Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

EXPLICIT GENERATORS OF SOME PRO-p GROUPS VIA BRUHAT–TITS THEORY

Benoit Loisel

Tome 149
Fascicule 2

2021

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 309-388

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel
de la Société Mathématique de France.

Fascicule 2, tome 149, juin 2021

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 135 € ($ 202),
avec supplément papier : Europe 179 €, hors Europe 197 € ($ 296)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Fabien DURAND

Bull. Soc. Math. France
149 (2), 2021, p. 309-388

EXPLICIT GENERATORS OF SOME PRO-p GROUPS VIA BRUHAT–TITS THEORY

by Benoit Loisel

Abstract. — Given a semisimple group over a local field of residual characteristic p, its topological group of rational points admits maximal pro-p subgroups. The maximal pro-p subgroups of quasisplit simply connected semisimple groups can be described in the combinatorial terms of a valued root groups datum, thanks to the Bruhat–Tits theory. In this context, it becomes possible to compute explicitly a minimal generating set of the (all conjugated) maximal pro-p subgroups thanks to parametrizations of a suitable maximal torus and of the corresponding root groups. We show that the minimal number of generators is then linear with respect to the rank of a suitable root system.

Résumé (*Générateurs explicites de certains sous-groupes pro-p via la théorie de Bruhat–Tits*). — Étant donné un groupe semi simple sur un corps local de caractéristique résiduelle p, le groupe topologique de ses points rationnels admet des sous-groupes pro-p maximaux. Grâce à la théorie de Bruhat–Tits, ceux des groupes semisimples simplement connexes quasi-déployés peuvent être décrits en des termes combinatoires de donnée radicielle de groupes valuée. Dans ce contexte, il devient possible de calculer explicitement un ensemble minimal de générateurs des sous-groupes pro-p maximaux (tous conjugués) grâce aux paramétrisations d'un tore maximal convenable et des groupes radiciels correspondants. On montre que le nombre minimal de générateurs est alors linéaire en le rang d'un système de racines convenable.

Texte reçu le 31 janvier 2017, modifié le 17 décembre 2019, accepté le 12 novembre 2020.

Benoit Loisel, ENS de Lyon site Monod, UMPA UMR 5669 CNRS, 46 allée d'Italie, 69364 Lyon Cedex 07, France • *E-mail :* `benoit.loisel@ens-lyon.fr` • *Url :* `http://benoit.loisel.perso.math.cnrs.fr/`

Mathematical subject classification (2010). — 20G25, 20E18, 20E42, 20F05, 17B22.

Key words and phrases. — Profinite groups, Buildings, Linear algebraic groups, Local fields, Finite presentations.

The author is supported by the project ANR Geolie, ANR-15-CE40-0012 (The French National Research Agency).

 0037-9484/2021/309/$ 5.00
 doi:10.24033/bsmf.2831

1. Introduction

In this paper, a smooth connected affine group scheme of finite type over a field K will be called a K-group. Given a base field K and a K-group denoted by G, we get an abstract group called the group of rational points, denoted by $G(K)$. When K is a non-Archimedean local field, this group inherits a topology from the field. In particular, the topological group $G(K)$ is totally disconnected and locally compact. The maximal compact or pro-p subgroups of such a group $G(K)$, when they exist, provide many examples of profinite groups. Thus, one can investigate maximal pro-p subgroups from the profinite group theory point of view.

1.1. Minimal number of generators. — When H is a profinite group, we say that H is **topologically generated** by a subset X, if H is equal to its smallest closed subgroup containing X; such a set X is called a **generating set**. We investigate the minimal number of generators of a maximal pro-p subgroup of the group of rational points of an algebraic group over a local field.

Suppose that $K = \mathbb{F}_q((t))$ is a nonzero characteristic local field, where $q = p^m$ and G is a simple K-split simply connected K-group of rank l. By a recent result of Capdeboscq and Rémy [6, 2.5], we know that any maximal pro-p subgroup of $G(K)$ admits a finite generating set X; moreover, the minimal number of elements of such an X is $m(l+1)$.

We would like to generalize this result to more general algebraic groups defined over any local field. If G is a smooth algebraic group scheme over a local field K of residual characteristic p, we know by [11, 1.4.3] that $G(K)$ admits maximal pro-p subgroups (called pro-p Sylows) if, and only if, G is quasireductive (this means that the split unipotent radical over K of G is trivial). When K is of characteristic 0, this corresponds to reductive groups because a unipotent group is always split over a perfect field. To provide explicit descriptions of a pro-p Sylow thanks to Bruhat–Tits theory, we restrict the study to the case of a simply connected, quasisplit semisimple group G over a local field K.

Such a group G can be decomposed as a direct product of K-simple groups. Moreover, by [2, 6.21] for a simply connected group, we know that for any simply connected K-simple group H, there exists a finite extension of local fields K'/K and an absolutely simple K'-group H', such that H is isomorphic to the Weil restriction $R_{K'/K}(H')$, which means H' seen as a K-group. Since $H(K) = H'(K')$ by definition of the Weil restriction, we will assume that the simply connected, semisimple group G is absolutely simple.

In the Bruhat–Tits theory, given a reductive K-group G, we define a polysimplicial complex $X(G,K)$ (a Euclidean affine building), called the Bruhat–Tits building of G over K together with a suitable action of $G(K)$ onto $X(G,K)$.

There exists an unramified extension K'/K, such that the K-group G quasisplits over K'. There are two steps in the theory. The first part, corresponding to Chapter 4 of [5], provides the building $X(G',K')$ of $G_{K'}$ by gluing together affine spaces, called apartments. The second part, corresponding to Chapter 5 of [5], applies a Galois descent to the base field K, using fixed point theorems.

In the non quasisplit case, the geometry of the building does not faithfully reflect the structure of the group. There is an anisotropic kernel of the action of $G(K)$ on $X(G,K)$. As an example, when G is anisotropic over K, its Bruhat–Tits building is a point; the Bruhat–Tits theory completely fails to be explicit in combinatorial terms for anisotropic groups. Thus, the general case may require, moreover, arithmetical methods. Hence, to do explicit computations with a combinatorial method based on Lie theory we have to assume that G contains a torus with enough characters over K. More precisely, we say that a reductive group G is **quasisplit** if it admits a Borel subgroup defined over K or, equivalently, if the centralizer of any maximal K-split torus is a torus [5, 4.1.1].

Now, assume that K is any non-Archimedean local field of residual characteristic $p \neq 2$ and residue field $\kappa \simeq \mathbb{F}_q$, where $q = p^m$. Let G be an absolutely simple, simply connected quasisplit K-group.

Theorem 1.1. — *Denote by l the rank of the relative root system of G, and by n the rank of the absolute root system of G. Assume that $l \geq 2$. If G has a relative root system Φ of type G_2 or BC_l, assume that $p \neq 3$. Let P be a maximal pro-p subgroup of $G(K)$. Denote by $d(P)$ the minimal number of generators of P. Then, we have:*

$$d(P) = m(l+1) \text{ or } m(n+1)$$

depending on whether or not the minimal splitting field extension of short roots is ramified.

This theorem is formulated more precisely and proven in Corollary 5.4. According to [15, 4.2], we know that $d(P)$ can also be computed via cohomological methods: $d(P) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(P, \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathrm{Hom}(P, \mathbb{Z}/p\mathbb{Z})$.

From now on, we need to be more explicit. In the following, given a local field L, we denote by ω_L the discrete valuation on L, by $\mathcal{O}_L$ the ring of integers, by $\mathfrak{m}_L$ its maximal ideal, by ϖ_L a uniformizer, and by $\kappa_L = \mathcal{O}_L/\mathfrak{m}_L$ the residue field. Because we have to compare valuations of elements in L^*, we will normalize the discrete valuation $\omega_L : L^* \to \mathbb{Q}$, so that $\omega_L(L^*) = \mathbb{Z}$. When $l \in \mathbb{R}$, we denote by $\lfloor l \rfloor$ the largest integer less than or equal to l and by $\lceil l \rceil$ the smallest integer greater than or equal to l.

If it is clear in the context, we can omit the index L in these notations. When L/K is an extension, we denote by G_L the extension of scalars of G from K to L. When H is an algebraic L-group, we denote by $R_{L/K}(G)$ the K-group obtained by the Weil restriction functor $R_{L/K}$ defined in [7, I§1 6.6].