.9 and theorem 3.8):

Theorem. *Assume $p > n+1$ and χ is analytic. Then the space of the globally analytic vectors of $\mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}}$ is an admissible and globally analytic representation of G. Furthermore, this globally analytic representation is irreducible if and only if for all negative roots $\alpha = (i, j), i > j$, we have $-\mu(H_\alpha) + i - j \notin \{1, 2, 3, ...\}$.*

Here, the admissibility is in the sense of [Eme17] (see also [Clo16, sec. 2.3]). For the global analyticity, we compute explicitly the action of G on the Tate algebra of globally analytic functions of $\mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}}$ and show that the action map is a globally analytic function on G seen as a rigid-analytic space. For the irreducibility we first use the action of the Lie algebra of G to show that any non-zero closed G-invariant subspace of the globally analytic vectors of $\mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}}$ contains the constant function 1. The remaining part of the argument for the proof of irreducibility uses the notion of Verma modules and its condition of irreducibility, a result of Bernstein-Gelfand.

Finally, in section 3.3.2, we extend these results to the pro-p Iwahori group of $GL_n(L)$ where L is an unramified finite extension of $\mathbb{Q}_p$. Then, in theorem 3.18, we use the Steinberg tensor product [Ste63] in order to construct the base change in the context of Langlands functoriality.

In section 3.4 we deal with the globally analytic vectors induced from the Weyl orbit of the upper triangular Borel subgroup of the Iwahori subgroup B, i.e. the globally analytic vectors of $\mathrm{ind}_{P_w^+}^B(\chi^w)_{\mathrm{loc}}$, where $\chi_w(h) = \chi(w^{-1}hw)$.

3.2 Base change maps for analytic functions

We introduce the basic notions of rigid-analytic geometry including a brief discussion on the restriction of scalars. Then we briefly recall (following [Clo16]) the notions of holomorphic and Langlands base change functors producing from a globally analytic representation over $\mathbb{Q}_p$, to a representation over L. The Langlands base change is related to the "Steinberg tensor product" described at the end of section 1.1 of [Clo17] for $GL(2)$.

3.2.1 Restriction of scalars

Let L be a finite unramified extension of $\mathbb{Q}_p$ of degree N, (B^1/L) be the (rigid-analytic) closed unit ball over L with its Tate algebra of analytic functions $\mathcal{T}_L = L\langle x\rangle$, G_L be a rigid-analytic group isomorphic as a rigid analytic space to $(B^1/L)^d$ which is a rigid-analytic space with affinoid algebra $\mathcal{A}(G_L) := \widehat{\otimes}^d\mathcal{T}_L = L\langle x_1, ..., x_d\rangle$, the Tate algebra of analytic functions in d variables with coefficients in L. (With the notations of section 3.1, for $L = \mathbb{Q}_p$, we can take G_L to be the pro-p Iwahori group G assuming $p > n+1$). The restriction of scalars functor [Ber00] associates to G_L a rigid analytic space $\mathrm{Res}_{L/\mathbb{Q}_p}G_L$ over $\mathbb{Q}_p$. In general, this functor does not behave trivially, but L being unramified, we obtain

$$\mathrm{Res}_{L/\mathbb{Q}_p}(B^1/L) \cong (B^1/\mathbb{Q}_p)^N,$$

[Clo16, lemma 1.1] which is canonically obtained by the choice of a basis (e_i) of $\mathcal{O}_L$ over $\mathbb{Z}_p$. Precisely, for an affinoid $\mathbb{Q}_p$-algebra $\mathcal{B}$ and for $f \in \mathrm{Hom}_L(L\langle x\rangle, \mathcal{B}\otimes_{\mathbb{Q}_p} L)$ with $f(x) = \sum b_i e_i$ ($b_i \in \mathcal{B}$), we canonically define a function $g \in \mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p\langle x_1, ..., x_N\rangle, \mathcal{B})$ with $g(x_i) = b_i$ which is given by

$$g(x_1, ..., x_N) = f(\sum e_i x_i),$$

[Clo16, section 1.1]. As the restriction of scalars is compatible with direct products [Ber00, prop. 1.8], $\mathrm{Res}_{L/\mathbb{Q}_p}G_L = (B^1/\mathbb{Q}_p)^{dN}$. Henceforth, we write Res G_L to denote $\mathrm{Res}_{L/\mathbb{Q}_p}G_L$.

3.2.2 Holomorphic base change

Assume now that $G_L \cong (B^1/L)^d$ is obtained by *extension* of scalars from $\mathbb{Q}_p$. Then, the Tate algebra $\mathcal{A}(G_L) = \mathcal{A}(G_{\mathbb{Q}_p})\otimes L$. The co-multiplication map m^*, defined by a morphism

$$m^* : \mathcal{A}(G_L) \to \mathcal{A}(G_L)\widehat{\otimes}\mathcal{A}(G_L)$$

with image inside the completed tensor product, is obtained by extension of scalars from

$$m_0^* : \mathcal{A}(G_{\mathbb{Q}_p}) \to \mathcal{A}(G_{\mathbb{Q}_p})\widehat{\otimes}\mathcal{A}(G_{\mathbb{Q}_p}).$$

To an analytic function $f \in \mathcal{A}(G_L)$, we associate a function $g \in \mathcal{A}(\mathrm{Res}\ G_L)\otimes L$, Res G_L defined as in section 3.2.1. Then, by composing with the natural map $\mathcal{A}(G_{\mathbb{Q}_p}) \to \mathcal{A}(G_L)$, we obtain a "holomorphic base change" map

$$b_1 : \mathcal{A}(G_{\mathbb{Q}_p}) \to \mathcal{A}(\mathrm{Res}\ G_L)\otimes L.$$

The Galois group $\Sigma = \mathrm{Gal}(L/\mathbb{Q}_p)$ of the unramified Galois extension L acts naturally on G_L (by automorphisms on the Tate algebra) and acts on Res G_L by $\mathbb{Q}_p$-automorphism. Define the map

$$b : \mathcal{A}(G_{\mathbb{Q}_p}) \to \mathcal{A}(\mathrm{Res}\ G_L)\otimes L$$
$$b(f) = \prod_{\sigma\in\Sigma} b_1(f)^\sigma.$$

Then, by [Clo16, prop. 1.5], the natural maps b_1, b commute with co-multiplications and under the isomorphism $\mathcal{A}_L(\mathrm{Res}\, G_L) \cong \widehat{\otimes}_\sigma\, \mathcal{A}(G_L)$, the map $b = \otimes_\sigma\, b_1^\sigma$ (the isomorphism $\mathcal{A}_L(\mathrm{Res}\, G_L) \cong \widehat{\otimes}_\sigma\, \mathcal{A}(G_L)$ follows from $\mathrm{Res}\, G_L \otimes_{\mathbb{Q}_p} L \cong \prod_\sigma G_L$, see the discussion before proposition 1.5 of [Clo16]).

Fix a finite extension K of $\mathbb{Q}_p$ and an injection $i : L \subset K$. If $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$, we then have the injection $i \circ \sigma : L \to K$. Denote by V a (globally) analytic representation of $G_{\mathbb{Q}_p}$ on a K-Banach space. Then V naturally extends to an analytic representation of G_L; this is called the *holomorphic base change* of V in [Clo16]. For $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$, write V^σ the representation of G_L associated to $i \circ \sigma$. Then, the *full (Langlands) base change* of V is defined to be the globally analytic representation of $\mathrm{Res}_{L/\mathbb{Q}_p}(G_L)$ on $\widehat{\otimes}_\sigma\, V^\sigma$ (cf. [Clo16, def. 3.2]).

3.3 Globally analytic principal series for $GL(n)$ and base change

We first recall the notion of locally analytic principal series representation induced from the Borel to the Iwahori subgroup of $GL(n, \mathbb{Z}_p)$. Then we treat the action of the pro-p Iwahori on the subspace of rigid-analytic functions within the locally analytic principal series and show that this action is a globally analytic action (theorem 3.8). This gives us the globally analytic induced principal series representation under the pro-p Iwahori subgroup G. Furthermore, we treat the condition of irreducibility of the globally analytic principal series by translating an irreducibility condition of a suitable Verma module (theorem 3.9). Finally in section 3.3.2 we base change our globally analytic representation to a finite unramified extension L of $\mathbb{Q}_p$.

3.3.1 Global analyticity and irreducibility of the principal series representation

We consider the case of the principal series for $GL_n(\mathbb{Z}_p)$. Denote by G the pro-p Iwahori subgroup of $GL_n(\mathbb{Z}_p)$, i.e. the group of matrices in $GL_n(\mathbb{Z}_p)$ that are lower unipotent modulo $p\mathbb{Z}_p$, B the subgroup of matrices in $GL_n(\mathbb{Z}_p)$ which are lower triangular modulo $p\mathbb{Z}_p$, $P_0 \supset T_0$ be the set of upper triangular (resp. diagonal) matrices in B, $\chi : T_0 \to K^\times$ be a locally analytic character with

$$\chi(t_1, ..., t_n) = \chi_1(t_1) \cdots \chi_n(t_n),$$

and $\chi_i(t) = t^{c_i}$ where $c_i = \frac{d}{dt}\chi_i(t)|_{t=1}$ for t sufficiently close to 1. Hence, $c_i \in K$.

We first consider, as in [Clo16], the locally analytic induced representation of B,

$$J_{\mathrm{loc}} = \mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}} = \{f \in \mathcal{A}_{\mathrm{loc}}(B, K) : f(gb) = \chi(b^{-1})f(g), b \in P_0, g \in B\},$$

where χ is naturally extended to P_0 and $\mathcal{A}_{\mathrm{loc}}(B, K)$ is the space of locally analytic functions on B. With U the lower unipotent subgroup of B with entries in $\mathbb{Z}_p$ in the lower triangular part, 1 in the diagonal entries and 0 elsewhere, we have the natural decomposition

$$B = UP_0 \tag{3.1}$$

Since χ is fixed, the restriction of the functions of J_{loc} to $G \subset B$ is injective. With $Q_0 = P_0 \cap G$, we deduce that the vector space of J_{loc} is

$$I_{\mathrm{loc}} = \{f \in \mathcal{A}_{\mathrm{loc}}(G, K) : f(gb) \equiv \chi(b^{-1})f(g), b \in Q_0, g \in G\}. \tag{3.2}$$

With the decomposition $G = UQ_0$, we see that $I_{\mathrm{loc}} \cong \mathcal{A}_{\mathrm{loc}}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K) = \mathcal{A}_{\mathrm{loc}}(U, K)$. Here, $\mathbb{Z}_p$ is seen as the rigid analytic (additive) group $B^1(\mathbb{Z}_p)$. The group G acts by left translation

$$h \cdot f(g) \longmapsto f(h^{-1}g). \tag{3.3}$$

Let $E_{i,j}$ be the elementary matrices with 1 in the $(i,j)^{th}$ place and 0 elsewhere. From now on, we assume

$$p > n + 1, \tag{3.4}$$

then G is p-saturated in the sense of Lazard [Laz65, III, 3.2.7.5] and thus, it is the ordered product (as a rigid analytic group) of the following one-parameter subgroups:

1. first, for $y \in \mathbb{Z}_p$, take the one-parameter lower unipotent matrices by the following lexicographic order: the 1-parameter group of matrices $(1 + yE_{i,j})$ comes before the 1-parameter group of matrices $(1 + yE_{k,l})$ if and only if $i < k$ or $i = k$ and $j < l$,

2. then, for $t_k \equiv 1[p]$ and $k \in [1,n]$, take the one-parameter diagonal subgroups $(t_k E_{k,k} + \sum_{i=1, i\neq k}^{n} E_{i,i})$ starting from the top left extreme to the low right extreme and,

3. finally, for $y \in p\mathbb{Z}_p$, take the upper unipotent matrices in the following order: the 1-parameter group of matrices $(1 + yE_{i,j})$ comes before the 1-parameter group of matrices $(1 + yE_{k,l})$ if and only if $i \geq k$ or $i = k$ and $j > l$.

That is, for the lower unipotent matrices, we start with the top and left extreme and then fill the lines from the left, going down and for the upper unipotent matrices we start with the low and right extreme and then fill the lines from the right, going up. (Cf. [Laz65, III, 3.3.2] for the rigid-analyticity and see theorem 2.5 and remark 2.7 of section 2.2 for the order of the product i.e. an ordered Lazard basis of G, although in section 2.2 we have taken G to be upper unipotent matrices modulo p but this does not matter).

Let now $\mathcal{A} = \mathcal{A}(U,K) = \mathcal{A}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K)$ be the subspace of globally analytic functions of $I_{\text{loc}} = \mathcal{A}_{\text{loc}}(U,K)$. Thus $f \in \mathcal{A}$ is a globally analytic function in the variables $a_{i,j}$ on U, that is,

$$f(A) = \sum_{\nu \in \mathbb{N}^d} c_\nu a^\nu$$

such that $c_\nu \in K$ and $|c_\nu| \to 0$ as $|\nu| \to \infty$. Here $d = \frac{n(n-1)}{2}$, $a = (a_{2,1}, a_{3,1}, a_{3,2}, ..., a_{n,n-1}) \in \mathbb{Z}_p^d$ with the lexicographic ordering of $a_{i,j}$ as in (1), $\nu = (\nu_{2,1}, \nu_{3,1}, ..., \nu_{n,n-1}) \in \mathbb{N}^d$, $a^\nu = a_{2,1}^{\nu_{2,1}} \cdots a_{n,n-1}^{\nu_{n,n-1}}$ and $|\nu| = \nu_{2,1} + \cdots + \nu_{n,n-1}$.

We now seek conditions such that if f is a globally analytic function on G and the action of G is defined as above then, the map $h \longmapsto h \cdot f(g) = f(h^{-1}g)$ is globally analytic.

Lemma 3.1. *With the above notations, for $p > n+1$, the action of G on $f \in \mathcal{A}(U,K)$, i.e the map $h \mapsto h \cdot f$ is a globally analytic function on G if and only if it is so for all 1-parameter (rigid-analytic) subgroups and the diagonal subgroup of which G is the product.*

Proof. Follows from the same argument as in the discussion after lemma 3.4 of [Clo16]. □

Thus, our goal is to verify the analyticity of the action of the diagonal subgroup, the 1-parameter lower unipotent subgroups and the 1-parameter upper unipotent subgroups of G which are treated in lemmas 3.2, 3.3 and 3.7 respectively.

Let $A = (a_{i,j})_{i,j}$ be any matrix in U (i.e. $a_{i,i} = 1$ and $a_{i,j} = 0$ for $i < j$) and $T = diag(t_1, ..., t_n) = \sum_{k=1}^{n} t_k E_{k,k}$ be any element in the diagonal $T_0 \cap G$, where $t_k \in 1 + p\mathbb{Z}_p$. Assume $f \in I_{\text{loc}}$, then the action of T on f, given by 3.3, is

$$\begin{aligned}
T \cdot f(A) = f\Big(Diag(t_1^{-1}, ..., t_n^{-1})A\Big) &= f\Big((\sum_{k=1}^{n} t_k^{-1} E_{k,k})(\sum_{i,j=1}^{n} a_{i,j} E_{i,j})\Big), \\
&= f(\sum_{j,k=1}^{n} t_k^{-1} a_{k,j} E_{k,j}), \\
&= f\Big((\sum_{k,j=1}^{n} t_k^{-1} t_j a_{k,j} E_{k,j})(\sum_{j=1}^{n} t_j^{-1} E_{j,j})\Big), \\
&= f(\sum_{k,j=1}^{n} t_k^{-1} t_j a_{k,j} E_{k,j}) \chi(t_1, ..., t_n) \text{ (from 3.2)},
\end{aligned}$$

Interchanging indices $k \to i$, we obtain

$$(\sum_{i=1}^{n} t_i E_{i,i}) \cdot f(\sum_{i,j=1}^{n} a_{i,j} E_{i,j}) = f(\sum_{i,j=1}^{n} t_i^{-1} t_j a_{i,j} E_{i,j}) \chi(t_1, ..., t_n) \tag{3.5}$$

with $a_{i,i} = 1$, $a_{i,j} = 0$ for $i < j$ and $t_i \equiv 1(\mod p)$.

Taking $f = 1$ we see that $\chi(t_1, ..., t_n)$ must be an analytic function. By 3.5, for fixed $k \in [1, n]$ considering the action of the matrix $(t_k E_{k,k} + \sum_{i=1, i\neq k}^{n} E_{i,i})$ on f we obtain,

$$(t_k E_{k,k} + \sum_{i=1, i\neq k}^{n} E_{i,i}) f(A) = f(\sum_{\substack{u,v\neq k \\ u>v}} a_{u,v}E_{u,v} + a_{k,k}E_{k,k} + \sum_{j=1}^{k-1} t_k^{-1} a_{k,j}E_{k,j} + \sum_{i=k+1}^{n} t_k a_{i,k}E_{i,k}) \tag{3.6}$$

$$\times \chi(1, ..., t_k, ..., 1) \tag{3.7}$$

$$:= f(\mathcal{C})\chi(1, ..., t_k, ..., 1) \tag{3.8}$$

where $\mathcal{C}$ is the matrix $(\sum_{\substack{u,v\neq k \\ u>v}} a_{u,v}E_{u,v} + a_{k,k}E_{k,k} + \sum_{j=1}^{k-1} t_k^{-1} a_{k,j}E_{k,j} + \sum_{i=k+1}^{n} t_k a_{i,k}E_{i,k})$. Assume now that f is globally analytic in the variables $a_{i,j}$ on U, that is,

$$f(A) = \sum_{\nu \in \mathbb{N}^d} c_\nu a^\nu, \tag{3.9}$$

such that $c_\nu \in K$ and $|c_\nu| \to 0$. Then, with $t_k = 1 + p\xi_k$, $\xi_k \in \mathbb{Z}_p$,

$$f(\mathcal{C}) = \sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) (\prod_{j=1}^{k-1} (t_k^{-1} a_{k,j})^{\nu_{k,j}}) (\prod_{i=k+1}^{n} (t_k a_{i,k})^{\nu_{i,k}}) \tag{3.10}$$

$$= \sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) (\prod_{j=1}^{k-1} (1 + p\xi_k)^{-\nu_{k,j}} a_{k,j}^{\nu_{k,j}}) (\prod_{i=k+1}^{n} (1 + p\xi_k)^{\nu_{i,k}} a_{i,k}^{\nu_{i,k}}). \tag{3.11}$$

Recall that for $|v| < 1$, $m \in \mathbb{N}$, we have $(1 - v)^{-m} = \sum_{q=0}^{\infty} \binom{m+q-1}{q} v^q$. Now, inserting the expressions

$$(1 + p\xi_k)^{-\nu_{k,j}} = \sum_{q_{k,j}=0}^{\infty} \binom{\nu_{k,j} + q_{k,j} - 1}{q_{k,j}} (-p\xi_k)^{q_{k,j}}$$

and $(1+p\xi_k)^{\nu_{i,k}} = \sum_{u_{i,k}=0}^{\nu_{i,k}} \binom{\nu_{i,k}}{u_{i,k}} p^{u_{i,k}} \xi_k^{u_{i,k}}$ in equation 3.11 we obtain, with $|q| := q_{k,1} + \cdots + q_{k,k-1}$, $|u| = u_{k+1,k} + \cdots + u_{n,k}$ and $v_{max} = \prod_{i=k+1}^{n} \nu_{i,k}$,

$$f(\mathcal{C}) = \sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) \Big(\prod_{j=1}^{k-1} (\sum_{q_{k,j}=0}^{\infty} \binom{\nu_{k,j} + q_{k,j} - 1}{q_{k,j}} (-p\xi_k)^{q_{k,j}} a_{k,j}^{\nu_{k,j}}) \Big)$$

$$\times \Big(\prod_{i=k+1}^{n} \sum_{u_{i,k}=0}^{\nu_{i,k}} \binom{\nu_{i,k}}{u_{i,k}} p^{u_{i,k}} \xi_k^{u_{i,k}} a_{i,k}^{\nu_{i,k}} \Big)$$

$$= \sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) \Big(\sum_{N\geq 0}^{\infty} \xi_k^N (\sum_{|q|=N} \prod_{j=1}^{k-1} \binom{\nu_{k,j} + q_{k,j} - 1}{q_{k,j}} (-p)^{q_{k,j}} a_{k,j}^{\nu_{k,j}}) \Big)$$

$$\times \Big(\sum_{M=0}^{v_{max}} \xi_k^M (\sum_{|u|=M} \prod_{i=k+1}^{n} \binom{\nu_{i,k}}{u_{i,k}} p^{u_{i,k}} a_{i,k}^{\nu_{i,k}}) \Big).$$

Let f_N and g_M be defined by

$$f_N = (\sum_{|q|=N} \prod_{j=1}^{k-1} \binom{\nu_{k,j} + q_{k,j} - 1}{q_{k,j}} (-p)^{q_{k,j}} a_{k,j}^{\nu_{k,j}}), \tag{3.12}$$

$$g_M = (\sum_{|u|=M} \prod_{i=k+1}^{n} \binom{\nu_{i,k}}{u_{i,k}} p^{u_{i,k}} a_{i,k}^{\nu_{i,k}}). \tag{3.13}$$

Then,

$$f(\mathcal{C}) = \sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) (\sum_{N\geq 0}^{\infty} \xi_k^N f_N)(\sum_{M=0}^{v_{max}} \xi_k^M g_M) \tag{3.14}$$

$$= \sum_{m\geq 0}^{\infty} \xi_k^m \Big(\sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) \sum_{N+M=m} f_N g_M \Big). \tag{3.15}$$

Any element $f \in \mathcal{A}(U,K)$ is of the form $f = \sum_{\nu\in\mathbb{N}^d} c_\nu a^\nu$ with $\lim_{|\nu|\to\infty} |c_\nu| = 0$. The space $\mathcal{A}(U,K)$ is a K-Banach space with the sup norm on f defined by

$$|f| = \sup |c_\nu|$$

(cf. [Bos14, chapter 2]). Recall that for any K-Banach space V with norm $|\cdot|$, a representation π of G on V is called a globally analytic representation if the map

$$g \longmapsto g \cdot v = \pi(g)v$$

is globally analytic on G for all $v \in V$. Thus, in coordinates $(x_1, ..., x_l)$ with $l = \dim(G)$:

$$g \cdot v = \sum_k x^k v_k$$

where $v_k \in V$ and $|v_k| \to 0$. Here $k = (k_1, ..., k_l)$ and $x^k = x_1^{k_1} \cdots x_l^{k_l}, k_i \in \mathbb{N}$ (cf. [Eme17], [Clo16, section 2]).

Now, with $t_k = 1 + p\xi_k$, $\xi_k \in \mathbb{Z}_p$, in order to show that the action of the one-parameter diagonal subgroup $t_k(E_{k,k}) + \sum_{\substack{i=1 \\ i\neq k}}^{n} E_{i,i}$ on $f \in \mathcal{A}(U,K)$ is analytic we have to show that the map

$$\mathbb{Z}_p \to \mathcal{A}(U,K)$$
$$\xi_k \longmapsto \Big((1+p\xi_k)E_{k,k} + \sum_{i=1, i\neq k}^{n} E_{i,i}\Big) f = f(\mathcal{C})\chi(1, .., 1+p\xi_k, ..., 1)$$

is a globally analytic map on $\mathbb{Z}_p$. The norm of the coefficient of ξ_k^m, in equation 3.15, is

$$|\Big(\sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) \sum_{N+M=m} f_N g_M \Big)|.$$

Notice that, since $N, M \leq m$ and $f_N, g_M \in \mathbb{Z}_p$ from 3.12 and 3.13, the quantity
$(a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}} \sum_{N+M=m} f_N g_M)$ has finite sum and product and hence lies in $\mathbb{Z}_p$. Hence,

$$|\Big(\sum_{\nu} c_\nu (a_{k,k}^{\nu_{k,k}} \prod_{\substack{u,v\neq k \\ u>v}} a_{u,v}^{\nu_{u,v}}) \sum_{N+M=m} f_N g_M \Big)| \to 0$$

as $|c_\nu| \to 0$ with $\nu \to \infty$. This gives the analyticity of the action $f \to f(\mathcal{C})$. We now consider the analyticity of the character χ. Write $\chi = (\chi_1, ..., \chi_n)$, $\chi_i(1+pu_i) = e^{c_i \log(1+pu_i)}$ for $c_i \in K$, u_i close to 0, $i \in [1, n]$. The exponential is analytic (in K) in the domain $v_p(z) > \frac{e}{p-1}$ where $e = e(K)$ and v_p is the normalized valuation, $v_p(p) = 1$. Now,

$$v_p(c_i \log(1+pu_i)) = v_p(c_i) + 1 + v_p(u_i).$$

So we must have $v_p(c_i) + 1 > \frac{e}{p-1}$, i.e.

$$v_p(c_i) > \frac{e}{p-1} - 1, \tag{3.16}$$

$$= \frac{-p}{p-1} \text{ (if } K \text{ is unramified)}. \tag{3.17}$$

We say that χ is "analytic" if and only if c_i's verify these conditions and in the rest of this text we assume that our character χ is analytic. It is easy to see that if χ is analytic, then $\chi(1,...,1+p\xi_k,...,1)$ is an analytic function on ξ_k. The character

$$\begin{aligned}\chi(1,...,1+p\xi_k,...,1) = \chi_k(1+p\xi_k) &= \sum_{n=0}^{\infty} c_n(1+p\xi_k)^n \qquad \text{(since } \chi_k \text{ is analytic)}\\ &= \sum_{n=0}^{\infty} c_n \sum_{u=0}^{n} \binom{n}{u} p^u \xi_k^u \\ &= \sum_{u=0}^{\infty} \xi_k^u \Big(p^u \sum_{n\geq u}^{\infty} c_n \binom{n}{u}\Big).\end{aligned}$$

The norm of the coefficient of ξ_k^u is $|p^u \sum_{n\geq u}^{\infty} c_n \binom{n}{u}|$ which goes to 0 as $|c_n| \to 0$ with $n \to \infty$. Thus, we have shown

Lemma 3.2. *Under the hypothesis 3.16, for each $k \in [1,n]$, the action of the one-parameter diagonal subgroup $(t_k E_{k,k} + \sum_{i=1, i\neq k}^{n} E_{i,i})$ of G on $\mathcal{A}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K)$ given by 3.7 is an analytic action.*

For $y \in \mathbb{Z}_p$ and $i > j$, i, j fixed between $1, ..., n$, the action of the 1-parameter (rigid-analytic) subgroup $(1 + yE_{i,j})$ on $f(A)$, given by 3.3 is

$$(1+yE_{i,j})f(A) = f\Big((1+yE_{i,j})^{-1}A\Big) = f\Big((1-yE_{i,j})A\Big), \tag{3.18}$$

$$= f\Big((1-yE_{i,j})(\sum_{\substack{k\geq l\\ k,l\in[1,n]}} a_{k,l}E_{k,l})\Big), \tag{3.19}$$

$$= f\Big(\sum_{\substack{k\geq l\\ k,l\in[1,n]}} a_{k,l}E_{k,l} - \sum_{l=1,...,j} y a_{j,l}E_{i,l}\Big) := f(\mathcal{B}), \tag{3.20}$$

where $\mathcal{B}$ is the matrix $\sum_{\substack{k\geq l\\ k,l\in[1,n]}} a_{k,l}E_{k,l} - \sum_{l=1}^{j} y a_{j,l}E_{i,l}$. One can easily see that the matrix $\mathcal{B} = (b_{u,v})$ is lower unipotent and differs from matrix A only in the first j entries of its i^{th} row. In particular, $b_{i,v} = a_{i,v} - y a_{j,v}$ for all $v \in [1,j], (a_{j,j} = 1)$ and all other $b_{u,v}$ are the same as $a_{u,v}$ (recall that A is lower unipotent).

Now, let f be a globally analytic function on U as in 3.9. That is, $f(a) = \sum_{\nu\in\mathbb{N}^d} c_\nu a^\nu$ with $a^\nu = a_{2,1}^{\nu_{2,1}} \cdots a_{n,n-1}^{\nu_{n,n-1}}$ and $|c_\nu| \to 0$. Then, we have to show that $(1 + yE_{i,j})f = f(\mathcal{B})$ gives an analytic map

$$\begin{aligned}\mathbb{Z}_p &\to \mathcal{A}(U,K)\\ y &\to (1+yE_{i,j})f = f(\mathcal{B}).\end{aligned}$$

The power series

$$f(\mathcal{B}) = \sum_{\nu} c_\nu \Big((\prod_{\substack{u>v\\ u=i \implies v>j}} a_{u,v}^{\nu_{u,v}})(\prod_{k=1}^{j}(a_{i,k} - y a_{j,k})^{\nu_{i,k}})\Big) = \sum_{\nu} c_\nu a^{\nu'} \prod_{k=1}^{j}(a_{i,k} - y a_{j,k})^{\nu_{i,k}}$$

where

$$a^{\nu'} = \prod_{\substack{u>v\\ u=i \implies v>j}} a_{u,v}^{\nu_{u,v}}.$$

Let us define

$$b(\nu) := \prod_{k=1}^{j}(a_{i,k} - y a_{j,k})^{\nu_{i,k}} = \sum_{m_{i,k}=0}^{\nu_{i,k}} \binom{\nu_{i,k}}{m_{i,k}} y^{m_{i,k}} (-a_{j,k})^{m_{i,k}} a_{i,k}^{\nu_{i,k}-m_{i,k}}.$$

Then, with $N = \sum_{k=1}^{j} \nu_{i,k}$ and $|m| = m_{i,1} + \cdots + m_{i,j}$, we obtain

$$\begin{aligned} f(\mathcal{B}) &= \sum_{\nu} c_\nu a^{\nu'} b(\nu) \\ &= \sum_{\nu} c_\nu a^{\nu'} \sum_{\mu=0}^{N} y^\mu \sum_{\substack{|m|=\mu \\ m_{i,k}\le\nu_{i,k}}} \prod_{k=1}^{j} \binom{\nu_{i,k}}{m_{i,k}} (-a_{j,k})^{m_{i,k}} a_{i,k}^{\nu_{i,k}-m_{i,k}} \\ &= \sum_{\mu=0}^{\infty} y^\mu \sum_{\nu:|\nu|\ge\mu} c_\nu a^{\nu'} \sum_{\substack{|m|=\mu \\ m_{i,k}\le\nu_{i,k}}} \prod_{k=1}^{j} \binom{\nu_{i,k}}{m_{i,k}} (-a_{j,k})^{m_{i,k}} a_{i,k}^{\nu_{i,k}-m_{i,k}} \\ &= \sum_{\mu=0}^{\infty} y^\mu f_\mu \qquad (\text{with } f_\mu := \sum_{\nu:|\nu|\ge\mu} c_\nu a^{\nu'} \sum_{\substack{|m|=\mu \\ m_{i,k}\le\nu_{i,k}}} \prod_{k=1}^{j} \binom{\nu_{i,k}}{m_{i,k}} (-a_{j,k})^{m_{i,k}} a_{i,k}^{\nu_{i,k}-m_{i,k}}). \end{aligned}$$

With $m'_{i,k} = \nu_{i,k} - m_{i,k}$,

$$f_\mu = \sum_{\nu:|\nu|\ge\mu} c_\nu a^{\nu'} \sum_{\substack{|m|=\mu \\ m_{i,k}\le\nu_{i,k}}} \prod_{k=1}^{j} \binom{\nu_{i,k}}{m_{i,k}} (-a_{j,k})^{m_{i,k}} a_{i,k}^{m'_{i,k}}. \tag{3.21}$$

We have that $|c_\nu| \to \infty$ as $|\nu| \to \infty$ and $\nu_{i,k} - m_{i,k} = m'_{i,k} \le |\nu|$. Then, the norm of the coefficient of $a^{\nu'} \prod_{k=1}^{j} a_{j,k}^{m_{i,k}} a_{i,k}^{m'_{i,k}}$ in f_μ goes to 0 as $(\nu', m_{i,k}, m'_{i,k}) \to \infty$.

Therefore, $|f_\mu| \to 0$ as $\mu \to \infty$, because we have $|\nu| \ge \mu$ for *all* the terms of f_μ (cf. 3.21). This yields a convergent expression of $f(\mathcal{B})$ in $\mathcal{A}(U, K)$.

This gives the analyticity of the map $y \to (1 + E_{i,j})f = f(\mathcal{B})$.

Therefore, we have shown,

Lemma 3.3. *For $y \in \mathbb{Z}_p$ and $i > j$, the action of the lower unipotent (rigid-analytic) 1-parameter subgroup $(1 + yE_{i,j})$ of G on $f \in \mathcal{A}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K)$, given by 3.18 is an analytic action.*

It remains to check the analyticity of the action 3.3 by triangular superior matrices of the form $(1 + yE_{i,j})$ for $i < j, i, j \in [1, n], y \in p\mathbb{Z}_p$. Recall that the action of $(1 + yE_{i,j})$ on $f \in I_{\text{loc}}$ given by 3.3, is

$$(1 + yE_{i,j})f(A) = f\Big((1 + yE_{i,j})^{-1}A\Big) = f\Big((1 - yE_{i,j})A\Big).$$

Recall the action of Q_0 given by 3.2, that is, $f(gb) \equiv \chi(b^{-1})f(g)$ with $b \in Q_0$. Hence, our objective is to write the matrix $(1 - yE_{i,j})A$ as the product of two matrices X and Z with $X \in U$ and $Z \in Q_0$, that is:

$$(1 - yE_{i,j})A = XZ,$$

where X is a lower unipotent matrix with entries in $\mathbb{Z}_p$ and Z is a upper triangular matrix with diagonal elements in $1 + p\mathbb{Z}_p$ and such that the elements above the diagonal have entries in $p\mathbb{Z}_p$.

Lemma 3.4. *For $i < j$ and $y \in p\mathbb{Z}_p$, there exists a unique matrix decomposition $(1-yE_{i,j})A = XZ$ with $X = (x_{k,l})_{k,l} \in U$ and $Z = (z_{r,s})_{r,s} \in Q_0$. Also,*

1. *all the diagonal elements $z_{r,r}$ of Z are of the form $\frac{1-yh_{r,r}(y,a)}{1-yg_{r,r}(y,a)}$,*
2. *all the elements $z_{r,s}$, for $r < s$, of Z are of the form $\frac{yh_{r,s}(y,a)}{1-yg_{r,s}(y,a)}$,*
3. *all the elements $x_{k,l}$ with $k > l$ of the lower triangular unipotent matrix X are of the form $\frac{h_{k,l}(y,a)}{1-yg_{k,l}(y,a)}$,*

where $h_{\star,\star}(y, a)$ and $g_{\star,\star}(y, a)$ are polynomial functions with integral coefficients in y and $a_{2,1}, a_{3,1}, a_{3,2}, ..., a_{n,n-1}$ (entries of the lower unipotent matrix A).

Proof. We prove the lemma by an easy inductive argument. The base case $n = 2$ is clear from the matrix equation

$$\begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a_{2,1} & 1 \end{pmatrix} = \begin{pmatrix} 1-ya_{2,1} & -y \\ a_{2,1} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x_{2,1} & 1 \end{pmatrix}\begin{pmatrix} z_{1,1} & z_{1,2} \\ 0 & z_{2,2} \end{pmatrix}$$
$$= \begin{pmatrix} z_{1,1} & z_{1,2} \\ z_{1,1}x_{2,1} & z_{2,2}+z_{1,2}x_{2,1} \end{pmatrix}$$

with $x_{2,1} = \frac{a_{2,1}}{1-ya_{2,1}}, z_{1,1} = 1-ya_{2,1}, z_{1,2} = -y, z_{2,2} = \frac{1}{1-ya_{2,1}}$. Assume, by induction hypothesis that our lemma is true for $GL(n-1)$. We show it for $GL(n)$. Let us first suppose that $i > 1$, that is,

$$(1-yE_{i,j}) = \left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline 0 & \\ \vdots & 1-yE' \\ 0 & \end{array}\right) \text{ (with some elementary matrix } E', 1-yE' \in GL(n-1))$$

The matrix A, being lower unipotent, can be written in the following block form:

$$A = \left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline a_{2,1} & \\ \vdots & A' \\ a_{n,1} & \end{array}\right) \text{ (with } A' \in GL(n-1))$$

Setting $\underline{a}$ to be the column vector $\begin{pmatrix} a_{2,1} \\ a_{3,1} \\ \vdots \\ a_{n,1} \end{pmatrix}$,

$$(1-yE_{i,j})A = \left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline 0 & \\ \vdots & 1-yE' \\ 0 & \end{array}\right)\left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline a_{2,1} & \\ \vdots & A' \\ a_{n,1} & \end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline (1-yE')\underline{a} & (1-yE')A' \end{array}\right)$$

We want to decompose the above matrix in the form

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline (1-yE')\underline{a} & (1-yE')A' \end{array}\right) = \left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline x_{2,1} & \\ \vdots & X' \\ x_{n,1} & \end{array}\right)\left(\begin{array}{c|c} z_{1,1} & z_{1,2}\cdots z_{1,n} \\ \hline 0 & \\ \vdots & Z' \\ 0 & \end{array}\right)$$

with $x_{2,1}, ..., x_{n,1} \in \mathbb{Z}_p$, $z_{1,1} \in 1+p\mathbb{Z}_p$ and $z_{1,2}, ..., z_{1,n} \in p\mathbb{Z}_p$. Denote $\underline{z}$ to be the row vector $[z_{1,2}, ..., z_{1,n}]$, $\underline{x}$ to be the column vector $\begin{pmatrix} x_{2,1} \\ x_{3,1} \\ \vdots \\ x_{n,1} \end{pmatrix}$. Hence, we want to solve

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline (1-yE')\underline{a} & (1-yE')A' \end{array}\right) = \left(\begin{array}{c|c} z_{1,1} & \underline{z} \\ \hline z_{1,1}\underline{x} & \underline{x}\cdot\underline{z} + X'Z' \end{array}\right)$$

So we must have

1. $z_{1,1} = 1$,
2. $\underline{z} = 0$,
3. $z_{1,1}\underline{x} = \underline{x} = (1-yE')\underline{a}$ (using $z_{1,1} = 1$ from (1)),
4. $\underline{x}\cdot\underline{z} + X'Z' = X'Z' = (1-yE')A'$ (as $\underline{z} = 0$ from (2)).

By the induction hypothesis, we can find X' and Z' satisfying (4) with entries in as lemma 3.4. Also, (3) is of the form

$$\begin{pmatrix} 1 & & \\ & -y & \\ & \ddots & \\ & & 1 \end{pmatrix} \begin{pmatrix} a_{2,1} \\ a_{3,1} \\ \vdots \\ a_{n,1} \end{pmatrix} = \begin{pmatrix} x_{2,1} \\ x_{3,1} \\ \vdots \\ x_{n,1} \end{pmatrix}$$

Clearly, we can solve $x_{2,1}, .., x_{n,1}$ from the above matrix equation satisfying lemma 3.4 and in fact the solutions do not have any denominators.

So by induction we are reduced to the case $i = 1$, that is, when

$$(1 - yE_{i,j}) = \left(\begin{array}{c|c} 1 & 0 \cdots - y \cdots 0 \\ \hline 0 & \\ \vdots & \quad 1 \\ 0 & \end{array}\right)$$

Our goal is to solve, for X and Z, the following matrix equation:

$$(1 - yE_{1,j})A = XZ. \tag{3.22}$$

Expanding right hand side of 3.22, we obtain

$$\begin{aligned} \mathcal{B} = (b_{u,v})_{u,v} = XZ &= \Big(1 + \sum_{\substack{k\in[1,n] \\ l\in[1,k-1]}} x_{k,l}E_{k,l}\Big)\Big(\sum_{\substack{r\in[1,n] \\ s\in[r,n]}} z_{r,s}E_{r,s}\Big) \\ &= \sum_{\substack{r\in[1,n] \\ s\in[r,n]}} z_{r,s}E_{r,s} + \sum_{\substack{k\in[1,n] \\ r\in[1,k-1] \\ s\in[r,n]}} x_{k,r}z_{r,s}E_{k,s}. \end{aligned}$$

Therefore,

$$b_{u,v} = \begin{cases} \sum_{r=1}^{v} x_{u,r}z_{r,v}, & \text{if } u > v \\ z_{u,v} + \sum_{r=1}^{u-1} x_{u,r}z_{r,v}, & \text{if } u \leq v \end{cases} \tag{3.23}$$

Recall that our matrix $A = \sum_{k\geq l} a_{k,l}E_{k,l}$ is lower unipotent, that is, $a_{k,k} = 1$ for all $k \in [1, n]$ and $a_{k,l} = 0$ for $k < l$. Expanding the left hand side of 3.22, we obtain

$$\begin{aligned} (1 - yE_{1,j})A = (1 - yE_{1,j})(\sum_{k\geq l} a_{k,l}E_{k,l}) &= \sum_{k\geq l} a_{k,l}E_{k,l} - \sum_{l=1}^{j} ya_{j,l}E_{1,l}, \\ &= \sum_{\substack{k\in[1,n] \\ l\in[1,k] \\ k\neq 1}} a_{k,l}E_{k,l} + \sum_{l=2}^{j}(-ya_{j,l})E_{1,l} + (1 - ya_{j,1})E_{1,1}. \end{aligned}$$

Note that the 1^{st} row of the matrix $(1 - yE_{1,j})A$ is

$$\sum_{l=2}^{j}(-ya_{j,l})E_{1,l} + (1 - ya_{j,1})E_{1,1}.$$

From 3.22, the matrices $(1 - yE_{1,j})A$ and $\mathcal{B} = (b_{u,v})_{u,v}$ are equal. Thus, equating $b_{u,v}$ from 3.23 with the above expression of the matrix $(1 - yE_{1,j})A$, we obtain the following equations (with the convention that $x_{k,l} = 0$ for $k \leq l$ and $z_{r,s} = 0$ for $r > s$):

1. for $u \neq 1$ and $u > v$, $b_{u,v} = \sum_{r=1}^{v} x_{u,r}z_{r,v} = a_{u,v}$,
2. for $u \neq 1$ and $u = v$, $b_{u,v} = z_{u,u} + \sum_{r=1}^{u-1} x_{u,r}z_{r,v} = a_{u,u} = 1$,
3. for $u \neq 1$ and $u < v$, $b_{u,v} = z_{u,v} + \sum_{r=1}^{u-1} x_{u,r}z_{r,v} = a_{u,v} = 0$,
4. for $u = v = 1$, $b_{1,1} = z_{1,1} = 1 - ya_{j,1}$,

5. for $u = 1$ and $u < v$, $b_{1,v} = z_{1,v} = -ya_{j,v}$.

Note that in (5), for $v > j$, $b_{1,v} = -ya_{j,v} = 0$ (as A is lower unipotent). Setting $v = 1$ in formula (1), for $u \in [2, n]$, we obtain

$$x_{u,1} = \frac{a_{u,1}}{z_{1,1}} = \frac{a_{u,1}}{1 - ya_{j,1}} \text{ (as } z_{1,1} = 1 - ya_{j,1} \text{ from (4))}. \tag{3.24}$$

Now, let $C = (c_{k,l})_{k,l} = (1 - yE_{1,j})A$ and $\mathcal{B} = (b_{u,v})_{u,v}$ as above. We proceed by equating, in the 1^{st} stage, the first row of the matrix $\mathcal{B}$ with the first row of the matrix C, starting from the leftmost entry (i.e. given by equations (4) and (5) above) and solve for $z_{\star,\star}$. Then in the next stage (say stage $1 + \frac{1}{2}$) we equate the first column of the matrix $\mathcal{B}$ with the first column of the matrix C starting from the uppermost entry ($b_{2,1} = c_{2,1}$) and solve for $x_{\star,\star}$ (i.e. those given by 3.24). In the second stage we do the same with the second row and in the stage $2 + \frac{1}{2}$ we equate the second column of the matrix $\mathcal{B}$ with C (given by (1), (2) and (3)) and proceed like this until the last n^{th} stage. Our objective is to solve $x_{\star,\star}$ and $z_{\star,\star}$ while equating the matrix $\mathcal{B}$ with C and show (1), (2) and (3) of lemma 3.4. We prove this by induction.

Assume, by induction hypothesis, at the m^{th} and the stage $m + \frac{1}{2}$ ($1 \leq m < n$), that we have found $x_{k,l}$ for $k \in [2, n], l \in [1, m], k > l$ and $z_{r,s}$ for $r \in [1, m], s \in [1, n], r \leq s$ having the form (1), (2) and (3) of lemma 3.4. Then, at the $(m+1)^{th}$ stage we have to equate $b_{m+1,v} = c_{m+1,v}$ for $v \in [m + 1, n]$. Equating $b_{m+1,m+1} = c_{m+1,m+1}$, we deduce, by formula (2) after 3.23, that

$$\begin{aligned} z_{m+1,m+1} &= 1 - \sum_{r=1}^{m} x_{m+1,r} z_{r,m+1}, \\ &= 1 - \frac{yh_1(y,a)}{1 - yg_1(y,a)} \text{ (by induction hypothesis)}, \\ &= \frac{1 - y(h_1 + g_1)}{1 - yg_1}, \end{aligned}$$

for some polynomial functions $h_1(y, a)$ and $g_1(y, a)$ with integral coefficients in y and $a_{2,1}, a_{3,1}, a_{3,2}, ..., a_{n,n-1}$.

Similarly, equating $b_{m+1,v} = c_{m+1,v}$ for $v \in [m + 2, n]$, we obtain, by formula (3) after 3.23, that

$$\begin{aligned} z_{m+1,v} &= -\sum_{r=1}^{m} x_{m+1,r} z_{r,v}, \\ &= \frac{-yh_2(y,a)}{1 - yg_2(y,a)} \text{ (again by induction hypothesis)}, \end{aligned}$$

At the stage $(m + 1) + \frac{1}{2}$ we have to equate $b_{u,m+1} = c_{u,m+1}$ for all $u \in [m + 2, n]$. So, by formula (1) after 3.23, we get

$$\begin{aligned} x_{u,m+1} z_{m+1,m+1} &= a_{u,m+1} - \sum_{r=1}^{m} x_{u,r} z_{r,m+1}, \\ &= a_{u,m+1} - \frac{yh_3(y,a)}{1 - yg_3(y,a)} \text{ (again by induction hypothesis)}, \\ &= \frac{h_4(y,a)}{1 - yg_3(y,a)}, \end{aligned}$$

for some h_4 and g_3 with integral coefficients. Therefore,

$$x_{u,m+1} = \frac{h_4(y,a)}{1 - yg_3(y,a)} \cdot \frac{1}{z_{m+1,m+1}} = \frac{h_4(y,a)}{1 - yg_3(y,a)} \frac{1 - yg_1}{1 - y(h_1 + g_1)} = \frac{h_5(y,a)}{1 - yg_5(y,a)},$$

with polynomials h_5 and g_5 having integral coefficients. This completes our induction argument and finishes the proof of lemma 3.4.

□

Now, let $f \in I_{\text{loc}}$. Then, by lemma 3.4, the action of $(1 + yE_{i,j})$ on f is given by

$$(1 + yE_{i,j})f(A) = f(X)\chi(z_{1,1}^{-1}, ..., z_{n,n}^{-1}) \text{ (with } X \text{ and } z_{\star,\star} \text{ as in lemma 3.4)}. \tag{3.25}$$

Recall that for $|v| < 1$, we have

$$(1-v)^{-m} = \sum_{q=0}^{\infty} \binom{m+q-1}{q} v^q.$$

Assume now that $f \in \mathcal{A}(\mathbb{Z}^{\frac{n(n-1)}{2}}, K)$ is a globally analytic function. Thus, f is an element in the Tate algebra of U with $\frac{n(n-1)}{2}$ variables. In order to show that the action of $(1+yE_{i,j})$ on $f \in \mathcal{A}(U,K)$, given by equation 3.25, is globally analytic we have to show that

$$f \mapsto \prod_{r=1}^{n} \chi_r(z_{r,r}^{-1}) f(X)$$

is a globally analytic function in y with values in $\mathcal{A}(U,K)$.

Lemma 3.5. *If the action $f \to g$, $g(A) = f(X)$ where $A = XZ$ is globally analytic, then $f \to \prod_{r=1}^{n} \chi_r(z_{r,r}^{-1}) g$ is globally analytic.*

Proof. With 3.16, our character χ is analytic. Hence,

$$\begin{aligned} \chi_r(z_{r,r}^{-1}) &= \chi_r\Big(\frac{1-yg_{r,r}(y,a)}{1-yh_{r,r}(y,a)}\Big) && (\text{ from lemma 3.4}) \\ &= \sum_{n=0}^{\infty} c_n \Big(\frac{1-yg_{r,r}(y,a)}{1-yh_{r,r}(y,a)}\Big)^n && (\text{ for } |c_n| \to 0). \end{aligned}$$

We are reduced to show that $(y,a) \to \frac{1-yg_{r,r}(y,a)}{1-yh_{r,r}(y,a)}$ is analytic in y. Since $y \in p\mathbb{Z}_p$, this is true because

$$\frac{1-yg_{r,r}(y,a)}{1-yh_{r,r}(y,a)} = (1-yg_{r,r}(y,a))\Big(\sum_{n=0}^{\infty}(yh_{r,r}(y,a))^n\Big).$$

Hence, we have shown the lemma. □

Therefore, with lemma 3.5, to prove that the action of $(1+yE_{i,j})$ on $f \in \mathcal{A}(U,K)$, given by equation 3.25, is globally analytic, we only need to show that the action $f \to g$, $g(A) = f(X)$ where $A = XZ$ is globally analytic.

Lemma 3.6. *The action $f \to g$, $g(A) = f(X)$ where $A = XZ$ is globally analytic.*

Proof. Recall that the lower unipotent matrix X is $((x_{k,l})_{k,l})$ with $x_{k,l} = \frac{h_{k,l}(y,a)}{1-yg_{k,l}(y,a)}$ given by lemma 3.4. Write

$$\begin{aligned} x_{k,l} &= h_{k,l}(y,a) \sum_{n=0}^{\infty} y^n g_{k,l}(y,a)^n \\ &= \sum_{n=0}^{\infty} y^n g_{n,k,l}(y,a). \end{aligned}$$

Since f is analytic, $f = \sum_\nu c_\nu a^\nu$, $a^\nu = \prod_{k>l} a_{k,l}^{\nu_{k,l}}$. The norm $|c_\nu| \to 0$ as $\nu \to \infty$. Then,

$$f(X) = f((x_{k,l})_{k,l}) = \sum_{\nu} c_\nu \prod_{\substack{k,l \\ k>l}} (\sum_{n=0}^{\infty} y^n g_{n,k,l}(y,a))^{\nu_{k,l}}.$$

As

$$(\sum_{n=0}^{\infty} y^n g_n)^M = \sum_{v \geq 0} y^v \sum_{v_1+\cdots+v_M=v} g_{v_1} \cdots g_{v_M},$$

we obtain that

$$f(X) = \sum_{\nu=(\nu_{k,l})} c_\nu \prod_{k,l} \sum_{v \geq 0} y^v \Big(\sum_{v_1+\cdots+v_{\nu_{k,l}}=v} g_{v_1,k,l} \cdots g_{v_{\nu_{k,l}},k,l} \Big).$$

Define $a_{k,l}(v) = (\sum_{v_1+\cdots+v_{\nu_{k,l}}=v} g_{v_1,k,l}\cdots g_{v_{\nu_{k,l}},k,l})$ then,

$$\begin{aligned} f(X) &= \sum_{\nu=(\nu_{k,l})} c_\nu \prod_{k,l}\sum_{v\geq 0} y^v a_{k,l}(v) \\ &= \sum_{\nu=(\nu_{k,l})} c_\nu \sum_{v\geq 0}^{\infty} y^v \sum_{\sum v_{k,l}=v} \prod_{k,l} a_{k,l}(v_{k,l}) \\ &= \sum_{\nu=(\nu_{k,l})} c_\nu \sum_{v\geq 0}^{\infty} y^v \sum_{\sum v_{k,l}=v} \prod_{k,l} \sum_{v_1+\cdots+v_{\nu_{k,l}}=v_{k,l}} g_{v_1,k,l}\cdots g_{v_{\nu_{k,l}},k,l}. \end{aligned}$$

The coefficient of y^v is

$$\sum_{\nu=(\nu_{k,l})} c_\nu \sum_{\sum v_{k,l}=v} \prod_{k,l} \sum_{v_1+\cdots+v_{\nu_{k,l}}=v_{k,l}} g_{v_1,k,l}\cdots g_{v_{\nu_{k,l}},k,l} := \sum_{\nu=(\nu_{k,l})} c_\nu s_\nu$$

where

$$s_\nu := \sum_{\sum v_{k,l}=v} \prod_{k,l} \sum_{v_1+\cdots+v_{\nu_{k,l}}=v_{k,l}} g_{v_1,k,l}\cdots g_{v_{\nu_{k,l}},k,l}.$$

So $f(X) = \sum_{v=0}^{\infty} y^v f_v$ with $f_v = \sum_\nu c_\nu s_\nu$. Moreover, $|y| < 1$, the p-adic analytic variable is $y' = y/p$, so

$$f(X) = \sum_{v=0}^{\infty} (y')^v (p^v f_v)$$

yields a convergent expression in $\mathcal{A}(U, K)$. This completes the proof. □

This shows the analyticity of the action given by 3.25. So we have shown

Lemma 3.7. *For $y \in p\mathbb{Z}_p$ and $i < j$, the action of the upper unipotent (rigid-analytic) 1-parameter subgroup $(1 + yE_{i,j})$ of G on $f \in \mathcal{A}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K)$, given by 3.25 is an analytic action.*

Note that, by section 3.3.1, the vector space of locally analytic functions of the principal series

$$\mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}} = \{f \in \mathcal{A}_{\mathrm{loc}}(B, K) : f(gb) = \chi(b^{-1})f(g), b \in P_0, g \in B\}$$

is isomorphic to the vector space of the locally analytic functions
$I_{\mathrm{loc}} \cong \mathcal{A}_{\mathrm{loc}}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K)$. Denote by $\mathrm{ind}_{P_0}^B(\chi)$ the space of globally analytic vectors of $\mathrm{ind}_{P_0}^B(\chi)_{\mathrm{loc}}$ which is $\mathcal{A} := \mathcal{A}(\mathbb{Z}_p^{\frac{n(n-1)}{2}}, K)$.

Also, the representation on $\mathcal{A}$ is admissible: indeed, $\mathcal{A}$ is a subspace of $\mathcal{A}(G)$ defined by the conditions $f(gb) = \chi(b^{-1})f(g)$ (f is then analytic on G since χ is so) and this is a closed subspace. Thus by lemmas (3.1- 3.3) and lemma 3.7 we have shown the following theorem.

Theorem 3.8. *Assume $p > n + 1$. Let χ be an analytic character of T_0 (cf. 3.16). The action of G on the induced principal series $\mathrm{ind}_{P_0}^B(\chi)$ is a globally analytic action. Moreover, the globally analytic representation of G on $\mathrm{ind}_{P_0}^B(\chi)$ is admissible in the sense of Emerton ([Eme17], [Clo16, sec. 2.3]).*

Recall that $\chi = (\chi_1, .., \chi_n)$ where $\chi_i(1 + pu_i) = e^{c_i \log(1+pu_i)}$ for $c_i \in K$, u_i close to 0, $i \in [1, n]$. Also, recall from 3.9 that $f \in \mathcal{A}$ implies that $f(A) = \sum_{\nu\in\mathbb{N}^d} c_\nu a^\nu$ with $|c_\nu| \to 0$ as $|\nu| = \nu_{2,1} + \nu_{3,1} + \cdots + \nu_{n,n-1} \to \infty$.

In the following, we will have conditions on the character χ such that the globally analytic representation of G on $\mathcal{A}$ is irreducible.

Let μ be the linear form from the Lie algebra of the torus T_0 to K given by

$$\mu = (-c_1, ..., -c_n) : Diag(t_1, ..., t_n) \mapsto \sum_{i=1}^{n} -c_i t_i$$

where $t = (t_i) \in \mathrm{Lie}(T_0)$. For negative root $\alpha = (i, j), i > j$, let $H_{(i,j)}$ be the matrix $E_{i,i} - E_{j,j}$ where $E_{i,i}$ is the standard elementary matrix. Let $\Phi, \Phi^-, \Phi^+, \Pi$ be the roots, negative roots, positive roots and simple roots respectively associated to G.

Theorem 3.9. *Let c_i's satisfy 3.16, that is, χ is analytic, and $p > n+1$, then the globally analytic representation $\mathcal{A} \cong \mathrm{ind}_{P_0}^{B}(\chi)$ of G is topologically irreducible if and only if for all $\alpha = (i,j) \in \Phi^-$, $-\mu(H_{\alpha=(i,j)}) + i - j \notin \{1, 2, 3, ...\}$.*

Assume $\mathcal{X} \subset \mathcal{A}$ is a closed G-invariant subspace. Consider $f \in \mathcal{A}$. Then, from 3.9,

$$f = \sum_{\nu \in \mathbb{N}^d} c_\nu a^\nu$$

where $d = \frac{n(n-1)}{2}, c_\nu \in K$, $|c_\nu| \to 0$ as $|\nu| := \sum_{\alpha \in \Phi^-} \nu_\alpha \to \infty$.
Here, $\nu = (\nu_\alpha, \alpha \in \Phi^-) \in \mathbb{N}^d$ and $a_\nu = \prod_{\alpha \in \Phi^-} a_\alpha^{\nu_\alpha}$. In some arguments we will have to order the exponents ν_α's. We use the following lexicographic order. Let $\alpha = (i,j)$ and $\alpha' = (k,l)$. Then ν_α comes before $\nu_{\alpha'}$ if and only if $i < k$ or $i = k$ and $j < l$, i.e. $\nu = (\nu_{2,1}, \nu_{3,1}, \nu_{3,2}, ..., \nu_{n,n-1})$ (see also the discussion before equation 3.9). For $N \geq 0$, let τ_N be the natural truncation

$$\mathcal{A} \to K[a]_N := \oplus_{|\nu| \leq N} K a^\nu.$$

The later space is the space of polynomials in several variables with total degree $\leq N$. As τ_N is equivariant under the action of the diagonal subgroup of G given by formulas 3.5 and 3.6 and the associated characters of the diagonal torus of G are linearly independent, $\tau_N(\mathcal{X})$ is a direct sum of monomials given by

$$\tau_N(\mathcal{X}) := \mathcal{X}_N = \{ \sum_{\nu \in M_N} c_\nu a^\nu \}$$

where M_N is the set of exponents of a of elements in $\mathcal{X}_N$. If $N \leq N'$ and $\nu \in M_N$, then by surjectivity

$$K[a]_{N'} \twoheadrightarrow K[a]_N,$$

we obtain $\mu \in M_{N'}$. Conversely, $\nu \in M_{N'}$ and $|\nu| \leq N$ implies $\nu \in M_N$. Therefore, the multi-sets M_N and $M_{N'}$ are compatible and thus there exists M (the exponents of elements of $\mathcal{X}$) such that

1. $f \in \mathcal{X} \implies c_\nu = 0$ for all $\nu \notin M$.
2. If $\nu \in M$, $a^\nu \in \tau_N(\mathcal{X})$ for all $N \geq |\nu|$, thus there exists

$$f := a^\nu + \sum_{|r| > N} c_r a^r \in \mathcal{X}$$

(here $r = (r_\alpha, \alpha \in \Phi^-) \in \mathbb{N}^d, |c_r| \to 0$) .

For $\alpha \in \Phi^-$, let $Y_\alpha \in \mathfrak{g} = \mathrm{Lie}(G)$ be the infinitesimal generator associated to the unipotent subgroup $1 + yE_\alpha, y \in \mathbb{Z}_p$, E_α being the standard elementary matrix at α.

Lemma 3.10. *The multi-index $0 \in M$.*

Proof. $M \neq$ null, because if so, then $\mathcal{X} = 0$, which is not true by assumption. Now if $\nu = (\nu_\alpha, \alpha \in \Phi^-) \in M$, then by (2) above

$$f = a^\nu + \sum_{|r| > N} c_r a^r \in \mathcal{X}$$

(here $N \geq |\nu|, r \in \mathbb{N}^d$). By 3.20, the action of $Y_\beta = Y_{(i,j)}$ on f (where $\beta = (i,j) \in \Phi^-$ is fixed) is

given by

$$Y_\beta(f) = \frac{d}{dy}\Big|_{y=0}\Big((\prod_{\substack{\alpha=(u,v)\\ u=i \Longrightarrow v>j}} a_\alpha^{\nu_\alpha})(\prod_{k=1}^{j}(a_{i,k}+ya_{j,k})^{\nu_{i,k}})$$

$$+\sum_{|r|>N} c_r(\prod_{\substack{\alpha=(u,v)\\ u=i \Longrightarrow v>j}} a_\alpha^{r_\alpha})(\prod_{k=1}^{j}(a_{i,k}+ya_{j,k})^{r_{i,k}})\Big)$$

$$= \prod_{\substack{\alpha=(u,v)\\ u=i \Longrightarrow v>j}} a_\alpha^{\nu_\alpha}(\sum_{l=1}^{j}\nu_{i,l}a_{j,l}a_{i,l}^{\nu_{i,l}-1}\prod_{\substack{k\in[1,j]\\ k\neq l}} a_{i,k}^{\nu_{i,k}})$$

$$\sum_{|r|>N} c_r \prod_{\substack{\alpha=(u,v)\\ u=i \Longrightarrow v>j}} a_\alpha^{r_\alpha}(\sum_{l=1}^{j} r_{i,l}a_{j,l}a_{i,l}^{r_{i,l}-1}\prod_{\substack{k\in[1,j]\\ k\neq l}} a_{i,k}^{r_{i,k}})$$

$$= A + \sum_{|r|>N} c_r B$$

The first term in the R.H.S of the above equation is

$$A := \prod_{\substack{\alpha=(u,v)\\ u=i \Longrightarrow v>j}} a_\alpha^{\nu_\alpha}(\sum_{l=1}^{j}\nu_{i,l}a_{j,l}a_{i,l}^{\nu_{i,l}-1}\prod_{\substack{k\in[1,j]\\ k\neq l}} a_{i,k}^{\nu_{i,k}}) = \sum_{l=1}^{j}\nu_{i,l}a_{j,l}^{\nu_{j,l}+1}a_{i,l}^{\nu_{i,l}-1}\prod_{\substack{\alpha\neq(i,l)\\ \alpha\neq(j,l)}} a_\alpha^{\nu_\alpha}$$

and

$$B = \prod_{\substack{\alpha=(u,v)\\ u=i \Longrightarrow v>j}} a_\alpha^{r_\alpha}(\sum_{l=1}^{j} r_{i,l}a_{j,l}a_{i,l}^{r_{i,l}-1}\prod_{\substack{k\in[1,j]\\ k\neq l}} a_{i,k}^{r_{i,k}}) = \sum_{l=1}^{j} r_{i,l}a_{j,l}^{r_{j,l}+1}a_{i,l}^{r_{i,l}-1}\prod_{\substack{\alpha\neq(i,l)\\ \alpha\neq(j,l)}} a_\alpha^{r_\alpha}$$

Notice that the monomials in B has total degree $|r|$ except the term (when $l=j$) $r_{i,j}a_{i,j}^{r_{i,j}-1}\prod_{\alpha\neq(i,j)} a_\alpha^{r_\alpha}$ (note that $a_{j,j}=1$ by convention) which has total degree $|r|-1$.

As $Y_{(i,j)}(f)\in\mathcal{X}$, we see that $(\nu_\alpha, \nu_{i,j}-1, \alpha\in\Phi^-, \alpha\neq(i,j))\in M$; these are the exponents when we take $l=j$ in A. This shows that if $M\neq$ null, then $0\in M$ because we can descend the $v_{i,j}$'s successively for every negative root (i,j) and this completes the proof of lemma 3.10. □

Lemma 3.11. *The constants $a^0\in\mathcal{X}$.*

Proof. Let $T_k\in\mathfrak{g}$ be the infinitesimal generator associated to the diagonal subgroup $Diag(1,...,t_k,...,1)$, $t_k\in 1+p\mathbb{Z}_p$, t_k is at the (k,k)-th place. By lemma 3.10, $0\in M$. This implies that

$$f = c_0 + \sum_{|r|>0} c_r a^r \in \mathcal{X}$$

($c_0\neq 0$). We will essentially follow the proof given by Clozel for $GL(2)$. By equation 3.10, from the action of $Diag(1,...,t_k,...,1)$ on f, the function obtained from $T_k(f)$,

$$\sum_{|r|>0} c_r(\sum r_\delta - \sum r_\beta)a^r \in \mathcal{X} \tag{3.26}$$

where $\sum r_\delta$ is $\sum_{\substack{\delta=(i,k)\\ i\in[k+1,n]}} r_\delta$ and $\sum r_\beta$ is $\sum_{\substack{\beta=(k,j)\\ j\in[1,k-1]}} r_\beta$.

The function obtained from $T_k^{p-1}(f)$,

$$\sum_{|r|>0} c_r(\sum r_\delta - \sum r_\beta)^{p-1}a^r \in \mathcal{X}.$$

This implies that

$$E_k f := c_0 + \sum_{|r|>0} c_r(1-(\sum r_\delta - \sum r_\beta)^{p-1})a^r \in \mathcal{X}.$$

If $p \mid \sum r_\delta - \sum r_\beta$, then $(1-(\sum r_\delta - \sum r_\beta)^{p-1})^l \to 1$ as $l \to \infty$. If $p \nmid \sum r_\delta - \sum r_\beta$, then $(1-(\sum r_\delta - \sum r_\beta)^{p-1})^l \to 0$ as $l \to \infty$. Then

$$A_{k,1}f := c_0 + \sum_{\substack{|r|>0 \\ p|\sum r_\delta - \sum r_\beta}} c_r a^r \in \mathcal{X}.$$

Similar to 3.26, applying now, the transformation T_k on $A_{k,1}f$, dividing by p, and iterating all the above steps, we see that

$$A_{k,2}(f) := c_0 + \sum_{\substack{|r|>0 \\ p^2|\sum r_\delta - \sum r_\beta}} c_r a^r \in \mathcal{X}.$$

Iterating again and again s times, for $s \in \mathbb{N}$, we obtain

$$A_{k,s}(f) := c_0 + \sum_{\substack{|r|>0 \\ p^s|\sum r_\delta - \sum r_\beta}} c_r a^r \in \mathcal{X}.$$

This implies, for $s \in \mathbb{N}$,

$$(\prod_{k=1}^{n} A_{k,s})(f) = c_0 + Q_s(f) \in \mathcal{X} \tag{3.27}$$

where $Q_s(f) = \sum c_r a^r$ where the sum runs over all $r = (r_\alpha, \alpha \in \Phi^-)$ with $|r| > 0$ such that for all $k \in [1,n]$:

$$p^s \mid \sum_{\substack{\delta=(i,k) \\ i\in[k+1,n]}} r_\delta - \sum_{\substack{\beta=(k,j) \\ j\in[1,k-1]}} r_\beta.$$

We need to show that $Q_s(f) \to 0$ as $s \to \infty$, i.e., we have to show that

$$\forall N_\epsilon, \exists S, \text{ such that } \forall s > S, val_p(c_r) > N_\epsilon, \forall r \in \mathbb{N}^d \text{ such that } |r| > 0, \tag{3.28}$$

$$\text{and } p^s \mid \Big(\sum_{\substack{\delta=(i,k) \\ i\in[k+1,n]}} r_\delta - \sum_{\substack{\beta=(k,j) \\ j\in[1,k-1]}} r_\beta \Big) \qquad \text{for all } k \in [1,n]. \tag{3.29}$$

But as f is globally analytic, $|c_r| \to 0$ as $|r| = \sum_{\alpha\in\Phi^-} r_\alpha \to \infty$, which means that

$$\forall N_\epsilon, \exists S' \text{ such that whenever } |r| > S' \tag{3.30}$$

$$\text{we have } val_p(c_r) > N_\epsilon. \tag{3.31}$$

Any S such that $p^S > S'$ will work in 3.28. This is because, take any r, such that $|r| > 0$ and

$$p^s \mid \Big(\sum_{\substack{\delta=(i,k) \\ i\in[k+1,n]}} r_\delta - \sum_{\substack{\beta=(k,j) \\ j\in[1,k-1]}} r_\beta \Big) \qquad \text{for all } k \in [1,n]$$

(i.e. satisfying equation 3.29) with $s > S$ (cf. (3.28)).

For $k = 1$, (3.29) implies $p^s \mid r_{2,1}+r_{3,1}+r_{4,1}+\cdots+r_{n,1}$ which means $r_{2,1}+r_{3,1}+r_{4,1}+\cdots+r_{n,1} \geq p^s > S'$ except when $r_{2,1} = r_{3,1} = r_{4,1} = \cdots = r_{n,1} = 0$. If this happens, then consider (3.29) with $k = 2$, i.e. $p^s \mid r_{3,2} + r_{4,2} + \cdots + r_{n,2} - (r_{2,1} = 0)$, i.e. $r_{3,2} + r_{4,2} + \cdots + r_{n,2} \geq p^s > S'$ except when $r_{3,2} = r_{4,2} = \cdots = r_{n,2} = 0$. Repeating this process, since we have started with an r such that $|r| > 0$, we see that any r as in (3.29), with $|r| > 0$, satisfies $|r| > S'$ for all $s > S$ and this by (3.30) and (3.31) implies that $val_p(c_r) > N_\epsilon$ which was the desired condition in (3.28). (Here S is chosen such that $p^S > S'$). This shows that $Q_s(f) \to 0$ as $s \to \infty$ which gives $c_0 \in \mathcal{X}$ (cf. (3.27)). This completes the proof of lemma 3.11. □

In the following, we complete the proof of Theorem 3.9 which was to find conditions such that the globally analytic representation $\mathcal{A}$ of G is topologically irreducible. It uses an argument concerning the Verma modules and the condition of irreducibility of $\mathcal{A}$ comes from a result of Bernstein-Gelfand determining the condition of irreducibility of that Verma module.

With notations as in section 3.3.1, let $\mathfrak{g} = \mathrm{Lie}(G), \mathfrak{h} = \mathrm{Lie}(T_0), \mathfrak{b}$ (resp. $\mathfrak{b}^-$) be the upper (resp. lower) triangular Borel subalgebra containing $\mathfrak{h}$. Let $\mathfrak{u}^- = \mathrm{Lie}(U)$. Recall that here c_i's $\in K$ are such that $\chi_i(t) = t^{c_i}$, for $t \to 1$. Let

$$V_{-\mu} := U(\mathfrak{g}) \otimes_{U(\mathfrak{b}^-)} K$$

be the Verma module where $U(\mathfrak{b}^-)$ acts on K via the action of $\mathfrak{b}^- = \mathfrak{u}^- \oplus \mathfrak{h}, \mathfrak{u}^-$ acting trivially and $\mathfrak{h}$ via

$-\mu \in \mathfrak{h}^\star = \mathrm{Hom}(\mathfrak{h}, K)$ given by

$$-\mu = (c_1, ..., c_n) : Diag(t_1, ..., t_n) \mapsto \sum_{i=1}^{n} c_i t_i \tag{3.32}$$

where $t = (t_i) \in \mathfrak{h}, U(\mathfrak{g})$ is the universal enveloping algebra of $\mathfrak{g}$. (Note that Dixmier has a different normalization for the Verma module [Dix77, section 7.1.14]).

Let $\mathcal{A}_{\mathrm{fin}}$ be the set of polynomials within the rigid analytic functions $\mathcal{A}$. For $k \in [1, n]$, let $T_k \in \mathfrak{h}$ be the infinitesimal generator associated to the one parameter diagonal subgroup $Diag(1, ..., t_k, ..., 1)$, $t_k \in 1 + p\mathbb{Z}_p$, t_k is at the (k, k)-th place and $f = a^r \in \mathcal{A}_{\mathrm{fin}}$. The elements T_k form a basis of $\mathfrak{h}$. By equations 3.8 and 3.10, the action of $Diag(1, ..., t_k, ..., 1)$ on f is given by

$$Diag(1, ..., t_k, ..., 1)(f) = \Big((\prod_{\substack{\alpha=(u,v)\\ u,v\neq k}} a_\alpha^{r_\alpha})(\prod_{\substack{\delta=(i,k)\\ i\in[k+1,n]}} a_\delta^{r_\delta} t_k^{r_\delta})(\prod_{\substack{\beta=(k,j)\\ j\in[1,k-1]}} a_\beta^{r_\beta} t_k^{-r_\beta}) \Big) \Big(\chi_k(t_k) \Big)$$

As $\chi_k(t_k) = t_k^{c_k}$, so the action of T_k on f is

$$T_k \cdot f = c_k a^r + (\sum_{\substack{\delta=(i,k)\\ i\in[k+1,n]}} r_\delta - \sum_{\substack{\beta=(k,j)\\ j\in[1,k-1]}} r_\beta) a^r \tag{3.33}$$

$$= (c_k + \sum_{\substack{\delta=(i,k)\\ i\in[k+1,n]}} r_\delta - \sum_{\substack{\beta=(k,j)\\ j\in[1,k-1]}} r_\beta) a^r \tag{3.34}$$

$$= (-\mu - \sum_{i=1}^{d} \alpha_i r_{\alpha_i})(T_k) a^r \tag{3.35}$$

Here α_i's are the negative roots.

Thus if $H \in \mathfrak{h}$, then

$$H \cdot a^r = (-\mu - \sum_{i=1}^{d} \alpha_i r_{\alpha_i})(H) a^r \tag{3.36}$$

Decomposing $\mathcal{A}_{\mathrm{fin}} = \oplus_{\xi \in \mathfrak{h}^\star} \mathcal{A}_{\mathrm{fin}}(\xi)$ in the form of $\mathfrak{h}$- eigenspaces, we see from 3.36 that the monomials a^r are $\mathfrak{h}$-finite and and the dimensions of eigenspaces of $\mathcal{A}_{\mathrm{fin}}$ under $\mathfrak{h}$ are finite: The eigenvectors are of the form $\xi \in -\mu - \sum_{i=1}^{d} \mathbb{N}\alpha_i \in \mathfrak{h}^\star$ and the multiplicity $\mathrm{mult}(\xi) = \dim \mathcal{A}(\xi)$ of ξ equals

$$\dim \mathcal{A}(\xi) = \mathrm{mult}(\xi) = \{\text{number of families } (r_{\alpha_i}) \in \mathbb{N}^d \mid \xi = -\mu - \sum_{i=1}^{d} r_{\alpha_i} \alpha_i\}, \tag{3.37}$$

which is finite.

With $f_0 = 1 \in \mathcal{A}_{\mathrm{fin}}$, $H \cdot f_0 = -\mu(H) f_0$ and the action $\mathfrak{u}^- \cdot f_0 = 0$ because the action of any element of $\mathfrak{u}^-$ on f_0 is given by derivation (cf. proof of Lemma 3.10). So, the map $u \to u \cdot f_0$ for $u \in \mathfrak{g}$ induces a $\mathfrak{g}$-homomorphism

$$\phi : V_{-\mu} \to \mathcal{A}, \tag{3.38}$$

where $V_{-\mu} := U(\mathfrak{g}) \otimes_{U(\mathfrak{b}^-)} K$.

Moreover, $v \in V_{-\mu}$ implies v is $\mathfrak{h}$ - finite (cf. [Dix77, Chapter 7]). This gives $\phi(v) \in \mathcal{A}$ is $\mathfrak{h}$ - finite which means that $\phi(v) \in \mathcal{A}_{\mathrm{fin}}$. This is because equation 3.36 gives, by continuity, that $f \in \mathcal{A}$, $f = \sum_{r=(r_{\alpha_i})} c_r a^r$ implies

$$H \cdot f = \sum_{r=(r_{\alpha_i})} (-\mu - \sum_{i=1}^{d} r_{\alpha_i} \alpha_i)(H) c_r a^r. \tag{3.39}$$

Then $H \cdot f = \lambda f$ implies $\lambda = (-\mu - \sum_{i=1}^{d} r_{\alpha_i}\alpha_i)(H)$ if $c_r \neq 0$. Therefore the cardinality of the set $\{c_r \neq 0\}$ is finite, the $\mathfrak{h}$-finite vectors of $\mathcal{A}$ are just $\mathcal{A}_{\text{fin}}$.

The map $\phi : V_{-\mu} \to \mathcal{A}_{\text{fin}}$ in 3.38 is clearly non-zero because the vector $1 \in V_{-\mu}$ goes to f_0.

Lemma 3.12. *If the Verma module $V_{-\mu}$ is irreducible then the globally analytic G- representation $\mathcal{A}$ is irreducible.*

Proof. Suppose that the Verma module $V_{-\mu}$ is irreducible. Then the map $\phi : V_{-\mu} \to \mathcal{A}_{\text{fin}}$ is injective. Also, by 3.37, under the action of $\mathfrak{h}$, since the eigenvectors of $V_{-\mu}$ and $\mathcal{A}_{\text{fin}}$ and their multiplicities match, that is, $\dim \mathcal{A}(\xi) = \dim \mathcal{A}_{\text{fin}}(\xi) = \dim V_{-\mu}(\xi)$, we deduce that ϕ is an isomorphism.

Indeed the dimension of $\dim \mathcal{A}(\xi)$ is given by 3.37, on the other hand, using that our Verma module $V_{-\mu}$ is defined by $\mathfrak{b}^-$ and $-\mu$ (rather than $\lambda - \rho^-$ as in Dixmier's parametrization [Dix77, 7.1.4]), Dixmier's formula [Dix77, 7.1.6] yields

$$\dim V_{-\mu}(\xi) = \text{mult}(\xi) = \{\text{number of families } (r_{\alpha_i}) \in \mathbb{N}^d \mid \xi = \lambda - \rho^- - \sum_{i=1}^{d} r_{\alpha_i}\alpha_i\}$$

where $\rho^- = \frac{1}{2}\sum_{\alpha \in \Phi^-} \alpha$ is half the sum of negative roots (because notice that we have used $\mathfrak{b}^-$ to define the Verma module instead of Dixmier's $\mathfrak{b}^+$). We easily see that the above dimension $\dim V_{-\mu}(\xi)$ is equivalent to $\dim \mathcal{A}(\xi)$ (3.37) with $\lambda - \rho^- = -\mu$.

So $V_{-\mu} \cong \mathcal{A}_{\text{fin}}$. Suppose $\mathcal{X}$ is a nonzero closed subspace of $\mathcal{A}$. Then by lemma 3.11, we have $1 \in \mathcal{X}$. This gives $\mathcal{A}_{\text{fin}} = U(\mathfrak{g}) \cdot 1 \subset \mathcal{X}$. Since $\mathcal{X}$ is closed $\mathcal{X} = \mathcal{A}$. □

Now we prove the converse of Lemma 3.12.

Recall that a closed subspace of $\mathcal{A}$ is G-invariant if and only if it is invariant by $\mathfrak{g}$ ([Clo16, Proposition 2.4]). Moreover, it follows from the definition of globally analytic representations (compare [Clo16, Section 2.2]) that the action of $\mathfrak{g}$ on $\mathcal{A}$ is continuous. If $V \subset \mathcal{A}_{\text{fin}}$ is invariant by $\mathfrak{g}$, it follows that its closure $\overline{V}$ is G-invariant.

Recall that $\mathcal{A}_{\text{fin}}$ is the set of $\mathfrak{h}$-finite vectors in $\mathcal{A}$. In particular, if $\mathcal{X} \subset \mathcal{A}$ is closed, the space $\mathcal{X}_{\mathfrak{h}-\text{fin}}$ of $\mathfrak{h}$-finite vectors in $\mathcal{X}$ is $\mathcal{X} \cap \mathcal{A}_{\text{fin}}$.

Lemma 3.13. *Assume $V \subset \mathcal{A}_{\text{fin}}$ is invariant by $\mathfrak{g}$. Then $V = \overline{V} \cap \mathcal{A}_{\text{fin}} = \overline{V}_{\mathfrak{h}-\text{fin}}$.*

Proof. By 3.37, $\mathcal{A}(\xi)$ is the subspace of the Tate algebra spanned by a finite number of monomials a^r. In particular, the obvious projection $p_\xi : \mathcal{A} \to \mathcal{A}(\xi)$ is continuous. Assume $v \in \overline{V} \cap \mathcal{A}_{\text{fin}}$. Thus $v \in \oplus_\xi \mathcal{A}(\xi)$ (finite sum of finite-dimensional subspaces) and $v = \lim v_m, v_m \in V$. If P is the projection on $\oplus_\xi \mathcal{A}(\xi)$, $v = Pv = \lim Pv_m$. But $Pv' \in V \cap \oplus_\xi \mathcal{A}(\xi)$ for any $v' \in V$. Thus, $v \in V$, as a limit in a finite-dimensional space. □

Lemma 3.13 obviously gives the following Corollary.

Corollary 3.14. *Suppose V is a non-zero proper subspace of $\mathcal{A}_{\text{fin}}$ stable by $\mathfrak{g}$. Then $\overline{V}$ is a non-zero proper closed G-invariant subspace of $\mathcal{A}$.*

Lemma 3.15. *If the globally analytic G- representation $\mathcal{A}$ is irreducible then the Verma module $V_{-\mu}$ is irreducible.*

Proof. Let $W \subset \mathcal{A}_{\text{fin}}$ be the image of $V_{-\mu}$ by ϕ. Then $W \neq 0$. If $\mathcal{A}$ is an irreducible G-module, $W = \mathcal{A}_{\text{fin}}$ by corollary 3.14. Thus, we have a surjective map $\phi : V_{-\mu} \to \mathcal{A}_{\text{fin}}$. But, as we noticed, the dimensions of $V_{-\mu}(\xi)$ and of $\mathcal{A}_{\text{fin}}(\xi)$ coincide. This implies that ϕ is an isomorphism. On the other hand (again by the corollary 3.14) W is irreducible. Thus, $V_{-\mu}$ is irreducible.

□

Now we determine the condition when the Verma module $V_{-\mu}$ is irreducible. Recall that

$$\mu = (-c_1, ..., -c_n) : Diag(t_1, ..., t_n) \mapsto \sum_{i=1}^{n} -c_i t_i$$

where $t = (t_i) \in \mathfrak{h}$. For negative root $\alpha = (i, j), i > j$, let $H_{\alpha=(i,j)}$ be the matrix $E_{i,i} - E_{j,j}$ where $E_{i,i}$ is the standard elementary matrix.

Lemma 3.16. *The Verma module $V_{-\mu}$ is irreducible if and only if for all $\alpha = (i,j) \in \Phi^-$, $(-\mu)(H_{\alpha=(i,j)}) + i - j \notin \{1,2,3,...\}$.*

Proof. Let $\rho^- = \frac{1}{2}\sum_{\alpha\in\Phi^-}\alpha$. For $\alpha = (i,j) \in \Phi^-$, $H_\alpha = H_{i+1,i} + \cdots + H_{j,j-1}$ and $\rho^-(H_{k+1,k}) = 1$. This gives that $\rho^-(H_{\alpha=(i,j)}) = i-j$. By Theorem 7.6.24 of [Dix77], the condition of irreducibility of our $V_{-\mu}$ is $(-\mu+\rho^-)(H_\alpha) \notin \{1,2,3,...\}$ for all negative roots $\alpha \in \Phi^-$ (This is because Dixmier's $\mathfrak{b}^+$ is our $\mathfrak{b}^-$ and so we have to work with negative roots.) This gives the condition $(-\mu)(H_\alpha)+i-j \notin \{1,2,3,...\}$ □

Lemma 3.16, Lemma 3.15, and Lemma 3.12 together proves Theorem 3.9. [Q.E.D]

3.3.2 Base change of the principal series representation

With L an unramified finite extension of $\mathbb{Q}_p$. All the arguments of section 3.3.1 extend automatically to the group $G(L)$. As L is unramified, the conditions on the character χ to be analytic, that is, those given by 3.16, remain unchanged. Moreover, note that the representation $\mathcal{A}(B_1^{\frac{n(n-1)}{2}}, K)$ (where now $B_1^{\frac{n(n-1)}{2}}$ is seen as a product of $\frac{n(n-1)}{2}$ closed rigid balls of radius 1 as an L-analytic space) given by the lemmas 3.2, 3.3, 3.7 are L-analytic. The restriction of $\mathcal{A}(B_1^{\frac{n(n-1)}{2}}, K)$ to $G(\mathbb{Q}_p)$ is simply the previous representation. Indeed, the representation of $G(L)$ is obtained from the representation of $G(\mathbb{Q}_p)$ by holomorphic base change (cf. section 3.2.2 and [Clo16, prop. 3.1]). Denote by $I_{\mathbb{Q}_p}(\chi)$ and $I_L(\chi)$, respectively, the two *globally analytic* representations (the character χ is defined by the parameters $(c_1,...,c_n)$, we agree to identify the characters for the two fields). Then we have:

Theorem 3.17. *For a given embedding $L \hookrightarrow K$, with μ as in 3.32, if $-\mu(H_\alpha)+i-j \notin \{1,2,3,...\}$ for all $\alpha = (i,j) \in \Phi^-$, then $I_L(\chi)$ is an admissible, irreducible (under both $G(L)$ and $G(\mathbb{Q}_p)$) globally analytic representation and it is the holomorphic base change of $I_{\mathbb{Q}_p}(\chi)$.*

$I_L(\chi)$ is admissible, as holomorphic base change respects admissibility [Clo16, prop. 3.1]. With the notations of section 3.2.2, define the full (Langlands) base change of $I_{\mathbb{Q}_p}$ to be the representation of $\mathrm{Res}_{L/\mathbb{Q}_p}G(\mathbb{Q}_p)$ on $\widehat{\otimes}_\sigma\ (I_L(\chi))^\sigma := I(\chi \circ N_{L/\mathbb{Q}_p})$, where $N_{L/\mathbb{Q}_p}$ is the norm map from L to $\mathbb{Q}_p$ and $\widehat{\otimes}$ is the completed tensor product (see also [Clo16, def. 3.8]) and $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$. Note that, for each factor, the embedding $i : L \to K$ must be replaced by $i \circ \sigma$. Finally, we then have

Theorem 3.18. *Let μ be as in 3.32, Assume $-\mu(H_\alpha)+i-j \notin \{1,2,3,...\}$ for all $\alpha = (i,j) \in \Phi^-$. Then the completed tensor product $\widehat{\otimes}_\sigma\ (I_L(\chi))^\sigma$ is irreducible, and is the representation of $G(L)$ on the space of globally analytic vectors, induced from $\chi \circ N_{L/\mathbb{Q}_p}$.*

Proof. Notice that by assumption, each factor in the completed tensor product is irreducible and admits the same description as in theorem 3.17. The space of the representation $I(\chi \circ N_{L/\mathbb{Q}_p})$ is $\widehat{\otimes}_\sigma\ \mathcal{A}(U,K) = \mathcal{A}(\mathrm{Res}_{L/\mathbb{Q}_p}U, K)$ which is a space of globally analytic vectors (by theorem 3.17) in the locally analytic representation $I_{\mathrm{loc}}(\chi \circ N_{L/\mathbb{Q}_p})$ of $\mathrm{Res}_{L/\mathbb{Q}_p}(G)$. The proof of irreducibility of $\widehat{\otimes}_\sigma\ (I_L(\chi))^\sigma$ follows from Theorem 3.9 using a natural generalization of Clozel's argument in Theorem 3.11, part (ii) of [Clo16], revised version. □

3.4 Induction from the Weyl orbits of the upper triangular Borel

In this section, we briefly sketch the arguments needed to extend the result of theorem 3.8 to the principal series induced from Weyl orbits of the Borel subgroup (theorem 3.21). Then we base change our globally analytic representation to L (section 3.5).

3.4.1 Global analyticity for the induction from different Weyl orbits

Denote by $\mathbb{P}$ the Borel subgroup of the upper triangular matrices in $GL_n(\mathbb{Q}_p)$, $\mathbb{T}$ the maximal torus of $GL_n(\mathbb{Q}_p)$, P^+ the Borel subgroup of the upper triangular matrices in $GL_n(\mathbb{Z}_p)$, W the ordinary Weyl group of $GL_n(\mathbb{Q}_p)$ with respect to $\mathbb{T}$ which is isomorphic to the group of $n \times n$ permutation matrices, $P_w^+ = B \cap wP^+w^{-1}$, where B is the Iwahori subgroup in section 3.3.1, $\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}}$ the locally analytic induction, that is:

$$\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}} = \{f \in \mathcal{A}_{\mathrm{loc}}(GL_n(\mathbb{Q}_p), K) : f(gb) = \chi(b^{-1})f(g), g \in GL_n(\mathbb{Q}_p), b \in \mathbb{P}\}.$$

The Iwasawa decomposition [OS10, sec. 3.2.2] gives

$$\mathrm{ind}_{\mathbb{P}}^{GL_n(\mathbb{Q}_p)}(\chi)_{\mathrm{loc}} \cong \mathrm{ind}_{P^+}^{GL_n(\mathbb{Z}_p)}(\chi)_{\mathrm{loc}} \tag{3.40}$$

as $GL_n(\mathbb{Z}_p)$-equivariant topological isomorphism. By the Bruhat-Tits decomposition (*loc. cit.* and [Car79, sec. 3.5])

$$GL_n(\mathbb{Z}_p) = \sqcup_{w\in W} BwP^+,$$

we obtain the decomposition

$$\mathrm{ind}_{P^+}^{GL_n(\mathbb{Z}_p)}(\chi)_{\mathrm{loc}} \cong \oplus_{w\in W}\mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}, \tag{3.41}$$

a B-equivariant decomposition of topological vector spaces, where the action of χ^w is given by $\chi^w(h) = \chi(w^{-1}hw)$. Let $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ be the space of globally analytic functions of $\mathrm{ind}_{P_w^+}^{B}(\chi^w)_{\mathrm{loc}}$. Our goal is to show that for all $w \in W$, $\mathrm{ind}_{P_w^+}^{B}(\chi^w)$ is a globally analytic representation of G. We have already showed, in section 3.3, that for $w = Id$, χ analytic, the induction $\mathrm{ind}_{P_0}^{B}(\chi)$ is a globally analytic representation of G. (Note that $B \cap P^+ = P_0$). Recall that U is the lower triangular unipotent subgroup of $GL_n(\mathbb{Z}_p)$. Consider the decomposition (cf. lemma 3.3.2 of [OS10])

$$B = (wUw^{-1} \cap B)(wP^+w^{-1} \cap B) = (wUw^{-1} \cap B)(P_w^+).$$

For GL_3, and $w = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ the above decomposition is like

$$B = \begin{pmatrix} \mathbb{Z}_p^\times & p\mathbb{Z}_p & p\mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p^\times & p\mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p^\times \end{pmatrix} = \begin{pmatrix} 1 & p\mathbb{Z}_p & p\mathbb{Z}_p \\ 0 & 1 & 0 \\ 0 & \mathbb{Z}_p & 1 \end{pmatrix} \begin{pmatrix} \mathbb{Z}_p^\times & 0 & 0 \\ \mathbb{Z}_p & \mathbb{Z}_p^\times & p\mathbb{Z}_p \\ \mathbb{Z}_p & 0 & \mathbb{Z}_p^\times \end{pmatrix}.$$

For a character χ of $\mathbb{T} \cap GL_n(\mathbb{Z}_p)$, we extend it to a character of P_w^+ by acting trivially on the non-diagonal elements of P_w^+. By definition,

$$\mathrm{ind}_{P_w^+}^{B}(\chi)_{\mathrm{loc}} = \{f \in \mathcal{A}_{\mathrm{loc}}(B, K) : f(gb) = \chi(b^{-1})f(g), b \in P_w^+, g \in B\}.$$

With the decomposition $B = (wUw^{-1} \cap B)(P_w^+)$, the vector space of locally analytic functions $\mathrm{ind}_{P_w^+}^{B}(\chi)_{\mathrm{loc}}$ is the same as $\mathcal{A}_{\mathrm{loc}}(wUw^{-1} \cap B, K)$. Let $\mathcal{A}(wUw^{-1} \cap B, K)$ be the subspace of globally analytic functions of $\mathcal{A}_{\mathrm{loc}}(wUw^{-1} \cap B, K)$. With $i \neq j$ fixed, $y \in \mathbb{Z}_p$ if $i > j$ and $y \in p\mathbb{Z}_p$ if $i < j$, recall that the action of the one-parameter subgroup on $f \in \mathcal{A}(wUw^{-1} \cap B, K)$ is given by

$$\begin{aligned}(1 + yE_{i,j})f(C) &= f((1 + yE_{i,j})^{-1}C) && \text{(with } C \in wUw^{-1} \cap B) && (3.42)\\ &= f((1 - yE_{i,j})C) && && (3.43)\\ &= f((1 - yE_{i,j})wAw^{-1}) && \text{(with } C = wAw^{-1} \text{ for } A \in U). && (3.44)\end{aligned}$$

Our goal is to show that this action is globally analytic.

Since $w^{-1} \in W$, write w^{-1} in the form of a permutation matrix, i.e. $w^{-1} = \sum_{r=1}^{n} E_{r,j_r}$ with $j_r \neq j_s$ for $r \neq s$. Then,

$$w^{-1}(1 - yE_{i,j}) = (\sum_{r=1}^{n} E_{r,j_r})(1 - yE_{i,j}) = (\sum_{r=1}^{n} E_{r,j_r}) - yE_{k,j}$$

where k is such that $j_k = i$. As the inverse of a permutation matrix is its transpose, we obtain

$$\begin{aligned}w^{-1}(1 - yE_{i,j})w &= \Big((\sum_{r=1}^{n} E_{r,j_r}) - yE_{k,j}\Big)(\sum_{s=1}^{n} E_{j_s,s})\\ &= 1 - yE_{k,l} \qquad (\text{use } j_r \neq j_s \text{ for } r \neq s)\end{aligned}$$

where l is such that $j_l = j$. So we have deduced that

$$(1 - yE_{i,j})w = w(1 - yE_{k,l}) \qquad (k, l \text{ such that } j_k = i, j_l = j). \tag{3.45}$$

Inserting equation 3.45 in 3.44 we obtain

$$(1+yE_{i,j})f(C) = f(w(1-yE_{k,l})Aw^{-1}) \tag{3.46}$$

Now, the globally analytic function f on $w(1-yE_{k,l})Aw^{-1}$ equals to some globally analytic function g on $(1-yE_{k,l})A$, because the conjugacy action of w on the matrix $(1-yE_{k,l})A$ is just permuting the entries of $(1-yE_{k,l})A$. So, equation 3.46 is

$$\begin{aligned} f(w(1-yE_{k,l})Aw^{-1}) &= g((1-yE_{k,l})A) \\ &= (1+yE_{k,l})g(A) \qquad \text{(recall } A \in U\text{)} \end{aligned}$$

and we know from lemmas 3.3 and 3.7 that the action of $(1+yE_{k,l})$ on $g(A)$ is globally analytic. Thus, we have shown that

Lemma 3.19. *The action of the lower and the upper unipotent one-parameter subgroups of G of the form $(1+yE_{i,j})$ on $f \in \mathcal{A}(wUw^{-1}\cap B, K)$ is a globally analytic action.*

Similar argument also shows that the action of the diagonal subgroup of G on $\mathcal{A}(wUw^{-1}\cap B, K)$ is globally analytic. More precisely, we write $w^{-1}Diag(t_1,...,t_n)w = Diag(t'_1,...,t'_n)$ with $(t'_1,...,t'_n)$ a permutation of $(t_1,...,t_n)$. Then, with $C \in wUw^{-1}\cap B$,

$$\begin{aligned} Diag(t_1^{-1},...,t_n^{-1})f(C) &= f\Big(Diag(t_1,...,t_n)wAw^{-1}\Big) \qquad (C = wAw^{-1}) \\ &= f\Big(w[Diag(t'_1,...,t'_n)]Aw^{-1}\Big) \\ &= g\Big(Diag(t'_1,...,t'_n)A\Big) \qquad \text{(for some analytic } g\text{)} \\ &= Diag(t_1^{-1},...,t_n^{-1})g(A) \end{aligned}$$

and by lemmas 3.2 and 3.1, the action of the diagonal subgroup of G on $g(A)$ is a globally analytic action. Therefore, we have shown

Lemma 3.20. *The action of the diagonal subgroup of G on $\mathcal{A}(wUw^{-1}\cap B, K)$ is globally analytic.*

Recall that the vector space $\mathcal{A}(wUw^{-1}\cap B, K)$ is isomorphic to $\mathrm{ind}_{P_w^+}^B(\chi^w)$. Thus, lemmas 3.19 and 3.20 together gives

Theorem 3.21. *Assume $p > n+1$ and χ analytic. Then, for all $w \in W$, the action of the pro-p Iwahori group G on $\mathrm{ind}_{P_w^+}^B(\chi^w)$ is globally analytic.*

3.5 Langlands base change for the full globally analytic principal series

Following the notations of section 3.3.2, we fix L a finite unramified extension of $\mathbb{Q}_p$ inside K. For each $w \in W$, consider the globally analytic admissible representation $I_{w,\mathbb{Q}_p}(\chi) := \mathcal{A}(wUw^{-1}\cap B, K)$ of $G(\mathbb{Q}_p)$. By section 3.2.2, $\mathcal{A}(wUw^{-1}\cap B, K)$ extends naturally to a globally analytic admissible representation of $G(L)$ called the "holomorphic base change" which we denote by $I_{w,L}(\chi)$. With the notations of section 3.2.2, define the full Langland's base change to be the representation of $\mathrm{Res}_{L/\mathbb{Q}_p}G(\mathbb{Q}_p)$ on $\oplus_{w\in W}(\widehat{\otimes}_\sigma\ I_{w,L}(\chi)^\sigma)$ (cf. [Clo16, sec. 3.5]). Finally, like theorem 3.18, we will then have

Theorem 3.22. *The Langlands base change $\oplus_{w\in W}(\widehat{\otimes}_\sigma\ I_{w,L}(\chi^w)^\sigma)$ is a globally analytic admissible representation of $G(L)$.*

In conclusion, for $p > n+1$, we have shown that for all $w \in W$, $\mathrm{ind}_{P_w^+}^B(\chi^w)$ is a globally analytic representation of the pro-p Iwahori G under the analyticity assumption on the character χ. Furthermore, we have treated the case of irreducibility of the principal series when $w = Id$. We hope that it is possible to adapt and generalize the argument of our irreducibility proof to treat the case when $w \neq Id$. Also, it is an interesting future project to determine the globally analytic vectors of more general p-adic representations of $GL(2,\mathbb{Q}_p)$, for example the "trianguline" representation of Colmez [Col08] (see also [Col14]), which corresponds to a quotient of principal series. Also one can explore the connection with the globally analytic vectors of p-adic representations (under the pro-p Iwahori or a suitable rigid-analytic subgroup of $GL(2)$) and (φ,Γ)-modules [Col10], similar to the existing correspondence for locally analytic representations [CD14, Sec VI.3].

Part II
Galois representations with open image and p-rational fields

Table of Contents

4 Galois representation with open image

The results of this section are already published in International Journal of Number Theory [CR18].

Abstract

For an odd prime p, we determine a minimal set of topological generators of the pro-p Iwahori subgroup of a split reductive group G over $\mathbb{Z}_p$. In the simple adjoint case and for any sufficiently large regular prime p, we also construct Galois extensions of $\mathbb{Q}$ with Galois group between the pro-p and the standard Iwahori subgroups of G.

4.1 Introduction (work in collaboration with Christophe Cornut)

Let p be an odd prime, let $\mathbf{G}$ be a split reductive group over $\mathbb{Z}_p$, fix a Borel subgroup $\mathbf{B} = \mathbf{U} \rtimes \mathbf{T}$ of $\mathbf{G}$ with unipotent radical $\mathbf{U} \lhd \mathbf{B}$ and maximal split torus $\mathbf{T} \subset \mathbf{B}$. The Iwahori subgroup I and pro-p-Iwahori subgroup $I(1) \subset I$ of $\mathbf{G}(\mathbb{Z}_p)$ are defined [Tit79, 3.7] by

$$I = \{g \in \mathbf{G}(\mathbb{Z}_p) : \ \mathrm{red}(g) \in \mathbf{B}(\mathbb{F}_p)\},$$
$$I(1) = \{g \in \mathbf{G}(\mathbb{Z}_p) : \ \mathrm{red}(g) \in \mathbf{U}(\mathbb{F}_p)\},$$

where 'red' is the reduction map red: $\mathbf{G}(\mathbb{Z}_p) \to \mathbf{G}(\mathbb{F}_p)$. The subgroups I and $I(1)$ are both open subgroups of $\mathbf{G}(\mathbb{Z}_p)$. Thus, $I = I(1) \rtimes T_{tors}$ and $\mathbf{T}(\mathbb{Z}_p) = T(1) \times T_{tors}$ where $T(1)$ and T_{tors} are respectively the pro$-p$ and torsion subgroups of $\mathbf{T}(\mathbb{Z}_p)$. Following [Gre16] (who works with $\mathbf{G} = \mathbf{GL}_n$), we construct in section 4.2 a minimal set of topological generators for $I(1)$.

More precisely, let $M = X^*(\mathbf{T})$ be the group of characters of $\mathbf{T}$, $R \subset M$ the set of roots of $\mathbf{T}$ in $\mathfrak{g} = \mathrm{Lie}(\mathbf{G})$, $\Delta \subset R$ the set of simple roots with respect to $\mathbf{B}$, $R = \coprod_{c \in \mathcal{C}} R_c$ the decomposition of R into irreducible components, $\Delta_c = \Delta \cap R_c$ the simple roots in R_c, $\alpha_{c,max}$ the highest positive root in R_c. We let $\mathcal{D} \subset \mathcal{C}$ be the set of irreducible components of type G_2 and for $d \in \mathcal{D}$, we denote by $\delta_d \in R_{d,+}$ the sum of the two simple roots in Δ_d. We denote by $M^\vee = X_*(\mathbf{T})$ the group of cocharacters of $\mathbf{T}$, by $\mathbb{Z}R^\vee$ the subgroup spanned by the coroots $R^\vee \subset M^\vee$ and we fix a set of representatives $\mathcal{S} \subset M^\vee$ for an $\mathbb{F}_p$-basis of

$$(M^\vee/\mathbb{Z}R^\vee) \otimes \mathbb{F}_p = \oplus_{s \in \mathcal{S}} \mathbb{F}_p \cdot s \otimes 1.$$

We show (see theorem 4.1):

Theorem. *The following elements form a minimal set of topological generators of the pro-p-Iwahori subgroup $I(1)$ of $G = \mathbf{G}(\mathbb{Q}_p)$:*

1. *The semi-simple elements $\{s(1+p) : s \in \mathcal{S}\}$ of $T(1)$,*
2. *For each $c \in \mathcal{C}$, the unipotent elements $\{x_\alpha(1) : \alpha \in \Delta_c\}$,*
3. *For each $c \in \mathcal{C}$, the unipotent element $x_{-\alpha_{c,max}}(p)$,*
4. *(If $p = 3$) For each $d \in \mathcal{D}$, the unipotent element $x_{\delta_d}(1)$.*

This result generalizes Greenberg [Gre16] proposition 5.3, see also Schneider and Ollivier ([OS16], proposition 3.64, part i) for $G = SL_2$.

Let $\mathbf{T}^{ad}$ be the image of $\mathbf{T}$ in the adjoint group $\mathbf{G}^{ad}$ of $\mathbf{G}$. The action of $\mathbf{G}^{ad}$ on $\mathbf{G}$ induces an action of $\mathbf{T}^{ad}(\mathbb{Z}_p)$ on I and $I(1)$ and the latter equips the Frattini quotient $\tilde{I}(1)$ of $I(1)$ with a structure of $\mathbb{F}_p[T^{ad}_{tors}]$-module, where T^{ad}_{tors} is the torsion subgroup of $\mathbf{T}^{ad}(\mathbb{Z}_p)$ (cf. section 4.2.8). Any element β in $\mathbb{Z}R = M^{ad} = X^*(\mathbf{T}^{ad})$ induces a character $\beta : T^{tors}_{ad} \to \mathbb{F}_p^\times$ and we denote by $\mathbb{F}_p(\beta)$ the corresponding simple (1-dimensional) $\mathbb{F}_p[T^{ad}_{tors}]$-module. With these notations, the theorem implies that

Corollary. *The $\mathbb{F}_p[T^{ad}_{tors}]$-module $\tilde{I}(1)$ is isomorphic to*

$$\mathbb{F}_p^{\sharp\mathcal{S}} \oplus \Big(\oplus_{\alpha \in \Delta} \mathbb{F}_p(\alpha) \Big) \oplus \Big(\oplus_{c \in \mathcal{C}} \mathbb{F}_p(-\alpha_{c,max}) \Big) \Big(\oplus \Big(\oplus_{d \in \mathcal{D}} \mathbb{F}_p(\delta_c) \Big) \text{ if } p = 3 \Big).$$

Here $\sharp\mathcal{S}$ is the cardinality of $\mathcal{S}$. Suppose from now on in this introduction that $\mathbf{G}$ is simple and of adjoint type. Then:

Corollary *The $\mathbb{F}_p[T_{tors}]$-module $\tilde{I}(1)$ is multiplicity free unless $p = 3$ and $\mathbf{G}$ is of type A_1, B_ℓ or C_ℓ ($\ell \geq 2$), F_4 or G_2.*

Let now K be a Galois extension of $\mathbb{Q}$, Σ_p the set of primes of K lying above p. Let M be the compositum of all finite p-extensions of K which are unramified outside Σ_p, a Galois extension over $\mathbb{Q}$. Set

$$\Gamma = \mathrm{Gal}(M/K), \quad \Omega = \mathrm{Gal}(K/\mathbb{Q}) \quad \text{and} \quad \Pi = \mathrm{Gal}(M/\mathbb{Q}).$$

We say that K is p-rational if Γ is a free pro$-p$ group, see [MNQD90]. The simplest example is $K = \mathbb{Q}$, where $\Gamma = \Pi$ is also abelian and M is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Other examples of p-rational fields are $\mathbb{Q}(\mu_p)$ where p is a regular prime.

Assume K is a p-rational, totally complex, abelian extension of $\mathbb{Q}$ and such that $(p-1)\cdot\Omega = 0$. Then Greenberg in [Gre16] constructs a continuous homomorphism

$$\rho_0 : \ \mathrm{Gal}(M/\mathbb{Q}) \to GL_n(\mathbb{Z}_p)$$

such that $\rho_0(\Gamma)$ is the pro-p Iwahori subgroup of $SL_n(\mathbb{Z}_p)$, assuming that there exists n distinct characters of Ω, trivial or odd, whose product is the trivial character.

In section 4.3, we establish the existence of p-adic Lie extensions of $\mathbb{Q}$ whose Galois group corresponds to certain specified p-adic Lie algebras. More precisely, for p-rational fields, we construct continuous morphisms with open image $\rho : \Pi \to I$ such that $\rho(\Gamma) = I(1)$. We show in corollary 4.18 that

Corollary *Suppose that K is a p-rational totally complex, abelian extension of $\mathbb{Q}$ and $(p-1)\cdot\Omega = 0$. Assume also that if $p = 3$, our split simple adjoint group $\mathbf{G}$ is not of type A_1, B_ℓ or C_ℓ ($\ell \geq 2$), F_4 or G_2. Then there is a morphism $\rho : \Pi \to I$ such that $\rho(\Gamma) = I(1)$ if and only if there is morphism $\overline{\rho} : \Omega \to T_{tors}$ such that the characters $\alpha \circ \overline{\rho} : \Omega \to \mathbb{F}_p^\times$ for $\alpha \in \{\Delta \cup -\alpha_{max}\}$ are all distinct and belong to $\hat{\Omega}^{\mathcal{S}}_{odd}$.*

Here $\hat{\Omega}^{\mathcal{S}}_{odd}$ is a subset of the characters of Ω with values in $\mathbb{F}_p^\times$ (cf. section 4.3.2). Furthermore, assuming $K = \mathbb{Q}(\mu_p)$ we show the existence of such a morphism $\overline{\rho} : \Omega \to T_{tors}$ provided that p is a sufficiently large regular prime:

Corollary *There is a constant c depending only upon the type of $\mathbf{G}$ such that if $p > c$ is a regular prime, then for $K = \mathbb{Q}(\mu_p)$, M, Π and Γ as above, there is a continuous morphism $\rho : \Pi \to I$ with $\rho(\Gamma) = I(1)$.*

The constant c can be determined from lemmas 4.19, 4.20 and remark 4.21.

In section 4.2, we find a minimal set of topological generators of $I(1)$ and study the structure of $\tilde{I}(1)$ as an $\mathbb{F}_p[T^{ad}_{tors}]$-module. In section 4.3, assuming our group $\mathbf{G}$ to be simple and adjoint, we discuss the notion of p-rational fields and construct continuous morphisms $\rho : \Pi \to I$ with open image.

4.2 Topological generators of the pro-p Iwahori

This section is organized as follows. In section 4.2.1 we introduce the notations, then section 4.2.2 states our main result concerning the minimal set of topological generators of $I(1)$ (see theorem 4.1) with a discussion of the Iwahori factorisation in section 4.2.3. Its proof for $\mathbf{G}$ simple and simply connected is given in sections (4.2.4-4.2.7), where section 4.2.7 deals with the case of a group of type G_2. The proof for an arbitrary split reductive group over $\mathbb{Z}_p$ is discussed in section 4.2.8 and in particular, we establish the minimality of our set of topological generators. Finally, in section 4.2.9 we study the structure of the Frattini quotient $\tilde{I}(1)$ of $I(1)$ as an $\mathbb{F}_p[T^{ad}_{tors}]$-module and determine when it is multiplicity free.

4.2.1 Preliminary notations

Let p be an odd prime, $\mathbf{G}$ be a split reductive group over $\mathbb{Z}_p$. Fix a pinning of $\mathbf{G}$ [GP11, XXIII 1]

$$(\mathbf{T}, M, R, \Delta, (X_\alpha)_{\alpha\in\Delta}) .$$

Thus, $\mathbf{T}$ is a split maximal torus in $\mathbf{G}$, $M = X^*(\mathbf{T})$ is its group of characters,

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \oplus_{\alpha\in R}\mathfrak{g}_\alpha$$

is the weight decomposition for the adjoint action of $\mathbf{T}$ on $\mathfrak{g} = \mathrm{Lie}(\mathbf{G})$, $\Delta \subset R$ is a basis of the root system $R \subset M$ and for each $\alpha \in \Delta$, X_α is a $\mathbb{Z}_p$-basis of $\mathfrak{g}_\alpha$.

We denote by $M^\vee = X_*(\mathbf{T})$ the group of cocharacters of $\mathbf{T}$, by $\alpha^\vee$ the coroot associated to $\alpha \in R$ and by $R^\vee \in M^\vee$ the set of all such coroots. We expand $(X_\alpha)_{\alpha\in\Delta}$ to a Chevalley system $(X_\alpha)_{\alpha\in R}$ of $\mathbf{G}$ [GP11, XXIII 6.2]. For $\alpha \in R$, we denote by $\mathbf{U}_\alpha \subset \mathbf{G}$ the corresponding unipotent group, by $x_\alpha : \mathbf{G}_{a,\mathbb{Z}_p} \to \mathbf{U}_\alpha$ the isomorphism given by $x_\alpha(t) = \exp(tX_\alpha)$. The height $h(\alpha) \in \mathbb{Z}$ of $\alpha \in R$ is the sum of the coefficients of α in the basis Δ of R. Thus, $R_+ = h^{-1}(\mathbb{Z}_{>0})$ is the set of

positive roots in R, corresponding to a Borel subgroup $\mathbf{B} = \mathbf{U} \rtimes \mathbf{T}$ of $\mathbf{G}$ with unipotent radical $\mathbf{U}$. We let $\mathcal{C}$ be the set of irreducible components of R, so that

$$R = \coprod_{c \in \mathcal{C}} R_c, \quad \Delta = \coprod_{c \in \mathcal{C}} \Delta_c, \quad R_+ = \coprod_{c \in \mathcal{C}} R_{c,+}$$

with R_c irreducible, $\Delta_c = \Delta \cap R_c$ is a basis of R_c and $R_{c,+} = R_+ \cap R_c$ is the corresponding set of positive roots in R_c. We denote by $\alpha_{c,max} \in R_{c,+}$ the highest root of R_c. We let $\mathcal{D} \subset \mathcal{C}$ be the set of irreducible components of type G_2 and for $d \in \mathcal{D}$, we denote by $\delta_d \in R_{d,+}$ the sum of the two simple roots in Δ_d.

Since $\mathbf{G}$ is smooth over $\mathbb{Z}_p$, the reduction map

$$\mathrm{red} : \mathbf{G}(\mathbb{Z}_p) \to \mathbf{G}(\mathbb{F}_p)$$

is surjective and its kernel $G(1)$ is a normal pro-p-subgroup of $\mathbf{G}(\mathbb{Z}_p)$. The Iwahori subgroup I and pro-p-Iwahori subgroup $I(1) \subset I$ of $\mathbf{G}(\mathbb{Z}_p)$ are defined [Tit79, 3.7] by

$$\begin{aligned} I &= \{g \in \mathbf{G}(\mathbb{Z}_p) : \mathrm{red}(g) \in \mathbf{B}(\mathbb{F}_p)\}, \\ I(1) &= \{g \in \mathbf{G}(\mathbb{Z}_p) : \mathrm{red}(g) \in \mathbf{U}(\mathbb{F}_p)\}. \end{aligned}$$

Thus, $I(1)$ is a normal pro-p-Sylow subgroup of I which contains $\mathbf{U}(\mathbb{Z}_p)$ and

$$I/I(1) \simeq \mathbf{B}(\mathbb{F}_p)/\mathbf{U}(\mathbb{F}_p) \simeq \mathbf{T}(\mathbb{F}_p).$$

Since $\mathbf{T}(\mathbb{Z}_p) \twoheadrightarrow \mathbf{T}(\mathbb{F}_p)$ is split by the torsion subgroup $T_{tors} \simeq \mathbf{T}(\mathbb{F}_p)$ of $\mathbf{T}(\mathbb{Z}_p)$,

$$\mathbf{T}(\mathbb{Z}_p) = T(1) \times T_{tors} \qquad \text{and} \qquad I = I(1) \rtimes T_{tors}$$

where

$$T(1) = \mathbf{T}(\mathbb{Z}_p) \cap I(1) = \ker\left(\mathbf{T}(\mathbb{Z}_p) \to \mathbf{T}(\mathbb{F}_p)\right)$$

is the pro-p-Sylow subgroup of $\mathbf{T}(\mathbb{Z}_p)$. Note that

$$\begin{aligned} T(1) &= \mathrm{Hom}\,(M, 1 + p\mathbb{Z}_p) = M^\vee \otimes (1 + p\mathbb{Z}_p), \\ T_{tors} &= \mathrm{Hom}\,(M, \mu_{p-1}) = M^\vee \otimes \mathbb{F}_p^\times. \end{aligned}$$

4.2.2 Main theorem concerning the minimal set of topological generators of the pro-p Iwahori

Let $\mathcal{S} \subset M^\vee$ be a set of representatives for an $\mathbb{F}_p$-basis of

$$(M^\vee/\mathbb{Z}R^\vee) \otimes \mathbb{F}_p = \oplus_{s \in \mathcal{S}} \mathbb{F}_p \cdot s \otimes 1.$$

Theorem 4.1. *The following elements form a minimal set of topological generators of the pro-p-Iwahori subgroup $I(1)$ of $G = \mathbf{G}(\mathbb{Q}_p)$:*

1. *The semi-simple elements $\{s(1+p) : s \in \mathcal{S}\}$ of $T(1)$.*
2. *For each $c \in \mathcal{C}$, the unipotent elements $\{x_\alpha(1) : \alpha \in \Delta_c\}$.*
3. *For each $c \in \mathcal{C}$, the unipotent element $x_{-\alpha_{c,max}}(p)$.*
4. *(If $p = 3$) For each $d \in \mathcal{D}$, the unipotent element $x_{\delta_d}(1)$.*

4.2.3 Iwahori decomposition

By [GP11, XXII 5.9.5] and its proof, there is a canonical filtration

$$\mathbf{U} = \mathbf{U}_1 \supset \mathbf{U}_2 \supset \cdots \supset \mathbf{U}_h \supset \mathbf{U}_{h+1} = 1$$

of $\mathbf{U}$ by normal subgroups such that for $1 \leq i \leq h$, the product map (in any order)

$$\prod_{h(\alpha)=i} \mathbf{U}_\alpha \to \mathbf{U}$$

factors through $\mathbf{U}_i$ and yields an isomorphism of group schemes

$$\prod_{h(\alpha)=i} \mathbf{U}_\alpha \xrightarrow{\simeq} \overline{\mathbf{U}}_i, \quad \overline{\mathbf{U}}_i = \mathbf{U}_i/\mathbf{U}_{i+1}.$$

By [GP11, XXII 5.9.6] and its proof,

$$\overline{\mathbf{U}}_i(R) = \mathbf{U}_i(R)/\mathbf{U}_{i+1}(R)$$

for every $\mathbb{Z}_p$-algebra R. It follows that the product map

$$\prod_{h(\alpha)=i} \mathbf{U}_\alpha \times \mathbf{U}_{i+1} \to \mathbf{U}_i$$

is an isomorphism of $\mathbb{Z}_p$-schemes and by induction, the product map

$$\prod_{h(\alpha)=1} \mathbf{U}_\alpha \times \prod_{h(\alpha)=2} \mathbf{U}_\alpha \times \cdots \times \prod_{h(\alpha)=h} \mathbf{U}_\alpha \to \mathbf{U}$$

is an isomorphism of $\mathbb{Z}_p$-schemes. Similarly, the product map

$$\prod_{h(\alpha)=-h} \mathbf{U}_\alpha \times \prod_{h(\alpha)=-h+1} \mathbf{U}_\alpha \times \cdots \times \prod_{h(\alpha)=-1} \mathbf{U}_\alpha \to \mathbf{U}^-$$

is an isomorphism of $\mathbb{Z}_p$-schemes, where $\mathbf{U}^-$ is the unipotent radical of the Borel subgroup $\mathbf{B}^- = \mathbf{U}^- \rtimes \mathbf{T}$ opposed to $\mathbf{B}$ with respect to $\mathbf{T}$. Then by [GP11, XXII 4.1.2], there is an open subscheme Ω of $\mathbf{G}$ (the "big cell") such that the product map

$$\mathbf{U}^- \times \mathbf{T} \times \mathbf{U} \to \mathbf{G}$$

is an open immersion with image Ω. Plainly, $\mathbf{B} = \mathbf{U} \rtimes \mathbf{T}$ is a closed subscheme of Ω. Thus by definition of I, $I \subset \Omega(\mathbb{Z}_p)$ and therefore any element of I (resp. $I(1)$) can be written uniquely as a product

$$\prod_{h(\alpha)=-h} x_\alpha(a_\alpha) \times \cdots \times \prod_{h(\alpha)=-1} x_\alpha(a_\alpha) \times t \times \prod_{h(\alpha)=1} x_\alpha(a_\alpha) \times \cdots \times \prod_{h(\alpha)=h} x_\alpha(a_\alpha)$$

where $a_\alpha \in \mathbb{Z}_p$ for $\alpha \in R_+$, $a_\alpha \in p\mathbb{Z}_p$ for $\alpha \in R_- = -R_+$ and $t \in \mathbf{T}(\mathbb{Z}_p)$ (resp. $T(1)$). This is the Iwahori decomposition of I (resp. $I(1)$). If I^+ is the group spanned by $\{x_\alpha(\mathbb{Z}_p) : \alpha \in R_+\}$ and I^- is the group spanned by $\{x_\alpha(p\mathbb{Z}_p) : \alpha \in R_-\}$, then $I^+ = \mathbf{U}(\mathbb{Z}_p)$, $I^- \subset \mathbf{U}^-(\mathbb{Z}_p)$ and every $x \in I$ (resp. $I(1)$) has a unique decomposition $x = u^- t u^+$ with $u^\pm \in I^\pm$ and $t \in \mathbf{T}(\mathbb{Z}_p)$ (resp. $t \in T(1)$).

4.2.4 The case for semi-simple, simply connected groups

Suppose first that $\mathbf{G}$ is semi-simple and simply connected. Then $M^\vee = \mathbb{Z}R^\vee$, thus $\mathcal{S} = \emptyset$. Moreover, everything splits according to the decomposition $R = \coprod R_c$:

$$\mathbf{G} = \prod \mathbf{G}_c, \quad \mathbf{T} = \prod \mathbf{T}_c, \quad \mathbf{B} = \prod \mathbf{B}_c, \quad I = \prod I_c \quad \text{and} \quad I(1) = \prod I_c(1).$$

To establish the theorem in this case, we may thus furthermore assume that $\mathbf{G}$ is simple. From now on until section 4.2.8, we therefore assume that

$$\mathbf{G} \text{ is (split) simple and simply connected.}$$

As a first step, we show that

Lemma 4.2. *The group generated by I^+ and I^- contains $T(1)$.*

Proof. Since $\mathbf{G}$ is simply connected,

$$\prod_{\alpha\in\Delta} \alpha^\vee : \prod_{\alpha\in\Delta} \mathbf{G}_{m,\mathbb{Z}_p} \to \mathbf{T}$$

is an isomorphism, thus

$$T_c(1) = \prod_{\alpha\in\Delta} \alpha^\vee(1+p\mathbb{Z}_p).$$

Now for any $\alpha \in \Delta$, there is a unique morphism [GP11, XX 5.8]

$$f_\alpha : \mathbf{SL}(2)_{\mathbb{Z}_p} \to \mathbf{G}$$

such that for every $u, v \in \mathbb{Z}_p$ and $x \in \mathbb{Z}_p^\times$,

$$f_\alpha \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = x_\alpha(u), \quad f_\alpha \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} = x_{-\alpha}(v) \quad \text{and} \quad f_\alpha \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} = \alpha^\vee(x).$$

Since for every $x \in 1+p\mathbb{Z}_p$ [GP11, XX 2.7],

$$\begin{pmatrix} 1 & 0 \\ x^{-1}-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$$

in $\mathbf{SL}(2)(\mathbb{Z}_p)$, it follows that $\alpha^\vee(1+p\mathbb{Z}_p)$ is already contained in the subgroup of $\mathbf{G}(\mathbb{Z}_p)$ generated by $x_\alpha(\mathbb{Z}_p^\times)$ and $x_{-\alpha}(p\mathbb{Z}_p)$. This proves the lemma. □

4.2.5 Commutator relations

Recall from [GP11, XXI 2.3.5] that for any pair of non-proportional roots $\alpha \neq \pm\beta$ in R, the set of integers $k \in \mathbb{Z}$ such that $\beta + k\alpha \in R$ is an interval of length at most 3, i.e. there are integers $r \geq 1$ and $s \geq 0$ with $r + s \leq 4$ such that

$$R \cap \{\beta + \mathbb{Z}\alpha\} = \{\beta - (r-1)\alpha, \cdots, \beta + s\alpha\}.$$

The above set is called the α-chain through β and any such set is called a root chain in R. Let $\|-\| : R \to \mathbb{R}_+$ be the length function on R.

Proposition 4.3. *Suppose $\|\alpha\| \leq \|\beta\|$. Then for any $u, v \in \mathbf{G}_a$ the commutator*

$$[x_\beta(v) : x_\alpha(u)] = x_\beta(v)x_\alpha(u)x_\beta(-v)x_\alpha(-u)$$

is given by the following table, with (r, s) as above:

(r,s)	$[x_\beta(v) : x_\alpha(u)]$
$(-,0)$	1
$(1,1)$	$x_{\alpha+\beta}(\pm uv)$
$(1,2)$	$x_{\alpha+\beta}(\pm uv) \cdot x_{2\alpha+\beta}(\pm u^2 v)$
$(1,3)$	$x_{\alpha+\beta}(\pm uv) \cdot x_{2\alpha+\beta}(\pm u^2 v) \cdot x_{3\alpha+\beta}(\pm u^3 v) \cdot x_{3\alpha+2\beta}(\pm u^3 v^2)$
$(2,1)$	$x_{\alpha+\beta}(\pm 2uv)$
$(2,2)$	$x_{\alpha+\beta}(\pm 2uv) \cdot x_{2\alpha+\beta}(\pm 3u^2 v) \cdot x_{\alpha+2\beta}(\pm 3uv^2)$
$(3,1)$	$x_{\alpha+\beta}(\pm 3uv)$

The signs are unspecified, but only depend upon α and β.

Proof. This is [GP11, XXIII 6.4]. □

Corollary 4.4. *If $r + s \leq 3$ and $\alpha + \beta \in R$ (i.e. $s \geq 1$), then for any $a, b \in \mathbb{Z}$, the subgroup of G generated by $x_\alpha(p^a\mathbb{Z}_p)$ and $x_\beta(p^b\mathbb{Z}_p)$ contains $x_{\alpha+\beta}(p^{a+b}\mathbb{Z}_p)$.*

Proof. This is obvious if $(r, s) = (1, 1)$ or $(2, 1)$ (using $p \neq 2$ in the latter case). For the only remaining case where $(r, s) = (1, 3)$, note that

$$[x_\beta(v) : x_\alpha(u)][x_\beta(w^2 v) : x_\alpha(uw^{-1})]^{-1} = x_{\alpha+\beta}(\pm uv(1-w)).$$

Since $p \neq 2$, we may find $w \in \mathbb{Z}_p^\times$ with $(1-w) \in \mathbb{Z}_p^\times$. Our claim easily follows. □

Lemma 4.5. *If R contains any root chain of length 3, then $\mathbf{G}$ is of type G_2.*

Proof. Suppose that the α-chain through β has length 3. By [GP11, XXI 3.5.4], there is a basis Δ' of R such that $\alpha \in \Delta'$ and $\beta = a\alpha + b\alpha'$ with $\alpha' \in \Delta'$, $a, b \in \mathbb{N}$. The root system R' spanned by $\Delta' = \{\alpha, \alpha'\}$ [GP11, XXI 3.4.6] then also contains an α-chain of length 3. By inspection of the root systems of rank 2, for instance in [GP11, XXIII 3], we find that R' is of type G_2. In particular, the Dynkin diagram of R contains a triple edge (linking the vertices corresponding to α and α'), which implies that actually $R = R'$ is of type G_2. □

4.2.6 The case for semi-simple, simply connected groups not of type G_2

We now establish our theorem 4.1 for a group $\mathbf{G}$ which is simple and simply connected, but not of type G_2.

Lemma 4.6. *The group I^+ is generated by $\{x_\alpha(\mathbb{Z}_p) : \alpha \in \Delta\}$.*

Proof. Let $H \subset I^+$ be the group spanned by $\{x_\alpha(\mathbb{Z}_p) : \alpha \in \Delta\}$. We show by induction on $h(\gamma) \geq 1$ that $x_\gamma(\mathbb{Z}_p) \subset H$ for every $\gamma \in R_+$. If $h(\gamma) = 1$, γ already belongs to Δ and there is nothing to prove. If $h(\gamma) > 1$, then by [Bou81, VI.1.6 Proposition 19], there is a simple root $\alpha \in \Delta$ such that $\beta = \gamma - \alpha \in R_+$. Then $h(\beta) = h(\gamma) - 1$, thus by induction $x_\beta(\mathbb{Z}_p) \subset H$. Since also $x_\alpha(\mathbb{Z}_p) \subset H$, $x_\gamma(\mathbb{Z}_p) \subset H$ by Corollary 4.4. □

Lemma 4.7. *The group generated by I^+ and $x_{-\alpha_{max}}(p\mathbb{Z}_p)$ contains I^-.*

Proof. Let $H \subset I$ be the group spanned by I^+ and $x_{-\alpha_{max}}(p\mathbb{Z}_p)$. We show by descending induction on $h(\gamma) \geq 1$ that $x_{-\gamma}(p\mathbb{Z}_p) \subset H$ for every $\gamma \in R_+$. Suppose $h(\gamma) = h(\alpha_{max})$, then $\gamma = \alpha_{max}$ and there is nothing to prove. If $h(\gamma) < h(\alpha_{max})$, then by [Bou81, VI.1.6 Proposition 19], there is a pair of positive roots α, β such that $\beta = \gamma + \alpha$. Then $h(\beta) = h(\gamma) + h(\alpha) > h(\gamma)$, thus by induction $x_{-\beta}(p\mathbb{Z}_p) \subset H$. Since also $x_\alpha(\mathbb{Z}_p) \subset H$, $x_{-\gamma}(p\mathbb{Z}_p) \subset H$ by Corollary 4.4. □

Remark 4.8. From the Hasse diagrams in [Rin13], it seems that in the previous proof, we may always require α to be a simple root.

Proof. (Of theorem 4.1 for $\mathbf{G}$ simple, simply connected, not of type G_2) By lemma 4.2, 4.6, 4.7 and the Iwahori decomposition of section 4.2.3, $I(1)$ is generated by

$$\{x_\alpha(\mathbb{Z}_p) : \alpha \in \Delta\} \cup \{x_{-\alpha_{max}}(p\mathbb{Z}_p)\}$$

thus topologically generated by

$$\{x_\alpha(1) : \alpha \in \Delta\} \cup \{x_{-\alpha_{max}}(p)\}.$$

None of these topological generators can be removed: the first ones are contained in $I^+ \subsetneq I(1)$, and all of them are needed to span the image of

$$I(1) \twoheadrightarrow \mathbf{U}(\mathbb{F}_p) \twoheadrightarrow \overline{\mathbf{U}}_1(\mathbb{F}_p) \simeq \prod_{\alpha \in \Delta} \mathbf{U}_\alpha(\mathbb{F}_p),$$

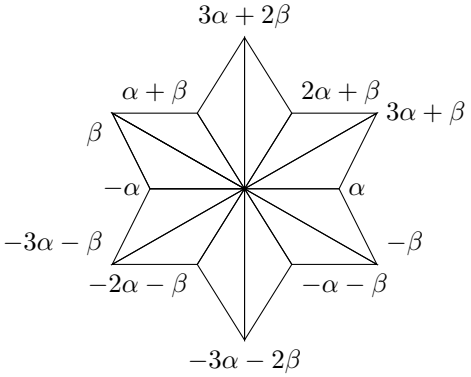
a surjective morphism that kills $x_{-\alpha_{max}}(p)$. □

4.2.7 Case for groups of type G_2

Let now $\mathbf{G}$ be simple of type G_2, thus $\Delta = \{\alpha, \beta\}$ with $\|\alpha\| < \|\beta\|$ and

$$R_+ = \{\alpha, \beta, \beta + \alpha, \beta + 2\alpha, \beta + 3\alpha, 2\beta + 3\alpha\}.$$

The whole root system looks like this:



Lemma 4.9. *The group generated by I^+ and $x_{-2\beta-3\alpha}(p\mathbb{Z}_p)$ contains I^-.*

Proof. Let $H \subset I(1)$ be the group generated by I^+ and $x_{-2\beta-3\alpha}(p\mathbb{Z}_p)$. Then, for every $u, v \in \mathbb{Z}_p$, H contains

$$\begin{aligned}
[x_{-2\beta-3\alpha}(pv) : x_\beta(u)] &= x_{-\beta-3\alpha}(\pm puv) \\
[x_{-2\beta-3\alpha}(pv) : x_{\beta+3\alpha}(u)] &= x_{-\beta}(\pm puv) \\
[x_{-2\beta-3\alpha}(pv) : x_{\beta+2\alpha}(u)] &= x_{-\beta-\alpha}(\pm puv) \cdot x_\alpha(\pm pu^2v) \cdot x_{\beta+3\alpha}(\pm pu^3v) \cdot x_{-\beta}(\pm p^2u^3v^2)
\end{aligned}$$

It thus contains $x_{-\beta-3\alpha}(p\mathbb{Z}_p)$, $x_{-\beta}(p\mathbb{Z}_p)$ and $x_{-\beta-\alpha}(p\mathbb{Z}_p)$, along with

$$\begin{aligned}
[x_{-\beta-3\alpha}(pv) : x_\alpha(u)] &= x_{-\beta-2\alpha}(\pm puv) \cdot x_{-\beta-\alpha}(\pm pu^2v) \cdot x_{-\beta}(\pm pu^3v) \cdot x_{-2\beta-3\alpha}(\pm p^2u^3v^2) \\
[x_{-\beta-3\alpha}(pv) : x_{\beta+2\alpha}(u)] &= x_{-\alpha}(\pm puv) \cdot x_{\beta+\alpha}(\pm pu^2v) \cdot x_{2\beta+3\alpha}(\pm pu^3v) \cdot x_\beta(\pm p^2u^3v^2)
\end{aligned}$$

It therefore also contains $x_{-\beta-2\alpha}(p\mathbb{Z}_p)$ and $x_{-\alpha}(p\mathbb{Z}_p)$. □

The filtration $(\mathbf{U}_i)_{i\geq 1}$ of $\mathbf{U}$ in section 4.2.3 induces a filtration

$$I^+ = I_1^+ \supset \cdots \supset I_5^+ \supset I_6^+ = 1$$

of $I^+ = \mathbf{U}(\mathbb{Z}_p)$ by normal subgroups $I_i^+ = \mathbf{U}_i(\mathbb{Z}_p)$ whose graded pieces

$$\overline{I}_i^+ = \overline{\mathbf{U}}_i(\mathbb{Z}_p) = I_i^+/I_{i+1}^+$$

are free $\mathbb{Z}_p$-modules, namely

$$\begin{gathered}
\overline{I}_1^+ = \mathbb{Z}_p \cdot \overline{x}_\alpha \oplus \mathbb{Z}_p \cdot \overline{x}_\beta, \qquad \overline{I}_2^+ = \mathbb{Z}_p \cdot \overline{x}_{\alpha+\beta} \\
\overline{I}_3^+ = \mathbb{Z}_p \cdot \overline{x}_{2\alpha+\beta}, \qquad \overline{I}_4^+ = \mathbb{Z}_p \cdot \overline{x}_{3\alpha+\beta}, \qquad \overline{I}_5^+ = \mathbb{Z}_p \cdot \overline{x}_{3\alpha+2\beta}
\end{gathered}$$

where $\overline{x}_\gamma$ is the image of $x_\gamma(1)$. The commutator defines $\mathbb{Z}_p$-linear pairings

$$[-,-]_{i,j} : \overline{I}_i^+ \times \overline{I}_j^+ \to \overline{I}_{i+j}^+$$

with $[y,x]_{j,i} = -[x,y]_{i,j}$, $[x,x]_{i,i} = 0$ and, by Proposition 4.3,

$$\begin{gathered}
[\overline{x}_\beta, \overline{x}_\alpha] = \pm\overline{x}_{\alpha+\beta}, \quad [\overline{x}_{\alpha+\beta}, \overline{x}_\alpha] = \pm 2\overline{x}_{2\alpha+\beta}, \quad [\overline{x}_{2\alpha+\beta}, \overline{x}_\alpha] = \pm 3\overline{x}_{3\alpha+\beta}, \\
[\overline{x}_{\alpha+\beta}, \overline{x}_{2\alpha+\beta}] = \pm x_{3\alpha+2\beta} \quad \text{and} \quad [\overline{x}_\beta, \overline{x}_{3\alpha+\beta}] = \pm x_{2\alpha+2\beta}
\end{gathered}$$

Let H be the subgroup of I^+ generated by $x_\alpha(\mathbb{Z}_p)$ and $x_\beta(\mathbb{Z}_p)$ and denote by H_i its image in $I^+/I_{i+1}^+ = G_i$. Then $H_1 = G_1$, H_2 contains $[\overline{x}_\beta, \overline{x}_\alpha] = \pm\overline{x}_{\alpha+\beta}$ thus $H_2 = G_2$, H_3 contains $[\overline{x}_{\alpha+\beta}, \overline{x}_\alpha] = \pm 2\overline{x}_{2\alpha+\beta}$ thus $H_3 = G_3$ since $p \neq 2$, H_4 contains $[\overline{x}_{2\alpha+\beta}, \overline{x}_\alpha] = \pm 3\overline{x}_{3\alpha+\beta}$ thus $H_4 = G_4$ if $p \neq 3$, in which case actually $H = H_5 = G_5 = I^+$ since H always contains $[\overline{x}_{\alpha+\beta}, \overline{x}_{2\alpha+\beta}] = \pm x_{3\alpha+2\beta}$.

If $p = 3$, let us also consider the exact sequence

$$0 \to J_4 \to G_4 \to \overline{I}_1^+ \to 0$$

The group $J_4 = I_2^+/I_5^+$ is commutative, and in fact again a free $\mathbb{Z}_3$-module:

$$J_4 = (\mathbf{U}_2/\mathbf{U}_5)(\mathbb{Z}_p) = \mathbb{Z}_3\tilde{x}_{\alpha+\beta} \oplus \mathbb{Z}_3\tilde{x}_{2\alpha+\beta} \oplus \mathbb{Z}_3\overline{x}_{3\alpha+\beta}$$

where $\tilde{x}_\gamma$ is the image of $x_\gamma(1)$. The action by conjugation of $\overline{I}_1^+$ on J_4 is given by

$$\overline{x}_\alpha \mapsto \begin{pmatrix} 1 & & \\ \pm 2 & 1 & \\ \pm 3 & \pm 3 & 1 \end{pmatrix} \quad \overline{x}_\beta \mapsto \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

in the indicated basis of J_4. The $\mathbb{Z}_3$-submodule $H_4' = H_4 \cap J_4$ of J_4 satisfies

$$H_4' + \mathbb{Z}_3\overline{x}_{3\alpha+\beta} = J_4 \quad \text{and} \quad 3\overline{x}_{3\alpha+\beta} \in H_4'.$$

Naming signs $\epsilon_i \in \{\pm 1\}$ in formula $(1,3)$ of proposition 4.3, we find that H_4' contains

$$\epsilon_1 uv \cdot \tilde{x}_{\alpha+\beta} + \epsilon_2 u^2 v \cdot \tilde{x}_{2\alpha+\beta} + \epsilon_3 u^3 v \cdot \overline{x}_{3\alpha+\beta}$$

for every $u, v \in \mathbb{Z}_3$. Adding these for $v = 1$ and $u = \pm 1$, we obtain

$$\tilde{x}_{2\alpha+\beta} \in H_4'.$$

It follows that H'_4 actually contains the following $\mathbb{Z}_3$-submodule of J_4:

$$J'_4 = \{a \cdot \tilde{x}_{\alpha+\beta} + b \cdot \tilde{x}_{2\alpha+\beta} + c \cdot \overline{x}_{3\alpha+\beta} : a, b, c \in \mathbb{Z}_3,\ \epsilon_1 a \equiv \epsilon_3 c \bmod 3\}.$$

Now observe that J'_4 is a normal subgroup of G_4, and the induced exact sequence

$$0 \to J_4/J'_4 \to G_4/J'_4 \to \overline{I}_1^+ \to 0$$

is an *abelian* extension of $\overline{I}_1^+ \simeq \mathbb{Z}_3^2$ by $J_4/J'_4 \simeq \mathbb{F}_3$. Since H_4/J'_4 is topologically generated by two elements and surjects onto $\overline{I}_1^+$, it actually defines a splitting:

$$G_4/J'_4 = H_4/J'_4 \oplus J_4/J'_4.$$

Thus, $H'_4 = J'_4$, H_4 is a normal subgroup of G_4, H is a normal subgroup of I^+ and

$$I^+/H \simeq G_4/H_4 \simeq J_4/J'_4 \simeq \mathbb{F}_3$$

is generated by the class of $x_{\alpha+\beta}(1)$ or $x_{3\alpha+\beta}(1)$. We have shown:

Lemma 4.10. *The group I^+ is spanned by $x_\alpha(\mathbb{Z}_p)$ and $x_\beta(\mathbb{Z}_p)$ plus $x_{\alpha+\beta}(1)$ if $p = 3$.*

Proof. (Of theorem 4.1 for $\mathbf{G}$ simple of type G_2) By lemma 4.2, 4.9, 4.10 and the Iwahori decomposition of section 4.2.3, the pro-p-Iwahori $I(1)$ is generated by $x_\alpha(\mathbb{Z}_p)$, $x_\beta(\mathbb{Z}_p)$, $x_{-2\beta-3\alpha}(p\mathbb{Z}_p)$, along with $x_{\alpha+\beta}(1)$ if $p = 3$. It is therefore topologically generated by $x_\alpha(1)$, $x_\beta(1)$, $x_{-2\beta-3\alpha}(p)$, along with $x_{\alpha+\beta}(1)$ if $p = 3$. The surjective reduction morphism $I(1) \twoheadrightarrow \mathbf{U}(\mathbb{F}_p) \twoheadrightarrow \overline{\mathbf{U}}_1(\mathbb{F}_p)$ shows that the first two generators can not be removed. The third one also can not, since all the others belong to the closed subgroup $I_+ \subsetneq I(1)$. Finally, suppose that $p = 3$ and consider the extension

$$1 \to \mathbf{U}_2/\mathbf{U}_5 \to \mathbf{U}/\mathbf{U}_5 \to \mathbf{U}/\mathbf{U}_1 \to 1$$

With notations as above, the reduction of

$$J'_4 \subset J_4 = \mathbf{U}_2(\mathbb{Z}_3)/\mathbf{U}_5(\mathbb{Z}_3) = (\mathbf{U}_2/\mathbf{U}_5)(\mathbb{Z}_3)$$

is a normal subgroup Y of $X = (\mathbf{U}/\mathbf{U}_5)(\mathbb{F}_3)$ with quotient $X/Y \simeq \mathbb{F}_3^3$. The surjective reduction morphism

$$I(1) \twoheadrightarrow \mathbf{U}(\mathbb{F}_3) \twoheadrightarrow \mathbf{U}(\mathbb{F}_3)/\mathbf{U}_5(\mathbb{F}_3) = X \twoheadrightarrow X/Y$$

then kills $x_{-2\beta-3\alpha}(p)$. The fourth topological generator $x_{\alpha+\beta}(1)$ of $I(1)$ thus also can not be removed, since the first two certainly do not span $X/Y \simeq \mathbb{F}_3^3$. □

4.2.8 The case for arbitrary split reductive groups

We now return to an arbitrary split reductive group $\mathbf{G}$ over $\mathbb{Z}_p$. Let

$$\mathbf{G}^{sc} \twoheadrightarrow \mathbf{G}^{der} \hookrightarrow \mathbf{G} \twoheadrightarrow \mathbf{G}^{ad}$$

be the simply connected cover $\mathbf{G}^{sc}$ of the derived group $\mathbf{G}^{der}$ of $\mathbf{G}$, and the adjoint group $\pi : \mathbf{G} \twoheadrightarrow \mathbf{G}^{ad}$ of $\mathbf{G}$. Then

$$\left(\mathbf{T}^{ad}, M^{ad}, R^{ad}, \Delta^{ad}, \left(X_\alpha^{ad}\right)_{\alpha\in\Delta^{ad}}\right) = \left(\pi(\mathbf{T}), \mathbb{Z}R, R, \Delta, (\pi(X_\alpha))_{\alpha\in\Delta}\right)$$

is a pinning of $\mathbf{G}^{ad}$ and this construction yields a bijection between pinnings of $\mathbf{G}$ and pinnings of $\mathbf{G}^{ad}$. Applying this to $\mathbf{G}^{sc}$ or $\mathbf{G}^{der}$, we obtain pinnings

$$\left(\mathbf{T}^{sc}, M^{sc}, R^{sc}, \Delta^{sc}, (X_\alpha^{sc})_{\alpha\in\Delta^{sc}}\right) \quad \text{and} \quad \left(\mathbf{T}^{der}, M^{der}, R^{der}, \Delta^{der}, \left(X_\alpha^{der}\right)_{\alpha\in\Delta^{sc}}\right)$$

for $\mathbf{G}^{sc}$ and $\mathbf{G}^{der}$: all the above constructions then apply to $\mathbf{G}^{ad}$, $\mathbf{G}^{sc}$ or $\mathbf{G}^{der}$, and we will denote with a subscript *ad*, *sc* or *der* for the corresponding objects. For instance, we have a sequence of Iwahori (resp. pro-p-Iwahori) subgroups

$$I^{sc} \to I^{der} \hookrightarrow I \to I^{ad} \quad \text{and} \quad I^{sc}(1) \to I^{der}(1) \hookrightarrow I(1) \to I^{ad}(1).$$

The action of $\mathbf{G}$ on itself by conjugation factors through a morphism

$$\mathrm{Ad} : \mathbf{G}^{ad} \to \mathrm{Aut}(\mathbf{G}).$$

For $b \in \mathbf{B}^{ad}(\mathbb{F}_p)$, $\mathrm{Ad}(b)(\mathbf{B}_{\mathbb{F}_p}) = \mathbf{B}_{\mathbb{F}_p}$ and $\mathrm{Ad}(b)(\mathbf{U}_{\mathbb{F}_p}) = \mathbf{U}_{\mathbb{F}_p}$. We thus obtain an action of the Iwahori subgroup I^{ad} of $G^{ad} = \mathbf{G}^{ad}(\mathbb{Q}_p)$ on I or $I(1)$. Similar consideration of course apply to $\mathbf{G}^{sc}$ and $\mathbf{G}^{der}$, and the sequence

$$I^{sc}(1) \to I^{der}(1) \hookrightarrow I(1) \to I^{ad}(1)$$

is equivariant for these actions of $I^{ad} = I^{ad}(1) \rtimes T^{ad}_{tors}$.

Let J be the image of $I^{sc}(1) \to I(1)$, so that J is a normal subgroup of I. From the compatible Iwahori decompositions for $I(1)$ and $I^{sc}(1)$ in section 4.2.3, we see that $T(1) \hookrightarrow I(1)$ induces a T^{ad}-equivariant isomorphism

$$T(1)/T(1) \cap J \to I(1)/J.$$

Since the inverse image of $\mathbf{T}(\mathbb{Z}_p)$ in $\mathbf{G}^{sc}(\mathbb{Z}_p)$ equals $\mathbf{T}^{sc}(\mathbb{Z}_p)$ and since also

$$T^{sc}(1) = \mathbf{T}^{sc}(\mathbb{Z}_p) \cap I^{sc}(1),$$

we see that $T(1) \cap J$ is the image of $T^{sc}(1) \to T(1)$. Also, the kernel of $I^{sc}(1) \to I(1)$ equals $Z \cap I^{sc}(1)$ where

$$Z = \ker(\mathbf{G}^{sc} \to \mathbf{G})(\mathbb{Z}_p) = \ker(\mathbf{T}^{sc} \to \mathbf{T})(\mathbb{Z}_p).$$

Therefore, $Z \cap I^{sc}(1)$ is the kernel of $T^{sc}(1) \to T(1)$, which is trivial since Z is finite and $T^{sc}(1) \simeq \mathrm{Hom}(M^{sc}, 1 + p\mathbb{Z}_p)$ has no torsion. We thus obtain exact sequences

$$\begin{array}{ccccccccc} 1 & \to & T^{sc}(1) & \to & T(1) & \to & Q & \to & 0 \\ & & \cap & & \cap & & \| & & \\ 1 & \to & I^{sc}(1) & \to & I(1) & \to & Q & \to & 0 \end{array}$$

where the cokernel Q is the finitely generated $\mathbb{Z}_p$-module

$$Q = (M^\vee/\mathbb{Z}R^\vee) \otimes (1 + p\mathbb{Z}_p)\,.$$

Remark 4.11. If $\mathbf{G}$ is simple, then $M^\vee/\mathbb{Z}R^\vee$ is a finite group of order c, with $c \mid \ell + 1$ if $\mathbf{G}$ is of type A_ℓ, $c \mid 3$ if $\mathbf{G}$ is of type E_6 and $c \mid 4$ in all other cases. Thus, $Q = 0$ and $I^{sc}(1) = I(1)$ unless $\mathbf{G}$ is of type A_ℓ with $p \mid c \mid \ell + 1$ or $p = 3$ and $\mathbf{G}$ is adjoint of type E_6. In these exceptional cases, $M^\vee/\mathbb{Z}R^\vee$ is cyclic, thus $Q \simeq \mathbb{F}_p$.

It follows that $I(1)$ is generated by $I^{sc}(1)$ and $s(1+p\mathbb{Z}_p)$ for $s \in \mathcal{S}$, thus topologically generated by $I^{sc}(1)$ and $s(1+p)$ for $s \in \mathcal{S}$. In view of the results already established in the simply connected case, this shows that the elements listed in $(1-4)$ of Theorem 4.1 indeed form a set of topological generators for $I(1)$.

None of the semi-simple elements in (1) can be removed: they are all needed to generate the above abelian quotient Q of $I(1)$ which indeed kills the unipotent generators in $(2-4)$. Likewise, none of the unipotent elements in (2) can be removed: they are all needed to generate the abelian quotient

$$I(1) \twoheadrightarrow \mathbf{U}(\mathbb{F}_p) \twoheadrightarrow \overline{\mathbf{U}}_1(\mathbb{F}_p) \simeq \prod_{\alpha \in \Delta} \mathbf{U}_\alpha(\mathbb{F}_p)$$

which kills the other generators in (1), (3) and (4). One checks easily using the Iwahori decomposition of $I(1)$ and the product decomposition $\mathbf{U}^- = \prod_{c \in \mathcal{C}} \mathbf{U}^-_c$ that none of the unipotent elements in (3) can be removed. Finally if $p = 3$ and $d \in \mathcal{D}$, the central isogeny $\mathbf{G}^{sc} \to \mathbf{G}^{ad}$ induces an isomorphism $\mathbf{G}^{sc}_d \to \mathbf{G}^{ad}_d$ between the simple (simply connected *and* adjoint) components corresponding to d, thus also an isomorphism between the corresponding pro-p-Iwahori's $I^{sc}_d(1) \to I^{ad}_d(1)$. In particular, the projection $I(1) \to I^{ad}(1) \twoheadrightarrow I^{ad}_d(1)$ is surjective. Composing it with the projection $I^{ad}_d(1) \twoheadrightarrow \mathbb{F}_3^3$ constructed in section 4.2.7, we obtain an abelian quotient $I(1) \twoheadrightarrow \mathbb{F}_3^3$ that kills all of our generators except $x_\alpha(1)$, $x_\beta(1)$ and $x_{\alpha+\beta}(1)$ where $\Delta_d = \{\alpha, \beta\}$. In particular, the generator $x_{\alpha+\beta}(1)$ from (4) is also necessary. This finishes the proof of Theorem 4.1.

4.2.9 The structure of the Frattini quotient of the pro-p Iwahori

The action of $I^{ad} = I^{ad}(1) \rtimes T^{ad}_{tors}$ on $I(1)$ induces an $\mathbb{F}_p$-linear action of

$$T^{ad}_{tors} = \mathrm{Hom}\left(M^{ad}, \mu_{p-1}\right) = \mathrm{Hom}\left(\mathbb{Z}R, \mathbb{F}_p^\times\right)$$

on the Frattini quotient $\tilde{I}(1)$ of $I(1)$. Our minimal set of topological generators of $I(1)$ reduces to an eigenbasis of $\tilde{I}(1)$, i.e. an $\mathbb{F}_p$-basis of $\tilde{I}(1)$ made of eigenvectors for the action of T^{ad}_{tors}. We denote by $\mathbb{F}_p(\alpha)$ the 1-dimensional representation of T^{ad}_{tors} on $\mathbb{F}_p$ defined by $\alpha \in \mathbb{Z}R$. We thus obtain:

Corollary 4.12. *The $\mathbb{F}_p[T^{ad}_{tors}]$-module $\tilde{I}(1)$ is isomorphic to*

$$\mathbb{F}_p^{\sharp\mathcal{S}} \oplus \Big(\oplus_{\alpha\in\Delta}\, \mathbb{F}_p(\alpha)\Big) \oplus \Big(\oplus_{c\in\mathcal{C}}\, \mathbb{F}_p(-\alpha_{c,max})\Big)\Big(\oplus \Big(\oplus_{d\in\mathcal{D}}\, \mathbb{F}_p(\delta_c)\Big) \ \text{ if } p=3\Big).$$

Here $\sharp\mathcal{S}$ denotes the cardinality of the set $\mathcal{S}$. The map $\alpha \mapsto \mathbb{F}_p(\alpha)$ yields a bijection between $\mathbb{Z}R/(p-1)\mathbb{Z}R$ and the isomorphism classes of simple $\mathbb{F}_p[T^{ad}_{tors}]$-modules. In particular some of the simple modules in the previous corollary may happen to be isomorphic. For instance if $\mathbf{G}$ is simple of type B_ℓ and $p=3$, then $-\alpha_{max} \equiv \alpha \bmod 2$ where $\alpha \in \Delta$ is a long simple root. An inspection of the tables in [Bou81] yields the following:

Corollary 4.13. *If $\mathbf{G}$ is simple, the $\mathbb{F}_p[T^{ad}_{tors}]$-module $\tilde{I}(1)$ is multiplicity free unless $p=3$ and $\mathbf{G}$ is of type A_1, B_ℓ or C_ℓ ($\ell \geq 2$), F_4 or G_2.*

In the next section we use this result to construct Galois representations landing in I^{ad} with image containing $I^{ad}(1)$.

4.3 The construction of Galois representations

Let $\mathbf{G}$ be a split simple adjoint group over $\mathbb{Z}_p$ and let $I(1)$ and $I = I(1) \rtimes T_{tors}$ be the corresponding Iwahori groups, as defined in the previous section. We want here to construct Galois representations of a certain type with values in I with image containing $I(1)$. After a short review of p-rational fields in section 4.3.1, we establish a criterion for the existence of our representations in section 4.3.2 and finally give some examples in section 4.3.3.

4.3.1 Short review of p-rational fields

Let K be a number field, $r_2(K)$ the number of complex primes of K, Σ_p the set of primes of K lying above p, M the compositum of all finite p-extensions of K which are unramified outside Σ_p, M^{ab} the maximal abelian extension of K contained in M, and L the compositum of all cyclic extensions of K of degree p which are contained in M or M^{ab}. If $\Gamma = \mathrm{Gal}(M/K)$ then Γ is a pro-p group, $\Gamma^{ab} \cong \mathrm{Gal}(M^{ab}/K)$ is the maximal abelian quotient of Γ, and $\tilde{\Gamma} \cong \Gamma^{ab}/p\Gamma^{ab} \cong \mathrm{Gal}(L/K)$ is the Frattini quotient of Γ.

Definition 4.14. *We say that K is p-rational if the following equivalent conditions are satisfied:*

1. $\mathrm{rank}_{\mathbb{Z}_p}(\Gamma^{ab}) = r_2(K)+1$ *and Γ^{ab} is torsion-free as a $\mathbb{Z}_p$-module,*
2. *Γ is a free pro-p group with $r_2(K)+1$ generators,*
3. *Γ is a free pro-p group.*

The equivalence of (1), (2) and (3) follows from [MNQD90], see also proposition 3.1 and the discussion before remark 3.2 of [Gre16]. There is a considerable literature concerning p-rational fields, including [Mov90], [JNQD93].

Example 4.15. *Suppose that K is a quadratic field and that either $p \geq 5$ or $p=3$ and is unramified in $K/\mathbb{Q}$. If K is real, then K is p-rational if and only if p does not divide the class number of K and the fundamental unit of K is not a p-th power in the completions K_v of K at the places v above p. On the other hand, if K is complex and p does not divide the class number of K, then K is a p-rational field (cf. proposition 4.1 of [Gre16]). However, there are p-rational complex K's for which p divides the class number (cf. chapter 2, section 1, p. 25 of [Mov88b]). For similar results, see also [Fuj08] and [Min86] if K is complex.*

Example 4.16. *Let $K = \mathbb{Q}(\mu_p)$. If p is a regular prime, then K is a p-rational field (cf. [Sha66], see also [Gre16], proposition 4.9 for a shorter proof).*

4.3.2 Construction of Galois representations with open image

Suppose that K is Galois over $\mathbb{Q}$ and p-rational with $p \nmid [K : \mathbb{Q}]$.

Since K is Galois over $\mathbb{Q}$, so is M and we have an exact sequence

$$1 \to \Gamma \to \Pi \to \Omega \to 1$$

where $\Omega = \mathrm{Gal}(K/\mathbb{Q})$ and $\Pi = \mathrm{Gal}(M/\mathbb{Q})$. Conjugation in Π then induces an action of Ω on the Frattini quotient $\tilde{\Gamma} = \mathrm{Gal}(L/K)$ of Γ. Any continuous morphism $\rho : \Pi \to I$ maps Γ to $I(1)$ and induces a morphism $\overline{\rho} : \Omega \to I/I(1) = T_{tors}$ and a $\overline{\rho}$-equivariant morphism $\tilde{\rho} : \tilde{\Gamma} \to \tilde{I}(1)$. If $\rho(\Gamma) = I(1)$, then $\tilde{\rho}$ is also surjective.

Suppose conversely that we are given the finite data

$$\overline{\rho} : \Omega \to T_{tors} \quad \text{and} \quad \tilde{\rho} : \tilde{\Gamma} \twoheadrightarrow \tilde{I}(1).$$

Since Ω has order prime to p, the Schur-Zassenhaus theorem ([Wil98], proposition 2.3.3) implies that the above exact sequence splits. The choice of a splitting $\Pi \simeq \Gamma \rtimes \Omega$ yields a non-canonical action of Ω on Γ which lifts the canonical action of Ω on the Frattini quotient $\tilde{\Gamma}$. By [Gre16], proposition 2.3, $\tilde{\rho}$ lifts to a continuous Ω-equivariant surjective morphism $\rho' : \Gamma \twoheadrightarrow I(1)$, which plainly gives a continuous morphism

$$\rho = (\rho', \overline{\rho}) : \Pi \simeq \Gamma \rtimes \Omega \to I = I(1) \rtimes T_{tors}$$

inducing $\overline{\rho} : \Omega \to T_{tors}$ and $\tilde{\rho} : \tilde{\Gamma} \twoheadrightarrow \tilde{I}(1)$. Thus:

Proposition 4.17. *Under the above assumptions on K, there is a continuous morphism $\rho : \Pi \to I$ such that $\rho(\Gamma) = I(1)$ if and only if there is a morphism $\overline{\rho} : \Omega \to T_{tors}$ such that the induced $\mathbb{F}_p[\Omega]$-module $\overline{\rho}^* \tilde{I}(1)$ is a quotient of $\tilde{\Gamma}$.*

The Frattini quotient $\tilde{I}(1)$ is an $\mathbb{F}_p[T_{tors}]$-module and by the map $\overline{\rho}$, we can consider $\tilde{I}(1)$ as an $\mathbb{F}_p[\Omega]$-module which we denote by $\overline{\rho}^* \tilde{I}(1)$.

Suppose now that

A(K): K is a totally complex abelian (thus CM) Galois extension of $\mathbb{Q}$ which is p-rational of degree $[K : \mathbb{Q}] \mid p - 1$.

Let $\hat{\Omega}$ be the group of characters of Ω with values in $\mathbb{F}_p^\times$, $\hat{\Omega}_{odd} \subset \hat{\Omega}$ the subset of odd characters (those taking the value -1 on complex conjugation), and $\chi_0 \in \hat{\Omega}$ the trivial character. Then by [Gre16] proposition 3.3,

$$\tilde{\Gamma} = \oplus_{\chi \in \hat{\Omega}_{odd} \cup \{\chi_0\}} \mathbb{F}_p(\chi)$$

as an $\mathbb{F}_p[\Omega]$-module. In particular, $\tilde{\Gamma}$ is multiplicity free. Suppose therefore also that the $\mathbb{F}_p[T_{tors}]$-module $\tilde{I}(1)$ is multiplicity free, i.e. by corollary 4.13,

B$(\mathbf{G})$: If $p = 3$, then $\mathbf{G}$ is not of type A_1, B_ℓ or C_ℓ $(\ell \geq 2)$, F_4 or G_2.

For $\mathcal{S}$ as in section 4.2.2, we define

$$\hat{\Omega}_{odd}^{\mathcal{S}} = \begin{cases} \hat{\Omega}_{odd} \cup \chi_0, & \text{if } \mathcal{S} = \emptyset \\ \hat{\Omega}_{odd}, & \text{if } \mathcal{S} \neq \emptyset. \end{cases}$$

Note that $\mathcal{S} = \emptyset$ unless $\mathbf{G}$ if of type A_ℓ with $p \mid \ell + 1$ or $\mathbf{G}$ is of type E_6 with $p = 3$, in which both cases $\mathcal{S}$ is a singleton. We thus obtain:

Corollary 4.18. *Under assumptions $\boldsymbol{A}(K)$ and $\boldsymbol{B}(\mathbf{G})$, there is a morphism $\rho : \Pi \to I$ such that $\rho(\Gamma) = I(1)$ if and only if there is morphism $\overline{\rho} : \Omega \to T_{tors}$ such that the characters $\alpha \circ \overline{\rho} : \Omega \to \mathbb{F}_p^\times$ for $\alpha \in \Delta \cup \{-\alpha_{max}\}$ are all distinct and belong to $\hat{\Omega}_{odd}^{\mathcal{S}}$.*

4.3.3 Some examples.

Write $\Delta = \{\alpha_1, ..., \alpha_\ell\}$ and $\alpha_{max} = n_1\alpha_1 + \cdots + n_\ell\alpha_\ell$ using the conventions of the tables in [Bou81]. In this part we suppose that p is a regular (odd) prime and take $K = \mathbb{Q}(\mu_p)$, so that K is p-rational and $\Omega = \mathbb{Z}/(p-1)\mathbb{Z}$.

Lemma 4.19. *Suppose* $\mathbf{G}$ *is of type* A_ℓ, B_ℓ, C_ℓ *or* D_ℓ *and* $p \geq 2l+3$ *(resp.* $p \geq 2l+5$*) if* $p \equiv 1 \mod 4$ *(resp.* $p \equiv 3 \mod 4$*). Then we can find distinct characters* $\phi_1, ..., \phi_{\ell+1} \in \hat{\Omega}_{odd} \cup \chi_0$ *such that* $\phi_1^{n_1}\phi_2^{n_2}\cdots\phi_\ell^{n_\ell}\phi_{\ell+1} = \chi_0$*. Furthermore, if* $\mathbf{G}$ *is of type* A_ℓ *and* ℓ *is odd, then one can even choose the characters* $\phi_1, ..., \phi_{\ell+1}$ *to be inside* $\hat{\Omega}_{odd}$*.*

Proof. Since Ω is (canonically) isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$, $\sharp\hat{\Omega}_{odd} = \frac{p-1}{2}$ and there are exactly $[\frac{p-1}{4}]$ pairs of characters $\{\chi, \chi^{-1}\}$ with $\chi \neq \chi^{-1}$ in $\hat{\Omega}_{odd}$. The condition on p is equivalent to $\ell \leq 2[\frac{p-1}{4}] - 1$.

If $\mathbf{G}$ is of type A_ℓ, then $\alpha_{max} = \alpha_1 + \cdots + \alpha_\ell$. If ℓ is even and $\frac{\ell}{2} \leq [\frac{p-1}{4}]$, then we can pick $\frac{\ell}{2}$ distinct pairs of odd characters $\{\chi, \chi^{-1}\}$ as above for $\{\phi_1, \cdots, \phi_\ell\}$ and set $\phi_{\ell+1} = \chi_0$. If ℓ is odd and $\frac{\ell+1}{2} \leq [\frac{p-1}{4}]$, then we can choose $\frac{\ell+1}{2}$ distinct such pairs for the whole set $\{\phi_1, \cdots, \phi_{\ell+1}\}$.

If $\mathbf{G}$ is of type D_ℓ (with $\ell \geq 4$), then $\alpha_{max} = \alpha_1 + 2\alpha_2 + ... + 2\alpha_{\ell-2} + \alpha_{\ell-1} + \alpha_\ell$. Now if ℓ is odd we can pick $\frac{\ell+1}{2}$ such pairs $\{\chi, \chi^{-1}\}$, one for $\{\phi_{\ell-1}, \phi_\ell\}$, another pair for $\{\phi_1, \phi_{\ell+1}\}$ and $\frac{\ell-3}{2}$ such pairs for $\{\phi_2, ..., \phi_{\ell-2}\}$. If ℓ is even, we let ϕ_2 be the trivial character, and we can choose $\frac{\ell}{2}$ such pairs of characters $\{\chi, \chi^{-1}\}$, one pair for $\{\phi_1, \phi_{\ell-1}\}$, another pair for $\{\phi_\ell, \phi_{\ell+1}\}$ and $\frac{\ell-4}{2}$ such pairs for $\{\phi_3, ..., \phi_{\ell-2}\}$. So the inequality that we will need is $4 \leq \ell \leq 2[\frac{p-1}{4}] - 1$.

If $\mathbf{G}$ is of type B_ℓ (with $\ell \geq 2$), then $\alpha_{max} = \alpha_1 + 2\alpha_2 + ... + 2\alpha_\ell$. If ℓ is odd then we pick $\frac{\ell+1}{2}$ pairs of characters $\{\chi, \chi^{-1}\}$; one pair for $\{\phi_1, \phi_{\ell+1}\}$ and $\frac{\ell-1}{2}$ such pairs for $\{\phi_2, ..., \phi_\ell\}$. If ℓ is even then we need $\frac{\ell}{2}$ pairs of $\{\chi, \chi^{-1}\}$; one pair for $\{\phi_1, \phi_{\ell+1}\}$ and $\frac{\ell-2}{2}$ such pairs for $\{\phi_3, ..., \phi_\ell\}$ and we let ϕ_2 be the trivial character. So in this case we need $3 \leq \ell \leq 2[\frac{p-1}{4}] - 1$.

The remaining C_ℓ case is analogous. □

Lemma 4.20. *Suppose* $\mathbf{G}$ *is of type* E_6, E_7, E_8, F_4 *or* G_2 *and*

$$p \geq \sum_{i=1}^{\ell}(2i-1)n_i + 2\ell.$$

Then we can find distinct characters $\phi_1, ..., \phi_{\ell+1} \in \hat{\Omega}_{odd}$ *such that*

$$\phi_1^{n_1}\phi_2^{n_2}\cdots\phi_\ell^{n_\ell}\phi_{\ell+1} = \chi_0.$$

Proof. The choice of a generator ξ of $\mathbb{F}_p^\times$ yields an isomorphism $\mathbb{Z}/(p-1)\mathbb{Z} \simeq \hat{\Omega}$, mapping i to χ_i and $1 + 2\mathbb{Z}/(p-1)\mathbb{Z}$ to $\hat{\Omega}_{odd}$. We set $\phi_i = \chi_{2i-1} \in \hat{\Omega}_{odd}$ for $i = 1, \cdots, \ell$ and $\phi_{\ell+1} = \chi_{-r}$ where $r = \sum_{i=1}^{\ell} n_i \cdot (2i-1)$. The tables in [Bou81] show that $h = \sum_{i=1}^{\ell} n_i$ is odd, thus also $\phi_{\ell+1} \in \hat{\Omega}_{odd}$ and plainly $\phi_1^{n_1}\cdots\phi_\ell^{n_\ell}\phi_{\ell+1} = 1$. If $p \geq \sum_{i=1}^{\ell}(2i-1)n_i + 2\ell$, the elements $\{2i-1, -\sum_{i=1}^{\ell} n_i \cdot (2i-1); i \in [1, \ell]\}$ are all distinct modulo $p-1$, which proves the lemma. □

Remark 4.21. For $\mathbf{G}$ of type E_6, E_7, E_8, F_4 or G_2, the tables in [Bou81] show that the constant $\sum_{i=1}^{\ell}(2i-1)n_i + 2\ell$ of lemma 4.20 is $79, 127, 247, 53, 13$ respectively.

Recall that $\Pi = \mathrm{Gal}(M/\mathbb{Q})$ and $\Gamma = \mathrm{Gal}(M/K)$.

Corollary 4.22. *There is a constant* c *depending only upon the type of* $\mathbf{G}$ *such that if* $p > c$ *is a regular prime, then for* $K = \mathbb{Q}(\mu_p)$*,* M*,* Π *and* Γ *as above, there is a continuous morphism* $\rho : \Pi \to I$ *with* $\rho(\Gamma) = I(1)$*.*

In conclusion, we have determined a minimal set of topological generators of the pro-p Iwahori subgroup of split reductive groups over $\mathbb{Z}_p$ (theorem 4.1) and used it to study the structure of the Frattini quotient $\tilde{I}(1)$ as an $\mathbb{F}_p[T_{tors}^{ad}]$-module (corollary 4.12). Then we have used corollary 4.12 to determine when $\tilde{I}(1)$ is multiplicity free (see corollary 4.13). Furthermore, in proposition 4.17 and corollary 4.18, assuming p-rationality, we have shown that we can construct Galois representations if and only if we can find a suitable list of distinct characters in Ω, the existence of which is established in section 4.3.3 under the assumption $K = \mathbb{Q}(\mu_p)$, for any sufficiently large regular prime p (see corollary 4.22).

5 SAGE computations on p-rational fields and heuristics on Greenberg's p-rationality conjecture

5.1 Introduction (work in collaboration with Razvan Barbulescu)

The notion of p-rationality of number fields naturally appears in several branches of number theory. In Iwasawa theory, the study of Galois groups of infinite towers of number fields, a celebrated conjecture of Greenberg concerns the λ-invariant [Gre76] which has been connected to p-rationality [Sau98, Th. 1.1]. In the study of the inverse Galois problem, Greenberg [Gre16] proposed a method to prove that a p-adic Lie group appears as a Galois group over $\mathbb{Q}$ under the assumption of existence of p-rational fields. In algorithmic number theory, the density of p-rational number fields is related to the Cohen-Lenstra-Martinet heuristic [CL84b, CM90] and to the valuation of the p-adic regulator [Gra16b, HZ16].

The context in which the notion of p-rationality was introduced includes the work of Shafarevich [Sha66] which, for any regular prime p, proved properties of the p-part of the Ray class group of the p-th cyclotomic fields. Gras and Jaulent [GJ89] defined p-regular number fields, which have similar properties to cyclotomic fields associated to regular primes. Movahhedi [Mov88b, Chap II] and Thong Nguyen Quang Do defined the notion of p-rational fields. Nguyen Quang Do and Jaulent [JNQD93] proved that there is a large intersection between the set of p-regular and p-rational fields. Our object is to describe families of p-rational Galois fields over $\mathbb{Q}$.

Let K be a Galois number field of signature (r_1, r_2), p an odd prime, $\mu(K)_p$ the roots of unity in K whose order is a power of p, S_p the set of prime ideals of K above p, M the compositum of all finite p-extensions of K which are unramified outside S_p and M^{ab} the maximal abelian extension of K contained in M. Note that the group $\Gamma := \mathrm{Gal}(M/K)$ is a pro-p group and that $\Gamma^{ab} \cong \mathrm{Gal}(M^{ab}/K)$ is the maximal abelian quotient of Γ. From section 4.3.1, we recall the definition of p-rational fields.

Proposition-Definition 5.1 ([MNQD90])**.** *The number field K is said to be p-rational if the following equivalent conditions are satisfied:*

1. $\mathrm{rank}_{\mathbb{Z}_p}(\Gamma^{ab}) = r_2 + 1$ *and Γ^{ab} is torsion-free as a $\mathbb{Z}_p$-module,*
2. Γ *is a free pro-p group with $r_2 + 1$ generators,*
3. Γ *is a free pro-p group.*

If K satisfies Leopoldt's conjecture [Was97, Sec 5.5] (e.g. K is abelian) then the above conditions are also equivalent to

4. *(a)* $\left\{\alpha \in K^\times \mid \begin{array}{c} \alpha\mathcal{O}_K = \mathfrak{a}^p \text{ for some fractional ideal } \mathfrak{a} \\ \text{and } \alpha \in (K_\mathfrak{p}^\times)^p \text{ for all } \mathfrak{p} \in S_p \end{array}\right\} = (K^\times)^p$,
   (b) and the map $\mu(K)_p \to \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism.

If $p > [K : \mathbb{Q}] + 1$ then condition 4, (b) is ok. Indeed, the cyclotomic polynomial $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ and $\mathbb{Q}_p[x]$ so $\deg(\mathbb{Q}(\zeta_p)) > \deg K$ and $\deg \mathbb{Q}_p(\zeta_p) > \deg K_\mathfrak{p}$ for any $\mathfrak{p} \mid p$, so $\mu(K)_p = \{1\}$ and $\prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p = \{1\}$, which proves that the condition 4.(b) is met.

The equivalent conditions of (1), (2), (3) and (4) can be found in [Gre16, Sec. 3] and [Mov88b, Chapter II]. One can directly prove that a field is p-rational using this definition, but more elaborated results allow us to write shorter proofs. We illustrate the strength of each result by proving p-rationality of some number fields.

Examples 5.2.

1. *The imaginary quadratic fields of class number one, i.e. $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$ are p-rational for any primes $p \geq 5$. Indeed, in order to use point (4) of Definition 5.1, let K be any of the above fields and α an element of K which is a p-th power in all the p-adic completions of K and such that the principal ideal generated by α is a p-th power. Since the ring of integers of K is a principal ideal domain, α is a p-th power in K, up to multiplication by a unit. Since the unit rank of K is zero and since K has no p-th roots of unity we conclude that α is a p-th power of K. As $p \geq 5$, $\mathbb{Q}_p$ and its quadratic extensions have no p-th roots of unity so that $\mu(K)_p \to \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism.*

2. *$\mathbb{Q}(i)$ is 2-rational. After (1), for $p \geq 5$, we are left with showing that if a unit of $\mathbb{Q}(i)$ is a square in the 2-adic completion then it is a square in $\mathbb{Q}(i)$. Suppose that i is a square in the completion of $\mathbb{Z}[i]$ with respect to $\mathfrak{p} = \langle 1+i \rangle$. Then there exist two integers a and b such that*

$$(a+ib)^2 \equiv i \pmod{\mathfrak{p}^2}.$$

But $\mathfrak{p}^2 = 2\mathbb{Z}[i]$, so $2ab \equiv 1 \pmod 2$, which is a contradiction. Hence, the only elements of $\mathbb{Q}(i)$ which are squares in the 2-adic completion of $\mathbb{Q}(i)$ are also squares in $\mathbb{Q}(i)$.

These examples are also treated in [Mov90, Example (c), page 24].

For many properties of p-rational fields we refer the reader to the corresponding chapter of [Gra13, Ch IV.3].

In the following, we recall the use of p-rationality in constructing Galois representations with open image. Greenberg's result [Gre16, Prop 6.1] is as follows: if K is abelian over $\mathbb{Q}$ and p-rational with the order of $\mathrm{Gal}(K/\mathbb{Q})$ dividing $p-1$ then, for all $n \in \mathbb{N}$, there exists an explicit continuous representation

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}(n, \mathbb{Z}_p)$$

such that $\rho(\Gamma)$ is the pro-p Iwahori subgroup of $\mathrm{SL}(n, \mathbb{Z}_p)$, i.e. the subgroup of $\mathrm{SL}(n, \mathbb{Z}_p)$ whose reduction mod p is the upper unipotent subgroup, under an assumption on the characters of $\mathrm{Gal}(K/\mathbb{Q})$. We recall that M is the compositum of all finite p-extensions of K which are unramified outside the places of K above p. We obtain hence the existence of the morphism ρ above as soon as we can prove the existence of p-rational fields K with an additional property on the characters.

Greenberg also noted that the hypothesis on the characters are met if K is complex and $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^t$ for some t, which raises the question of existence of p-rational fields with such Galois groups. The goal of this work is to investigate the following conjecture:

Conjecture 5.3 (Greenberg [Gre16])**.** *For any odd prime p and for any t, there exist a p-rational field K such that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$.*

Let us generalize Greenberg's conjecture to all finite groups.

Problem 5.4. *Given a finite group G and a prime p, decide if the following statements hold:*

1. *there exists a number field of Galois group G which is p-rational, in this case we say Greenberg's conjecture holds for G and p or simply that $\mathrm{GC}(G,p)$ holds;*
2. *there exist infinitely many number fields of Galois group G which are p-rational, in this case we say that the infinite version of Greenberg's conjecture holds for G and p or simply that $\mathrm{GC}_\infty(G,p)$ holds.*

Note that this problem is a strengthening of the inverse Galois problem, which is itself open in the non-abelian case (cf [MM13]). Also, note that we don't discuss the related conjecture of Gras [Gra16b, Conj. 8.11] which states that every number field is p-rational for all but finitely many primes.

Remark 5.5. One should not confound this new conjecture to an older conjecture on Iwasawa invariants (cf [Gre76]). Let $\mathcal{K}$ be the pairs of totally real fields K and primes p which splits totally in K. Due to Remark 2.2 of [Gra16a], a particular case of the celebrated conjecture of Greenberg concerning the Iwasawa invariants and a strengthening of the newer p-rationality conjecture of Greenberg can be stated as follows :

$$\begin{array}{lll} \text{invariants conjecture:} & \forall (K,p) \in \mathcal{K}, & \lambda = \mu = 0 \\ p\text{-rationality conjecture:} & \forall t,\ \forall p,\ \exists K, (K,p) \in \mathcal{K},\ \mathrm{Gal}(K) = (\frac{\mathbb{Z}}{2\mathbb{Z}})^t, & \lambda = \mu = \nu = 0, \end{array}$$

where $\lambda = \lambda_p(K), \mu = \mu_p(K), \nu = \nu_p(K)$ are the Iwasawa invariants associated to the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K (cf. [Gre76], see also [Was97] for the fact that $\mu = 0$ when K is abelian). The case of totally split p is a particular case of Greenberg's invariants conjecture, but it is an open case. Greenberg's p-rationality conjecture doesn't put conditions on K being totally real but any compositum of quadratic fields has a maximal real subfield whose degree is at least half of the total degree. The condition that p is totally split is not discussed in the rest of the text but numerical experiments show that it is not hard to satisfy this additional constraint.

The main result in this section is summarized by the following theorem. Let Φ_m denote the cyclotomic polynomial associated to m and $\varphi(m)$ its degree.

Theorem 5.6.

1. *For all odd primes p, $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds.*
2. *Assume there exist infinitely many odd integers a such that $m = \frac{1}{4}(a^2+27)$ is prime and such that the arithmetic conditions in Hypothesis 5.35 are satisfied. Then $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, 5)$ holds.*
3. *Under conjectures based on heuristics and numerical experiments (Conjecture 5.41 and Conjecture 5.39), when $q = 2$ or 3, for any prime p and any integer t such that $p > 5q^t$, $\mathrm{GC}_\infty((\mathbb{Z}/q\mathbb{Z})^t, p)$ holds.*

Roadmap. In Section 5.2, we relate the notion of p-rationality to that of class number and p-adic regulator, which is enough to prove $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, 3)$, which is point (1) of Theorem 5.6, and to give an example of a p-rational field with Galois group $(\mathbb{Z}/2\mathbb{Z})^7$. We also recall the existing conjectures on the class number due to Cohen, Lenstra and Martinet and on the p-adic regulator.

In Section 5.6, we start by recalling an algorithm to test the divisibility by p of the class number of cyclic cubic fields without computing the class number, inspired by an article of M.-N. Gras. Furthermore, we give a new algorithm to produce units in cyclic cubic fields which are used to test the valuation in p of the p-adic regulator, which is faster than computing a system of fundamental units. Then we recall the algorithm of Pitoun and Varescon to test p-rationality for arbitrary number fields, which allows us to give examples of p-rational number fields of non-abelian Galois groups.

In Section 5.11, we find a family of cyclic cubic number fields which contains infinitely many 5-rational fields under a list of arithmetic assumptions; this proves point (2) of Theorem 5.6.

In Section 5.12, we do a numerical experiment to test divisibility by p of the class number of cyclic cubic fields with discriminant up to 10^{14}, which extends the existing calculations [CM87], confirming the Cohen-Lenstra-Martinet conjecture. Then we do a numerical experiment for number fields of Galois group $(\mathbb{Z}/3\mathbb{Z})^2$ and discriminant up to 10^{12}. As our computations agree with the Cohen-Lenstra-Martinet heuristic, we can write down Conjecture 5.39 on the divisibility by p of the class number of such fields. Next we prove a Kuroda-like formula for p-adic regulators of fields of Galois group $(\mathbb{Z}/2\mathbb{Z})^2$, which relates the p-adic regulator of the compositum to those of the quadratic subfields. Based on a heuristic and numerical experiments we write down Conjecture 5.41 which applies to fields of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ where $q = 2$ or 3. We show that two conjectures from the literature imply that $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, p)$ holds, and that Conjecture 5.41 and the Cohen-Lenstra-Martinet conjecture imply Greenberg's p-rationality conjecture (point (3) of Theorem 5.6).

5.2 Preliminaries

In the general case, p-rationality is hard to test so that it is important to have a simple criterion in terms of classical invariants as the class number and the p-adic regulator (Sec 5.3). This raises the question of the density of number fields whose class number is not divisible by p (Sec 5.4) and of the valuation in p of the p-adic regulator (Sec 5.5).

In this sequel, p denotes an odd prime and K an abelian number field, $\mathrm{Disc}(K)$ the discriminant of K, $\mathcal{O}_K$ the ring of integers, E_K the unit group, h_K the class number of K, (r_1, r_2) the signature of K, $r = r_1 + r_2 - 1$ the rank of E_K, S_p the set of primes of K lying above p, $K_\mathfrak{p}$ the completion of K at a prime $\mathfrak{p} \in S_p$. For $c \in \mathbb{N}^*$ we denote ζ_c a primitive c-th root of unity.

5.3 A simple criterion to prove p-rationality

Let us call p-primary unit, any unit in K which is a p-th power in $K_\mathfrak{p}$ for any $\mathfrak{p} \mid p$ but which is not a p-th power in K.

Lemma 5.7 ([Mov88b] Chap II, [Gre16] Rem 3.2)**.** *Let K be a number field which satisfies Leopoldt's conjecture (e.g. $\mathrm{Gal}(K/\mathbb{Q})$ is abelian) and a prime p such that the map $\mu(K)_p \to \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism (e.g. $p > [K:\mathbb{Q}]+1$) and $p \nmid h_K$. Then K is p-rational if and only if K has no p-primary units.*

Proof. If K has a p-primary unit α then $\alpha\mathcal{O}_K = (\mathcal{O}_K)^p = \mathcal{O}_K$ and, by point 4.(a) of Proposition-Definition 5.1, K is not p-rational.

Conversely, assume that K has no p-primary units. Let $\alpha \in K^*$ be such that $\alpha\mathcal{O}_K = \mathfrak{a}^p$ and $\forall \mathfrak{p} \mid p$, $\alpha \in (K_\mathfrak{p})^p$. Then $\mathfrak{a}$ is a p-torsion element in the class group, which has order relatively prime to p so $\mathfrak{a}$ is a principal ideal. If β be a generator of $\mathfrak{a}$ then $\alpha\mathcal{O}_K = \beta^p\mathcal{O}_K$ so $\varepsilon := \alpha\beta^{-p}$ is a unit. For all $\mathfrak{p} \mid p$, $\alpha \in (K_\mathfrak{p})^p$ so $\varepsilon \in (K_\mathfrak{p})^p$. Since K is assumed without p-primary units and K has no p-th roots of unity, there exists $\eta \in K$ such that $\alpha\beta^{-p} = \eta^p$, so $\alpha \in K^p$. Hence point 4.(a) of Proposition-Definition 5.1 holds and, since we assumed that 4.(b) holds, K is p-rational. □

Note that in the case of quadratic and cubic number fields K it suffices to take $p \geq 5$ in order to ensure that point 4.(b) of Proposition-Definition 5.1 holds. In the sequel $p \geq 5$ so that we can forget of point 4.(b).

Lemma 5.8. *For any prime $p \geq 5$ not belonging to $\{\frac{1}{2}a^2 \pm 1 \mid a \in \mathbb{N}\}$ the real quadratic number field $K = \mathbb{Q}(\sqrt{p^2-1})$ is p-rational.*

Proof. Let us note first that $\varepsilon = p + \sqrt{p^2-1}$ is a fundamental unit of K. Indeed, let ε_0 be the fundamental unit of K which is larger than 1 and let n be such that $\varepsilon = \varepsilon_0^n$. If n is even then $\eta := \varepsilon_0^{n/2}$ is such that $\varepsilon = \eta^2$. Then $N_{K/\mathbb{Q}}(\varepsilon) = N_{K/\mathbb{Q}}(\eta)^2 = 1$. Furthermore, η^2 cancels the minimal polynomial of ε so η cancels $P(x) := x^4 - 2px^2 + 1 = 0$. Since η is a unit it's minimal polynomial is $\mu_\eta := x^2 - 2ax \pm 1 = 0$, where $a = \mathrm{Tr}(\eta)$. Since $\mu_\eta(x)$ divides $P(x)$ we obtain that $p = \frac{1}{2}a^2 \pm 1$, which contradicts the assumption on p. Therefore, n is odd and we have

$$(\varepsilon_0^n + \frac{1}{\varepsilon_0^n}) = \omega(\varepsilon_0 + \frac{1}{\varepsilon_0}),$$

where $\omega = \varepsilon_0^{n-1} + \varepsilon_0^{n-3} + \cdots + \frac{1}{\varepsilon_0^{n-3}} + \frac{1}{\varepsilon_0^{n-1}}$. Since $\varepsilon_0 \cdot (\varepsilon_0 - \mathrm{Tr}(\varepsilon_0)) = \pm 1$ we have $\omega \in \mathbb{Z}[\varepsilon_0]$. We also have $\omega = \mathrm{Tr}(\varepsilon)/\mathrm{Tr}(\varepsilon_0) \in \mathbb{Q}$ so ω belongs to $\mathbb{Q} \bigcap \mathbb{Z}[\varepsilon_0] = \mathbb{Z}$. Since $\mathrm{Tr}(\varepsilon) = 2p$ the only possibilities for μ_{ε_0} are $x^2 \pm 2px \pm 1$, $x^2 \pm px \pm 1$, $x^2 \pm 2x \pm 1$ and $x^2 \pm x \pm 1$. The discriminants of these polynomials cannot divide $p^2 - 1$ except for $x^2 \pm 2px \pm 1$, so $\varepsilon_0 \in \{\pm\varepsilon, \pm\frac{1}{\varepsilon_0}\}$. If ε_0 is chosen such that it is larger than 1 then $\varepsilon_0 = \varepsilon$.

By a result of Louboutin [Lou98, Theorem 1] we have the effective bound

$$h(K) \leq \sqrt{\mathrm{Disc}(K)}\frac{e\log(\mathrm{Disc}(K))}{4\log\varepsilon}.$$

Since $\mathrm{Disc}(K) \leq p^2 - 1$, we conclude that $h(K) < p$ and hence $p \nmid h(K)$.

Let us show that ε is not a p-primary unit. We have

$$\begin{aligned}\varepsilon^{p^2-1} - 1 &\equiv (p^2-1)^{\frac{p^2-1}{2}} - 1 + p(p^2-1)^{\frac{p^2-3}{2}}\sqrt{p^2-1} \pmod{p^2\mathbb{Z}[\sqrt{p^2-1}]} \\ &\equiv \pm p\sqrt{p^2-1} \pmod{p^2\mathbb{Z}[\sqrt{p^2-1}]}.\end{aligned}$$

Since $p^2\mathbb{Z}[\sqrt{p^2-1}] \subset p^2\mathcal{O}_K$ this shows that the p-adic logarithm of ε is not a multiple of p^2, so ε is not p-primary. By Lemma 5.7 we conclude that K is p-rational. □

In the sequel the number fields K have no p-th roots of unity.

Lemma 5.9 ([Gre16] Prop 4.1.1(i), [Mov88b] Chapter II)**.** *Let p be an odd prime and $K = \mathbb{Q}(\sqrt{-d})$, with $d > 0$, $d \neq 3$ and squarefree, an imaginary quadratic field such that $p \nmid h_K$. If $p \geq 5$ then K is p-rational. If $p = 3$ then $\mathbb{Q}(\sqrt{-d})$ is 3-rational if and only if $d \not\equiv 3 \mod 9$.*

Proof. Since the unit rank of imaginary fields is zero, we can conclude by Lemma 5.7 if we show that the map $\mu(K)_p \to \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism.

The case when $p \geq 5$ is direct because $5 > 3 = [K : \mathbb{Q}] + 1$.

Let us now consider the case when $p = 3$. Since $\Phi_3(x)$ has no roots in $\mathbb{Q}_3$ we have $[\mathbb{Q}_3(\zeta_3) : \mathbb{Q}] = 2$, so the only 3-adic quadratic field which contains primitive 3rd roots of unity is $\mathbb{Q}_3(\zeta_3) = \mathbb{Q}_3(\sqrt{-3})$. The 3-completion of K, $\mathbb{Q}_3(\sqrt{-d})$ equals $\mathbb{Q}_3(\sqrt{-3})$ if and only if $3 \mid d$ and $d/3$ is a square in $\mathbb{Q}_3$ or equivalently if $d \equiv 3 \mod 9$.

If $3 \nmid d$, then we know that $\prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p = \{1\}$. We also know that 3 is not ramified in K so K does not contain $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ and $\mu_p(K) = \{1\}$.

If $3 \mid d$, $d \equiv 3 \mod 9$ and $d \neq 3$ then $\mu(K)_p = \{1\}$ whereas $\prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p \neq \{1\}$.

If $3 \mid d$ and $d \not\equiv 3 \mod 9$, then $\mu(K)_p = \{1\} = \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$. □

Hartung proved what it takes to conclude that $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds for $p = 3$ and he noted that his method works for any larger prime p:

Lemma 5.10 ([Har74]). *For all odd primes p there exist infinitely many square-free integers $D < 0$ such that $h_{\mathbb{Q}(\sqrt{D})} \cdot D \not\equiv 0 \pmod{p}$.*

Corollary 5.11. *For all odd prime p, $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds.*

Almost forty years after Hartung's work on imaginary fields, Byeon proved the corresponding result for the existence of real p-rational fields.

Lemma 5.12 ([Bye01a] Prop. 3.3, [Bye01b] Thm. 1.1). *For $p \geq 5$, there exists infinitely many integers $D > 0$ such that $h_{\mathbb{Q}(\sqrt{D})} \cdot D \not\equiv 0 \pmod{p}$ and $\mathbb{Q}(\sqrt{D})$ has no p-primary units.*

Corollary 5.13. *For all prime $p \geq 5$ there exist infinitely many real quadratic fields K which are p-rational.*

The study of p-rationality in the general case of $G = (\mathbb{Z}/2\mathbb{Z})^t$ with $t \geq 1$ reduces to the case of quadratic fields as proven by a result of Greenberg.

Lemma 5.14. *([Gre16, Prop 3.6]) Let q and p be two distinct primes and K a number field such that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^t$. Then K is p-rational if and only if all the subfields of K of degree q are p-rational.*

We combine Lemmas 5.14 and 5.7 to obtain:

Proposition 5.15. *Let K be a number field such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$ for some prime q and let $p \geq 5$ be a prime different from q. If for all cyclic subfields of K the class number is not divisible by p and has no p-primary units then K is p-rational.*

Remark 5.16. Henceforth, everywhere we assume that $p \nmid [K : \mathbb{Q}]$ because the p-rational extensions of $\mathbb{Q}$ of degree p are characterized in Example 3.5.1 of Section IV of [Gra13]. Assume L is a p-extension of $\mathbb{Q}$ which satisfies Leopoldt's conjecture at p. Then L is p-rational if and only if the following two conditions are satisfied:

1. $L/\mathbb{Q}$ is unramified outside p,
2. $L/\mathbb{Q}$ is unramified outside of $\{p, l\}$, where $l \neq p$ is prime and satisfies $p^2 \nmid (l^{p-1} - 1)$ if $p \geq 3$ or $8 \nmid (l \pm 1)$ if $p = 2$.

See *loc. cit.* for 2-rational abelian 2-extensions of $\mathbb{Q}$ and 3-rational abelian 3-extensions of $\mathbb{Q}$.

Example 5.17. *For each prime between 5 and 97, Table 1 gives examples of complex fields K of the form $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$ which are p-rational. The last column indicates the representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with open image, as constructed thanks to Proposition 6.7 in [Gre16].*

For each of these fields we applied Proposition 5.15, for which we verified that the $2^{t-1} - 1$ real quadratic subfields have class number non divisible by p and no p-primary units, and that the 2^{t-1} imaginary quadratic subfields have class number non divisible by p.

The examples were found using sage scripts available in the online complement [BR17a] by testing the smallest possible value of $d_1 \geq 1$, and recursively for $i = 2, 3, \ldots, t-1$ we found the smallest possible value of $d_i \geq d_{i-1} + 1$ so that $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_i})$ is p-rational. Finally, we selected d_t as the negative integer of the smallest absolute value such that the class numbers of all the imaginary quadratic subfields of K are not divisible by p.

Note that d_1, ..., d_{t-2} are relatively small showing that it was easy to find examples with small t. However, there can be large gaps between d_{t-2} and d_{t-1} showing that the search becomes much more difficult as t increases. We give an explanation for this observation in Remark 5.42. The value of $|d_t|$ is not very large showing that it was relatively easy to go from a totally real field to a totally complex one, as required by Greenberg's method to construct Galois representations with open image (cf. discussion before Conjecture 5.3, see also Prop 6.7 and Prop 6.1 of [Gre16]). The search of the negative determinant d_t is fast also due to the Hurwitz-Eichler theorem which allows us to compute recursively the class numbers of imaginary quadratic fields [Coh13, Section 5.3.2].

Greenberg and Pollack [Gre16, Sec 4.2, page 99] gave the examples of the field
$\mathbb{Q}(\sqrt{13}, \sqrt{145}, \sqrt{209}, \sqrt{269}, \sqrt{373}, \sqrt{-1})$, which is 3-rational, and of the 5-rational field
$\mathbb{Q}(\sqrt{6}, \sqrt{11}, \sqrt{14}, \sqrt{59}, \sqrt{-1})$, for which $t = 5$ is smaller than that of the example on the first row of Table 1.

In order to investigate the existence of p-rational fields it is necessary to discuss the density of fields whose class number is divisible by p.

p	t	$d_1, \ldots, d_t$	open image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in
5	7	2,3,11,47,97,4691,-178290313	$\forall n \in [4, 61]$, $\mathrm{GL}(n, \mathbb{Z}_5)$
7	7	2,5,11,17,41,619,-816371,	$\forall n \in [4, 61]$, $\mathrm{GL}(n, \mathbb{Z}_7)$
11	8	2,3,5,7,37,101,5501,-1193167	$\forall n \in [4, 125]$, $\mathrm{GL}(n, \mathbb{Z}_{11})$
13	8	3,5,7,11,19,73,1097,-85279	$\forall n \in [4, 125]$, $\mathrm{GL}(n, \mathbb{Z}_{13})$
17	8	2,3,5,11,13,37,277,-203	$\forall n \in [4, 125]$, $\mathrm{GL}(n, \mathbb{Z}_{17})$
19	9	2,3,5,7,29,31,59,12461, -7663849	$\forall n \in [4, 253]$, $\mathrm{GL}(n, \mathbb{Z}_{19})$
23	9	2,3,5,11,13,19,59,2803,-194377	$\forall n \in [4, 253]$, $\mathrm{GL}(n, \mathbb{Z}_{23})$
29	9	2,3,5,7,13,17,59,293,-11	$\forall n \in [4, 253]$, $\mathrm{GL}(n, \mathbb{Z}_{29})$
31	9	3,5,7,11,13,17,53,326,-8137	$\forall n \in [4, 253]$, $\mathrm{GL}(n, \mathbb{Z}_{31})$
37	9	2,3,5,19,23,31,43,569,-523	$\forall n \in [4, 253]$, $\mathrm{GL}(n, \mathbb{Z}_{37})$
41	9	2,3,5,11,13,17,19,241,-1	$\forall n \in [4, 253]$, $\mathrm{GL}(n, \mathbb{Z}_{41})$
43	10	2,3,5,13,17,29,31,127,511,-2465249	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{43})$
47	10	2,3,5,7,11,13,17,113,349,-1777	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{47})$
53	10	2,3,5,7,11,13,17,73,181,-1213	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{53})$
59	10	2,3,5,11,13,17,31,257,1392,-185401	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{59})$
61	10	2,3,5,7,13,17,29,83,137, -24383	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{61})$
67	11	2,3,5,7,11,13,17,31,47,5011,-2131	$\forall n \in [4, 1023]$, $\mathrm{GL}(n, \mathbb{Z}_{67})$
71	10	2,3,5,11,13,17,19,59, 79,-943	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{71})$
73	10	2,3,5,7,13,17,23,37,61,-1	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{73})$
79	10	2,3,5,7,11,23,29,103,107,-1	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{79})$
83	10	2,3,5,7,11,13,17,43,97,-1	$\forall n \in [4, 509]$, $\mathrm{GL}(n, \mathbb{Z}_{83})$
89	11	2,3,5,7,11,23,31,41,97,401,-425791	$\forall n \in [4, 1023]$, $\mathrm{GL}(n, \mathbb{Z}_{89})$
97	11	2,3,5,7,11,13,19,23,43,73,-1	$\forall n \in [4, 1023]$, $\mathrm{GL}(n, \mathbb{Z}_{97})$

Table 1: Examples of p-rational complex number fields of the form $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$ and their consequences on the existence of continuous representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with open image.

5.4 Density of fields K where $p \mid h_K$: the Cohen-Lenstra heuristic

Cohen and Lenstra [CL84b, CL84a] created a heuristic principle which can be used to derive conjectures on the density of class numbers divisible by a given integer. We say that a set $\mathcal{S}$ of number fields has a density δ and write $\mathrm{Prob}(\mathcal{S}) = \delta$ if

$$\lim_{X \to \infty} \frac{\#\{K \in \mathcal{S} \mid \mathrm{Disc}(K) \leq X\}}{\#\{K \mid \mathrm{Disc}(K) \leq X\}} = \delta.$$

Here $\#\{K \mid \mathrm{Disc}(K) \leq X\}$ denotes the number of fields with discriminant less than or equal to X For simplicity we write Prob(property) to designate the density of the set of number fields satisfying the property. Cohen and Lenstra studied the case of quadratic fields, Cohen and Martinet [CM90, CM87] studied the case of fields K of degree 3 and 4, not necessarily cyclic, while more recently Miller [Mil15, Sec 3] studied the case of cyclic extensions:

Conjecture 5.18 ([Mil15] Sec 3)**.** *Let K be a cyclic extension of $\mathbb{Q}$ of odd prime degree q and p a prime not dividing q. Then* $\mathrm{Prob}(p \nmid h_K) = \prod_{k \geq 2}(1 - p^{-k\omega})^{\frac{q-1}{\omega}}$ *where ω is the multiplicative order of p modulo q.*

In the particular case of cubic cyclic fields this conjecture corroborates with the conjecture of Cohen and Martinet:

Conjecture 5.19 ([CM87] Sec 2, Ex 2(b))**.** *Let K be a cyclic cubic number fields and m an integer non divisible by 3. Then we have*

$$\mathrm{Prob}(m \mid h_K) = \prod_{p \mid m, p \equiv 1 \mod 3} \Big(1 - \frac{(p)_\infty^2}{(p)_1^2}\Big) \prod_{p \mid m, p \equiv 2 \mod 3} \Big(1 - \frac{(p^2)_\infty}{(p^2)_1}\Big),$$

where $(p)_\infty = \prod_{k \geq 1}(1 - p^{-k})$ and $(p)_1 = (1 - p^{-1})$.

5.5 Density of fields with p-primary units : valuation of the p-adic regulator

The condition about p-primary units in Lemma 5.7 can be stated in a simpler manner when K is totally real.

Definition 5.20. *Let K be a totally real Galois number field and p a prime which is unramified in K. Let $\varepsilon_1, \dots, \varepsilon_r$ be a system of fundamental units and σ_1, ..., σ_{r+1} the automorphisms of K. Let $\mathfrak{p}$ be a prime ideal above p and $\log_{\mathfrak{p}}$ the $\mathfrak{p}$-adic logarithm of $K_{\mathfrak{p}}$, $\log_{\mathfrak{p}}(x+1) = \sum_{i\geq 1}(-1)^i \frac{x^i}{i}$. Call $\mathcal{O}_{\mathfrak{p}}$ the ring of integers in $K_{\mathfrak{p}}$. We set $e = \mathrm{lcm}(\{N(\mathfrak{p}')-1, \mathfrak{p}' \mid p\})$ where $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$. By abuse of notations we also denote by $\log_{\mathfrak{p}}$ the following map that we only apply to elements of E_K:*

$$\begin{array}{rccc} \log_{\mathfrak{p}}: & \{x \in K^* \mid \ \forall \mathfrak{p}' \mid p, \mathrm{val}_{\mathfrak{p}'}(x) = 0\} & \to & \mathfrak{p}\mathcal{O}_{\mathfrak{p}} \\ & x & \mapsto & \frac{1}{e}\log_{\mathfrak{p}}(x^e). \end{array}$$

We are only taking the logarithm of elements in E_K and our definition coincides with that in Washington [Was97].

We call normalized p-adic regulator the quantity $R'_{K,p} = \det(\frac{1}{p}\log_{\mathfrak{p}}(\sigma_j(\varepsilon_j)_{1\leq i,j\leq r}))$. Note that we use the notation R' instead of R, which is reserved for the p-adic regulator, and that $R'_{K,p} = R_{K,p}/p^r$.

It is classical (see for example [Was97]) that $R'_{K,p}$ belongs to $\mathbb{Z}_p$ and is independent of the choice of $\mathfrak{p}$ and of the labeling of fundamental units and of the automorphisms. For completion we state a simple and classical property of $R'_{K,p}$.

Lemma 5.21. *For all $\gamma \in K$, if K has a p-primary unit then $R'_{K,p}$ is divisible by p.*

Proof. Let $\varepsilon = \prod_{i=1}^r \varepsilon_i^{a_i}$, $a_1, \dots, a_r \in \mathbb{Z}$ be a p-primary unit. Then $(a_1, \dots, a_r)$ is in the kernel of the matrix which defined $R'_{K,p}$ reduced modulo $\mathfrak{p}$. Hence, $R'_{K,p}$ is divisible by $\mathfrak{p}$ and, since it belongs to $\mathbb{Z}_p$, it is also divisible by p. □

Very little is known on the probability that the normalized regulator is divisible by p. Schirokauer [Sch93, p. 415] made the heuristic that the matrix which defines $R'_{K,p}$ modulo p is a random matrix with coefficients in $\mathbb{F}_{p^f}$ for some f and therefore the probability that p divides $R'_{K,p}$ is $\mathcal{O}(\frac{1}{p})$. Later Hofmann and Zhang studied the case of cyclic cubic fields and gave heuristic arguments and numerical experiments in favor of the following conjecture.

Conjecture 5.22 ([HZ16] Conj 1)**.** *For primes $p > 3$ we have*

$$\mathrm{Prob}(p \textit{ divides } R'_{K,p}) = \begin{cases} \frac{1}{p^2}, & \textit{if } p \equiv 2 \pmod 3 \\ \frac{2}{p} - \frac{1}{p^2}, & \textit{if } p \equiv 1 \pmod 3. \end{cases}$$

5.6 Algorithmic tools

complete information	class group	unit group	ray group
partial information	p divides h_K	p divides $R'_{K,p}$	K is p-rational

Table 2: List of invariants associated to a number field K and of partial information associated to a prime p.

Gathering numerical data on the class group, unit group and respectively ray class group of number fields is a hard task despite the important progress done in the design of algorithms. Indeed, the best algorithms to compute class number are derived from Buchmann's algorithm [BW89], with its p-adic variant [Zha13], and have a non-polynomial complexity. In the context of the Cohen-Lenstra-Martinet heuristic it is not necessary to compute h_K but only to test its divisibility by p. In Section 5.8 we recall an algorithm of polynomial complexity which tests the divisibility of h_K by p without other information on h_K. Similar questions can be studied for the unit and ray class groups.

In the context of the p-adic regulator valuation it is not necessary to compute the regulator to infinite precision, but only to test the divisibility of the normalized p-adic regulator by p. When using the best known algorithms there is no gain in complexity when the precision is reduced because one needs to compute a system of fundamental units, which is done by a variant of Buchmann's class number algorithm [BW89]. This motivates us in Section 5.9 to propose a fast method to compute units, which are not necessarily a basis of the unit group but which allow us in general to test the divisibility by p of the normalized p-adic regulator.

Ray class group is related to the cartesian product of the class number and the unit group and from an algorithmic view point, it is similar to these two groups, and it is not surprising that the algorithm of Cohen et al. [CDO98] has a non-polynomial complexity. Pitoun and Varescon [PV15] showed that it allows to test if K is p-rational by an algorithm that we recall in Section 5.10.

5.7 An algorithm to enumerate abelian number fields

Numerical computations of densities require us to make the list of all the number fields K of a given degree and Galois group such that $|\mathrm{Disc}(K)|$ is less than a given bound X. The task is very much simplified in the case of abelian extensions due the following classical result.

Lemma 5.23 ([Was97] Theorem 3.11,The Conductor-discriminant formula)**.** *Let K be an abelian number field and let Ξ be the group of characters $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^*$. Then we have*

$$\mathrm{Disc}(K) = (-1)^{r_2} \prod_{\chi \in \Xi} c_\chi,$$

where c_χ is the conductor of χ.

In particular if $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$, where q is a prime number, we have a very simple relation between the conductor and the discriminant. Although the result is classical (see for example [Gra75]) we recall the proof because one deduces from it an algorithm to enumerate number fields with Galois group equal to $(\mathbb{Z}/q\mathbb{Z})^t$ and discriminant bounded by a given constant.

Lemma 5.24. *Let K be a number field such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$. Then we have,*

1. *the conductor c_K of K can be written as $c_K = p_1 \cdots p_s$ or $c_K = q^2 p_1 \cdots p_{s-1}$ where $p_i \equiv 1 \mod q$ are distinct primes;*
2. $\mathrm{Disc}(K) = c_K^{(q-1)q^{s-1}}$.

Proof. (1) For any abelian group G we call q-rank of G, denoted by $\mathrm{rank}_q G$, the dimension of the $\mathbb{F}_q$ vector space G/G^q. Then one easily checks that for any prime $p_i \not\equiv 1 \mod q$ different than q, $\mathrm{rank}_q(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^* = 0$; for any prime $p_i \equiv 1 \pmod q$ and any $e_i \geq 1$, $\mathrm{rank}_q(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^* = \mathrm{rank}_q(\mathbb{Z}/p_i\mathbb{Z})^*$. Hence, $\mathrm{rank}_q(\mathbb{Z}/q\mathbb{Z})^* = 0$ and for any $e \geq 2$, $\mathrm{rank}_q(\mathbb{Z}/q^e\mathbb{Z})^* = 1$. If c is an integer of the form in point (1) and c' is a multiple of c then $(\mathbb{Z}/c\mathbb{Z})^*$ and $(\mathbb{Z}/c'\mathbb{Z})^*$ have the same q-rank. By definition, the conductor of a number field of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ is the smallest integer c so that the q-rank of $(\mathbb{Z}/c\mathbb{Z})^*$ is t.

(2) For each prime power a dividing c_K we have to count the number of characters defined on $(\mathbb{Z}/c_K\mathbb{Z})^*$ which are not trivial on $(\mathbb{Z}/a\mathbb{Z})^*$. This is the number of subgroups of $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$ whose quotient group is $\mathbb{Z}/q\mathbb{Z}$ and further the number of linear forms from $\mathbb{F}_q^t$ to $\mathbb{F}_q$ which are non-zero on the first component, hence the total number is $(q-1)q^{t-1}$. Due to the conductor-discriminant formula (Lemma 5.23) we obtain the result for $\mathrm{Disc}(K)$. □

In numerical experiments, we enumerate all fields K of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ with $|\mathrm{Disc}(K)| \leq X$ by enumerating all positive integers c less than $X^{\frac{1}{q^{t-1}(q-1)}}$ of the form given by point (1) of Lemma 5.24. Next we compute all subgroups H of $(\mathbb{Z}/c\mathbb{Z})^*$ such that $(\mathbb{Z}/c\mathbb{Z})^*/H \simeq (\mathbb{Z}/q\mathbb{Z})^t$. Finally, we compute the fixed field of H.

In the particular case of cubic cyclic fields one does not need any computations because there exists a canonical polynomial to define every cyclic cubic number fields of conductor m.

Lemma 5.25 ([Coh13] Theorem 6.4.6)**.** *Let m be an integer of the form $\prod_{i=1}^t p_i$ or $9\prod_{i=1}^{t-1} p_i$ where $p_i \equiv 1 \pmod 3$. Then there are 2^{t-1} cubic cyclic fields of conductor m. Each of them corresponds to one solution of the equation $m = \frac{a^2+27b^2}{4}$ by the formula*

$$f_a(x) = \begin{cases} x^3 + x^2 + \frac{1-m}{3}x - \frac{m(3+a)-1}{27}, & \text{if } 3 \nmid a \\ x^3 - \frac{m}{3}x - \frac{am}{27}, & \text{otherwise.} \end{cases} \tag{5.1}$$

The subfamily $m = \frac{a^2+27}{4}$ has a pleasant property that deserves our attention.

5.7.1 A family with explicit units

For a particular classical family of cubic cyclic fields we have a closed formula of the minimal polynomial of a unit of infinite order. We focus on the existence of the unit, which is not necessarily well explained in the literature.

Lemma 5.26. *Let a be an odd integer, $m = \frac{1}{4}(a^2+27)$ and let K be the number field defined by Equation (5.1). Then K contains an integer ω whose minimal polynomial is*

$$g_a(x) = x^3 - mx^2 + 2mx - m$$

and $\eta := \sigma(\omega)/\omega$ is a unit whose minimal polynomial is

$$\mu_a(x) = x^3 - \frac{2m-3-a}{2}x^2 + \frac{2m-3+a}{2}x - 1,$$

where $\mathrm{Gal}(K/\mathbb{Q})$ is generated by the automorphism σ. Additionally, K contains a unit whose minimal polynomial is

$$\nu_a(x) = x^3 + (m-3)x^2 + 3x - 1.$$

If u is a root of $\nu_a(x)$ then $A(a,u) = \frac{1}{16a}(x^2(4a^2+12)+x(a^4+18a^2-8a+21)+(-2a^3+6a^2-30a-6))$ is also a root of $\nu_a(x)$.

Proof. Let α be a root of f_a in K. One can plug in g_a the element

$$\omega = \begin{cases} \frac{a^2}{36} + \frac{\alpha a}{3} + \alpha^2 + \frac{3}{4}, & \text{if } 3 \nmid a \\ \frac{a^2}{36} + \frac{a\alpha}{3} + \alpha^2 + \frac{a}{9} + \frac{2}{3}\alpha + \frac{31}{36}, & \text{otherwise.} \end{cases}$$

and note that $g_a(\omega) = 0$, so g_a has a root in K for any a. We set $\eta = \frac{\sigma(\omega)}{\omega}$ and, for $i \in \mathbb{N}$, $\omega_i = \sigma^i(\omega)$. Let $x^3 - Ax^2 + Bx - 1$ be the minimal polynomial of η over $\mathbb{Q}$. Then, equating $x^3 - Ax^2 + Bx - 1 = (x-\eta)(x-\sigma(\eta))(x-\sigma^2(\eta))$, we obtain

$$\begin{aligned} A + B &= \sum_{i=0}^{2} \frac{\omega_{i+1}}{\omega_i} + \frac{\omega_i}{\omega_{i+1}} = \frac{1}{m}(\sum_{i=0}^{2} \omega_{i+1}^2\omega_i + \omega_{i+1}\omega_i^2) \\ &= \frac{1}{m}\left((\sum_{i=0}^{2} \omega_i\omega_{i+1})(\sum_{i=0}^{2} \omega_i) - 3\prod_{i=0}^{2}\omega_i\right) = 2m - 3. \end{aligned}$$

Note that $g_a(x)$ is the minimal polynomial of ω which links m with ω_i's giving us the second equality above. We also have

$$AB = (\sum_{i=0}^{2} \frac{\omega_{i+1}}{\omega_i})(\sum_{i=0}^{2} \frac{\omega_i}{\omega_{i+1}}) = m^2 - 4m + 9.$$

Hence, A and B are such that the minimal polynomial of $\eta = \sigma(\omega)/\omega$ is μ_a.

Finally, we test by direct computations that ν_a has a root

$$\eta' = \begin{cases} \alpha^2 + \frac{a-1}{3}\alpha + \frac{a^2}{36} - \frac{a}{18} + \frac{1}{36}, & \text{if } 3 \nmid a \\ \alpha^2 + \frac{(a-3)\alpha}{3} + \frac{a^2}{36} - \frac{a}{6} + \frac{1}{4}, & \text{otherwise.} \end{cases}$$

which is automatically a unit in K. □

The computations in the proof can be found in the online complement [BR17a].

5.8 An algorithm to test if p divides h_K

Marie-Nicole Gras [Gra75], Van der Linden [VdL82] and Hakkarainen [Hak09, Eq (5.1)] designed a fast criterion which allows to show that $p \nmid h_K$ without computing the class number h_K.

Definition 5.27. *Let $m \not\equiv 2 \mod 4$ be an integer. We call cyclotomic units of Sinnott in $\mathbb{Q}(\zeta_m)$ the intersection C_m of the unit group E_m with the multiplicative group generated by ζ_m and the elements of the form $1 - \zeta_m^a$ with $a \in \mathbb{Z}$. We also set $C_m^+ = E_m^+ \bigcap C_m$.*

Note that this definition coincides with one of Washington [Was97, Sec 8.1] in the case of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m)^+$. One can extend the definition to arbitrary $K \subset \mathbb{Q}(\zeta_m)^+$ but we don't use this extension, which is not the same for Washington and Sinnott.

Let h_m^+ denote the class number of $\mathbb{Q}(\zeta_m)^+$. The main ingredient of M.-N. Gras' algorithm is as follows:

Lemma 5.28 ([Sin78] main Theorem)**.** *Let $m \not\equiv 2 \mod 4$ be an integer. Let g be the number of prime factors of m and put $b = 0$ if $g = 1$ and $b = 2^{g-2} + 1 - g$ otherwise. Then we have*

$$h_m^+ = 2^b [E_m^+ : C_m^+].$$

We obtain a criterium to prove that p does not divide h_K:

Lemma 5.29. *(i) Let m be an odd prime coprime to p, p be inert in $\mathbb{Q}(\zeta_{\frac{m-1}{2}})$, $\varepsilon \in C_m^+$ be any cyclotomic unit. If ε is not a p-th power, then $p \nmid h_m^+$. In particular, if $p \nmid \frac{m-1}{3}$ then the class number of the unique cubic cyclic subfield K of $\mathbb{Q}(\zeta_m)^+$ is not divisible by p.*

(ii) Let m and p be as before. Assume that there exists a prime ℓ such that $\ell \equiv 1 \mod pm$ and $\Phi_m(x) \nmid (x+1)^{\frac{\ell-1}{p}} - 1$ in $\mathbb{F}_\ell[x]$. Then h_m^+ is not divisible by p.

Proof. (i) By Lemma 5.28, $h_m^+ = [E_m^+ : C_m^+]$ because $g = 1$. Let $v \in C_m^+$ be a generator of the group of cyclotomic units seen as a $\mathbb{Z}[G]$-module where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})$ (cf. the works of Leopoldt reproduced in [Was97, Prop. 8.11]). Since G is cyclic of order $(m-1)/2$, we identify the rings $\mathbb{Z}[G]$ and $\mathbb{Z}[\zeta_{\frac{m-1}{2}}]$. Let us show that if v is not a p-th power in E_m^+ then, for all $\omega \in \mathbb{Z}[\zeta_{\frac{m-1}{2}}]$ such that $p \nmid \omega$, the element v^ω is not a p-th power. Assume on the contrary, $v^\omega = u^p$ for some $u \in E_m^+$. Then $v^{N(\omega)} = u^{\frac{pN(\omega)}{\omega}}$ where $N(\omega) = N_{\mathbb{Q}(\zeta_{\frac{m-1}{2}})/\mathbb{Q}}(\omega)$. Since p is inert the condition $p \nmid \omega$ ensures that $\gcd(N(\omega), p) = 1$ and we can define $a := N(\omega)^{-1} \mod p$. We obtain then $v^{aN(\omega)} = u^{ap\frac{N(\omega)}{\omega}}$. But this implies that $v \in (u^{a\frac{N(\omega)}{\omega}} E_m^+)^p$ which is a contradiction. This shows that $p \nmid h_m^+$.

Since $p \nmid \frac{m-1}{3} = [\mathbb{Q}(\zeta_m)^+ : K]$, $\mathrm{val}_p(h_k) \leq \mathrm{val}_p(h_m^+)$ so $p \nmid h_K$.

(ii) We apply point (i) to the cyclotomic unit $\varepsilon := \zeta_m^{-\frac{1}{2}} \frac{\zeta_m^2 - 1}{\zeta_m - 1} \in C_m^+$. Since m is coprime to p, the roots of unity ζ_m is always a p-th power, so it suffices to prove that $\frac{\zeta_m^2-1}{\zeta_m-1} = \zeta_m + 1$ is not a p-th power. Since $\Phi_m(x) \nmid (x+1)^{\frac{\ell-1}{p}} - 1$ in $\mathbb{F}_\ell[x]$, $\zeta + 1$ is not a p-th power in $\mathbb{Z}[\zeta_m]/\ell\mathbb{Z}[\zeta_m]$ and therefore it isn't a p-th power in $\mathbb{Q}(\zeta_m)$. □

Algorithm 1 A criterion to show that $p \nmid h_K$

Require: an integer N and a cyclic cubic number field K given by an odd prime conductor m and a prime $p \nmid \frac{m-1}{3}$ which is inert in $\mathbb{Q}(\zeta_{\frac{m-1}{2}})$ and coprime to m.

Ensure: The algorithm returns 'false', if $p \nmid h_K$
The algorithm returns 'non-certified true', if $p \mid h_K$.

$i \leftarrow 0$
repeat
  $\ell \leftarrow$ next prime $\equiv 1 \bmod mp$,
  we increment i and continue
until i>N or the cyclotomic polynomial $\Phi_m(x) \nmid (x+1)^{\frac{\ell-1}{p}} - 1$ in $\mathbb{F}_\ell[x]$.

The implementation of SAGE code for Algorithm 1 is in Appendix B, and can be downloaded from the online complement [BR17a].

5.9 An algorithm to test if p divides the normalized p-adic regulator

The relevant notion in this section is the p-adic logarithm but for computational issues we focus on a truncation of it that deserves its own name. If $U = \{u_1, \ldots, u_r\}$ is a set of units of a number field of embeddings $\sigma_1, \ldots, \sigma_n$, we call normalized p-adic regulator of U, and write $R'_{U,p}$, the determinant of the matrix $(\frac{\log_p(\sigma_j(u_i))}{p})_{1 \leq i,j \leq r}$.

Proposition-Definition 5.30 ([Sch93], Sec 3.)**.** *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial and let p be a prime which does not divide the index of f, i.e. $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ where $\mathcal{O}_K$ is the ring*

of integers in the number field K of f and α is a root of f in its number field. The Schirokauer map associated to f and p is

$$\begin{array}{rccc}\lambda_{f,p}: & \{\frac{a_1(x)}{a_2(x)} \mid a_1,a_2 \in \mathbb{Z}[x], p \nmid \mathrm{Res}(a_1a_2,f)\} & \to & \mathbb{F}_p[x]/\langle f(x)\rangle \simeq \mathbb{F}_p^{\deg f} \\ & a_1/a_2 \in \mathbb{Q}(x) & \mapsto & \frac{(a_1^{p^c-1}-1)-(a_2^{p^c-1}-1)}{p} \bmod \langle p, f\rangle,\end{array}$$

where $c = \mathrm{lcm}(\{\deg f_i \mid f_i$ divides f in $\mathbb{F}_p[x]\}$ and Res *denotes the resultant.*

Also, note that we can identify $\mathbb{Q}[x]/\langle f(x)\rangle$ and K so that every element of K is represented by a polynomial. In this language the condition $p \nmid \mathrm{Res}(a_1a_2, f)$ states that $\forall \mathfrak{p} \mid p$, $\mathrm{val}_{\mathfrak{p}}(\frac{a_1}{a_2}) = 0$.

Assume that $p \nmid Disc(f)$ and let $\{u_1, \ldots, u_r\}$ be a set of units which are not necessarily fundamental. Let n be the degree of f and let $c_0, c_1, \ldots, c_{n-1}$ be the maps so that, for any $\beta \in \mathbb{Q}[x]/\langle f\rangle$, $c_0(\beta) + c_1(\beta)x + \ldots + c_{n-1}(\beta)x^{n-1}$ is the polynomial representative of β of degree less than n. If the matrix

$$M = \begin{pmatrix} c_0(\frac{u_1^{p^{n!}-1}-1}{p}) & \ldots & c_{n-1}(\frac{u_1^{p^{n!}-1}-1}{p}) \\ \vdots & & \vdots \\ c_0(\frac{u_r^{p^{n!}-1}-1}{p}) & \ldots & c_{n-1}(\frac{u_r^{p^{n!}-1}-1}{p}) \end{pmatrix}$$

has full rank then $p \nmid R'_{K,p}$.

Justification. If $(\varepsilon_j)_{j=1,\ldots,r}$ is a system of fundamental units and Ω is the matrix such that, for each i, $u_i = \prod_{j=1}^r \varepsilon_j^{\Omega_{i,j}}$, then $R'_{U,p} = (\det \Omega) R'_{K,p}$. Hence, it is sufficient to prove that $p \nmid R'_{U,p}$. One can compute $R'_{U,p} \mod p$ by replacing, for any β, $\log_p(\beta)$ by $(\log_p(\beta^c) \bmod p^2)$ for a fixed constant $c \in \mathbb{Z}$ such that $\mathrm{val}_p(c) = 0$. Hence, we are brought to computing the determinant of $N = (\frac{\sigma_j(u_i)^c - 1}{p})_{1 \le i,j \le r}$ for a constant c such that for all i, $u_i^c \equiv 1 \mod p$. We take $c = p^{n!} - 1$ so that, for any prime ideal $\mathfrak{p}$ above p and any $\gamma \in K$ such that $\mathrm{val}_{\mathfrak{p}}(\gamma) = 0$, $\gamma^c \equiv 1 \mod \mathfrak{p}$. If $\alpha_1, \ldots, \alpha_n$ are the n roots of f in $\mathbb{C}_p$ then $M = N\mathrm{Vand}(\alpha_1, \ldots, \alpha_n)$, where Vand is the Vandermonde matrix associated to $\alpha_1, \ldots, \alpha_r$. We conclude that it suffices to prove that M has rank $r = n - 1$ to conclude that $p \nmid R'_{K,p}$.

The remaining question is that of computing a system of generators for E_K/E_K^p. In the case of the family of Section 5.7.1, this is easily done using an explicit formula. However, in the general case of cyclic cubic fields we propose a new technique.

Lemma 5.31. *Let K be a number field of odd prime degree q and of cyclic Galois group and call m its conductor. Then we have:*

1. *for any prime factor ℓ of m other than q there exists an ideal $\mathfrak{l}$ so that $\mathfrak{l}^q = \ell\mathcal{O}_K$;*
2. *If $\mathfrak{l}$ is principal, for any generator $\omega \in \mathcal{O}_K$ of $\mathfrak{l}$ and any generator σ of $\mathrm{Gal}(K/\mathbb{Q})$, $\frac{\sigma(\omega)}{\omega}$ is a unit.*

Proof. (i) Let ℓ be a prime factor of m other than q. Then ℓ is ramified in K and, since $\deg K = q$ is prime, there exists a prime ideal $\mathfrak{l}$ so that $\ell = \mathfrak{l}^q$.

(ii) The ideal generated by $\frac{\sigma(\omega)}{\omega}$ is $\sigma(\mathfrak{l})\mathfrak{l}^{-1}$. Since σ is an automorphism of K, $\sigma(\mathfrak{l})$ is a prime ideal above ℓ. But ℓ is totally ramified in K so $\sigma(\mathfrak{l}) = \mathfrak{l}$. So $\frac{\sigma(\omega)}{\omega}$ is a unit. □

Remark 5.32. The ideal $\mathfrak{l}$ is not necessarily principal and even if it is, the computation of a generator ω can be slow in the worst cases. Indeed, since $\ell\mathbb{Z}[\zeta_\ell] = ((\zeta_\ell - 1)\mathbb{Z}[\zeta_\ell])^{(\ell-1)}$, $\ell\mathbb{Z}[\zeta_m] = ((\zeta_\ell - 1)\mathbb{Z}[\zeta_m])^{(\ell-1)}$ so that in $\mathbb{Z}[\zeta_m]$ we have

$$\mathfrak{l}^q = \langle \zeta_\ell - 1\rangle^{\ell-1}.$$

By unique factorization we deduce that $\mathfrak{l}\mathbb{Z}[\zeta_m] = \langle \zeta_\ell - 1\rangle^{\frac{\ell-1}{q}}$. We consider the norms and obtain that $N_{\mathbb{Q}(\zeta_m)/K}(\mathfrak{l}\mathbb{Z}[\zeta_m]) = \langle N_{\mathbb{Q}(\zeta_m)/K}(\zeta_\ell - 1)^{\frac{\ell-1}{q}}\rangle$ is principal, but this is not necessarily equal to $\mathfrak{l}$.

Among the 630 cyclic cubic number fields in Table 1 of [Gra75], having conductor between 1 and 4000 we have:

property	number	percentage	example
$\mathfrak{l}$ is principal and Algorithm 2 succeeds	272	43.1%	$x^3 + x^2 - 2x - 1$
Algorithm 2 succeeds but $\mathfrak{l}$ is not principal	95	15.1%	$x^3 - 21x^2 + 35$
$\mathfrak{l}$ is principal but Algorithm 2 fails	146	23.2%	$x^3 - x^2 - 30x - 27$.

The script remark3-10.sage in the online complement [BR17a] allows us to reproduce these data.

Here we write that $\mathfrak{l}$ is principal when there exists a prime ℓ above the conductor m of the number field of f such that $\mathfrak{l}$ is principal. The case in which $\mathfrak{l}$ is principal and Algorithm 2 fails is due to the usage of the LLL algorithm [LLL82]. Indeed, given a lattice L of dimension n the algorithm finds in polynomial time an element of the lattice whose euclidean norm is less than $c_n|\det(L)|^{\frac{1}{n}}$. If $\omega_1,\dots,\omega_n$ is an integer basis of $\mathcal{O}_K$ and LLL is applied to the lattice

$$L=\{(a_0,\dots,a_{n-1})\in\mathbb{Z}^n \mid \sum_{i=0}^{n} a_i\omega_i\in\mathfrak{l}\},$$

LLL computes an element $(\gamma_0,\dots,\gamma_n)\in\mathbb{Z}^n$ such that $\gamma=\sum_{i=0}^n\gamma_i\omega_i$ is such that $N_{K,\mathbb{Q}}(\gamma)\leq CN(\mathfrak{l})$ for some constant C independent on $\mathfrak{l}$. Since $C>1$, it is not always true that LLL finds a generator. Generic algorithms to replace LLL exist but they are much slower.

In the following we present Algorithm 2 which is used to compute rapidly a unit in cyclic cubic fields. The implementation using SAGE is in Appendix C, and the program can be downloaded from the online complement [BR17a].

Algorithm 2 Fast computation of a unit of cyclic cubic K.

Require: a cubic cyclic field K and a factorization of its conductor m
Ensure: a unit of K
1: **for** $\ell\equiv 1 \mod q$ factor of m **do**
2: factor ℓ in $\mathcal{O}_K$ to obtain $\mathfrak{l}$ using [Coh13, Sec 4.8.2]
3: search a generator ω_ℓ of the ideal $\mathfrak{l}$ using LLL [LLL82].
4: **end for**
5: **return** a product of the units $\eta_\ell:=\sigma(\omega_\ell)/\omega_\ell$

In order to do statistics about the p-adic regulator we proceed as in Algorithm 3. The implementation of SAGE code for the Algorithm is in Appendix D, and the program can be downloaded from the online complement [BR17a]. Note that Schirokauer's map $\lambda_{f,p}$ (Definition 5.30) has image in the $\mathbb{F}_p$-vector space $\mathbb{F}_p[x]/\langle f(x)\rangle$ which has the basis $(1,x,x^2)$ when f is cubic. Hence, for $i=0,1,2$, we put $\lambda_i=c_i(\frac{x^e-1}{p})$, where $e=\mathrm{lcm}(\{N(\mathfrak{p})-1,\mathfrak{p}\mid p\})$ and, for $i=0,1,2$, c_i are the coefficients of the elements of the number field of f in the basis $(1,x,x^2)$.

Algorithm 3 Test if $p\mid R'_{K,p}$ for a list of random cyclic cubic fields

Require: a list of cyclic cubic fields
Ensure: a certificate on the divisibility of $R'_{K,p}$ by p
for K in list of cyclic cubic fields **do**
Apply Algorithm 2 to compute a unit η
Apply algorithms in [WR76] to factor a defining polynomial of K in $K[x]$ and obtain a non-trivial automorphism σ of K
Compute the rank r of the matrix

$$\begin{pmatrix}\lambda_0(\varepsilon_1) & \lambda_1(\varepsilon_1) & \lambda_2(\varepsilon_1)\\ \lambda_0(\varepsilon_2) & \lambda_1(\varepsilon_2) & \lambda_2(\varepsilon_2)\end{pmatrix},$$

where $\lambda_0,\lambda_1,\lambda_2$ are the Schirokauer maps of a polynomial defining K
if r=2 **then**
return $p\nmid R'_{K,p}$
else
we compute a truncation of the normalized p-adic regulator using algorithms in [Pan95] and return the result of the test whether this rank is 2
end if
end for

5.10 An algorithm to decide p-rationality

For any n let $\mathcal{A}_{p^n}$ denote the p-part of the ray class group ([Gra13] Ch I.4) of K with respect to the ideal p^n. For any finite abelian group G we denote by $FI(G)$ the invariant factors of G i.e.

the integers $[d_1, \ldots, d_k]$ so that $G \simeq \oplus_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$ and $d_1 \mid d_2 \mid \cdots \mid d_k$. The following result reduces the problem of testing p-rationality to that of computing the ray class group, which is studied for example in [CDO98] and implemented in PARI [BBB+98].

Lemma 5.33 ([PV15] Thm 3.7 and Cor 4.1, see also Prop. 1.13 of [HM16]). *Let K be a number field which satisfies Leopoldt's conjecture. Let e be the ramification index of p in K. Then there exists $n \geq 2 + e$ so that the invariant factors of $FI(\mathcal{A}_{p^n})$ can be divided into two sets $FI(\mathcal{A}_{p^n}) = [b_1, \ldots, b_s, a_1, \ldots, a_{r_2+1}]$ such that*

1. $\min(\mathrm{val}_p(a_i)) > \max(\mathrm{val}_p(b_i)) + 1$;
2. $FI(\mathcal{A}_{p^{n+1}}) = [b_1, \ldots, b_s, pa_1, \ldots, pa_{r_2+1}]$.

Moreover, K is p-rational if and only if $\mathrm{val}_p(b_1) = \mathrm{val}_p(b_2) = \cdots = \mathrm{val}_p(b_s) = 0$.

The algorithm of Pitoun and Varescon was implemented in PARI [BBB+98] by Bill Allombert on a large number of imaginary quadratic fields. The algorithm applies to all number fields satisfying Leopoldt's conjecture not only to abelian fields. Indeed, the problem is not the answer which is always correct, but the fact that the algorithm doesn't terminate when Leopoldt's conjecture doesn't hold for K. To illustrate that the algorithm works also for non-abelian number fields we construct examples of p-rational fields for all possible Galois groups of quartic polynomials.

Example 5.34. *In Example 5.34 we list the set of primes less than* 100 *where the number fields of the listed polynomials are not p-rational. The case for the polynomial $x^4 + x^3 + x^2 + x + 1$ is already discussed by Greenberg [Gre16, Sec. 4.4], thanks to the computations of Robert Pollack. The SAGE code for the programme to verify p-rationality using Lemma 5.33 is in Appendix A, and the programme can be downloaded from the online complement [BR17a].*

Galois group	$\forall p \leq 100,\ p-$ rational	non 7-rational
$\mathbb{Z}/4\mathbb{Z}$	$x^4 + x^3 + x^2 + x + 1$	$x^4 - 23x^3 - 6x^2 + 23x + 1$
V_4	$x^4 - x^2 + 1$	$x^4 + 10x^2 + 1$
D_4	$x^4 - 3$	$x^4 - 6$
A_4	$x^4 + 8x + 12$	$x^4 - x^3 - 16x^2 - 7x + 27$
S_4	$x^4 + x + 1$	$x^4 + 35x + 1$

Table 3: p-rationality of a list of number fields.

To sum up we have a fast criterion for p-rationality given by Proposition 5.15 and a slow condition which works in the general case which is given by Lemma 5.33. For efficiency reasons we implemented a combination of the two as given by Algorithm 4. An implementation of this algorithm is available in the online complement [BR17a].

Algorithm 4 test p-rationality of a list of cyclic cubic fields

Require: a prime p and a list of cyclic cubic fields
Ensure: for each number field the information whether it is p-rationality
  for K in list of cyclic cubic fields **do**
    Apply Algorithm 1 to certify that p does divides h_K when it is possible
    Apply Algorithm 3 to certify that p does not divides $R'_{K,p}$ when it is possible
    if we have certificates that $p \nmid h_K R'_{K,p}$ **then**
      return True and certificates
    else
      Apply the algorithm of Pitoun and Varescon in Appendix A, based on Lemma 5.33 to decide if K is p-rational
      Return answer and certificate
    end if
  end for

In an experiment, using Algorithm 4, we tested p-rationality the 158542 cyclic cubic fields of conductor less than 10^6. The proportion of fields where $5 \mid h_K$ is expected to be $0,000016$ (Conjecture 5.19) and the proportion of fields where $5 \mid R'_{K,5}$ is expected to be 0.04 (Conjecture 5.22),

which is matched very well by the experiments: 5351 fields found for an expected number of $0.04 \cdot 158542 \approx 6127$. It turns out that in all the 5351 cases where we couldn't apply the criterion in Lemma 5.7 the field was actually non 5-rational. The data can be found in the online complement [BR17a]. The total time used by the 153191 number fields where the fast criterion could be applied was negligible with respect to the total time used for the 5351 number fields where the algorithm of Pitoun and Varescon was applied. Hence, we had a speed-up of approximatively $158542/5351 \approx 5^2$. In the general case, for a prime p, we expect a speed-up of $p/2$ when $p \equiv 1 \pmod 3$ and of p^2 when $p \equiv 2 \pmod 3$.

5.11 Some families of p-rational fields

Recall that, when given a cyclic cubic field K, in Algorithm 1 one searches for a prime ℓ where Lemma 5.29 applies, and hence certifies that the class number is not divisible by p. The idea of this section is to fix $p = 5$ and to search for cyclic cubic fields where Lemma 5.29 applies. Under some arithmetic assumptions this allows us to construct an infinite family of fields of class number non-divisible by 5. We can also find a family of number fields where the 5-adic regulators are not divisible by 5, thanks to the explicit formula in Section 5.7.1. Under the assumption that the two families intersect we obtain an infinite family of 5-rational cyclic cubic fields.

Hypothesis 5.35. *There exists infinitely many positive integer a such that*

1. $m = \frac{a^2+27}{4}$ *is an odd prime;*
2. $\frac{m-1}{3} \neq 0 \pmod 5$, $m \neq 0 \pmod 5$*;*
3. 5 *inert in* $\mathbb{Q}(\zeta_{\frac{m-1}{2}})$*;*
4. *there exits* $\ell \equiv 1 \pmod{5m}$ *such that* $\Phi_m(x) \nmid (x+1)^{\frac{l-1}{5}} - 1$ *in* $\mathbb{F}_\ell[x]$*;*
5. $a \neq 21, 23 \pmod{25}$.

Lemma 5.36. *For any m satisfying the conditions of Hypothesis 5.35, the polynomials $f_a(x) = x^3+x^2+\frac{1-m}{3}x-\frac{m(3+a)-1}{27}$, where a is such that $m = \frac{a^2+27}{4}$, define a cubic cyclic field of conductor m which is 5-rational. In particular, under Hypothesis 5.35, $GC_\infty(\mathbb{Z}/3\mathbb{Z}, 5)$ holds.*

Proof. We put $p = 5$ and we write p when the argument depends only on the points (1) to (4) of the Hypothesis 5.35 whereas we write 5 when the argument also requires the point (5).

By Lemma 5.25 the number field of f_a is cyclic cubic and has conductor m. By Lemma 5.29 the conditions on m guarantee that $p \nmid h_K$ where K is the cyclic cubic field defined by polynomials f_a, hence it suffices to show that $p \nmid R'_{K,p}$.

By condition (5), $\mathrm{Disc}(f_a)$ is not divisible by 5 and hence $\mathrm{Disc}(\mathbb{Q}(\alpha))[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]^2 \not\equiv 0 \mod 5$, where α is a root of f_a in its number field. By Lemma 5.26 the set $U = \{\beta, A(\beta, a)\}$, where β is a root of $\nu_a(x) = x^3 + (m-3)x^2 + 3x - 1$ and $A(x,a) = \frac{1}{16a}(x^2(4a^2+12) + x(a^4+18a^2-8a+21) + (-2a^3+6a^2-30a-6))$, is composed of two units. By Proposition-Definition 5.30 it suffices to prove that the following matrix has rank 2:

$$M_a := \begin{pmatrix} c_0(\frac{x^{p^6-1}-1}{p}) & c_1(\frac{x^{p^6-1}-1}{p}) & c_2(\frac{x^{p^6-1}-1}{p}) \\ c_0(\frac{A(x,a)^{p^6-1}-1}{p}) & c_1(\frac{A(x,a)^{p^6-1}-1}{p}) & c_2(\frac{A(x,a)^{p^6-1}-1}{p}) \end{pmatrix},$$

where c_0, c_1, c_2 are the coefficients of elements of $Q[x]/\langle \nu_a \rangle$ seen as polynomials. In the following, we are going to show that if a satisfies point (5) of Hypothesis 5.35, then $R'_{K,5} \not\equiv 0 \pmod 5$.

Given the polynomial form of the minors of M_a, if the rank of M_a is two for a value of a then it is the same for all a' such that $a' \equiv a \mod 5^2$. By a direct enumeration of the values of a in $[1, 5^2]$ we obtain that $5 \nmid R'_{K,5}$. □

Thus we obtain point (2) of Theorem 5.6.

Remark 5.37. In Appendix E, we provide an algorithm to find primes m, l satisfying Hypothesis 5.35. For example, $m = 7, l = 16906$ works.

5.12 Numerical investigation of the density of p-rational fields

The Cohen-Lenstra-Martinet heuristic predicts very simple formula for the density of number fields with class number prime to p and with Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ for every prime q and integer t. However, the authors of the heuristic conjectured only those heuristic statements which corroborate with numerical experiments. We bring new evidence in favor of the conjecture for cubic cyclic fields in Section 5.13. Then in Section 5.14 we bring evidence in many cases $(\mathbb{Z}/2\mathbb{Z})^t$ and $(\mathbb{Z}/3\mathbb{Z})^t$ for $t = 2, 3, 4$ and are able to state the corresponding conjectures. In Section 5.15, we extend the results of Hofmann and Zhang to the case of Galois groups $(\mathbb{Z}/3\mathbb{Z})^t$ and $(\mathbb{Z}/2\mathbb{Z})^t$ with $t = 2, 3, 4$ and conclude by proving point (3) of the main theorem (Th 5.6) in Section 5.16.

5.13 Numerical verification of the Cohen-Lenstra heuristics

One of the most interesting facts about the Cohen-Lenstra heuristic is how well it is supported by statistical data. Encouraged by the case of quadratic fields one would expect a similar situation for the case of cyclic cubic fields, but in 1989 Cohen and Martinet wrote that "we believe that the poor agreement [with the tables] is due to the fact that the discriminants are not sufficiently large".

Puzzled by this assertion we repeated their computations and made statistics on the fields of conductor less than 8000, i.e. discriminant less than 6410^6, which was the bound for the computations of that time (e.g. [Gra75] considered the fields of conductor less than 4000). Since then computers' capabilities have increased by more than a factor 1000 so that we could compute the statistics for fields of conductor less than 10^7, i.e. discriminant less than 10^{14}, in roughly one calendar month, in parallel on several 30 cores and summed up to roughly 2.5 CPU years.

Looking at the data in Table 4 we understand what happened: the convergence speed to the mean density is very slow and the statistics to 8000 have a relative error between 19% and 100% which didn't allow Cohen and Martinet to conclude. However, statistics to 10^7 have only a relative error between 0.2% and 15.5%, so we can conclude that the numerical data confirms their conjecture. More details are available in the online complement [BR17a].

p	theoretic density	stat. density cond. ≤ 8000	relative error	stat. density cond. $\leq 10^7$	relative error
5	0.00167	$\frac{3}{1269} \approx 0.0236$	46%	$\frac{3316}{1714450} \approx 0.00193$	15.5%
7	0.0469	$\frac{45}{1269} \approx 0.0355$	24%	$\frac{78063}{1714450} \approx 0.0456$	3%
11	0.0000689	0	100%	$\frac{133}{1714450} \approx 0.0000775$	12.5%
13	0.00584	$\frac{6}{1269} \approx 0.00472$	19%	$\frac{10232}{1714450} \approx 0.00584$	2%
19	0.0128	$\frac{11}{1269} \approx 0.0086$	48%	$\frac{21938}{1714450} \approx 0.0128$	0.2%

Table 4: Statistics on the density of cyclic cubic fields whose class number is divisible by $p = 5$, 7, 11, 13 and respectively 19.

5.14 Cohen-Lenstra-Martinet for Galois group $(\mathbb{Z}/3\mathbb{Z})^t$ and $(\mathbb{Z}/2\mathbb{Z})^t$

Lemma 5.38 (Kuroda's class number formula ([Lem94] Sec 3 and [Kur50] Sec 10)). *Let q be a prime and K a totally real Galois extension such that* $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^t$. *Then K contains $\frac{q^t-1}{q-1}$ subfields of degree q and there exists an integer A such that*

$$h_K = q^A \prod_{k_i \text{ subfield of degree } q} h_{k_i}.$$

The Cohen-Lenstra-Martinet heuristic implies that the class groups of the intermediate cyclic fields of prime k_i behave independently, and they obtain the following heuristic statement.

Conjecture 5.39 (reformulation of statements in [CM87]).

1. *If* $K = \mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_t})$, *and* p *an odd prime, then*

$$\text{Prob}(p \nmid h_K) = \frac{(p)_\infty}{(p)_1}^{2^t-1}.$$

2. *If* K *has degree* 3^t *and is the compositum of* t *cyclic cubic fields and* $p \geq 5$ *is a prime then*

$$\text{Prob}(p \nmid h_K) = \begin{cases} (\frac{(p)_\infty}{(p)_1})^{2\frac{3^t-1}{2}}, & \text{if } p \equiv 1 \pmod 3; \\ \frac{(p^2)_\infty}{(p^2)_1}^{\frac{3^t-1}{2}}, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

The conjecture is supported by the numerical evidence in Table 5. The data is available in the online complement [BR17a].

p	theoretic density	stat. density cond. $\leq 10^6$	relative error
5	0.00334	$\frac{933}{203559} \approx 0.00458$	37%
7	0.0916	$\frac{23912}{203559} \approx 0.0354$	28%
11	0.000138	$\frac{26}{203559} \approx 0.000128$	7.5%
13	0.0116	$\frac{6432}{203559} \approx 0.0316$	72%
17	0.0000140	$\frac{4}{203559} \approx 0.0000197$	40.5%
19	0.0254	$\frac{3536}{203559} \approx 0.0173$	31.5%

Table 5: Statistics on the density of fields of Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ whose class number is divisible by $p = 5$, 7, 11, 13, 17 and respectively 19.

5.15 On the p-adic regulator for Galois groups $(\mathbb{Z}/2\mathbb{Z})^t$ and $(\mathbb{Z}/3\mathbb{Z})^t$

We are interested in the probability that all the cyclic subfields of number field of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ are without p-primary unity, or equivalently we want to investigate the relations between the normalized p-adic regulators of a compositum and of its subfields. We have here a similar result to Kuroda's formula.

Lemma 5.40. *Let* p *be an odd prime and* $K = \mathbb{Q}(\sqrt{a}, \sqrt{b}))$ *with* a, b *and* ab *positive rational numbers which are not squares. Let* R *denote the normalized* p*-adic regulator of* K*, then* R_1, R_2 *and* R_3 *the* p*-adic regulators of* $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ *and* $\mathbb{Q}(\sqrt{ab})$*. Then there exists an integer* α *such that*

$$R = 2^\alpha R_1 R_2 R_3.$$

Proof. A simple regulator calculation (e.g. [BP79]) implies that there exists β such that

$$[E : E_1 E_2 E_3] = 2^\beta \frac{h}{h_1 h_2 h_3},$$

where E and h are the unit group and the class number of $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, and E_i and h_i are the unit groups and class numbers of the quadratic subfields.

By Kuroda's formula (Lemma 5.38), $h/(h_1, h_2 h_3)$ is a power of 2 so

$$[E : E_1 E_2 E_3] = 2^\gamma$$

for some integer γ. Hence the p-adic regulator of E is equal to the p-adic regulator of $E_1 E_2 E_3$ up to multiplication by a power of 2.

Let $\{\sigma_0 = \mathbf{id}, (\sigma_1 : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto \sqrt{b}), (\sigma_2 : \sqrt{a} \mapsto \sqrt{a}, \sqrt{b} \mapsto -\sqrt{b})$ and $(\sigma_3 : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto -\sqrt{b})\}$ be the automorphisms of K.

If ε_1 is a fundamental unit of $\mathbb{Q}(\sqrt{a})$ then $\varepsilon_1 \sigma_1(\varepsilon_1) = N_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\varepsilon_1) = \pm 1$ so that

$$\log_p(\sigma_1(\varepsilon_1)) = -\log_p(\varepsilon_1).$$

Since $\sigma_2(\varepsilon_1) = \varepsilon_1$ we have

$$\log_p(\sigma_2(\varepsilon_1)) = \log_p(\sigma_3(\varepsilon_1)) = \log_p(\varepsilon_1).$$

Similar equations hold for the fundamental units ε_2 and ε_3 of $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. Hence the p-adic regulator of the subgroup generated by $\varepsilon_1, \varepsilon_2$ and ε_3 is

$$\begin{vmatrix} \log_p(\varepsilon_1) & \log_p(\sigma_1(\varepsilon_1)) & \log_p(\sigma_2(\varepsilon_1)) \\ \log_p(\varepsilon_2) & \log_p(\sigma_1(\varepsilon_2)) & \log_p(\sigma_2(\varepsilon_2)) \\ \log_p(\varepsilon_3) & \log_p(\sigma_1(\varepsilon_3)) & \log_p(\sigma_2(\varepsilon_3)) \end{vmatrix} = \begin{vmatrix} \log_p(\varepsilon_1) & -\log_p(\varepsilon_1) & \log_p(\varepsilon_1) \\ \log_p(\varepsilon_2) & \log_p(\varepsilon_2) & -\log_p(\varepsilon_2) \\ \log_p(\varepsilon_3) & -\log_p(\varepsilon_3) & -\log_p(\varepsilon_3) \end{vmatrix}.$$

The latter determinant is equal to $(-4)\log_p \varepsilon_1 \log_p \varepsilon_2 \log_p \varepsilon_3$, which completes the proof. □

Our heuristic is to assume that the factors R_1, R_2 and R_3 in Lemma 5.40 are independent.

Conjecture 5.41. *Let $q = 2$ or 3, $p > q$ a prime and t an integer. Then the density of totally real number fields K such that $\mathrm{Gal}(K) = (\mathbb{Z}/q\mathbb{Z})^t$ for which the normalized p-adic regulator is divisible by p for at least one of the cyclic subgroups is*

1. $\mathrm{Prob}\left(\exists F \subset K, R'_{F,p} \equiv 0[p] | \mathrm{Gal}(K) = (\mathbb{Z}/2\mathbb{Z})^t \text{ tot. real}\right) = 1 - (1 - \frac{1}{p})^{2^t - 1}$
2. $\mathrm{Prob}\left(\exists F \subset K, R'_{F,p} \equiv 0[p] \mid \mathrm{Gal}(K) = (\mathbb{Z}/3\mathbb{Z})^t\right) = 1 - (1 - \mathcal{P})^{\frac{3^t-1}{2}}$, *where*

$$\mathcal{P} = \begin{cases} \frac{2}{p} - \frac{1}{p^2}, & \text{if } p \equiv 1 \pmod 3 \\ \frac{1}{p^2}, & \text{otherwise.} \end{cases}$$

In a numerical experiment, we considered all number fields to verify Conjecture 5.41 of the form $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ with $d_1, d_2 \in [2, 300]$ squarefree and distinct, then the fields of Galois group $(\mathbb{Z}/3\mathbb{Z})^3$ and conductor less than 10^5, i.e. discriminant less than 10^{30}. In Table 6 we compare the statistical density with $1 - (1 - \frac{1}{p})^7$. The numerical computations use Algorithm 3 with SAGE code in Appendix D. The programme can be downloaded from the online complement [BR17a].

p	experimental density	Conj 5.41 density	relative error
5	$\frac{29301}{37820} \approx 0.775$	0.790	2%
7	$\frac{19538}{37820} \approx 0.517$	0.660	22%
11	$\frac{17872}{37820} \approx 0.473$	0.487	3%

Table 6: Numerical verification of Conjecture 5.41 in the case where $\mathrm{Gal}(K) = (\mathbb{Z}/2\mathbb{Z})^3$. The sample consists of number fields which can be written as $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ with $2 \le d_1, d_2, d_3 \le 300$ squarefree and distinct.

Remark 5.42. Conjecture 5.41 describes well the computations required to find Example 5.17. With notations as in Example 5.17 we set $d_1 = -1$ and $d_2 = 2$ and, for $i \ge 3$ we define d_i as the smallest integer larger than d_{i-1} such that, for all subfield $F \subset \mathbb{Q}(d_1, \ldots, d_i)$, $R'_{F,p}$ is not divisible by p. Then the conjecture predicts $\log_2 d_i \approx c2^i$ for some constant c since the expectancy of d_i is the inverse of the probability of $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_{i-1}}, \sqrt{d})$ has normalized p-regulator non divisible by p when d is a random integer, which corroborates with experimental values:

i	3	4	5	6	7
d_i	3	11	47	97	4691
$2^{-i}\log_2(d_i)$	0.20	0.21	0.17	0.10	0.19

One can expect $d_9 \approx 2^{0.2 \cdot 2^9} \approx 2 \cdot 10^{15}$, which is out of reach of nowadays computers. Moreover, once the condition on p-adic regulators is satisfied, one has to also test the condition on class numbers. It seems to indicate that one needs new theoretical results before finding examples of the Greenberg's conjecture for $p = 5$ and Galois groups $(\mathbb{Z}/2\mathbb{Z})^t$ with t larger than 10.

5.16 Greenberg's conjecture as a consequence of previous conjectures

Since the Conjectures 5.22 and 5.19 predated Greenberg's conjecture and are supported by strong numerical evidence it is interesting to note that they imply that $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, p)$ holds.

Theorem 5.43. *Under Conjecture 5.19 and Conjecture 5.22, for all prime $p > 3$, $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, p)$ holds.*

Proof. For any D let $K(D)$ be the set of cubic cyclic number fields with conductor less than D. Then we have

$$\begin{aligned}\limsup_{D\to\infty} \frac{\#\{K \in K(D) \text{ non } p\text{-rational}\}}{\#K(D)} &\leq \limsup_{D\to\infty} \frac{\#\{K \in K(D),\ p \mid h_K R'_{K,p}\}}{\#K(D)} \\ &\leq \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(p \mid R'_{K,p}) \\ &\leq \frac{2}{p} + 1 - \prod_{i=1}^{\infty}(1 - p^{-i}) < \frac{1}{2}.\end{aligned}$$

Hence, there exist cyclic cubic fields K with arbitrarily large conductors such that p doesn't divide $h_K R'_{K,p}$, and which by Lemma 5.7 are p-rational. □

Thanks to Conjecture 5.41 we can prove a similar result in the case of composite of quadratic and respectively cubic cyclic real fields.

Theorem 5.44. *Let t be an integer, $q = 2$ or 3 and p a prime such that $p > 5q^t$. Under Conjecture 5.41 and Conjecture 5.39, there exist infinitely many p-rational number fields of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$, or equivalently $\mathrm{GC}_\infty((\mathbb{Z}/2\mathbb{Z})^t, p)$ and $\mathrm{GC}_\infty((\mathbb{Z}/3\mathbb{Z})^t, p)$ hold.*

Proof. Let $K(D)$ denote the set of totally real number fields of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ of conductor less than D. Then we have

$$\begin{aligned}\limsup_{D\to\infty} \frac{\#\{K \in K(D) \text{ non } p\text{-rational})}{\#K(D)} &\leq \limsup_{D\to\infty} \frac{\#\{K \mid K(D)\ \exists F \subset K\ p \mid h_F R'_{F,p}\}}{\#K(D)} \\ &\leq \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(\exists F \subset K, p \mid R'_{F,p}) \\ &\leq 2 - (1 - \frac{2}{p})^{\frac{q^t-1}{q-1}} - (1 - \sum_{i=1}^{\infty} p^{-i})^{\frac{q^t-1}{q-1}} \\ &\leq \frac{2q^t}{q-1}(\frac{2}{p} + \frac{1}{p(p-1)}) \\ &\leq \frac{5q^t}{p}(\frac{4}{5} + \frac{2}{5(p-1)}) < 1.\end{aligned}$$

□

Note that Theorem 5.44 has a conclusion which encompass the one of Theorem 5.43, but the difference in assumptions justifies to separate the two results. Also note that the condition $p > 5q^t$ is artificial and it could be improved if one proved

$$\mathrm{Prob}(p \mid h_K R'_{K,p}) < \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(p \mid R'_{K,p}).$$

If these two divisibility properties were orthogonal then Greenberg's conjecture for groups $(\mathbb{Z}/q\mathbb{Z})^t$, $q = 2$ or 3, would hold without any condition on p and t.

Conclusion and open questions

To sum up, Greenberg's conjecture is solved in the particular case of $G = \mathbb{Z}/2\mathbb{Z}$ and it is well supported by heuristics and numerical experiments for $G = (\mathbb{Z}/q\mathbb{Z})^t$ when $q = 2$ or 3. In the general case of non-abelian Galois groups however our results are limited to a list of examples.

The problem raises new questions about the independence of class numbers and of p-adic regulators, which could be tackled by techniques of analytic number theory, similar to the recent progress on the Cohen-Lenstra-Martinet heuristic. It is interesting to create new algorithms to test divisibility of p-regulator and of the class number by p with a better complexity than computing a system of fundamental units and respectively the class number.

Greenberg's p-rationality conjecture corresponding to the case $G = (\mathbb{Z}/2\mathbb{Z})^t$ offers a new technique to construct Galois representations with open image in $\mathrm{GL}_n(\mathbb{Z}_p)$ with $4 \leq n \leq 2^{t-1} - 3$ (cf [Gre16, Prop 6.7]), solving new cases of the inverse Galois problem. The previous results were restricted to $n = 2$ and $n = 3$, so that the known examples with $G = (\mathbb{Z}/2\mathbb{Z})^5$ are enough to improve on previous results.

Appendix

A The algorithm of Pitoun and Varescon

The following code computes the invariant factors as in lemma 5.33 and tests if a number field is p-rational.

```
def FI(K,p,n):
    f=K.defining_polynomial()
    r1,r2=K.signature()
    ab=pari(' K = bnfinit(' + str(f) + ',1);   '+\
           ' bnfcertify(K);               '+\
           ' Kr = bnrinit(K, ' + str(p^n)+ '); '+\
           ' Kr.clgp.cyc ')
    # Kr is the Ray class group.
    return ab
    # return val(ai) and val(bj)
    # where A_{p^{n}}(K) = Z/a1 x ... x Z/a_r2+1 x Z/b1 x ... x Z/bt
    # and val_p(a1) >= ... >=val_p(a_r2+1) >= val_p(b1) >= ...


"""
Test is the number field of f is p-rational.
If this number field doesn't verify Leopoldt's conjecture
 then the programme doesn't terminate.

"""
def is_p_rational(f,p):
    Zx=f.parent()
    K.<a>=NumberField(f)
    r1,r2=K.signature()
    OK=K.ring_of_integers()
    factorization_p=factor(p*OK) # pairs (pi,vi)
    e=max([pivi[1] for pivi in factorization_p]) # second component of (pi,vi)
    s=valuation(e,p)
    n=2+s
    old_ab=FI(K,p,n)
    old_a=FI(K,p,n)[:r2+1]  # first r2+1 components returned by FI
    #                         old_a=[val_p(a1),val_p(a2),...,val_p(a_r2+1)]
    old_b=FI(K,p,n)[r2+1:]  # old_b=[val_p(b1),val_p(b2),...,val_p(bt)]
    n+=1
    found=false
    while not found:
        new_ab=FI(K,p,n)
        new_a=FI(K,p,n)[:r2+1] # similar to old_a, corresponds to n+1
        new_b=list(FI(K,p,n)[r2+1:]) # similar to old_b, corresponds to n+1
        if new_a ==  [p*ai for ai in old_a] and min(new_a) > p*max(new_b+[1]):
            #  if new_b is empty we replace max(new_b) by 1
            found=true
            if new_b == len(new_b)*[1]: # the elements of new_b are non-negative
                answer=true       # their sum is 0 if they are all zero
            else:
                answer=false
        old_ab=new_ab             # increase n by 1
        old_a=new_a
        n+=1
    return answer
```

B Implementation of Algorithm 1

The following code implements algorithm 1.

```
def does_p_divide_class_number(p,K,N=100):
    m=K.disc().sqrt()
```

```
    if ZZ((m-1)/3) % p == 0 or m % p == 0:
        return true # cannot apply criterion
    if not cyclotomic_polynomial((m-1)//2).change_ring(GF(p)).is_irreducible():
        return true # p is not inert in Q(zeta_{(m-1)/2})
    i = 0
    for ell in range(1,N*m^2*p^2,m*p):
        if not ZZ(ell).is_prime():
            continue
        Fellx.<x>=GF(ell)[]
        if ((x+1)^((ell-1)//p) -1 ) % cyclotomic_polynomial(m) != 0:
            return false # could prove that p doesn't divide h
        i += 1
        if i >= N:
            break
    return true # couldn't prove that p doesn't divide the class number
```

C Implementation of Algorithm 2

This function takes as parameter a polynomial f whose number field K is cyclic cubic. The output is a unit u, which is not necessarily of infinite order. If $ord(u)$ is infinite and p is a prime which doesn't divide the p-adic regulator of K, then u is used to rapidly certify it.

```
def fast_units(f):
    K.<a>=NumberField(f)
    OK=K.ring_of_integers()
    m=K.disc().sqrt()    # m is the conductor of K because it is cyclic cubic
    # the following 5 lines compute gm, an ideal such that gm^3=(m)
    gm=OK
    for p in m.prime_factors():
       pfact=(p*OK).factor()
       gp=prod([pe[0]^(pe[1]//3) for pe in pfact])
       #                 # gp prime ideal such that gp^3=(p)
       gm=gm*gp
    if not gm.is_principal(): # is_principal uses LLL and \
                              # is not certified to find a generator\
                              #  even if gm is principal
        return K(1),K(1)
    omega=gm.gens_reduced()[0] # (omega)=gm. Uses LLL.
    sigma=K.automorphisms()[1] # sigma is a non-trivial automorphism of K
    eps=sigma(omega)/omega     # a unit of K, according to Remark 3.10
    return eps,sigma(eps)
```

D Implementation of Algorithm 3

The following code computes Schirokauer map associated to z and p.

```
def Schirokauer(z,p,E,gamma=None):
    v = exp_mod_pk(z,E,p,k=2)-1
    unramified = not (z.parent().disc() % p == 0) # p divides Disc(K) ?
    if unramified and gamma == None:
        gamma=p                                   # if NO we are done
    elif gamma == None:                           # if YES and we have a
        #                                           uniformizer we are done
        #                                   otherwise compute a uniformizer
        # next 6 lines compute a uniformizer gamma
        K = z.parent()                  # deduce K from z
        OK = K.ring_of_integers()       # ring of integers
        n=K.degree()                    # degree of K
        rad=prod([gp_[0]^(gp_[1]//n) for gp_ in  (p*OK).factor()] )
        # rad = product of prime ideals above p
        _,gamma=rad.gens_two()
        # gamma is such that <p,gamma> == rad
```

```
        Pcoeffs = (v/gamma).vector()
        # Compute a polynomial P such that P(a) = v/gamma
        # where a is such that K=Q(a).
        # Call Pcoeffs the coefficients of P.
    return [GF(p)(e) for e in Pcoeffs]
    #  Reduce the coefficients of P modulo p.
```

Given a polynomial f and a prime p, the following code tries to find a certificate that the p-adic regulator is not divisible by p and implements algorithm 3.

```
def criterium_p_not_divides_pRegulator(f,p):
    K.<a>=NumberField(f)            # K=Q(a) is the number field of f
    OK=K.ring_of_integers()         # ring of integers
    m = K.disc().sqrt()             # since K is cyclic cubic, m=cond(K)
    eps0,eps1=fast_units(f)         # try to find unit using Algorithm 2.
    if eps0 == 1:                   # in case of failure
        return "Maybe"              # we do not have a basis of subgroup
        #                             of finite index
        if (f.disc() // K.disc()) % p^2 == 0: # if p divides [OK:Z[a]]
            return "Maybe"                    # we answer "Maybe"
        # Compute E denoted e in Definition 3.9
        E=ZZ(lcm([ee[0].norm()-1 for ee in (p*OK).factor()]))
        # The next 9 lines compute gamma, a uniformizer of p
        if K.disc() % p == 0:
            OK=K.ring_of_integers()
            n=K.degree()
            rad=prod([gp_[0]^(gp_[1]//n) for gp_ in  (p*OK).factor()] )
            _,gamma=rad.gens_two()
            if gamma == p:
                gamma=p
        else:
            gamma=p
        # compute the rank of the matrix in Algorithm 3.
        Srank=Matrix(GF(p),2,3,[Schirokauer(eps0,p,E,gamma),Schirokauer(eps1,p,E,gamma)]).rank()
        if Srank == 2:
            return True
# Main enumeration.
Qx.<x>=QQ['x']
line=fd.readline()                      # line = next line of file fd
cond=0                                  # cond = conductor of previous field
while line != "":                       # until end f file
    if not line[0] == "x":              # skip comment lines
        cond=int(line)
    else:
        f=Qx(line.strip())              # f = polynomial read in file
        K.<a>=NumberField(f)            # K=Q(a) is the number field of f
        OK=K.ring_of_integers()         # ring of integers
        m = K.disc().sqrt()             # since K is cyclic cubic, m=cond(K)
        if m < cond:                    # skip f if its conductor is smaller
            line=fd.readline()          # than previous conductor because
            continue                    # it has been already treated
        for p in ps:
            bool = criterium_p_not_divides_pRegulator(f,p)
            if bool == "True":
                bools = bools + ",False"
            else:
                bools = bools + ",Maybe"
        gd.write(str(f)+":"+bools+"\n")
        gd.flush()
    line=fd.readline()
```

E SAGE code to determine a suitable set of primes satisfying Hypothesis 5.35

In the following, we give the sage code to find primes m, l satisfying Hypothesis 5.35.

```
a=1
while not ((a^2+27)//4).is_prime():
a += 2

m=(a^2+27)//4
l=1
found = false
while not found:
while not l.is_prime():
l += 5*m
Flx.<x>=GF(l)[]
if ((x+1)^((l-1)//5)-1) % cyclotomic_polynomial(m)(x) == 0:
found = true
l += 5*m
print m,l
```

This code gives that $m = 7, l = 16906$ satisfies Hypothesis 5.35.

References

[Abe69] Eiichi Abe. Chevalley groups over local rings. *Tôhoku Math. J. (2)*, 21:474–494, 1969.

[AC89] James Arthur and Laurent Clozel. *Simple algebras, base change, and the advanced theory of the trace formula*, volume 120 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1989.

[Ard04] Konstantin Ardakov. The centre of completed group algebras of pro-p groups. *Doc. Math.*, 9:599–606, 2004.

[BBB+98] Christian Batut, Karim Belabas, Dominique Bernardi, Henri Cohen, and Michel Olivier. *User's Guide to PARI-GP*. http://megrez.math.u-bordeaux.fr/pub/pari, 1998. see also http://pari.home.ml.org.

[Ber00] Alessandra Bertapelle. Formal Néron models and Weil restriction. *Math. Ann.*, 316(3):437–463, 2000.

[Bos14] Siegfried Bosch. *Lectures on formal and rigid geometry*, volume 2105 of *Lecture Notes in Mathematics*. Springer, Cham, 2014.

[Bou81] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1981. Groupes et algèbres de Lie. Chapitres 4, 5 et 6. [Lie groups and Lie algebras. Chapters 4, 5 and 6].

[BP79] Lyliane Bouvier and Jean-Jacques Payan. Sur la structure galoisienne du groupe des unités d'un corps abélien de type (p, p). *Annales de l'institut Fourier*, 29(1):171–187, 1979.

[BR17a] Razvan Barbulescu and Jishnu Ray. Electronic manuscript of computations of "Some remarks and experiments on Greenberg's p-rationality conjecture", 2017. available online at `https://webusers.imj-prg.fr/~razvan.barbaud/pRational/pRational.html`.

[BR17b] Razvan Barbulescu and Jishnu Ray. Some remarks and experiments on Greenberg's p-rationality conjecture. *Preprint arXiv:1706.04847*, 2017.

[BT72] François Bruhat and Jacques Tits. Groupes réductifs sur un corps local. *Inst. Hautes Études Sci. Publ. Math.*, (41):5–251, 1972.

[BW89] Johannes Buchmann and Hugh Williams. On the computation of the class number of an algebraic number field. *Mathematics of Computation*, 53(188):679–688, 1989.

[BW13] Da Bian and Feng Wei. Erratum: Normal elements of completed group algebras over $\mathrm{SL}_n(\mathbb{Z}_p)$ [MR2747414]. *Internat. J. Algebra Comput.*, 23(1):215, 2013.

[Bye01a] Dongho Byeon. Divisibility properties of class numbers. *Trends in mathematics, Information Center for Mathematical Sciences*, 4(1):26–30, 2001.

[Bye01b] Dongho Byeon. Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields. *Compositio Mathematica*, 126(3):249–256, 2001.

[Car79] Pierre Cartier. Representations of p-adic groups: a survey. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, pages 111–155. Amer. Math. Soc., Providence, R.I., 1979.

[CD14] Pierre Colmez and Gabriel Dospinescu. Complétés universels de représentations de $\mathrm{GL}_2(\mathbb{Q}_p)$. *Algebra Number Theory*, 8(6):1447–1519, 2014.

[CDO98] Henri Cohen, Francisco Diaz Y Diaz, and Michel Olivier. Computing ray class groups, conductors and discriminants. *Mathematics of Computation*, 67(222):773–795, 1998.

[CDP14] Pierre Colmez, Gabriel Dospinescu, and Vytautas Paškūnas. The p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$. *Camb. J. Math.*, 2(1):1–47, 2014.

[Che95] Claude Chevalley. Certains schémas de groupes semi-simples. In *Séminaire Bourbaki, Vol. 6*, pages Exp. No. 219, 219–234. Soc. Math. France, Paris, 1995.

[CL84a] Henri Cohen and Hendrik Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CL84b] Henri Cohen and Hendrik W Lenstra, Jr. Heuristics on class groups. In *Number theory (New York, 1982)*, volume 1052 of *Lecture Notes in Math.*, pages 26–36. Springer, Berlin, 1984.

[Clo11] Laurent Clozel. Presentation of an Iwasawa algebra: the case of $\Gamma_1 SL(2, \mathbb{Z}_p)$. *Doc. Math.*, 16:545–559, 2011.

[Clo16] Laurent Clozel. Globally analytic p-adic representations of the pro-p Iwahori subgroup of GL(2) and base change, II: a Steinberg tensor product theorem. *Pre-print*, 2016. Hal-01360765, v1, revised version to appear.

[Clo17] Laurent Clozel. Globally analytic p-adic representations of the pro-p Iwahori subgroup of GL(2) and base change, I : Iwasawa algebras and a base change map. *Bulletin of the Iranian Mathematical Society*, 43:55–76, 2017. Hal-01312419, v1.

[CM87] Henri Cohen and Jacques Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[CM90] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.

[Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate texts in mathematics*. Springer Science & Business Media, 2013.

[Col08] Pierre Colmez. Représentations triangulines de dimension 2. *Astérisque*, (319):213–258, 2008. Représentations p-adiques de groupes p-adiques. I. Représentations galoisiennes et (ϕ, Γ)-modules.

[Col10] Pierre Colmez. Représentations de $\mathrm{GL}_2(\mathbf{Q}_p)$ et (ϕ, Γ)-modules. *Astérisque*, (330):281–509, 2010.

[Col14] Pierre Colmez. La série principale unitaire de $\mathrm{GL}_2(\mathbf{Q}_p)$: vecteurs localement analytiques. *Automorphic Forms and Galois Representations*, 1:286–358, 2014.

[CR18] Christophe Cornut and Jishnu Ray. Generators of the pro-p Iwahori and Galois representations. *Int. J. Number Theory*, 14(1):37–53, 2018.

[Dix77] Jacques Dixmier. *Enveloping algebras*, volume 14. Newnes, 1977.

[DSMS03] John Douglas Dixon, Marcus Peter Francis du Sautoy, Avinoam Mann, and Daniel Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2003.

[Eme17] Matthew Emerton. Locally analytic vectors in representations of locally p-adic analytic groups. *Mem. Amer. Math. Soc.*, 248(1175):iv+158, 2017.

[Fon90] Jean-Marc Fontaine. Représentations p-adiques des corps locaux. I. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 249–309. Birkhäuser Boston, Boston, MA, 1990.

[Fuj08] Satoshi Fujii. On the maximal pro-p extension unramified outside p of an imaginary quadratic field. *Osaka J. Math.*, 45(1):41–60, 2008.

[Gar97] Paul Garrett. *Buildings and classical groups*. Chapman & Hall, London, 1997.

[GJ89] Georges Gras and Jean-François Jaulent. Sur les corps de nombres réguliers. *Mathematische Zeitschrift*, 202(3):343–365, 1989.

[GP11] Philippe Gille and Patrick Polo, editors. *Schémas en groupes (SGA 3). Tome III. Structure des schémas en groupes réductifs*, volume 8 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, 2011. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64], A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre, Revised and annotated edition of the 1970 French original.

[Gra75] Marie-Nicole Gras. Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de Q. *J. reine angew. Math*, 277(89):116, 1975.

[Gra13] Georges Gras. *Class Field Theory: from theory to practice*. Springer monographs of mathematics. Springer Science & Business Media, 2013.

[Gra16a] Georges Gras. Approche p-adique de la conjecture de Greenberg (cas galoisien réel p-décomposé). *Prépublication, arXiv:1611.09592*, 2016.

[Gra16b] Georges Gras. Les θ-régulateurs locaux d'un nombre algébrique: conjectures p-adiques. *Canad. J. Math.*, 68(3):571–624, 2016.

[Gre76] Ralph Greenberg. On the Iwasawa invariants of totally real number fields. *American Journal of Mathematics*, 98(1):263–284, 1976.

[Gre16] Ralph Greenberg. Galois representations with open image. *Ann. Math. Qué.*, 40(1):83–119, 2016.

[GS07] Jon González-Sánchez. On p-saturable groups. *Journal of Algebra*, 315(2):809–823, 2007.

[Hak09] Tuomas Hakkarainen. On the computation of class numbers of real abelian fields. *Mathematics of Computation*, 78(265):555–573, 2009.

[Har74] Paul Hartung. Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3. *Journal of Number Theory*, 6(4):276–278, 1974.

[Hen00] Guy Henniart. Une preuve simple des conjectures de Langlands pour GL(n) sur un corps p-adique. *Invent. Math.*, 139(2):439–455, 2000.

[HM16] Farshid Hajir and Christian Maire. Prime decomposition and the Iwasawa μ-invariant. *Preprint arXiv:1601.04195*, 2016.

[HT01] Michael Harris and Richard Taylor. *The geometry and cohomology of some simple Shimura varieties*, volume 151 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2001. With an appendix by Vladimir G. Berkovich.

[HW18] Dong Han and Feng Wei. Normal elements of completed group algebras over $\mathrm{SL}_3(\mathbb{Z}_p)$. *Preprint, arXiv:1802.02676*, 2018.

[HZ16] Tommy Hofmann and Yinan Zhang. Valuations of p-adic regulators of cyclic cubic fields. *Journal of Number Theory*, 169:86–102, 2016.

[Iwa59] Kenkichi Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65:183–226, 1959.

[JNQD93] Jean-François Jaulent and Thong Nguyen Quang Do. Corps p-rationnels, corps p-réguliers, et ramification restreinte. *Journal de théorie des nombres de Bordeaux*, 5(2):343–363, 1993.

[Kat17] Nicholas Katz. A note on Galois representations with big image. *https://web.math.princeton.edu/ nmk/bigimage23.pdf*, 2017.

[Kos66] Bertram Kostant. Groups over Z. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 90–98. Amer. Math. Soc., Providence, R.I., 1966.

[Kur50] Sigekatu Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, 1:1–10, 1950.

[Laz65] Michel Lazard. Groupes analytiques p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (26):389–603, 1965.

[Lem94] Franz Lemmermeyer. Kuroda's class number formula. *Acta Arith.*, 66(3):245–260, 1994.

[LLL82] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LO96] Huishi Li and Freddy van Oystaeyen. *Zariskian filtrations*, volume 2 of *K-Monographs in Mathematics*. Kluwer Academic Publishers, Dordrecht, 1996.

[Lou98] Stéphane Louboutin. Majorations explicites du résidu au point 1 des fonctions zêta de certains corps de nombres. *J. Math. Soc. Japan*, 50(1):57–69, 01 1998.

[Mil15] John C. Miller. Class numbers in cyclotomic $\mathbb{Z}_p$-extensions. *J. Number Theory*, 150:47–73, 2015.

[Min86] John Victor Minardi. *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*. ProQuest LLC, Ann Arbor, MI, 1986. Thesis (Ph.D.)–University of Washington.

[MM13] Gunter Malle and Bernd Heinrich Matzat. *Inverse Galois Theory*. Springer Science & Business Media, 2013.

[MNQD90] Abbas Movahhedi and Thong Nguyen Quang Do. Sur l'arithmétique des corps de nombres p-rationnels. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 155–200. Birkhäuser Boston, Boston, MA, 1990.

[Mov88a] A Movahhedi. Sur les p-extensions des corps p-rationnels. *Thése de doctorat, Paris* 7, 1988.

[Mov88b] Abbas Movahhedi. *Sur les p-extensions des corps p-rationnels*. PhD thesis, Université Paris VII, 1988.

[Mov90] Abbas Movahhedi. Sur les p-extensions des corps p-rationnels. *Math. Nachr.*, 149:163–176, 1990.

[OS10] Sascha Orlik and Matthias Strauch. On the irreducibility of locally analytic principal series representations. *Represent. Theory*, 14:713–746, 2010.

[OS16] Rachel Ollivier and Peter Schneider. A canonical torsion theory for pro-p iwahori-hecke modules. *Preprint arXiv:1602.00738*, 2016.

[Pan95] Peter N. Panayi. *Computation of Leopoldt's p-adic regulator*. PhD thesis, University of East Anglia, 1995.

[PV15] Frédéric Pitoun and Firmin Varescon. Computing the torsion of the p-ramified module of a number field. *Math. Comp.*, 84(291):371–383, 2015.

[Ray16] Jishnu Ray. Presentation of the Iwasawa algebra of the first congruence kernel of a semi-simple, simply connected chevalley group over $\mathbb{Z}_p$. *Preprint, arXiv:1609.03187*, 2016.

[Ray17] Jishnu Ray. Presentation of the Iwasawa algebra of the pro-p Iwahori subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$. *Preprint, arXiv:1707.06816*, 2017.

[Ray18] Jishnu Ray. Globally analytic principal series representation and Langlands base change. *Preprint, arXiv:1806.03670*, 2018.

[Rin13] Claus Michael Ringel. The $(n-1)$-antichains in a root poset of width n. *Preprint arXiv:1306.1593*, 2013.

[Sau98] Odile Sauzet. Theorie d'Iwasawa des corps p-rationnels et p-birationnels. *Manuscripta mathematica*, 96(3):263–273, 1998.

[Sch93] Oliver Schirokauer. Discrete logarithms and local units. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 345(1676):409–423, 1993.

[Sch11] Peter Schneider. *p-adic Lie groups*, volume 344 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2011.

[Ser87] Jean-Pierre Serre. *Complex semisimple Lie algebras*. Springer-Verlag, New York, 1987. Translated from the French by G. A. Jones.

[Sha66] Igor Shafarevich. Extensions with given points of ramification. *Americal mathematical society translations*, 2.59:128–149, 1966.

[Sin78] Warren Sinnott. On the stickelberger ideal and the circular units of a cyclotomic field. *Annals of Mathematics*, 108(1):107–134, 1978.

[ST02a] Peter Schneider and Jeremy Teitelbaum. Banach space representations and Iwasawa theory. *Israel journal of mathematics*, 127(1):359–380, 2002.

[ST02b] Peter Schneider and Jeremy Teitelbaum. Locally analytic distributions and p-adic representation theory, with applications to GL_2. *J. Amer. Math. Soc.*, 15(2):443–468, 2002.

[ST03] Peter Schneider and Jeremy Teitelbaum. Algebras of p-adic distributions and admissible representations. *Invent. Math.*, 153(1):145–196, 2003.

[Ste63] Robert Steinberg. Representations of algebraic groups. *Nagoya Math. J.*, 22:33–56, 1963.

[Ste67] Robert Steinberg. Lectures on Chevalley groups. *mimeographed notes, Yale University, New Haven, Connecticut, USA, 151,*, 1967.

[Tit79] Jacques Tits. Reductive groups over local fields. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, pages 29–69. Amer. Math. Soc., Providence, R.I., 1979.

[VdL82] Franciscus Jozef Van der Linden. Class number computations of real abelian number fields. *Mathematics of Computation*, 39(160):693–707, 1982.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wil98] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1998.

[WR76] Peter J. Weinberger and Linda Preiss Rothschild. Factoring polynomials over algebraic number fields. *ACM Transactions on Mathematical Software (TOMS)*, 2(4):335–350, 1976.

[Zha13] Yinan Zhang. *p-adic Verification of Class Number Computations*. PhD thesis, University of Sydney, 2013.