FINITE QUOTIENTS OF GALOIS PRO-p GROUPS AND RIGID FIELDS

C. QUADRELLI

Abstract. For a prime number p, we show that if two certain canonical finite quotients of a finitely generated Bloch-Kato pro-p group G coincide, then G has a very simple structure, i.e., G is a p-adic analytic pro-p group (see Theorem A). This result has a remarkable Galois-theoretic consequence: if the two corresponding canonical finite extensions $F^{(3)}/F$ and $F^{\{3\}}/F$ of a field F – with F containing a primitive p-th root of unity – coincide, then F is p-rigid (see Corollary B). The proof relies only on group-theoretic tools, and on certain properties of Bloch-Kato pro-p groups. This paper will appear on the *Annales mathématiques du Québec*.

1. Introduction

Let p be a prime number, and let G be a pro-p group. The Frattini subgroup $\Phi(G)$ of G is the closed subgroup of G generated by the p-powers and the commutators of the elements of G. In particular, the quotient $G/\Phi(G)$ is an elementary abelian p-group. Let $\Phi_2(G)$ be the Frattini subgroup of the Frattini subgroup of G, i.e., $\Phi_2(G) = \Phi(\Phi(G))$.

Also, let $P_n(G)$, $n \geq 1$, denote the p-descending central series of G. In particular, one has $P_2(G) = \Phi(G)$ and $P_3(G) = \Phi(G)^p[G, \Phi(G)] \supseteq \Phi_2(G)$. For the class of finitely generated Bloch-Kato pro-p groups, we prove the following result.

Theorem A. *One has the equality $\Phi_2(G) = P_3(G)$ if, and only if, G is p-adic analytic.*

In this case the group G has a very simple structure, as it is meta-abelian and it is possible to provide an explicit presentation for G (cf. [13, Theorem 4.6]).

One has also the following Galois-theoretic consequence. Let F be a field containing a primitive p-th root of unity. By $F^\times$ we denote the (multiplicative) group of non-zero elements of F. We consider the Galois extension $F^{(3)}$ of F obtained by first taking $F^{(2)}$ to be the compositum over F of all extensions of F of degree p, and then taking $F^{(3)}$ to be the compositum over

Date: March 22, 2015.

2010 *Mathematics Subject Classification.* 20E18, 12F10, 11S20.

Key words and phrases. Bloch-Kato pro-p groups, Zassenhaus filtration, absolute Galois groups, p-rigid fields, analytic pro-p groups.

$F^{(2)}$ of all the extensions of $F^{(2)}$ of degree p that are Galois over F. We also denote by $F^{\{3\}}$ the compositum over $F^{(2)}$ of all extensions of $F^{(2)}$ of degree p (cf. [3, § 2.3]). Thus

$$F^{\{3\}} = \left(F^{(2)}\right)^{(2)}.$$

Then one may characterize those fields F with the property that $F^{(3)} = F^{\{3\}}$. In fact, from Theorem A we shall obtain the following result.

Corollary B. *Let F be a field containing a primitive p-th root of unity, and assume that the quotient $F^\times/(F^\times)^p$ is finite. (Assume further that $\sqrt{-1} \in F$ if $p = 2$). Then $F^{(3)} = F^{\{3\}}$ if, and only if, F is p-rigid;*

(For the definition of p-rigid field, see Section 4.)

Bloch-Kato pro-p groups were introduced in [2] and studied first in [13]. A Bloch-Kato pro-p group is a pro-p group which satisfies the conclusion of the Rost-Voevodsky theorem (formerly known as the Bloch-Kato conjecture), i.e., such that the cohomology ring of every closed subgroup of G with coefficients in the finite field $\mathbb{F}_p$ is a quadratic algebra over $\mathbb{F}_p$. For example, absolute Galois groups of fields which are pro-p and Galois groups of the maximal p-extension of certain fields are Bloch-Kato pro-p groups. Thus, a Bloch-Kato pro-p group is a very natural "candidate" for being realized as absolute Galois group, and this shows the relevance of Bloch-Kato pro-p groups for Galois theory.

The problem to characterize a field F yielding the equality

$$F^{(3)} = F^{\{3\}} \tag{1.1}$$

arises rather naturally, and the case when equality (1.1) holds is considered very significant in field theory. Indeed, such problem has been widely studied in the past: in the case $p = 2$ Corollary B was proved in [1, Theorem 3.1], with arguments which make use of Galois cohomology, and later in [8, Theorem A], with arguments relying on the theory of quadratic forms. For p odd, Corollary B was proved in [3, Theorem A], and the proof relies on certain properties of Bloch-Kato pro-p groups, together with an essential arithmetic argument (cf. [3, Theorem 4.3]).

The above results provide a motivation for the paper, as Theorem A is the "group-theoretic translation", and it is in fact more genaral, as it holds for Bloch-Kato pro-p groups, and not only for Galois groups of maximal p-extensions. Moreover, part of the interest of this result lies in the fact that the proof is purely group-theoretical, and it does not rely on results form field theory. Further, the proof makes use of the Zassenhaus filtration of pro-p groups, which is gaining increasing importance as tool for the study of Galois groups (see, e.g., [5] and [11]).

The paper is organized as follows. In the second section, we state a number of properties on pro-p groups and on their descending series. In section 3 we prove Theorem A, and in section 4 we provide the "arithmetic translation" of Theorem A, and we prove Corollary B.

This paper will be published on the *Annales mathématiques du Québec.*

2. Preliminaries on pro-p groups

Throughout this paper, subgroups of pro-p groups are assumed to be closed (in the pro-p topology), and every generator is to be intended as topological generator. In particular, given two (closed) subgroups H_1 and H_2 of a pro-p group G, the subgroup $[H_1, H_2]$ is the (closed) subgroup of G generated by the commutators $[g_1, g_2]$, with $g_i \in H_i$ for $i = 1, 2$. Also, for a positive integer n, G^n denotes the (closed) subgroup of G generated by the n-powers of the elements of G.

For a finitely generated pro-p group G, let $\mathrm{d}(G)$ denote the minimal number of generators of G. In particular, $\mathrm{d}(G)$ is the dimension of the quotient $G/\Phi(G)$ as vector space over the finite field $\mathbb{F}_p$ (cf. [4, Prop. 1.14]). Then, one defines the rank of a pro-p group G to be the number

$$\mathrm{rk}(G) = \sup\{\mathrm{d}(H) \mid H \leq G \text{ closed}\} \in \mathbb{N} \cup \{\infty\}$$

(cf. [4, Definition 3.12]).

For a pro-p group G, the lower p-central series of G is the series $P_n = P_n(G)$, $n \geq 1$, of characteristic subgroups defined by $P_1 = G$ and

$$P_{n+1} = P_n^p[G, P_n].$$

In particular, one has that $P_2(G)$ is the Frattini subgroup $\Phi(G)$, and $[P_i, P_j] \leq P_{i+j}$ for every $i, j \geq 1$. Moreover, if G is finitely generated, then the lower p-central series is a base of neighbourhoods of 1 in G (cf. [4, Prop. 1.16]).

Definition. A pro-p group G is said to be *powerful* if G/G^p is abelian, if p is odd, or if G/G^4 is abelian, if $p = 2$.

In particular, one has the following (cf. [4, Theorems 3.6, 3.8]).

Proposition 2.1. *Let G be a powerful pro-p group.*

(1) $P_n(G) = G^{p^{n-1}}$ *for every* $n \geq 1$.
(2) *if G is finitely generated, then* $\mathrm{rk}(G) = \mathrm{d}(G)$.

Another important descending series of pro-p groups is the *Zassenhaus filtration*. For an arbitrary group G, the Zassenhaus filtration of G is the series $D_n = D_n(G)$, $n \geq 1$, of characteristic subgroups defined by $D_1 = G$ and

$$D_n = D_{\lceil n/p \rceil}^p \prod_{i+j=n} [D_i, D_j], \tag{2.1}$$

where $\lceil n/p \rceil$ is the least integer m such that $mp \geq n$. In particular, the Zassenhaus filtration is the fastest descending series starting at G such that $[D_i, D_j] \leq D_{i+j}$ and $D_i^p \leq D_{ip}$ for every $i, j \geq 1$. For computational purposes, one has the formula

$$D_n = \prod_{ip^h \geq n} \gamma_i(G)^{p^h}, \tag{2.2}$$

established by M. Lazard (cf. [4, Theorem 11.2]), where the $\gamma_i(G)$'s are the elements of the descending central series of G (i.e., $\gamma_1(G) = G$ and

$\gamma_{i+1}(G) = [G, \gamma_i(G)]$ for every $i \geq 1$). Thus, if G is a (pro-)p group, then $D_2(G)$ is the Frattini subgroup $\Phi(G)$.

For the Zassenhaus filtration of a pro-p group, one has the following remarkable result (cf. [4, Theorem 11.4]).

Theorem 2.2. *Let G be a finitely generated pro-p group. Then G has finite rank if, and only if, $D_n(G) = D_{n+1}(G)$ for some $n \geq 1$.*

Definition. A topological group G is a *p-adic analytic group* if G has the structure of analytic manifold over the field of p-adic numbers $\mathbb{Q}_p$ with the properties

(1) the multiplication function $G \times G \to G$ given by $(x, y) \mapsto xy$ is analytic;
(2) the inversion function $G \to G$ defined by $x \mapsto x^{-1}$ is analytic.

Powerful pro-p groups and p-adic analytic groups are tightly related. Indeed, a topological group G has the structure of a p-adic analytic group if, and only if, G has an open subgroup which is a powerful finitely generated pro-p group (cf. [4, Theorem 8.1]). In the case of Bloch-Kato pro-p groups, p-adic analytic groups have a rather simple structure, as stated by the following (cf. [13, Theorem 4.8]).

Theorem 2.3. *Let G be a finitely generated Bloch-Kato pro-p group, and assume furhter that G is torsion-free, if $p = 2$. The following are equivalent.*

(1) *G has finite rank.*
(2) *G is p-adic analytic.*
(3) *G is powerful.*
(4) *G has a presentation*

$$G = \left\langle \sigma, \tau_1, \ldots, \tau_d \;\middle|\; \sigma\tau_i\sigma^{-1} = \tau_i^{1+p^k}, \tau_i\tau_j = \tau_j\tau_i \;\forall\, i, j \right\rangle, \tag{2.3}$$

with $d = \mathrm{d}(G) - 1$, for some $k \geq 1$ ($k \geq 2$, if $p = 2$).

3. Proof of Theorem A

Lemma 3.1. *If G is a powerful Bloch-Kato group, then $\Phi_2(G) = P_3(G)$.*

Proof. Recall first that if G is a Bloch-Kato pro-p group, then every closed subgroup of G is again a Bloch-Kato pro-p group. By Proposition 2.1, one has $\Phi(G) = G^p$ and $P_3(G) = G^{p^2}$. Since $\mathrm{rk}(G)$ is finite, also $\mathrm{rk}(\Phi(G))$ is finite, thus $\Phi(G)$ is powerful by Theorem 2.3. Therefore,

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

and this yields the claim. □

Proof of Theorem A. Assume that G is a finitely generated p-adic analytic Bloch-Kato group. Then, the claim holds by Theorem 2.3 and Lemma 3.1.

Conversely, assume that $\Phi_2(G) = P_3(G)$. Since $[D_2, D_2] \leq D_4$ and $D_2^p \leq D_{2p}$, one has $\Phi_2(G) = D_2^p[D_2, D_2] \leq D_4$, as $\Phi(G) = D_2$. Moreover, one has the inclusion $\gamma_3(G) \leq P_3(G)$. Therefore, one has the chain of inclusions

$$\gamma_3(G) \leq P_3(G) = \Phi_2(G) \leq D_4. \tag{3.1}$$

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

(1) Assume $p > 3$. By (2.2), one has

$$D_3 = \prod_{ip^h \geq 3} \gamma_i(G)^{p^h} = \gamma_3(G) \cdot G^p$$
$$\text{and} \quad D_4 = \prod_{ip^h \geq 4} \gamma_i(G)^{p^h} = \gamma_4(G) \cdot G^p.$$

Therefore, (3.1) implies

$$D_3(G) = \gamma_3(G) \cdot G^p \leq P_3(G) = \Phi_2(G) \cdot G^p \leq D_4,$$

as $G^p \leq D_4$. Thus, one has the equality $D_3 = D_4$. Hence, Theorem 2.2 implies that $\mathrm{rk}(G)$ is finite, and thus by Theorem 2.3 G is a p-adic analytic Bloch-Kato pro-p group.

(2) Assume $p = 2$. From (2.2) one obtains

$$D_3 = \prod_{i2^h \geq 3} \gamma_i(G)^{2^h} = \gamma_3(G) \cdot \gamma_2(G)^2 \cdot G^4$$
$$\text{and} \quad D_4 = \prod_{i2^h \geq 4} \gamma_i(G)^{2^h} = \gamma_4(G) \cdot \gamma_2(G)^2 \cdot G^4.$$

Therefore, (3.1) implies

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

as $\gamma_2(G)^2 G^4 \leq D_4$. Thus, one has the equality $D_3 = D_4$. Hence, Theorem 2.2 implies that $\mathrm{rk}(G)$ is finite, and thus by Theorem 2.3 G is a p-adic analytic Bloch-Kato pro-p group.

(3) Assume $p = 3$. By (2.2), one has

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

Therefore, from (3.1) one obtains the chain of inclusions

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

which implies

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

as $G^9, \gamma_2(G)^3 \leq D_5$. Thus, one has the equality $D_4 = D_5$. Hence, Theorem 2.2 implies that $\mathrm{rk}(G)$ is finite, and thus by Theorem 2.3 G is a p-adic analytic Bloch-Kato pro-p group.

This establishes the theorem. $\square$

Note that if G is a finitely generated pro-p group, then $\Phi_2(G)$ is an open subgroup of G. Thus, the quotient $G/\Phi_2(G)$ is finite, and one may reduce the equality $\Phi_2(G) = P_3(G)$ to a condition on finite p-groups, as done in [3, Corollary 4.15].

Corollary 3.2. *A finitely generated Bloch-Kato pro-p group G is p-adic analytic if, and only if, $\Phi(G)/\Phi_2(G)$ is contained in the centre of $G/\Phi_2(G)$.*

Proof. Assume that G is p-adic analytic. Then Theorem A yields the equality $\Phi_2(G) = P_3(G)$. Since $[G, P_2] = [P_1, P_2] \leq P_3$, one has $[G, \Phi(G)] \leq \Phi_2(G)$, and $\Phi(G)/\Phi_2(G)$ is central in $G/\Phi_2(G)$.

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

$$\Phi(G)^p \leq \Phi_2(G) \quad \text{and} \quad P_3 = \Phi(G)^p[G, \Phi(G)],$$

it follows that $\Phi_2(G)$ contains $P_3(G)$, and thus the two subgroups are equal. Therefore G is p-adic analytic by Theorem A. $\square$

4. Proof of Corollary B

Throughout this section, a field F is always assumed to contain a primitive p-th root of unity (and also $\sqrt{-1}$, if $p = 2$). Also, $F^\times$ denotes the multiplicative group of non-zero elements of F, and $(F^\times)^p$ is the subgroup of p-powers of $F^\times$.

Definition. Let N denote the norm map $N\colon F(\sqrt[p]{a}) \to F$ of the p-cyclic extension $F(\sqrt[p]{a})/F$. An p-power-free unit $a \in F^\times$ is said to be *p-rigid* if

$$b \in N\left(F(\sqrt[p]{a})\right) \quad \text{if, and only if,} \quad b \in \bigcup_{k=0}^{p-1} a^k (F^\times)^p$$

for every $b \in F^\times \smallsetminus (F^\times)^p$. The field F is called *p-rigid* if every element of $F^\times \smallsetminus (F^\times)^p$ is p-rigid.

Recall from the Introduction that $F^{(2)} = F(\sqrt[p]{F})$ is the compositum over F of all extensions $F(\sqrt[p]{a})$ with $a \in F^\times$. Also,

- $F^{\{3\}} = F^{(2)}(\sqrt[p]{F^{(2)}})$ is the compositum over $F^{(2)}$ of all the extensions $F^{(2)}(\sqrt[p]{a})$ with $a \in (F^{(2)})^\times$;
- $F^{(3)}$ is the compositum over $F^{(2)}$ of all the extensions $F^{(2)}(\sqrt[p]{a})$ such that $F^{(2)}(\sqrt[p]{a})/F$ is Galois.

Therefore, both $F^{\{3\}}/F$ and $F^{(3)}/F$ are Galois extensions, and $F^{(3)} \subseteq F^{\{3\}}$ (cf. [3, § 2.3]).

Let G be the *maximal pro-p Galois group* of F, i.e.,

$$G = G_F(p) = \mathrm{Gal}(F(p)/F),$$

where $F(p)$ is the maximal p-extension of F. Recall that the maximal pro-p Galois group of a field containing a primitive p-th root of unity is a Bloch-Kato pro-p group (cf. [13, § 2]).

By Kummer theory, one has that the Galois group of $F^{(2)}/F$ is the quotient $G/\Phi(G)$. Note that G is finitely generated if, and only if, the quotient $F^\times/(F^\times)^p$ is finite (and in this case $\mathrm{d}(G) = \dim(F^\times/(F^\times)^p)$), as $G/\Phi(G)$ and $F^\times/(F^\times)^p$ are isomorphic as discrete groups of exponent p. Moreover,

$$\mathrm{Gal}(F^{(3)}/F) = G/P_3(G) \quad \text{and} \quad \mathrm{Gal}(F^{\{3\}}/F) = G/\Phi_2(G) \tag{4.1}$$

(cf. [3, § 4.1], see also [1, § 2]).

Remark 4.1. In the case $p = 2$, the Galois groups $\mathrm{Gal}(F^{(3)}/F)$ and $\mathrm{Gal}(F^{\{3\}}/F)$ are called W-group, resp. V-group, of the field F, for the relations with the Witt ring of F (cf. [10] and [1]).

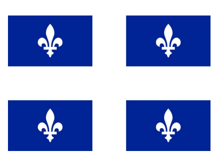
Proof of Corollary B. Let G be the maximal pro-p Galois group $G_F(p)$. By hypothesis, G is finitely generated. Moreover, G is torsion free, since we are assuming that $\sqrt{-1} \in F$ for $p = 2$.

Assume first that the equality $F^{(3)} = F^{\{3\}}$ holds. Then, by (4.1) one has also the equality $\Phi_2(G) = P_3(G)$, and thus Theorem A implies that G is a p-adic analytic Bloch-Kato pro-p group, and Theorem 2.3 implies that G is powerful. Therefore, by [3, Proposition 3.8] the field F is p-rigid.

Conversely, assume that F is p-rigid. Then, again by [3, Proposition 3.8] the Galoi group G is powerful, and thus p-adic analytic by Theorem 2.3. Therefore, Theorem A implies the equality $\Phi_2(G) = P_3(G)$, and the equality $F^{(3)} = F^{\{3\}}$ follows by (4.1). □

Acknowledgements

I want to espress my thanks to the referee for the *Annales mathématiques du Québec* for her/his valuable comments and remarks. Also, many thanks to A. Chapman and D. Neftin for their interest and support, to D. Riley for the thoughtful discussions about the Zassenhaus filtration and restricted Lie algebras, and to S.K. Chebolu and J. Mináč for working with me on p-rigid fields.



References

[1] A. Adem, W. Gao, D. Karagueuzian and J. Mináč. Field theory and the cohomology of some Galois groups. *J. Algebra* 235 (2001) 608–635.

[2] D. Benson, S.K. Chebolu, J. Mináč and J. Swallow. Bloch-Kato pro-p groups and a refinement of the Bloch-Kato conjecture. Preprint (2007).

[3] S.K. Chebolu, J. Mináč and C. Quadrelli. Detecting fast solvability of equations via small powerful Galois groups. *Trans. Amer. Math. Soc.*, to appear, available at `arXiv:1310.7623`.

[4] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal. *Analytic Pro-p Groups, Second edition.* Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, Cambridge, 1999.

[5] I. Efrat. The Zassenhaus filtration, Massey products and representations of profinite groups. *Adv. Math.* 263 (2014), 389–411.

[6] A.J. Engler, J. Koenigsmann. Abelian subgroups of pro-p Galois groups. *Trans. Amer. Math. Soc.* 350 (1998), no. 6, 2473–2485.

[7] H. Koch. *Galois theory of p-extensions. With a foreward by I.R. Šafarevič.* Springer Monographs in Mathematics, Springer, Berlin 2002.

[8] D.B. Leep and T.L. Smith. Multiquadratic extensions, rigid fields and pythagorean fields. *Bull. London Math. Soc.* 34 (2002), 140–148.

[9] J. Mináč and T.L. Smith. W-groups under quadratic extensions of fields. *Canad. J. Math.* 52 (2000), 833–848.

[10] J. Mináč and M. Spira. Witt rings and Galois groups. *Ann. Math.* 144 (1996), 35–60.

[11] J. Mináč and N.D. Tân. Triple Massey products and Galois theory. *J. Eur. Math. Soc.*, to appear, available at `arXiv:1307.6624`.

[12] J. Mináč and N.D. Tân. The Kernel Unipotent Conjecture and the vanishing of Massey products for odd rigid fields (with an appendix by I. Efrat). *Adv. Math.*, to appear, available at `arXiv:1312.2655`.

[13] C. Quadrelli. Bloch-Kato pro-p groups and locally powerful groups. *Forum Math.* 26 (2014), no. 3, 793–814.

[14] R. Ware, Galois groups of maximal p-extensions. *Trans. Amer. Math. Soc.* 33 (1992), no. 2, 721–728.

Department of Mathematics, Arts and Crafts, University of Milano-Bicocca, Ed. U5, Via R.Cozzi 53, 20125 Milano, Italy

E-mail address: `c.quadrelli1@campus.unimib.it`