HAL
open science

Generators of the pro-p Iwahori and Galois representations

Christophe Cornut, Jishnu Ray

To cite this version:

Christophe Cornut, Jishnu Ray. Generators of the pro-p Iwahori and Galois representations. International Journal of Number Theory, 2018, 14 (1), 10.1142/S1793042118500045 . hal-01398468

HAL Id: hal-01398468

https://hal.science/hal-01398468

Submitted on 17 Nov 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Generators of the pro-p Iwahori and Galois representations

Christophe Cornut[1] and Jishnu Ray[2]

[1]CNRS - Institut de Mathématiques de Jussieu - Paris Rive Gauche,
4, place Jussieu, 75252 Paris Cedex 05, France,
christophe.cornut@imj-prg.fr
[2]Département de Mathématiques, Université Paris-Sud 11,
91405 Orsay Cedex, France,
jishnu.ray@u-psud.fr

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.

1 Introduction

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 $\mathbf{U} \triangleleft \mathbf{B}$ 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 [13, 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 [3] (who works with $\mathbf{G} = \mathbf{GL}_n$), we construct in section 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 2.4.1):

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 [3] proposition 5.3, see also Schneider and Ollivier ([9], 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 2.12). 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 $\Gamma = \mathrm{Gal}(M/K)$, $\Omega = \mathrm{Gal}(K/\mathbb{Q})$ and $\Pi = \mathrm{Gal}(M/\mathbb{Q})$. We say that K is p-rational if Γ is a free pro$-p$ group, see [6]. 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 $(p-1)\cdot\Omega = 0$. Then Greenberg in [3] 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 3, 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. 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 3.3.1 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 $\mathbb{F}_p^\times$ (it is defined after proposition 3.2.1). 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 (cf. section 3.2):

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 3.4.1, 3.4.2 and remark 3.4.3.

In section 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 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.

We would like to thank Marie-France Vignéras for useful discussions and for giving us the reference [9]. We are also deeply grateful to Ralph Greenberg for numerous conversations on this topic.

2 Topological Generators of the pro-p Iwahori

This section is organized as follows. In sections $(2.1 - 2.3)$ we introduce the notations, then section 2.4 states our main result concerning the minimal set of topological generators of $I(1)$ (see theorem 2.4.1) with a discussion of the Iwahori factorisation in section 2.5. Its proof for $\mathbf{G}$ simple and simply connected is given in sections $(2.6 - 2.10)$, where section 2.10 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 sections $(2.11 - 2.14)$. In particular, section 2.14 establishes the minimality of our set of topological generators. Finally, in section 2.15 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 the cases when it is multiplicity free.

2.1 Let p be an odd prime, $\mathbf{G}$ be a split reductive group over $\mathbb{Z}_p$. Fix a pinning of $\mathbf{G}$ [11, 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 $\mathfrak{g}_\alpha$.

2.2 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 $\mathbf{G}$ [11, 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.

2.3 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 [13, 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

$$\begin{aligned} T(1) &= \mathrm{Hom}\,(M, 1+p\mathbb{Z}_p) = M^\vee \otimes (1+p\mathbb{Z}_p), \\ T_{tors} &= \mathrm{Hom}\,(M, \mu_{p-1}) = M^\vee \otimes \mathbb{F}_p^\times. \end{aligned}$$

2.4 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 2.4.1. *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 $x_{\delta_d}(1)$.*

2.5 By [11, 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 [11, 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 [11, 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. $t \in T(1)$).

2.6 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 2.11, we therefore assume that

$$\mathbf{G} \text{ is (split) simple and simply connected.}$$

2.7 As a first step, we show that

Lemma 2.7.1. *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 [11, 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 $x \in 1 + p\mathbb{Z}_p$ [11, 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. □

2.8 Recall from [11, 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 2.8.1. *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 [11, XXIII 6.4]. □

Corollary 2.8.2. *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 2.8.3. *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 [11, 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 $\Delta' = \{\alpha, \alpha'\}$ [11, 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 [11, 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. □

2.9 We now establish our theorem 2.4.1 for a group $\mathbf{G}$ which is simple and simply connected, but not of type G_2.

Lemma 2.9.1. *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 [1, 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 2.8.2. □

Lemma 2.9.2. *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 $\gamma \in R_+$. If $h(\gamma) = h(\alpha_{max})$, then $\gamma = \alpha_{max}$ and there is nothing to prove. If $h(\gamma) < h(\alpha_{max})$, then by [1, 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 2.8.2. □

Remark 2.9.3. *From the Hasse diagrams in [10], it seems that in the previous proof, we may always require α to be a simple root.*

Proof. (Of theorem 2.4.1 for $\mathbf{G}$ simple, simply connected, not of type G_2) By lemma 2.7.1, 2.9.1, 2.9.2 and the Iwahori decomposition of section 2.5, $I(1)$ 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

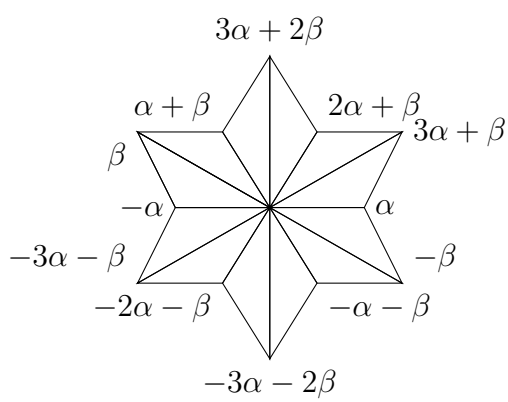
$$I(1) \twoheadrightarrow \mathbf{U}(\mathbb{F}_p) \twoheadrightarrow \overline{\mathbf{U}}_1(\mathbb{F}_p) \simeq \prod_{\alpha \in \Delta} \mathbf{U}_\alpha(\mathbb{F}_p),$$

a surjective morphism that kills $x_{-\alpha_{max}}(p)$. □

2.10 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 2.10.1. *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

$$\begin{aligned}
[x_{-2\beta-3\alpha}(pv) : x_\beta(u)] &= x_{-\beta-3\alpha}(\pm puv) \\
[x_{-2\beta-3\alpha}(pv) : x_{\beta+3\alpha}(u)] &= x_{-\beta}(\pm puv) \\
[x_{-2\beta-3\alpha}(pv) : x_{\beta+2\alpha}(u)] &= x_{-\beta-\alpha}(\pm puv) \cdot x_\alpha(\pm pu^2 v) \cdot x_{\beta+3\alpha}(\pm pu^3 v) \cdot x_{-\beta}(\pm p^2 u^3 v^2)
\end{aligned}$$

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 2.5 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 2.8.1,

$$\begin{gathered}[\overline{x}_\beta, \overline{x}_\alpha] = \pm\overline{x}_{\alpha+\beta}, \quad [\overline{x}_{\alpha+\beta}, \overline{x}_\alpha] = \pm 2\overline{x}_{2\alpha+\beta}, \quad [\overline{x}_{2\alpha+\beta}, \overline{x}_\alpha] = \pm 3\overline{x}_{3\alpha+\beta}, \\ [\overline{x}_{\alpha+\beta}, \overline{x}_{2\alpha+\beta}] = \pm x_{3\alpha+2\beta} \quad \text{and} \quad [\overline{x}_\beta, \overline{x}_{3\alpha+\beta}] = \pm x_{2\alpha+2\beta}\end{gathered}$$

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 2.8.1, 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 2.10.2. *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 2.4.1 for $\mathbf{G}$ simple of type G_2) By lemma 2.7.1, 2.10.1, 2.10.2 and the Iwahori decomposition of section 2.5, 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 $X/Y \simeq \mathbb{F}_3^3$. $\square$

2.11 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 of 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

$$I^{sc} \to I^{der} \hookrightarrow I \to I^{ad} \quad \text{and} \quad I^{sc}(1) \to I^{der}(1) \hookrightarrow I(1) \to I^{ad}(1).$$

2.12 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 $I^{ad} = I^{ad}(1) \rtimes T^{ad}_{tors}$.

2.13 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 2.5, 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 2.13.1. *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* $Q \simeq \mathbb{F}_p$*.*

2.14 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 2.4.1 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 $\mathbf{G}_d^{sc} \to \mathbf{G}_d^{ad}$ between the simple (simply connected *and* adjoint) components corresponding to d, thus also an isomorphism between the corresponding pro-p-Iwahori's $I_d^{sc}(1) \to I_d^{ad}(1)$. In particular, the projection $I(1) \to I^{ad}(1) \twoheadrightarrow I_d^{ad}(1)$ is surjective. Composing it with the projection $I_d^{ad}(1) \twoheadrightarrow \mathbb{F}_3^3$ constructed in section 2.10, 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 2.4.1.

2.15 The action of $I^{ad} = I^{ad}(1) \rtimes T_{tors}^{ad}$ on $I(1)$ induces an $\mathbb{F}_p$-linear action of

$$T_{tors}^{ad} = \mathrm{Hom}\left(M^{ad}, \mu_{p-1}\right) = \mathrm{Hom}\left(\mathbb{Z}R, \mathbb{F}_p^\times\right)$$

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_{tors}^{ad}. We denote by $\mathbb{F}_p(\alpha)$ the 1-dimensional representation of T_{tors}^{ad} on $\mathbb{F}_p$ defined by $\alpha \in \mathbb{Z}R$. We thus obtain:

Corollary 2.15.1. *The* $\mathbb{F}_p[T_{tors}^{ad}]$*-module* $\tilde{I}(1)$ *is isomorphic to*

$$\mathbb{F}_p^{\sharp\mathcal{S}} \oplus \left(\oplus_{\alpha\in\Delta} \mathbb{F}_p(\alpha)\right) \oplus \left(\oplus_{c\in\mathcal{C}} \mathbb{F}_p(-\alpha_{c,max})\right)\left(\oplus\left(\oplus_{d\in\mathcal{D}} \mathbb{F}_p(\delta_c)\right) \text{ if } p = 3\right).$$

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 $\mathbb{F}_p[T_{tors}^{ad}]$-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 [1] yields the following:

Corollary 2.15.2. *If* $\mathbf{G}$ *is simple, the* $\mathbb{F}_p[T_{tors}^{ad}]$*-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 $I^{ad}(1)$.

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 3.1, we establish a criterion for the existence of our representations in sections 3.2 and 3.3 and finally give some examples in section 3.4.

3.1 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 we let Γ denote $\mathrm{Gal}(M/K)$, 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 *A number field K is p-rational if the following equivalent conditions are satisfied:*

(1) *$rank_{\mathbb{Z}_p}(\Gamma^{ab}) = r_2(K) + 1$ 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 [6], see also proposition 3.1 and the discussion before remark 3.2 of [3]. There is a considerable literature concerning p-rational fields, including [8], [4].

Examples:

(1) 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 [3]). However, there are p-rational complex K's for which p divides the class number (cf. chapter 2, section 1, p. 25 of [7]). For similar results, see also [2] and [5] if K is complex.

(2) Let $K = \mathbb{Q}(\mu_p)$. If p is a regular prime, then K is a p-rational field (cf. [12], see also [3], proposition 4.9 for a shorter proof).

3.2 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

$$1 \to \Gamma \to \Pi \to \Omega \to 1 \tag{3.2.1}$$

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

$$\overline{\rho} : \Omega \to T_{tors} \quad \text{and} \quad \tilde{\rho} : \tilde{\Gamma} \twoheadrightarrow \tilde{I}(1).$$

Then as Ω has order prime to p, the Schur-Zassenhaus theorem ([14], proposition 2.3.3) implies that the exact sequence 3.2.1 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 [3], 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 3.2.1. *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 $\overline{\rho}^* \tilde{I}(1)$.

3.3 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 [3] 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 2.15.2,

B(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 2.4, 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 3.3.1. *Under the assumptions **A(K)** on K and **B(G)** on $\mathbf{G}$, 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 $\hat{\Omega}_{odd}^{\mathcal{S}}$.*

3.4 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 [1]. 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 3.4.1. *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 3.4.2. *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 $\hat{\Omega}_{odd}$. 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 [1] 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 3.4.3. *For* $\mathbf{G}$ *of type* E_6, E_7, E_8, F_4 *or* G_2*, the tables in [1] show that the constant* $\sum_{i=1}^{\ell}(2i-1)n_i + 2\ell$ *of lemma 3.4.2 is* $79, 127, 247, 53, 13$ *respectively.*

Corollary 3.4.4. *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 a split reductive groups over $\mathbb{Z}_p$ (theorem 2.4.1) and used it to study the structure of the Frattini quotient $\tilde{I}(1)$ as an $\mathbb{F}_p[T_{tors}^{ad}]$-module (corollary 2.15.1). Then we have used corollary 2.15.1 to determine when $\tilde{I}(1)$ is multiplicity free (see corollary 2.15.2). Furthermore in proposition 3.2.1 and corollary 3.3.1, 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 discussed in section 3.4 under the assumption $K = \mathbb{Q}(\mu_p)$, for any sufficiently large regular prime p (see corollary 3.4.4).

References

[1] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines. Actualités Scientifiques et Industrielles*, No. 1337, Hermann, Paris, (1968).

[2] S. Fujii, *On the maximal pro-p extension unramified outside p of an imaginary quadratic field*, Osaka J. Math. 45, (2008), 41-60.

[3] R. Greenberg, *Galois representation with open image*, Annales mathématiques du Québec, Volume 40, Issue 1, (2016), 83-119.

[4] J. F. Jaulent, T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers, et ramification restreinte*, Séminaire de Théorie des Nombres de Bordeaux, (1987-88), Exposé 10, 10-01 10-26.

[5] J. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, University of Washington Ph. D. thesis, (1986).

[6] A. Movahhedi, T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Prog. Math. 81, Birkhauser, (1990), 155-200.

[7] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Thèse de doctorat en Mathématiques, Paris 7, (1988).

[8] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Math. Nach, 149, (1990), 163-176.

[9] R. Ollivier, P. Schneider, *A canonical torsion theory for pro-p Iwahori-Hecke modules*, https://arxiv.org/pdf/1602.00738v1.pdf, (2016).

[10] C. M. Ringel, *The $(n-1)$-antichains in a root poset of width n*, http://arxiv.org/abs/1306.1593v1, (2013).

[11] *Séminaire de Géométrie Algébrique du Bois Marie - 1962-64 - Schémas en groupes - (SGA 3)* Philippe Gille and Patrick Polo, editors.

[12] I. R. Shafarevich, *Extensions with given points of ramification*, Amer. Math. Soc, Translations 59, (1966), 128-149.

[13] J. 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).

[14] J. S. Wilson, *Profinite Groups*, Oxford Science Publications, London Mathematical Society Monographs, New Series 19, (2005).