TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 367, Number 12, December 2015, Pages 8439–8464
http://dx.doi.org/10.1090/tran/6304
Article electronically published on April 1, 2015

# DETECTING FAST SOLVABILITY OF EQUATIONS VIA SMALL POWERFUL GALOIS GROUPS

S. K. CHEBOLU, J. MINÁČ, AND C. QUADRELLI

*Dedicated to Professors Tsit-Yuen Lam and Helmut Koch with admiration and respect*

Abstract. Fix an odd prime $p$, and let $F$ be a field containing a primitive $p$th root of unity. It is known that a $p$-rigid field $F$ is characterized by the property that the Galois group $G_F(p)$ of the maximal $p$-extension $F(p)/F$ is a solvable group. We give a new characterization of $p$-rigidity which says that a field $F$ is $p$-rigid precisely when two fundamental canonical quotients of the absolute Galois groups coincide. This condition is further related to analytic $p$-adic groups and to some Galois modules. When $F$ is $p$-rigid, we also show that it is possible to solve for the roots of any irreducible polynomials in $F[X]$ whose splitting field over $F$ has a $p$-power degree via non-nested radicals. We provide new direct proofs for hereditary $p$-rigidity, together with some characterizations for $G_F(p)$ – including a complete description for such a group and for the action of it on $F(p)$ – in the case $F$ is $p$-rigid.

## 1. Introduction

The problem of solving algebraic equations by radicals has a long and rich history which dates back to the 7th century when the Indian mathematician Brahmagupta obtained the famous quadratic formula. After the Italian mathematicians Niccolò Tartaglia and Girolamo Cardano obtained the solution of the cubic equation in the 16th century, mathematicians naturally wondered whether it is possible to solve equations of any degree by radicals. Évariste Galois, in his theory of equations, gave an elegant answer in the 19th century. It is possible to solve an equation by radicals, provided the Galois group of the underlying equation is a solvable group. An important consequence is the result on the insolvability of general algebraic equations of degree 5 and above by radicals. Since every finite $p$-group is a solvable group, we know that every irreducible polynomial in $F[X]$ whose splitting field over $F$ has $p$-power degree, is solvable by radicals. In this paper, we will show that if the underlying field $F$ is $p$-rigid (see definition below), then it is possible to do even better: we can "fast-solve" for the roots. That is, we can solve for the roots of these irreducible polynomials via non-nested radicals, i.e., elements of the type $\sqrt[n]{a}$ with $a \in F \smallsetminus \{0\}$. (An element of the form $\sqrt[n]{a + \sqrt[m]{b}}$, with $a, b \in F \smallsetminus \{0\}$ and $n, m > 1$ is, for instance, nested.) This improves the following result: the Galois

Received by the editors June 13, 2012 and, in revised form, September 17, 2013.
2010 *Mathematics Subject Classification.* Primary 12F10, 12G10, 20E18.
*Key words and phrases.* Rigid fields, Galois modules, absolute Galois groups, Bloch-Kato groups, powerful pro-$p$ groups.
The first author was partially supported by NSA grant H98230-13-1-0238.
The second author was partially supported by NSERC grant RO37OA1OO6.
The third author was partially supported by an INDAM-GNSAGA travel grant.

group of the maximal $p$-extension $F(p)/F$ is a solvable group if and only if the field $F$ is $p$-rigid (proved first in [EK98]).

We make the blanket assumption that $p$ is an odd prime, and all fields in this paper contain a primitive $p$th root of unity – unless explicitly stated otherwise. Let $F$ be such a field and let $F^p$ denote the collection of elements in $F$ that are $p$th powers. An element $a$ in $F \smallsetminus F^p$ is said to be $p$-rigid if the image of the norm map $F(\sqrt[p]{a}) \to F$ is contained in $\bigcup_{k=0}^{p-1} a^k F^p$. We say that $F$ is *$p$-rigid* if all of the elements of $F \smallsetminus F^p$ are $p$-rigid. The notion of $p$-rigidity was introduced by K. Szymiczek in [Sz77, Ch. III, §2], and it was developed and thoroughly studied first in the case of $p = 2$, and then in the case of $p$ odd.

For $p = 2$, the definition of 2-rigidity depends on the behavior of certain quadratic forms. The consequences of 2-rigidity were studied in several papers including [Wr78, Wr81, Ja81, JW89, AGKM01, LS02]. Today many results about 2-rigid fields are known, and these fields are relatively well understood.

For $p$ odd, the study of $p$-rigid fields was developed by Ware in [Wr92], and later on by others (see [Ef06] and [MST] for some highlights on the history of $p$-rigidity). In [Wr92], Ware introduced a different notion of rigidity called *hereditary $p$-rigidity*. A field $F$ is said to be hereditarily $p$-rigid if every subextension of the maximal $p$-extension $F(p)/F$ is $p$-rigid. As Ware pointed out, to conclude that $F$ is hereditary $p$-rigid, it is enough to check that each finite extension $K$ of $F$ is $p$-rigid. Ware also gave a Galois-theoretic description of hereditarily $p$-rigid fields. In [EK98], A. Engler and J. Koenigsmann showed that $p$-rigidity implies hereditary $p$-rigidity.

In this paper we establish some new characterizations and deeper connections for $p$-rigid fields. Associated to a field $F$, we now introduce some important field extensions. Let $F^{(2)} = F(\sqrt[p]{F})$. Let $F^{\{3\}}$ denote the compositum of all Galois extensions $K/F^{(2)}$ of degree $p$. Similarly, let $F^{(3)}$ denote the compositum of all Galois extensions $K/F^{(2)}$ of degree $p$ for which $K/F$ is also Galois. Finally, let $F(p)$ denote the compositum of all Galois extensions $K/F$ that are of degree a power of $p$. Our main theorem then states

**Theorem A.** *Let $p$ be an odd prime, and let $F$ be a field containing a primitive $p$th root of unity. $F$ is $p$-rigid if and only if $F^{(3)} = F^{\{3\}}$.*

It is worth pointing out that the fields $F^{(3)}$ and $F^{\{3\}}$ play an important role in studying the arithmetic and Galois cohomology of fields. For instance, in [MSp96] it is shown that $\mathrm{Gal}(F^{(3)}/F)$ in the case when $p = 2$ determines essentially the Witt ring of quadratic forms. More recently, in [CEM12] it is shown that $\mathrm{Gal}(F^{(3)}/F)$ determines the Galois cohomology of $G_F(p) := \mathrm{Gal}(F(p)/F)$ with $\mathbb{F}_p$ coefficients! In [EM13], an even smaller Galois group over $F$, namely $\mathrm{Gal}(F^{\{3\}}/F)$, was shown to have this property. Therefore, Theorem A answers the natural question: "For which fields $F$, does one have $F^{\{3\}} = F^{(3)}$?", a question which has its own importance beyond the connection to $p$-rigid fields.

Furthermore, we provide a Galois-theoretic characterization for $p$-rigid fields, together with an explicit description of the maximal $p$-extension $F(p)$ of a $p$-rigid field $F$, and of its maximal pro-$p$ Galois group $G_F(p)$. In particular, we prove the equivalence of the following three statements: $G_F(p)$ is solvable; $F$ is $p$-rigid; and $F$ is hereditarily $p$-rigid (see Theorem 3.16 and Corollary 3.22). Although this result is proved in [EK98, Prop. 2.2], this earlier proof is less direct than our approach. In particular, it relies on a number of results on Henselian valuations, covered in

several papers, and on some results of [Wr92]. On the other hand, we refer to [Wr92] only for some definitions, and we develop and prove our results independently of both [Wr92] and [EK98]. In fact our approach is substantially different from the approach of Engler and Koenigsmann, as our proofs use only elementary methods from Galois theory and the theory of cyclic algebras – in the spirit of Ware's paper.

Using a relatively simple argument but the powerful Serre's theorem on cohomological dimensions of open subgroups of pro-$p$ groups and a corollary of Rost-Voevodsky's proof of the Bloch-Kato conjecture we are able to prove the "going down $p$-rigidity theorem" in the case when $G_F(p)$ is finitely generated; see Theorem 4.16. Then, using this result and the well-known Lazard's group theoretic characterization of $p$-adic analytic pro-$p$ groups, we are able to show that if $G_F(p)$ is finitely generated then $F$ is $p$-rigid if and only if $G_F(p)$ is a $p$-adic analytic pro-$p$ group.

We also investigate how $p$-rigid fields are related to certain powerful pro-$p$ groups, studied by the third author in [Qu13], and with certain Galois modules, studied by J. Swallow and the second author in [MS03].

Maximal pro-$p$ Galois groups play a fundamental role in the study of absolute Galois groups of fields. Moreover, the cases where $F$ is a $p$-rigid field and where $G_F(p)$ is a free pro-$p$ group, or a Demuškin group, are cornerstones in the study of maximal pro-$p$ Galois groups. Therefore, it is important to have a clear, complete and explicit description of the former case. In fact we will be able to recover the entire group $G_F(p)$ from rather small Galois groups and the structure of the $p$th roots of unity contained in $F$.

This paper is organized as follows. In Section 2 we review some preliminary definitions and basic facts about pro-$p$ groups and their cohomology. In Section 3 we state and prove results on the cohomology and the group structure of the Galois group $G_F(p)$, which will be used in proving that $p$-rigidity implies hereditary $p$-rigidity, and in characterizing $G_F(p)$ for $p$-rigid fields. Finally in Section 4 we prove Theorem A and we study the connections with the fast-solvability of equations and other group-theoretic consequences of $p$-rigidity.

## 2. Preliminaries

2.1. **Pro-$p$ groups.** Henceforth we will work in the category of pro-$p$ groups and assume that all our subgroups of pro-$p$ groups will be closed. Let $G$ be a pro-$p$-group. For $\sigma, \tau$ in $G$, ${}^{\sigma}\tau := \sigma\tau\sigma^{-1}$, and $[\sigma, \tau] := {}^{\sigma}\tau \cdot \tau^{-1}$ is the commutator of $\sigma$ and $\tau$. The closed subgroup of $G$ generated by all of the commutators, will be denoted by $[G, G]$.

For a profinite group $G$, the Frattini subgroup $\Phi(G)$ of $G$ is defined to be the intersection of all maximal normal subgroups of $G$. If $G$ is a pro-$p$ group, it can be shown that

$$\Phi(G) := G^p[G, G]$$

[DdSMS03, Prop. 1.13], where $G^p$ is the subgroup generated by the $p$-powers of the elements of $G$. Hence $G/\Phi(G)$ is a $p$-elementary abelian group of possibly infinite rank.

We define the subgroups $\gamma_i(G)$ and $\lambda_i(G)$ of $G$ to be the elements of the lower descending central series, resp. of the lower $p$-descending central series, of the pro-$p$ group $G$. That is, $\gamma_1(G) = \lambda_1(G) = G$, and

$$\gamma_{i+1}(G) := [\gamma_i(G), G], \quad \lambda_{i+1}(G) := \lambda_i(G)^p[\lambda_i(G), G],$$

for $i \geq 1$. In this terminology, note that the Frattini subgroup $\Phi(G)$ is exactly $\lambda_2(G)$. If $G$ is finitely generated, the subgroups $\lambda_i(G)$ make up a system of open neighborhoods of 1 in $G$.

Finally, we denote by $d(G)$ the minimal number of generators of $G$. It follows that $d(G) = \dim(G/\Phi(G))$ as an $\mathbb{F}_p$-vector space. If $d = d(G)$, we say that $G$ is $d$-generated. If $G$ is finitely generated, then the rank $\mathrm{rk}(G)$ of the group $G$ is

$$\mathrm{rk}(G) = \sup_{C \leq G} \{d(C)\} = \sup_{C \leq G} \{d(C) | C \text{ is open}\}$$

(see [DdSMS03, §3.2]).

2.2. **Maximal pro-$p$ Galois groups and their cohomology.** Consider $\mathbb{F}_p$ as trivial $G$-module. The cohomology groups $H^k(G, \mathbb{F}_p)$ of $G$ with coefficients in $\mathbb{F}_p$ are defined for all $k \geq 0$. In particular,

$$H^0(G, \mathbb{F}_p) = \mathbb{F}_p \quad \text{and} \quad H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p). \tag{2.1}$$

By Pontryagin duality it follows that

$$H^1(G, \mathbb{F}_p) = G^\vee = (G/\Phi(G))^\vee \quad \text{and} \quad d(G) = \dim_{\mathbb{F}_p} \left(H^1(G, \mathbb{F}_p)\right), \tag{2.2}$$

where the symbol $\_^\vee$ denotes the Pontryagin dual (see [NSW, Ch. III §9]). The *cohomological dimension* $\mathrm{cd}(G)$ of a (pro-)$p$ group $G$ is the least positive integer $k$ such that $H^{k+1}(G, \mathbb{F}_p) = 0$, and if such $k$ does not exist, one sets $\mathrm{cd}(G) = \infty$.

The direct sum $H^\bullet(G, \mathbb{F}_p) = \bigoplus_{k \geq 0} H^k(G, \mathbb{F}_p)$, is equipped with the *cup product*

$$H^r(G, \mathbb{F}_p) \times H^s(G, \mathbb{F}_p) \xrightarrow{\cup} H^{r+s}(G, \mathbb{F}_p),$$

which gives it a structure of a graded commutative $\mathbb{F}_p$-algebra. For further facts on the cohomology of profinite groups we refer the reader to [NSW].

We say that a pro-$p$ group $G$ is a *Bloch-Kato* pro-$p$ group if for every closed subgroup $C$ of $G$ the $\mathbb{F}_p$-cohomology algebra $H^\bullet(C, \mathbb{F}_p)$ is *quadratic*, i.e., it is generated by $H^1(C, \mathbb{F}_p)$ and the relations are generated as ideal by elements in $H^2(C, \mathbb{F}_p)$ (see [Qu13]).

Given a field $F$, let $\bar{F}^s$ denote the separable closure of $F$, and let $F(p)$ be the maximal $p$-extension of $F$, i.e., $F(p)$ is the compositum of all finite Galois extensions $K/F$ of $p$-power degree. Then $G_F := \mathrm{Gal}(\bar{F}^s/F)$ is the *absolute Galois group* of $F$, and the *maximal pro-$p$ Galois group* $G_F(p)$ of $F$ is the maximal pro-$p$ quotient of $G_F$ or, equivalently, $G_F(p)$ is the Galois group of the maximal $p$-extension $F(p)/F$. We then have the Galois correspondence, according to which the closed subgroups of $G_F(p)$ correspond to subextensions of $F(p)/F$ and conversely.

By the proof of the Bloch-Kato conjecture, obtained by M. Rost and V. Voevodsky (with C. Weibel's patch), one knows that the maximal pro-$p$ Galois group of a field containing the $p$th roots of unity is a Bloch-Kato pro-$p$ group [We08, We09, Vo11].

Another important feature of maximal pro-$p$ Galois groups is the following: if $p$ is odd, then $G_F(p)$ is torsion-free. This Artin-Schreier type result is due to E. Becker (see [Be74]).

The study of maximal pro-$p$ Galois groups is extremely important, since they are easier to handle than absolute Galois groups; yet they provide substantial information about absolute Galois groups and the structure of their base fields.

2.3. **Important subextensions.** Throughout this paper, fields are assumed to contain the $p$th roots of unity.

Given a field $F$, we denote as $\dot{F}$ the multiplicative group of $F$. Let $F^{(2)} = F(\sqrt[p]{\dot{F}})$, i.e., $F^{(2)}$ is the compositum of all the extensions

$$F\left(\sqrt[p]{a}\right), \quad \text{with } a \in \dot{F}.$$

For $n \geq 3$, we define recursively the extensions $F^{\{n\}}/F$ and $F^{(n)}/F$ in the following way:

- the field $F^{\{n\}}$ denotes the compositum of all the extensions
$$F^{\{n-1\}}\left(\sqrt[p]{\gamma}\right), \quad \text{with } \gamma \in \dot{F^{\{n-1\}}} \smallsetminus \left(\dot{F^{\{n-1\}}}\right)^p,$$
where we put $F^{(2)}$ instead of $F^{\{2\}}$,
- the field $F^{(n)}$ denotes the compositum of all the extensions
$$F^{(n-1)}\left(\sqrt[p]{\gamma}\right), \quad \text{with } \gamma \in \dot{F^{(n-1)}} \smallsetminus \left(\dot{F^{(n-1)}}\right)^p,$$
such that $F^{(n-1)}(\sqrt[p]{\gamma})/F$ is Galois.

Notice that all extensions $F^{\{n\}}/F$ and $F^{(n)}/F$ are Galois.

**Proposition 2.1.** *For any field $F$ one has*

$$F(p) = \bigcup_{n>1} F^{(n)}.$$

*Proof.* The inclusion $F(p) \supseteq \bigcup_n F^{(n)}$ is obvious.

For the converse, let $K/F$ be a finite Galois $p$-extension of degree $|K : F| = p^m$, for some $m \in \mathbb{N}$. Then, by the properties of finite $p$-groups, one has a chain

$$F = K_0 \subset K_1 \subset \ldots \subset K_m = K$$

of fields such that $K_i/F$ is Galois and $|K_i : F| = p^i$ for every $i = 1, \ldots, m$. In particular, for every $i$ the extension $K_{i+1}/K_i$ is cyclic of degree $p$, and $\mathrm{Gal}(K_{i+1}/K_i)$ is central in $\mathrm{Gal}(K_{i+1}/F)$.

We claim that $K_i \subseteq F^{(i+1)}$ for every $i$. This is clear for $i = 0$ and $i = 1$. Assume $K_{i-1} \subseteq F^{(i)}$ by induction. Then $K_i/K_{i-1}$ is Galois and cyclic of degree $p$, thus $K_i = K_{i-1}(\sqrt[p]{\alpha})$ with $\alpha \in F^{(i)}$. Consequently $K_i \subseteq F^{(i+1)}$, and the statement of the lemma follows. □

Let $\dot{F} := F \smallsetminus \{0\}$. Then, for every Galois $p$-extension $K/F$, $\dot{K}$ is a $G_F(p)$-module. Moreover, since $\sigma.\gamma^p = (\sigma.\gamma)^p$ for any $\gamma \in \dot{F}(p)$ and $\sigma \in G_F(p)$, one has that $\dot{K}/\dot{K}^p$ is also a $G_F(p)$-module, with $K$ as above. We denote the module $\dot{F}^{(2)}/(\dot{F}^{(2)})^p$ by $J$. The module $J$ has been studied in [AGKM01] for $p = 2$, and in [MST] for $p$ odd, where it has been shown that $J$ provides substantial information about the field $F$.

We can generalize the construction of $J$ in the following way. For every $n \geq 3$ let

$$J_n = \frac{\dot{F^{(n)}}}{\left(\dot{F^{(n)}}\right)^p}.$$

We set $J = J_2$. Then each module $J_n$ is a $\mathbb{F}_p$-vector space and a $G_F(p)$-module. (Note that the notation used here is different from the one in [AGKM01] and [MST].)

The following lemma is a well-known fact from elementary Galois theory.

**Lemma 2.2.** *Let $K/F$ be a Galois $p$-extension of fields, and let $a \in \dot{K} \smallsetminus \dot{K}^p$. Then $K(\sqrt[p]{a})/F$ is Galois if and only if*

$$\frac{\sigma.a}{a} \in \dot{K}^p$$

*for every $\sigma \in \mathrm{Gal}(K/F)$.*

It follows that

$$F^{(n+1)} = F^{(n)}\left(\sqrt[p]{(J_n)^G}\right) \tag{2.3}$$

for every $n \geq 2$, where $J_n^G$ denotes the submodule of $J_n$ fixed by $G = G_F(p)$.

## 3. Rigid fields

Given a field $F$, the quotient group $\dot{F}/\dot{F}^p$ is a $p$-elementary abelian group, so that we may consider it as $\mathbb{F}_p$-vector space. Henceforth we will always assume that $\dot{F}/\dot{F}^p$ is not trivial. For an element $a \in \dot{F}$, $[a]_F = a\dot{F}^p$ denotes the coset of $\dot{F}/\dot{F}^p$ to which $a$ belongs. In particular, $k.[a]_F = [a^k]_F$ for $k \in \mathbb{F}_p$, and for $a, b \in \dot{F}$, $[a]_F$ and $[b]_F$ are $\mathbb{F}_p$-linearly independent if and only if $F(\sqrt[p]{a}) \neq F(\sqrt[p]{b})$. Moreover, let $\mu_p \subseteq F$ be the group of the roots of unity of order $p$. Then one may fix an isomorphism $\mu_p \cong \mathbb{F}_p$, so that by Kummer theory one has the isomorphism

$$\phi\colon \dot{F}/\dot{F}^p \xrightarrow{\sim} H^1\left(G_F(p), \mathbb{F}_p\right), \quad \phi\left([a]_F\right)(\sigma) = \frac{\sigma.\sqrt[p]{a}}{\sqrt[p]{a}}. \tag{3.1}$$

**Definition.** Let $N$ denote the norm map $N\colon F(\sqrt[p]{a}) \to F$. An element $a \in \dot{F} \smallsetminus \dot{F}^p$ is said to be $p$-**rigid** if $b \in N(F(\sqrt[p]{a}))$ implies that $b \in [a^k]_F$ for some $k \geq 0$. The field $F$ is called $p$-**rigid** if every element of $\dot{F} \smallsetminus \dot{F}^p$ is $p$-rigid.

In [Wr92], R. Ware calls a field $F$ *hereditarily* $p$-rigid if every $p$-extension of $F$ is a $p$-rigid field. In this paper we shall call such fields *hereditary* $p$-rigid.

**Example 3.1.**
i. Let $q$ be a power of a prime such that $p \mid (q-1)$. Let $F = \mathbb{F}_q((X))$, namely, $F$ is the field of Laurent series on the indeterminate $X$ with coefficients in the finite field $\mathbb{F}_q$. Then $F$ is $p$-rigid [Wr92, p. 727].
ii. Let $\zeta$ be a primitive $p$th root of unity and $\ell$ a prime different from $p$. Then $F = \mathbb{Q}_\ell(\zeta)$ is $p$-rigid. Indeed, by [NSW, Prop. 7.5.9] the maximal pro-$p$ Galois group $G_F(p)$ is 2-generated and it has cohomological dimension $cd(G_F(p)) = 2$. Hence $G_F(p)$ satisfies Corollary 3.21, and $F$ is $p$-rigid.

3.1. **Powerful pro-$p$ groups.** A pro-$p$ group $G$ is said to be *powerful* if

$$[G, G] \subseteq \begin{cases} G^p & \text{for } p \text{ odd}, \\ G^4 & \text{for } p = 2, \end{cases}$$

where $[G, G]$ is the closed subgroup of $G$ generated by the commutators of $G$, and $G^p$ is the closed subgroup of $G$ generated by the $p$-powers of the elements of $G$.

Moreover, a finitely generated pro-$p$ group $G$ is called *uniformly powerful*, or simply *uniform*, if $G$ is powerful, and

$$|\lambda_i(G) : \lambda_{i+1}(G)| = |G : \Phi(G)| \quad \text{for all } i \geq 1.$$

A finitely generated powerful group is uniform if and only if it is torsion-free (see [DdSMS03, Thm. 4.5]). Finally, a pro-$p$ group $G$ is called *locally powerful* if every finitely generated closed subgroup of $G$ is powerful.

In order to state the classification of torsion-free, finitely generated, locally powerful pro-$p$ groups – which we shall use to describe explicitly the maximal pro-$p$ groups of rigid fields in §3.2 – we shall introduce the notion of *oriented* pro-$p$ groups.

**Definition.** A pro-$p$ group $G$ together with a (continuous) homomorphism $\theta\colon G \to \mathbb{Z}_p^\times$ is called an **oriented** pro-$p$ group, and $\theta$ is called the orientation of $G$. If one has that $ghg^{-1} = h^{\theta(g)}$ for every $h \in \ker(\theta)$ and every $g \in G$, then $G$ is said to be **$\theta$-abelian**.

The above definition generalizes to all pro-$p$ groups the notion of cyclotomic character of an absolute (and maximal pro-$p$) Galois group. Such homomorphism has been studied previously for maximal pro-$p$ Galois groups in [Ef98] (where it is called a "cyclotomic pair"), and in [Ko01] for absolute Galois groups. (See also [JW89] for the case $p = 2$.)

**Proposition 3.2** ([Qu13, Proposition 3.4])**.** *Let $G$ be an oriented pro-$p$ group with orientation $\theta$. Then $G$ is $\theta$-abelian if and only if there exists a minimal set of generators $\{x_\circ, x_i | i \in \mathcal{I}\}$ for some set of indices $\mathcal{I}$, such that $G$ has a presentation*

$$G = \left\langle x_\circ, x_i \,\middle|\, [x_\circ, x_i] = x_i^{\theta(x_\circ)-1}, [x_i, x_j] = 1, i, j \in \mathcal{I} \right\rangle. \tag{3.2}$$

*That is, $G \cong \mathbb{Z}_p \ltimes Z$, with $Z \cong \mathbb{Z}_p^{\mathcal{I}}$, and the action of the first factor on $Z$ is the multiplication by $\theta(x_\circ)$.*

*Remark* 3.3. Notice that the statement of [Qu13, Prop. 3.4] refers only to finitely generated pro-$p$ groups, yet the proof does not use this fact, so that it holds also for infinitely generated pro-$p$ groups.

In fact, torsion-free, finitely generated, locally powerful pro-$p$ groups and $\theta$-abelian groups coincide.

**Theorem 3.4** ([Qu13, Thm. A])**.** *A finitely generated uniform pro-$p$ group $G$ is locally powerful if and only if there exists an orientation $\theta\colon G \to \mathbb{Z}_p^\times$ such that $G$ is $\theta$-abelian.*

Actually, it is possible to extend the above result to infinitely generated pro-$p$ groups.

**Proposition 3.5.** *A locally powerful torsion-free pro-$p$ group $G$ is $\theta$-abelian for some orientation $\theta\colon G \to \mathbb{Z}_p^\times$.*

*Proof.* By Theorem 3.4, we are left to the case when $G$ is infinitely generated. If $G$ is abelian, then $G$ is $\theta$-abelian with $\theta \equiv \mathbf{1}$. Hence, suppose $G$ is non-abelian.

Let $C < G$ be any finitely generated subgroup. Thus $C$ is $\theta_C$-abelian, for some homomorphism $\theta_C$. In particular, let $H_C = [C, C]$ be the commutator subgroup of $C$, and let $Z_C = \ker(\theta_C)$. Then $Z = \mathrm{C}_C(H)$, and $H_C = Z_C^{\lambda_C}$, for some $\lambda_C \in p\mathbb{Z}_p$.

Let $H = [G, G]$ be the commutator subgroup of $G$, and let $Z \leq G$ be the subgroup generated by all the elements $y \in G$ such that $y^\lambda \in H$ for some $\lambda \in p\mathbb{Z}_p$. Then one has

$$H = \overline{\bigcup_{C<G} H_C} \quad \text{and} \quad Z = \overline{\bigcup_{C<G} Z_C},$$

where $\overline{*}$ denotes the pro-$p$ closure inside $G$. Notice that all the $H_C$ and the $Z_C$ (and thus also $H$ and $Z$) are abelian. In particular, $G \supsetneq Z$, since $G$ is non-abelian, and $G/Z \cong \mathbb{Z}_p$.

For every element $x \in G \smallsetminus Z$, one has $[x, Z] = Z^{\lambda_x}$ for some $\lambda_x \in p\mathbb{Z}_p$, and take $x_0$ among all such $x$ such that $\lambda_{x_0}$ is minimal $p$-adic value. Define the homomorphism $\theta\colon G \to \mathbb{Z}_p^\times$ such that $\ker(\theta) = Z$ and $\theta(x_0) = 1 + \lambda_{x_0}$. Then $\theta|_C = \theta_C$ for every finitely generated large enough subgroup $C < G$, so that $G$ is in fact $\theta$-abelian. □

*Remark* 3.6.
i. Notice that, although the theory of powerful pro-$p$ groups works effectively only for finitely generated groups, it extends nicely to the infinitely generated case when we assume local powerfulness.
ii. It is possible to prove Proposition 3.5 using methods from Lie theory, since every uniformly powerful pro-$p$ group $G$ is associated to a $\mathbb{Z}_p$-Lie algebra $\log(G)$ (see [DdSMS03, §4.5] and [Qu13, §3.1]). In the case of a locally powerful group, such $\mathbb{Z}_p$-Lie algebra has a very simple shape, so that it is possible to "linearize" the proof.

3.2. **The maximal pro-$p$ Galois group of a rigid field.** Throughout this subsection we shall denote the maximal pro-$p$ Galois group $G_F(p)$ simply by $G$. Let $a, b \in \dot{F}$. The cyclic algebra $(a, b)_F$ is the $F$-algebra generated by elements $u, v$ subject to the relations $u^p = a$, $v^p = b$, and $uv = \zeta_p vu$, where $\zeta_p$ is a $p$th primitive root of unity.

From [Se79, Ch. XIV, §2, Proposition 5], one knows that $[(a, b)_F] = 1$ in the Brauer group $\mathrm{Br}(F)$ if and only if $\chi_a \cup \chi_b = 0$ in $H^2(G, \mathbb{F}_p)$, with $\chi_a = \phi([a]_F)$ and $\chi_b = \phi([b]_F)$ as in (3.1). (For the definition and the properties of the Brauer group of a field see [GS06, Ch. 2].) Moreover, it is well known that $[(a, b)_F] = 1$ if and only if $b$ is a norm of $F(\sqrt[p]{a})$. Therefore, $F$ is $p$-rigid if and only if the map

$$\Lambda_2(\cup)\colon H^1(G, \mathbb{F}_p) \wedge H^1(G, \mathbb{F}_p) \longrightarrow H^2(G, \mathbb{F}_p), \tag{3.3}$$

induced by the cup product, is injective.

The following theorem is due to P. Symonds and Th. Weigel.

**Theorem 3.7** ([SW00, Thm. 5.1.6])**.** *Let $G$ be a finitely generated pro-$p$ group. Then the map*

$$\Lambda_2(\cup)\colon H^1(G, \mathbb{F}_p) \wedge H^1(G, \mathbb{F}_p) \longrightarrow H^2(G, \mathbb{F}_p)$$

*is injective if and only if $G$ is powerful.*

By (2.2), (3.1), and [MS03] this implies the following.

**Proposition 3.8.** *Assume that $\dim_{\mathbb{F}_p}(\dot{F}/\dot{F}^p)$ is finite. Then $F$ is rigid if and only if $G$ is powerful. Moreover, $F$ is hereditary $p$-rigid if and only if $G$ is locally powerful.*

*Remark* 3.9. The hereditary $p$-rigidity of $F$ implies the locally powerfulness of $G$ for all fields by Proposition 3.8 and the definition of locally powerful groups.

Furthermore, it is possible to deduce that in the case $\dot{F}/\dot{F}^p$ is finite, $p$-rigidity implies hereditary $p$-rigidity. Indeed, for a field $F$ such that $\dim_{\mathbb{F}_p}(\dot{F}/\dot{F}^p) < \infty$, by [Qu13, Thm. B] one has that either $G_F(p)$ is locally powerful, or it contains a closed non-abelian free pro-$p$ group. For a $p$-rigid field, $G_F(p)$ is powerful, and therefore necessarily it is locally powerful, since powerful pro-$p$ groups contain no closed non-abelian free pro-$p$ groups, and thus $F$ is hereditary $p$-rigid.

*Remark* 3.10. Ware provided the same description for the maximal pro-$p$ Galois group $G_F(p)$ of a hereditary $p$-rigid field $F$, but with the further assumption that $F$ also contains a primitive $p^2$th root of unity [Wr92, Thm. 2]. The third author already got rid of such assumption in [Qu13, Cor. 4.9].

*Remark* 3.11. Observe that one can prove directly for all fields $F$ that if $G = G_F(p)$ is powerful then $F$ is $p$-rigid. Indeed if we assume using a contradiction argument that $G$ is powerful but $F$ is not $p$-rigid, then by [Wr78, Lemma 4], $G$ will have as a quotient the group $H_{p^3}$ (the unique non-abelian group of order $p^3$ and exponent $p$). But this means that $G/G^p$ is non-abelian and therefore $G$ is not powerful. On the other hand, from the explicit form of $G_F(p)$ for each rigid field, we shall see (Corollary 3.17 and Theorem 4.10) that $G/G^p$ is abelian and hence $G$ is powerful. Thus $F$ is $p$-rigid if and only if $G$ is powerful.

3.3. **Rigidity implies hereditary rigidity.** As above, let $G = G_F(p)$. Let $\mathrm{Br}_p(F)$ denote the subgroup of $\mathrm{Br}(F)$ consisting of elements of order $p$. From Merkuryev and Suslin's work, an element of $\mathrm{Br}_p(F)$ is a product of cyclic algebras, i.e., one has the following commutative diagram:

$$\begin{array}{ccc} \dot{F}/\dot{F}^p \wedge \dot{F}/\dot{F}^p & \twoheadrightarrow & \mathrm{Br}_p(F) \\ \downarrow{\scriptstyle \phi\wedge\phi} & & \downarrow \\ H^1(G,\mathbb{F}_p) \wedge H^1(G,\mathbb{F}_p) & \xrightarrow{\Lambda_2(\cup)} & H^2(G,\mathbb{F}_p) \end{array}$$

where the vertical arrows are isomorphisms, and $\phi$ is the Kummer isomorphism as in (3.1). Therefore $\mathrm{Br}_p(F)$ is a quotient of $\dot{F}/\dot{F}^p \wedge \dot{F}/\dot{F}^p$. (In particular, if $F$ is $p$-rigid, the horizontal arrows are also isomorphisms.) Hence, the following hold in $\mathrm{Br}_p(F)$ :

$$[(b,a)_F] = [(a,b)_F]^{-1}, \tag{3.4}$$

$$[(ab,c)_F] = [(a,c)_F] \cdot [(b,c)_F], \tag{3.5}$$

$$\left[(a^k,b)_F\right] = [(a,b)_F]^k = \left[(a,b^k)_F\right] \tag{3.6}$$

for every $a, b, c \in \dot{F}$ and $k \in \mathbb{F}_p$.

Let $E/F$ be a cyclic extension of degree $p$, namely, $E = F(\sqrt[p]{a})$ with $a \in \dot{F} \smallsetminus \dot{F}^p$. Let

$$\epsilon\colon \dot{F}/\dot{F}^p \longrightarrow \dot{E}/\dot{E}^p$$

be the homomorphism induced by the inclusion $F \hookrightarrow E$.

**Lemma 3.12.** *Let $F$ be $p$-rigid. For $E/F$ as above, one has*

$$\dot{E}/\dot{E}^p = \left\langle [\sqrt[p]{a}]_F \right\rangle \oplus \epsilon\left(\dot{F}/\dot{F}^p\right)$$

*as $\mathbb{F}_p$-vector space.*

*Proof.* By [MS03, Thm. 1], one has that $J = X \oplus Z$ as a $G$-module, where $X$ is an irreducible $G$-module, and $Z$ is a trivial $G$-module. Obviously, one has the following inclusions:

$$\left\langle [\sqrt[p]{a}]_F \right\rangle \subseteq X, \quad \epsilon\left(\dot{F}/\dot{F}^p\right) \subseteq J^G, \quad Z \subseteq J^G. \tag{3.7}$$

Fix a primitive $p$th root $\zeta_p$. If $\zeta_p$ is a norm of $E/F$, then by [MS03, Cor. 1] one has $\dim(X) = 1$, so that $J^G = J$, and by [MS03, Lemma 2] the claim follows. Otherwise, by [MS03, Cor. 1] one has $\dim(X) = 2$, so that necessarily

$$X = \left\langle [\sqrt[p]{a}]_F, [\zeta_p]_F \right\rangle,$$

for $[\zeta_p]_F = (\sigma - 1)[\sqrt[p]{a}]_F$, with $\sigma$ a suitable generator of $\mathrm{Gal}(E/F)$, and by [MS03, Lemma 2] one has $J^G = \epsilon(\dot{F}/\dot{F}^p)$, so that by (3.7) the claim follows. □

**Lemma 3.13.** *Let $E/F$ be as above, and let $\mathrm{Br}(E/F) \leq \mathrm{Br}(F)$ be the kernel of the morphism*

$$\mathrm{Br}(F) \longrightarrow \mathrm{Br}(E), \quad [(b,c)_F] \longmapsto [(b,c)_F \otimes_F E].$$

*Then $[(b,c)_F] \in \mathrm{Br}(E/F)$ if and only if $[(b,c)_F] = [(a,d)_F]$ for some $d \in \dot{F}$.*

*Proof.* Let $\bar{G} \cong \mathbb{Z}/p.\mathbb{Z}$ be the Galois group of $E/F$, and fix a primitive $p$th root $\zeta_p$. It is well known that

$$\mathrm{Br}(E/F) \cong H^2(\bar{G}, \dot{E}) \quad \text{and} \quad H^2(\bar{G}, \dot{E}) \cong \dot{F}/N_{E/F}(\dot{E}). \tag{3.8}$$

Namely, by the first isomorphism of (3.8), every element $[A]$ of $\mathrm{Br}(E/F)$ can be represented by a cross-product $F$-algebra $A$ induced by a cocycle $z\colon \bar{G}\times\bar{G} \to \dot{E}$, and by the second isomorphism of (3.8), the image of $z$ is $\{1, d\}$ with $d \in \dot{F} \smallsetminus N_{E/F}(\dot{E})$, and $A$ has a presentation such that $A = (a,d)_F$. □

**Theorem 3.14.** *Let $E = F(\sqrt[p]{a})$ with $a \in \dot{F} \smallsetminus \dot{F}^p$. If $F$ is $p$-rigid, then so is $E$.*

*Proof.* In order to prove that $E$ is $p$-rigid, we have to show that for $\alpha, \beta \in \dot{E}$, one has $[(\alpha,\beta)_E] = 1$ in $\mathrm{Br}(E)$ if and only if $[\alpha]_E, [\beta]_E$ are $\mathbb{F}_p$-linearly dependent in $\dot{E}/\dot{E}^p$.

Thus, suppose for contradiction that $[\alpha]_E, [\beta]_E$ are $\mathbb{F}_p$-linearly independent but $[(\alpha,\beta)_E] = 1$. By Lemma 3.12, and by (3.4), (3.5), and (3.6), we can reduce without loss of generality to the following to cases: either $\alpha, \beta \in \dot{F}$, or $\alpha = \sqrt[p]{a}$ and $\beta \in \dot{F}$.

*Case* 1. Assume $\alpha, \beta \in \dot{F}$. Since $[\alpha]_E, [\beta]_E$ are $\mathbb{F}_p$-linearly independent, so are $[\alpha]_F, [\beta]_F$ in $\dot{F}/\dot{F}^p$. Thus, by $p$-rigidity of $F$, $[(\alpha,\beta)_F] \neq 1$ in $\mathrm{Br}(F)$. Since we are assuming that

$$[(\alpha,\beta)_E] = [(\alpha,\beta)_F \otimes_F E] = 1 \quad \text{in } \mathrm{Br}(E),$$

it follows that $[(\alpha,\beta)_F] \in \mathrm{Br}(E/F)$. Therefore, by Lemma 3.13, there exists $b \in \dot{F}$ such that $[(\alpha,\beta)_F] = [(a,b)_F]$. Since $\mathrm{Br}_p(F) \cong \dot{F}/\dot{F}^p \wedge \dot{F}/\dot{F}^p$, it follows that

$$\begin{aligned} [\alpha]_F \wedge [\beta]_F &= [a]_F \wedge [b]_F \quad \text{in } \dot{F}/\dot{F}^p \wedge \dot{F}/\dot{F}^p, \\ \text{thus} \quad [\alpha]_E \wedge [\beta]_E &= [a]_F \wedge [b]_E \quad \text{in } \dot{E}/\dot{E}^p \wedge \dot{E}/\dot{E}^p \end{aligned}$$

so that $[\alpha]_E$ and $[\beta]_E$ are not linearly independent, as $[a]_E = 1$, a contradiction.

*Case* 2. Assume $\alpha = \sqrt[p]{a}$ and $\beta \in \dot{F}$. Let $C$ be the maximal pro-$p$ Galois group of $E$. Then by [GS06, Prop. 7.5.5] one has the following commutative diagrams:

$$\begin{array}{ccc} \dot{F}/\dot{F}^p & \xrightarrow{\epsilon} & \dot{E}/\dot{E}^p \\ \downarrow{\scriptstyle \phi_F} & & \downarrow{\scriptstyle \phi_E} \\ H^1(G, \mathbb{F}_p) & \xrightarrow{\mathrm{res}^1_{G/C}} & H^1(C, \mathbb{F}_p) \end{array} \qquad \begin{array}{ccc} \dot{E}/\dot{E}^p & \xrightarrow{N_{E/F}} & \dot{F}/\dot{F}^p \\ \downarrow{\scriptstyle \phi_E} & & \downarrow{\scriptstyle \phi_F} \\ H^1(C, \mathbb{F}_p) & \xrightarrow{\mathrm{cor}^1_{G/C}} & H^1(G, \mathbb{F}_p) \end{array}$$

where the vertical arrows are the Kummer isomorphisms, together with the morphism

$$\mathrm{cor}_{E/F}\colon \mathrm{Br}_p(E) \longrightarrow \mathrm{Br}_p(F)$$

induced by the corestriction $\mathrm{cor}^2_{G/C}\colon H^2(C,\mathbb{F}_p) \to H^2(G,\mathbb{F}_p)$. Then by the projection formula [GS06, Prop. 3.4.10] one has

$$\mathrm{cor}^2_{G/C}\left(\phi_E(\sqrt[p]{a}) \cup \mathrm{res}^1_{G/C}\left(\phi_F(b)\right)\right) = \mathrm{cor}^1_{G/C}\left(\phi_E(\sqrt[p]{a})\right) \cup \phi_F(b),$$

which implies

$$\mathrm{cor}_{E/F}\left([(\sqrt[p]{a},\beta)_E]\right) = \left[(N_{E/F}(\sqrt[p]{a}),\beta)_F\right] = \left[(a,\beta)_F\right].$$

Since $[(\sqrt[p]{a},\beta)_E] = 1$ in $\mathrm{Br}(E)$, it follows that $[(a,\beta)_F] = 1$ in $\mathrm{Br}(F)$. Thus, by $p$-rigidity of $F$, $[a]_F, [\beta]_F$ are $\mathbb{F}_p$-linearly dependent in $\dot{F}/\dot{F}^p$, i.e., $[\beta]_F = [a^k]_F$ for some $k \in \mathbb{F}_p$. Therefore $[\beta]_E$ is trivial in $\dot{E}/\dot{E}^p$, a contradiction. □

The following fact is an elementary consequence of the solvability of finite $p$-groups.

*Fact* 3.15. Let $K/F$ be a finite non-trivial $p$-extension with $K \subseteq F(p)$. Then there exists a chain of extensions

$$F = K_0 \subset K_1 \subset \ldots \subset K_{r-1} \subset K_r = K \tag{3.9}$$

for some $r \geq 1$, such that $|K_{i+1} : K_i| = p$ for every $i = 0, \ldots, r-1$.

This, together with Theorem 3.14, implies the following.

**Theorem 3.16.** *Every $p$-rigid field $F$ is also hereditary $p$-rigid.*

As mentioned in the Introduction, the above theorem was proved in a different way by Engler and Koenigsmann in [EK98, Prop. 2.2].

3.4. **Galois theoretical and cohomological characterizations for $p$-rigid fields.** In addition to Theorem 3.16, and earlier results in this section, we have the following implications.

$F$ is $p$-rigid $\implies$ $F$ is hereditary $p$-rigid $\implies$ $G := G_F(p)$ is locally powerful $\implies$ $G$ is $\theta$-abelian $\implies$ $G$ has presentation as in Proposition 3.2. So in other words, we obtain the next corollary.

**Corollary 3.17.** *The field $F$ is rigid if and only if there exists an orientation $\theta\colon G_F(p) \to \mathbb{Z}_p^\times$ such that $G_F(p)$ is $\theta$-abelian, so that $G$ has a presentation*

$$G_F(p) = \left\langle \sigma, \rho_i, i \in \mathcal{I} \,\middle|\, [\sigma,\rho_i] = \rho_i^\lambda, [\rho_i,\rho_j] = 1 \;\forall\, i,j \in \mathcal{I} \right\rangle \tag{3.10}$$

*for some set of indices $\mathcal{I}$ and $\lambda \in p.\mathbb{Z}_p$ such that $1 + \lambda = \theta(\sigma)$.*

In fact if $F$ is $p$-rigid, then the suitable orientation for $G_F(p)$ is the cyclotomic character of $F$ – as one would expect, and as we shall see this again explicitly in Section 4.2.

Also, in Section 4.2, we will obtain together with the results of previous section, self-contained field theoretic proof of this corollary. (Alternatively, one can also deduce this corollary using valuation theory in [EK98].)

**Definition.** We say that pro-$p$ group $G$ is solvable if it admits a normal series of closed subgroups such that each successive quotient is abelian. That is, we have a sequence of closed subgroups

$$1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{k-1} \leq G_k = G$$

such that each $G_j$ is closed and normal in $G_{j+1}$ and $G_{j+1}/G_j$ is abelian for all $j$.

**Corollary 3.18.** *The field $F$ is $p$-rigid if and only if the maximal pro-$p$ Galois group $G_F(p)$ is solvable.*

*Proof.* If $F$ is $p$-rigid, then by Corollary 3.17, $G_F(p)$ has a presentation as in (3.10), so that $G_F(p)$ is meta-abelian (i.e., its commutator is abelian), and thus solvable; in fact, the desired normal series is

$$1 = [[G,G],[G,G]] \leq [G,G] \leq G$$

where $G = G_F(p)$. Conversely, if $G_F(p)$ is solvable, than it contains no closed non-abelian free pro-$p$ subgroups. Hence, by [Qu13, Thm. B], $G_F(p)$ is $\theta$-abelian for some orientation $\theta$, and by Corollary 3.17, $F$ is $p$-rigid. □

As mentioned in the Introduction, Corollary 3.17 can be deduced also using valuations techniques, as in [EK98, § 1] and [Ef06, Ex. 22.1.6], whereas Corollary 3.18 is the double implication (ii)⇔(vi) in [EK98, Prop. 2.2].

**Corollary 3.19.** *The field $F$ is $p$-rigid if and only if*

$$H^\bullet\left(G_F(p),\mathbb{F}_p\right) \cong \bigwedge_{k=1}^{d(G_F(p))} \left(H^1(G_F(p),\mathbb{F}_p)\right). \tag{3.11}$$

*Proof.* Recall that $G_F(p)$ is a Bloch-Kato pro-$p$ group, so that the whole $\mathbb{F}_p$-cohomology ring $H^\bullet\left(G_F(p),\mathbb{F}_p\right)$ depends on $H^1(G_F(p),\mathbb{F}_p)$ and $H^2(G_F(p),\mathbb{F}_p)$. That is, $H^\bullet\left(G_F(p),\mathbb{F}_p\right)$ has generators in degree 1 and relations in degree 2.

If the isomorphism (3.11) holds, then in particular the morphism (3.3) is injective, and $F$ is $p$-rigid. Conversely, if $F$ is $p$-rigid then the morphism (3.3) is an isomorphism, and

$$H^1(G_F(p),\mathbb{F}_p) \wedge H^1(G_F(p),\mathbb{F}_p) \xrightarrow{\sim} H^2(G_F(p),\mathbb{F}_p).$$

Therefore the whole $\mathbb{F}_p$-cohomology ring is isomorphic to the exterior algebra generated by $H^1(G_F(p),\mathbb{F}_p)$. □

Ware proved the same result in the case $\dim(\dot{F}/\dot{F}^p) < \infty$, but with the further assumptions that $F$ is hereditary $p$-rigid and that it contains a primitive $p^2$th root of unity [Wr92, Thm. 4 and Corollary]. Moreover, his proof requires computations involving the Hochschild-Serre spectral sequence.

*Remark* 3.20. Clearly Corollaries 3.17 and 3.19 hold also for every $p$-extension $K/F$.

**Corollary 3.21.** *Given a field $F$, assume that $\dim(\dot{F}/\dot{F}^p) = d < \infty$. Then $F$ is $p$-rigid if and only if $\mathrm{cd}(G_F(p)) = d$.*

*Proof.* If $F$ is $p$-rigid, then $\mathrm{cd}(G_F(p)) = d(G_F(p))$ by Corollary 3.19, and $d(G_F(p)) = d$ by (2.2).

Conversely, if $\mathrm{cd}(G_F(p)) = d(G) = d$, then one has the isomorphism (3.11), since a non-trivial relation in $H^1(G_F(p),\mathbb{F}_p) \wedge H^1(G_F(p),\mathbb{F}_p)$ would imply that

$$H^d\left(G_F(p),\mathbb{F}_p\right) = \mathrm{Span}_{\mathbb{F}_p}\{\chi_1 \cup \cdots \cup \chi_d\} = 0,$$

with $\{\chi_1, \dots, \chi_d\}$ a basis for $H^1(G_F(p), \mathbb{F}_p)$, a contradiction (see [Qu13, Prop. 4.3] for more details). □

**Corollary 3.22.** *Given a field $F$, assume that $\dim(\dot{F}/\dot{F}^p) = d < \infty$. Then $F$ is $p$-rigid if and only if $\dim(\dot{K}/\dot{K}^p) = d$ for every finite $p$-extension $K/F$.*

*Proof.* Suppose that $\dim(\dot{K}/\dot{K}^p) = d$ for every finite $p$-extension $K/F$. By (2.2) and (3.1), this implies that $d(C) = d$ for every open subgroup $C \leq G$. Therefore the rank of $G$ is finite, and $G$ contains no closed non-abelian free pro-$p$ subgroups. Thus, by [Qu13, Thm. B], $G_F(p)$ is powerful, and $F$ is $p$-rigid; also see [EM13].

Conversely, if $F$ is $p$-rigid, then $G_F(p)$ is uniformly powerful (and finitely generated by hypothesis), and by [DdSMS03, Prop. 4.4] one has $d(C) = d(G_F(p))$ for every open subgroup $C \leq G_F(p)$, i.e., $\dim(\dot{K}/\dot{K}^p) = d$ for every finite $p$-extension $K/F$. □

*Remark* 3.23. A pro-$p$ group $G$ has *constant generating number on open subgroups* if

$$d(C) = d(G) \quad \text{for all open subgroups } C \leq G. \tag{3.12}$$

By Corollary 3.22, a maximal pro-$p$ Galois group has property (3.12) if and only if $F$ is $p$-rigid. The problem to classify all profinite groups with property (3.12) was raised by K. Iwasawa (see [KS11, §1]). Thus, Corollary 3.22 classifies all such groups in the category of maximal pro-$p$ Galois groups (and hence also in the category of pro-$p$ absolute Galois group). Actually, [Qu13, Thms. A and B] gives implicitly the same classification for the wider category of Bloch-Kato pro-$p$ groups.

A similar classification has been proven in [KS11] for the category of $p$-adic analytic pro-$p$ groups. It is interesting to remark that the groups listed in [KS11, Thm. 1.1.(1)-(2)] have a presentation as in (3.10), whereas the groups listed in [KS11, Thm. 1.1.(3)] cannot be realized as maximal pro-$p$ Galois groups, for they have non-trivial torsion.

## 4. New characterization for $p$-rigid fields

4.1. **Proof of Theorem A.** Let $G$ be the maximal pro-$p$ Galois group $G_F(p)$, and recall from Section 2.3 the definition of the modules $J_n$.

Moreover, let $G^{\{n\}}$ and $G^{(n)}$ denote the maximal pro-$p$ Galois group of $F^{\{n\}}$, resp. of $F^{(n)}$. Then it is clear that

$$\mathrm{Gal}\left(F^{\{n+1\}}/F^{\{n\}}\right) = \frac{G^{\{n\}}}{\Phi\left(G^{\{n\}}\right)},$$
$$\text{and} \quad G^{\{n+1\}} = \Phi\left(G^{\{n\}}\right) = \left(G^{\{n\}}\right)^p \left[G^{\{n\}}, G^{\{n\}}\right],$$

whereas by (2.2) and (3.1) one has $J_n \cong H^1(G^{(n)}, \mathbb{F}_p) = (G^{(n)})^\vee$, so that

$$(J_n)^G \cong H^1\left(G^{(n)}, \mathbb{F}_p\right)^G = \left(\frac{G^{(n)}}{[G, G^{(n)}]}\right)^\vee,$$

i.e., the $G$-invariant elements of $J_n$ are dual to the $G$-coinvariant elements of $G^{(n)}$, which implies that

$$\mathrm{Gal}\left(F^{(n+1)}/F^{\{n\}}\right) = \frac{G^{(n)}}{\left(G^{(n)}\right)^p \left[G, G^{(n)}\right]},$$

$$\text{and} \quad G^{(n+1)} = \Phi\left(G^{(n)}\right)\left[G, G^{(n)}\right] = \left(G^{(n)}\right)^p \left[G, G^{(n)}\right] = \lambda_{n+1}(G).$$

*Remark* 4.1. i. The $G$-module $J$ can be defined in a purely cohomological manner without involving the field $F$, since by Kummer theory one has the isomorphism

$$J \cong H^1(\Phi(G), \mathbb{F}_p)$$

as $G$-modules.

ii. Theorem A can be stated in the following way: $F$ is rigid if and only if $G^{\{n\}} = G^{(n)}$ for all $n \geq 2$ or, equivalently, if and only if $J_2^G = J_2$.

**Proposition 4.2.** *If $F$ is a $p$-rigid field, then $F^{\{n\}} = F^{(n)}$ for all $n \geq 2$.*

*Proof.* By Corollary 3.17, the maximal pro-$p$ Galois group $G$ is a locally powerful group, with a presentation as in (3.10). Direct computations imply that $\lambda_n(G) = G^{p^{n-1}}$ for all $n \geq 2$. In particular,

$$G^{\{3\}} = \Phi(G)^p[\Phi(G), \Phi(G)] = G^{p^2} = G^{(3)}.$$

Moreover, if we assume that $G^{\{n\}} = G^{(n)} = \lambda_n(G)$, then

$$\lambda_{n+1}(G) \leq G^{\{n+1\}} = \lambda_n(G)^p[\lambda_n(G), \lambda_n(G)] \leq \lambda_{n+1}(G),$$

so that $G^{\{n+1\}} = \lambda_{n+1}(G)$. Therefore, $G^{(n)} = G^{\{n\}} = \lambda_n(G)$ and, by Remark 4.1, $F^{\{n\}} = F^{(n)}$ for all $n \geq 2$. □

On the other hand, if $F$ is not $p$-rigid, we have the opposite.

**Theorem 4.3.** *If $F$ is not $p$-rigid, then $F^{\{3\}} \supsetneq F^{(3)}$.*

In order to prove the above theorem, we need two further lemmas.

**Lemma 4.4.** *Let $E/F$ be a bicyclic extension of degree $p^2$, and let $L = F^{(2)}$, i.e., $E = F(\sqrt[p]{a}, \sqrt[p]{b})$ with $a, b \in \dot{F} \setminus \dot{F}^p$ such that $[a]_F, [b]_F$ are $\mathbb{F}_p$-linearly independent in $\dot{F}/\dot{F}^p$. Assume $\gamma \in \dot{E}$. Then $\gamma \in \dot{L}^p$ if and only if $\gamma \in \dot{F} \cdot \dot{E}^p$.*

*Proof.* Let $\gamma = x\delta^p$, with $x \in \dot{F}$ and $\delta \in \dot{E}$. Then it is clear that $\gamma \in \dot{L}^p$, for $L = F(\sqrt[p]{F})$.

On the other hand, assume that $\gamma \in \dot{L}^p$. Then, either $\gamma$ is a $p$-power in $E$, or it becomes a $p$-power via the extension $L/E$, i.e., $\sqrt[p]{\gamma} \in L \setminus E$. Therefore, by Kummer theory, $\gamma$ is equivalent to an element $x \in \dot{F}$ modulo $\dot{F}^p$, namely, $\gamma \in x\dot{F}^p$. This proves the lemma. □

**Lemma 4.5.** *Let $E/F$ be a cyclic extension of degree $p$, i.e., $E = F(\sqrt[p]{a})$ with $a \in \dot{F} \setminus \dot{F}^p$. Then*

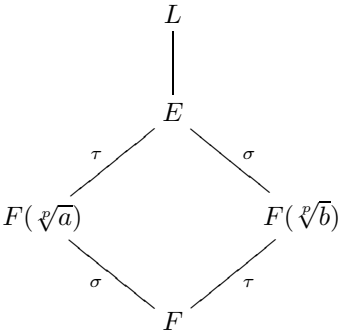
$$\sqrt[p]{a} \notin \dot{F} \cdot \dot{E}^p.$$

*Proof.* Let $\alpha \in \dot{F}\dot{E}^p$. Then there exist $x \in \dot{F}$, $\gamma \in \dot{E}$ such that $\alpha = x\gamma^p$. Thus

$$N_{E/F}(\alpha) = N_{E/F}(x\gamma^p) = x^p N_{E/F}(\gamma)^p \in \dot{F}^p,$$

with $N_{E/F}$ the norm of $E/F$. Since $N_{E/F}(\sqrt[p]{a}) = a \notin \dot{F}^p$, it follows that $\sqrt[p]{a} \notin \dot{F}\dot{E}^p$. □

*Proof of Theorem* 4.3. Since $F$ is not $p$-rigid, there exist two elements $a, b \in \dot{F}$ such that $[a]_F$ and $[b]_F$ are $\mathbb{F}_p$-linearly independent, and $a$ is a norm of $F(\sqrt[p]{b})/F$. Recall that the linear independence implies that $F(\sqrt[p]{a}) \neq F(\sqrt[p]{b})$, so that $E/F$ is a bicyclic extension of degree $p^2$, where $E = F(\sqrt[p]{a}, \sqrt[p]{b})$. Let $\mathrm{Gal}(E/F) \cong C_p \times C_p$ be generated by $\sigma, \tau$, with $F(\sqrt[p]{a}) = E^{\langle\tau\rangle}$ and $F(\sqrt[p]{b}) = E^{\langle\sigma\rangle}$. Then the lattice of the fields $L \supseteq E \supseteq F$ is the following:




Let $\delta \in F(\sqrt[p]{b})$ such that $N_{F(\sqrt[p]{b})/F}(\delta) = a$, and let $c = \sqrt[p]{a}$. Then

$$N_{E/F(\sqrt[p]{a})}(\delta) = \delta \cdot (\tau.\delta) \cdots (\tau^{p-1}.\delta) = N_{F(\sqrt[p]{b})/F}(\delta) = a$$
$$\text{and} \quad N_{E/F(\sqrt[p]{a})}(c) = c \cdot (\tau.c) \cdots (\tau^{p-1}.c) = c \cdot \zeta c \cdots \zeta^{p-1} c = c^p,$$

with $\zeta$ a primitive $p$th root of unity, so that

$$N_{E/F(\sqrt[p]{a})}\left(\frac{\delta}{c}\right) = \frac{N_{E/F(\sqrt[p]{a})}(\delta)}{N_{E/F(\sqrt[p]{a})}(c)} = \frac{a}{c^p} = 1.$$

Therefore, by Hilbert's Satz 90 there exists $\gamma \in \dot{E}$ such that

$$(\tau - 1).\gamma = \frac{\tau.\gamma}{\gamma} = \frac{\delta}{c}. \tag{4.1}$$

Suppose that $\delta/c \in \dot{L}^p$. Then by Lemma 4.4 one has that $\delta/c \in \dot{F} \cdot \dot{E}^p$. In particular, this implies that $c = \sqrt[p]{a} \in F(\sqrt[p]{b})^\times \cdot \dot{E}^p$, which is impossible by Lemma 4.5. Hence $\delta/c \notin \dot{L}^p$. Thus, by (4.1) and by Lemma 2.2 the extension $L(\sqrt[p]{\gamma})/F$ is not Galois and $\gamma^{1/p}$ is not in $F^{(3)}$. □

Now Proposition 4.2 and Theorem 4.3 imply Theorem A.

*Remark* 4.6. By the proof of Proposition 4.2 it follows that if $F$ is $p$-rigid, then $G^{(n)} = \lambda_n(G) = G^{p^{n-1}}$ for all $n > 1$.

4.2. **Recovering $G_F(p)$ and $F(p)$ from small Galois groups.** As in Section 4.1, let $G$ be the maximal pro-$p$ Galois group $G_F(p)$ of the field $F$. For $h > 0$, let $\mu_{p^h} \subseteq F(p)$ be the group of $p^h$ roots of unity. We also set $\mu_{p^\infty}$ to be the group of all roots of unity of order $p^m$ for some $m \geq 0$. Finally we set $k \in \mathbb{N} \cup \{\infty\}$ to be the maximum of all $h \in \mathbb{N} \cup \{\infty\}$ such that $\mu_{p^h} \subseteq F$.

For a field $F$ which is $p$-rigid, let $E/F$ be a Galois extension of degree $p$. Therefore $E = F(b^{1/p})$ for some $b \in \dot{F} \backslash \dot{F}^p$. Then by Kummer theory, we may choose a set of

representatives $\{b_i : i \in \mathcal{J}\} \subseteq \dot{F}$ of $\dot{F}\backslash\dot{F}^p$ with $b = b_j$ for some $j \in \mathcal{J}$. Thus Lemma 3.12 implies that

$$\dot{E}/\dot{E}^p = \left\langle [\sqrt[p]{b_j}]_E, [b_i]_E \right\rangle_{i\neq j}. \tag{4.2}$$

Assume now that $k < \infty$. Then we may pick a set of representatives $\mathcal{A} = \{\zeta_{p^k}, a_i, i \in \mathcal{I}\} \subseteq \dot{F}$, where $\zeta_{p^k}$ is a fixed primitive $p^k$th root of unity, so that $\bar{\mathcal{A}} = \{[\zeta_{p^k}]_F, [a_i]_F, i \in \mathcal{I}\}$ is a $\mathbb{F}_p$-basis for $\dot{F}/\dot{F}^p$. If $k = \infty$, then we still consider a basis $\bar{\mathcal{A}}$ for $\dot{F}/\dot{F}^p$, where the symbol $[\zeta_{p^k}]_F$ in this case is meant as an empty symbol to be ignored. Also in this case $[\zeta_{p^{k+n}}]_E$, with $n \in \mathbb{N}$ and $E/F$ a $p$-extension, is also an empty symbol. We assume that our system of roots of unity $\zeta_{p^l}$ for $l \geq 1$ in $F(p)$ is chosen such that

$$(\zeta_{p^{l+1}})^p = \zeta_{p^l}$$

for all $l \geq 1$.

Let $\mathcal{J}$ be a finite subset of $\mathcal{I}$. Set $\mathcal{J} = \{1, \cdots, t\}$ and let

$$K = F(a_1^{1/p}, \cdots, a_t^{1/p}, \zeta_{p^{k+1}}).$$

Then we have a series of Galois extensions

$$F \subset K_1 \subset K_2 \cdots K_t \subset K_{t+1} = K \subseteq F^{(2)},$$

where $K_1 = F(\zeta_{p^{k+1}})$, and $K_{i+1} = K_i(a_i^{1/p})$ for $1 \leq i \leq t$. Then by the above argument and induction one has

$$\dot{K}/\dot{K}^p = \langle [\zeta_{p^{k+1}}], [a_j^{1/p}]_K, j = 1, 2, \cdots, t, [f]_K, f \in \dot{F} \rangle. \tag{4.3}$$

Assuming this observation, we shall prove the following theorem.

**Theorem 4.7.** *If $F$ is a $p$-rigid field, then*

$$\frac{\dot{F}^{(n)}}{\left(\dot{F}^{(n)}\right)^p} = \left\langle [\zeta_{p^{k+n-1}}]_{F^{(n)}}, \left[a_i^{1/p^{n-1}}\right]_{F^{(n)}}, i \in \mathcal{I} \right\rangle$$

*for every $n \geq 1$.*

*Proof.* Let $\bar{\mathcal{A}} = \{[\zeta_{p^k}]_F, [a_i]_F, i \in \mathcal{I}\}$ be an $\mathcal{F}_p$ basis for $\dot{F}/(\dot{F})^p$ as above. We observe that for $n = 1$ our statement is clear because $F^{(1)} = F$. In order to see that our statement is also true for $n = 2$, consider any $[\alpha]_{F^{(2)}} \in \dot{F^{(2)}}/(\dot{F^{(2)}})^p$ with $\alpha$ in $\dot{F^{(2)}}$. Then there exists a finite subset $\mathcal{J} \subset \mathcal{I}$ such that $\alpha \in K = F(\zeta_{p^{k+1}}, a_j^{1/p}, j \in \mathcal{J})$. (Again, we ignore $\zeta_{p^{k+1}}$ if $k = \infty$.) Now we see that $[\alpha]_K$ can be expressed as a product of powers of $[\zeta_{p^{k+1}}]_K, [a_j^{1/p}]_K$ and a finite number of elements $[f_l]_K$, $l = 1, \cdots, n$, $f_l \in \dot{F}$. Passing to $F^{(2)}$, all elements $[f_j]_{[F^{(2)}]}$ become $[1]_{F^{(2)}}$. Therefore

$$\dot{F^{(2)}}/(\dot{F^{(2)}})^p = \left\langle [\zeta_{p^{k+1}}]_{F^{(2)}}, [\sqrt[p]{a_i}]_{F^{(2)}}, i \in \mathcal{I} \right\rangle. \tag{4.4}$$

This proves our statement for $n = 2$. Now going from $n$ to $n + 1$ is just like going from $n = 1$ to $n = 2$, done above, taking into account that

$$F^{(n+1)} = F^{(n)}(\zeta_{p^{k+n}}, a_i^{1/p^n}, i \in \mathcal{I}).$$

The last equality follows by induction hypothesis on $n$ and by observing that $F^{(n)}(a_i^{1/p^n}, i \in \mathcal{I})$ is Galois over $F$ for each $i \in I$ as $\zeta_{p^{k+n-1}}$, and hence also $\zeta_{p^n}$ belong to $F^{(n)}$. Hence we proved our statement for all $n$. □

*Remark* 4.8. In fact taking into account our convention about the symbol $[\zeta_{p^{k+n-1}}]_{F^{(n)}}$ when $k$ is $\infty$, one can show in a similar but slightly more complicated way as in the proof above that

$$\{[\zeta_{p^{k+n-1}}]_{F^{(n)}}, [{a_i}^{1/p^{n-1}}]_{F^{(n)}}, i \in \mathcal{I}\}$$

is a basis of $\dot{F^{(n)}}/(\dot{F^{(n)}})^p$ over $\mathbb{F}_p$ for all $n \in \mathcal{N}$.

**Corollary 4.9.** *Assume that $F$ is a $p$-rigid field. Then we have the following:*

*(a) For all $n \geq 1$,*

$$F^{(n)} = F(\zeta_{p^{k+n-1}}, a_i^{1/p^{n-1}}, i \in \mathcal{I}).$$

*(b)*

$$F(p) = \bigcup_{n \geq 1} F(\zeta_{p^{k+n}}, a_i^{1/p^n}, i \in \mathcal{I}).$$

*Proof.* (a) We use Theorem 4.7, its proof and induction on $n$. The statement is true for $n = 1$ because $\zeta_{p^k}$, $a_i$, $i \in \mathcal{I}$, all belong to $F$. Now assume that our statement is true for $n$. Using Theorem 4.7 and the fact that $F^{(n)}(a_i^{1/p^n})/F$ is Galois for each $i \in \mathcal{I}$, we conclude that

$$F^{(n+1)} = F(\zeta_{p^{k+n}}, a_i^{1/p^n}, i \in \mathcal{I}).$$

This completes the induction step and we are done.

(b) This follows from the fact that

$$F(p) = \bigcup_{n \geq 1} F^{(n)}.$$

(See Proposition 2.1.) □

Now we shall determine all Galois groups $G^{[n]} := \mathrm{Gal}(F^{(n)}/F)$, for all $n \geq 1$.

**Theorem 4.10.** *Suppose $F$ is a $p$-rigid field. Then we have the following:*

*(a)*

$$G^{[n]} = \begin{cases} (\prod_{\mathcal{I}} \mathbb{Z}/p^{n-1}\mathbb{Z}) \rtimes \mathbb{Z}/p^{n-1}\mathbb{Z} & \text{if } k < \infty, \\ \prod_{\mathcal{I}} \mathbb{Z}/p^{n-1}\mathbb{Z} & \text{if } k = \infty. \end{cases}$$

*(b)*

$$G = \mathrm{Gal}(F(p)/F) = \begin{cases} (\prod_{\mathcal{I}} \mathbb{Z}_p) \rtimes \mathbb{Z}_p & \text{if } k < \infty, \\ \prod_{\mathcal{I}} \mathbb{Z}_p & \text{if } k = \infty. \end{cases}$$

*Moreover, when $k < \infty$ there exists a generator $\sigma$ of the outer factor $\mathbb{Z}/p^{n-1}\mathbb{Z}$ in (a) and of the outer factor $\mathbb{Z}_p$ in (b) such that for each $\tau$ from the inner factor $\prod_{\mathcal{I}} \mathbb{Z}/p^{n-1}\mathbb{Z}$ in (a) and each $\tau$ from the inner factor $\prod_{\mathcal{I}} \mathbb{Z}_p$ in (b) we have*

$$\sigma\tau\sigma^{-1} = \tau^{p^k+1}.$$

*Proof.* If $k < \infty$, consider $F^{(n)}$ as the 2nd step extension of $F$

$$F \subset F(\zeta_{p^{k+n-1}}) \subset F^{(n)}.$$

Then there exists $\sigma \in G^{[n]}$ such that

$$\sigma(\zeta_{p^{k+n-1}}) = \zeta_{p^{k+n-1}}^{p^k+1}$$

and $\sigma$ restricts to identity in $\mathrm{Gal}(F^{(n)}/F(\zeta_{p^{k+n-1}})$. By standard Kummer theory (see Chapter 6, Sections 8 and 9 in [Lan02], Chapter 6, Section 2 in [AT09], and also for relevant similar calculations in [Wr92], proof of Theorem 2), we can deduce that such $\sigma$ exists and that

$$\begin{aligned} G^{[n]} &= \mathrm{Gal}(F^{(n)}/F(\zeta_{p^{k+n-1}})) \rtimes \langle\sigma\rangle \\ &\cong \prod_{\mathcal{I}} \mathbb{Z}/p^{n-1}\mathbb{Z} \rtimes \mathbb{Z}/p^{n-1}\mathbb{Z} \ \text{ if } k < \infty \end{aligned}$$

with the action $\sigma\tau\sigma^{-1} = \tau^{p^k+1}$ for all $\tau \in \mathrm{Gal}(F^{(n)}/F(\zeta_{p^{k+n-1}}))$. If $k = \infty$, then direct application of Kummer theory shows that

$$G^{[n]} = \prod_{\mathcal{I}} \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

This proves (a), and (b) follows from that fact that $F(p) = \bigcup_{n\geq 1} F^{(n)}$. Indeed, then $G = \varprojlim G^{[n]}$, which has precisely the description in (b). □

If $k < \infty$, then it is well known that the Galois group of the extension $F(\mu_{p^\infty})/F$ is pro-$p$-cyclic, i.e., $\mathrm{Gal}(F(\mu_{p^\infty})/F) \cong \mathbb{Z}_p$ [Wr92, Lemma 1]. As we see from our proof of the above theorem (part b), the outer factor of $G = \prod_{\mathcal{I}} \mathbb{Z}_p \rtimes \mathbb{Z}_p$ is isomorphic with $\mathrm{Gal}(F(\mu_{p^\infty}))$, and $\mathrm{Gal}(F(p)/F(\mu_{p^\infty})) \cong \prod_{\mathcal{I}} \mathbb{Z}_p$. We can pick generators $\rho_i$, $i \in \mathcal{I}$ of the pro $p$-group $\prod_{\mathcal{I}} \mathbb{Z}_p$ as elements of $\mathrm{Gal}(F(p)/F(\mu_{p^\infty}))$ such that

$$\rho_i(a_i^{1/p^n}) = \zeta_{p^n} a_i^{1/p^n} \text{ for all } i \in \mathcal{I} \text{ and } n \geq 1,$$

and

$$\rho_i(a_j^{1/p^n}) = a_j^{1/p^n} \text{ for all } j \in \mathcal{I}, j \neq i \text{ and } n \geq 1.$$

This isomorphism $\mathrm{Gal}(F(\mu_{p^\infty})) \cong \mathbb{Z}_p$ is induced by the cyclotomic character

$$\theta_F \colon G \longrightarrow \mathrm{Aut}_F(\mu_{p^\infty}), \tag{4.5}$$

where $\mathrm{Aut}_F(\mu_{p^\infty})$ is the image of $\theta_F$ in $\mathrm{Aut}(\mu_{p^\infty}) \cong \mathbb{Z}_p^\times$.

From the above theorem we further see that we have a presentation of $G$ by generators and relations as follows:

$$G = \left\langle \sigma, \rho_i, i \in \mathcal{I} \,\middle|\, [\sigma, \rho_i] = \rho_i^{p^k}, [\rho_i, \rho_j] = 1 \ \forall\, i, j \in \mathcal{I} \right\rangle. \tag{4.6}$$

If $k = \infty$, then we can omit $\sigma$ and $G = \prod_{\mathcal{I}} \mathbb{Z}_p = \prod_{\mathcal{I}} \langle\rho_i\rangle$. Thus we recover Corollary 3.17 and our orientation in $\theta$ in Corollary 3.17 can be chosen as the cyclotomic character $\theta \colon G \to \mathbb{Z}_p^\times$.

In the above theorem, we determined $G^{[n]}$ quotients of $G_F(p)$ if $F$ is $p$-rigid. If $k < \infty$ the described action is trivial iff $n \leq p^k + 1$. Thus we obtain the following interesting corollary.

**Corollary 4.11.** *Suppose that $F$ is a $p$-rigid field and $k < \infty$. Then $G^{[n]}$ is abelian iff $n \leq p^k + 1$.*

In Corollary 4.9 we determined the structure of $F(p)$ for $F$ a $p$-rigid field. It is the simplest possible structure $F(p)$ can have. Using this structure, we determine in Theorem 4.10 and the discussion after it, that if $d(G) \geq 1$, then $G_F(p)$ fits in the exact sequence

$$1 \to A \to G_F(p) \to \mathbb{Z}_p \to 1$$

where $A$ is a topological product of copies of $\mathbb{Z}_p$. Therefore, if we assume that

$$F(p) = \bigcup_{n\geq 1} F(\zeta_{p^{k+n}}, a_i^{1/p^n}, i \in \mathcal{I})$$

for some $\mathcal{I}$ using [Wr92] Theorem 1(b), we obtain the following refinement of Corollary 4.9.

**Corollary 4.12.** *Let $F$ be a field. Then $F$ is $p$-rigid if and only if*

$$F(p) = \bigcup_{n\geq 1} F(\zeta_{p^{k+n}}, a_i^{1/p^n}, i \in \mathcal{I}).$$

*Remark* 4.13. Note that our proofs were done using purely Galois field-theoretic methods. However, some of these arguments can be obtained by using the theory of uniform pro-$p$ groups. (See beginning of Section 3.1 for the definition of uniform pro-$p$ groups and recall from Section 4.1 that $\lambda_n(G) = G^{(n)}$.) Although this theory is worked out in [DdSMS03] only for finitely generated pro-$p$ groups, the techniques and methods can also be extended to our groups, i.e., groups of the form $G = G_F(p)$. In fact, because the structure of $G$ as described in Theorem 4.10 is very simple, these results can be proved in a straightforward manner. Here we will reformulate some of these results which are inspired by the theory of uniform pro-$p$ groups.

First of all, from Theorem 4.7 and Theorem 4.10 we see that if $G$ is finitely generated, then $G$ is a uniform pro-$p$ group. Observe that $G^{(2)} = \lambda_2(G) = G^p$. This follows from the fact that the commutators in $G$ are $p$th powers. In fact, by induction on $n$, we see that $G^{(n)} = G^{p^{n-1}}$ for all $n \geq 2$. Thus we see again slightly differently the validity of Remark 4.6. The following fact is a consequence of the group structure of $G$, and in fact in the case of finitely generated pro-$p$ groups, it holds for every uniform pro-$p$ group. We omit a straightforward direct proof.

*Fact* 4.14. The $p^n$th power map $G \to G^{p^n}$ induces an isomorphism of (finite) $p$-groups

$$G/G^p = G/G^{(2)} \xrightarrow{\ p^n\ } G^{p^n}/G^{p^{n+1}} = G^{(n+1)}/G^{(n+2)}$$

for every $n > 1$.

By duality the above map induces the following commutative diagram:

$$\begin{array}{ccc} H^1\left(G^{(n)}, \mathbb{F}_p\right) & \xrightarrow{(p^{n-1})^\vee} & H^1\left(G, \mathbb{F}_p\right) \\ \Big| \wr & & \Big| \wr \\ \dot{F}^{(n)}/(\dot{F}^{(n)})^p & \xleftarrow{\ \psi_n\ } & \dot{F}/\dot{F}^p \end{array}$$

where the upper arrow is the dual of the $p^n$th power map – and therefore $(p^{n-1})^\vee$ is an isomorphism – and the vertical arrows are the Kummer isomorphisms. Consequently also $\dot{F}/\dot{F}^p$ and $\dot{F}^{(n)}/(\dot{F}^{(n)})^p$ are isomorphic as $\mathbb{F}_p$-vector spaces. In particular,

$$\psi_n\left([\zeta_{p^k}]_F\right) = \left[\zeta_{p^{k+n-1}}\right]_{F^{(n)}} \quad \text{and} \quad \psi_n\left([a_i]_F\right) = \left[a_i^{1/p^{n-1}}\right]_{F^{(n)}}$$

for every $n > 1$ and $i \in \mathcal{I}$. This last conclusion is consistent with Theorem 4.7 and Remark 4.8.

From Theorem A it is possible now to sort out the following new characterization of $p$-rigidity which restricts to Galois groups of finite exponent.

**Corollary 4.15.** *The field $F$ is $p$-rigid if and only if one has*

$$\mathrm{Gal}\left(F^{(2)}/F^{\{3\}}\right) \subseteq \mathrm{Z}\left(\mathrm{Gal}\left(F^{\{3\}}/F\right)\right).$$

*Proof.* Recall first that

$$\mathrm{Gal}\left(F^{\{3\}}/F\right) = \frac{G}{G^{\{3\}}} \quad \text{and} \quad \mathrm{Gal}\left(F^{(2)}/F^{\{3\}}\right) = \frac{G^{(2)}}{G^{\{3\}}}. \tag{4.7}$$

Assume that $F$ is $p$-rigid. Then by Theorem A one has $F^{\{3\}} = F^{(3)}$. By the construction of $F^{(3)}$, we see that $\mathrm{Gal}(F^{(2)}/F^{(3)}) = \mathrm{Gal}(F^{(2)}/F^{\{3\}})$ is the central subgroup of $\mathrm{Gal}(F^{\{3\}}/F)$.

Conversely, assume that $\mathrm{Gal}(F^{\{3\}}/F^{(2)})$ is central in $\mathrm{Gal}(F^{\{3\}}/F)$. By (4.7), this implies that the commutator subgroup $[G, G^{(2)}]$ is contained in $G^{\{3\}}$. Since

$$G^{\{3\}} = \Phi\left(G^{(2)}\right) \geq \left(G^{(2)}\right)^p \quad \text{and} \quad G^{(3)} = \left(G^{(2)}\right)^p \left[G, G^{(2)}\right],$$

it follows that $G^{\{3\}}$ contains $G^{(3)}$, and thus $G^{\{3\}} = G^{(3)}$. Therefore $F$ is $p$-rigid by Theorem A. □

We proved that each $p$-rigid field is hereditary $p$-rigid. In particular, if $F$ is $p$-rigid, then for each finite extension $K/F$, $K \subset F(p)$ is again $p$-rigid. Then there is a natural question of whether $F$ is $p$-rigid in the above situation when we assume that $K$ is $p$-rigid. If $\dot{F}/\dot{F}^p$ is finite, the answer is yes as we will show below, and the proof is quite a remarkable use of Serre's theorem ([Se65]) on cohomological dimension of open subgroups of pro-$p$ groups, a consequence of Bloch-Kato conjecture on cohomological dimensions, and an elementary observation on the growth of $p$-power classes.

**Theorem 4.16.** *Suppose that $F$ is any field such that $G = G_F(p)$ is a finitely generated pro-$p$ group. If there exists a finite extension $K/F$, $K \subseteq F(p)$, such that $K$ is $p$-rigid, then so is $F$.*

*Proof.* Because $G$ is finitely generated, we see that the minimal number of generators of $G$ is equal to

$$d := d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = \dim_{\mathbb{F}_p} \dot{F}/\dot{F}^p < \infty.$$

In particular, $\dot{F}/(\dot{F})^p$ is a finite group. Since $K/F$ is a finite extension in $F(p)$, from basic Galois theory and the theory of $p$-groups we see that there is a chain of extensions

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$

such that $[K_{i+1} \colon K_i] = p$ for each $i = 0, 1, \cdots, s-1$. Thus by Kummer theory, each $K_{i+1}$ is of the form $K_{i+1} = K_i(c_i^{1/p})$ for some $c_i \in \dot{K}$. Now observe by induction on $i$ that

$$\dim_{\mathbb{F}_p} \dot{F}/\dot{F}^p \leq \dim_{\mathbb{F}_p} \dot{K}_i/{\dot{K}_i}^p \leq \dim_{\mathbb{F}_p} \dot{K}/\dot{K}^p.$$

Indeed, by Kummer theory, we have a natural embedding

$$\psi_i \colon (\dot{K}_i/{\dot{K}_i}^p)/\langle [c_i]_{K_i} \rangle \to \dot{K_{i+1}}/\dot{K_{i+1}}^p$$

where $[c_i]_{K_i}$ is the element of $\dot{K_i}/\dot{K_i}^p$ corresponding to $c_i$ and $\langle [c_i]_{K_i} \rangle$ is the subgroup of $\dot{K_i}/\dot{K_i}^p$ generated by $[c_i]_{K_i}$. Hence

$$\dim_{\mathbb{F}_p} \dot{K_i}/\dot{K_i}^p \leq 1 + \dim_{\mathbb{F}_p}(\dot{K_{i+1}}/\dot{K_{i+1}}^p).$$

However, the "loss of $[c_i]_{K_i}$" is compensated by $[c_i^{1/p}]_{K_i}$. Indeed in the group $\dot{K_{i+1}}/\dot{K_{i+1}}^p$, the element $[c_i^{1/p}]_{K_i}$ is independent from the $B_i :=$ image of $\psi_i$. This means that

$$[c_i^{1/p}]_{K_i} \cap B_i = \{[1]_{K_{i+1}}\}.$$

Indeed $N_{K_{i+1}/K_i}(c_i^{1/p}) = c_i \notin \dot{K_i}^p$, but the set of all norms $N_{K_{i+1}/K_i}$ of elements in $B_i$, $N_{K_{i+1}/K_i}(B_i) = \{[1]_{K_{i+1}}\}$. Because we assume that $K$ is $p$-rigid we see that

$$e := \dim_{\mathbb{F}_p} \dot{K}/\dot{K}^p = \operatorname{cd} G_K(p).$$

But since by [Be74], Satz 3, we know that $G_F(p)$ is torsion free, we can conclude from [Se65], théorème, that

$$\operatorname{cd} G_K(p) = \operatorname{cd} G_F(p).$$

Hence we conclude that

$$d \leq e = \operatorname{cd} G_F(p).$$

On the other hand, from the Bloch-Kato conjecture (now the Rost-Voevodsky Theorem) one can conclude that (see [CEM12])

$$e := \operatorname{cd} G_F(p) \leq d.$$

Hence $e = d$ and from Corollary 3.21 we conclude that $F$ is $p$-rigid. □

4.3. **Fast solvability of algebraic equations.** Recall from the Introduction that a *non-nested root* over a field $F$ is an element $\alpha \in \bar{F}^s$ such that $\alpha = \sqrt[n]{a}$ for $a \in F$. For example, given elements $a_i, b_i \in \dot{F}$, the expression

$$\sqrt[n]{a_0 + a_1 \sqrt[n_1]{b_1} + \ldots + a_r \sqrt[n_r]{b_r}}$$

is a nested root, if $n$ and some $n_i$ are both larger than 1.

**Definition.** A polynomial $f \in F[X]$ is said to be *fast-solvable* if it is solvable by radicals (in the sense of Galois) and its splitting field over $F$ is contained in a field $L$ generated by non-nested roots, i.e.,

$$L = F\left(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\right), \quad a_i \in \dot{F}, n_i > 1.$$

Therefore, by Corollary 4.12 every irreducible polynomial in $F[X]$ with splitting field of $p$-power degree is fast-solvable for $F$ in a $p$-rigid field. On the other hand, observe that Ferrari's formula for a solution of a quartic equation makes use of nested roots. This suggests that a general quartic polynomial is not fast-solvable in spite of the name of the author of the formula. Following the suggestion of the referee we leave the reader a non-trivial problem of showing that there is no "Porsche formula" which provides a fast solution for a general quartic equation.

4.4. **Analytic pro-$p$ group and dimension subgroups.** A *$p$-adic analytic pro-$p$ group* is a $p$-adic analytic manifold which is also a group such that the group operations are given by analytic functions (see [DdSMS03, Ch. 8]). Analytic pro-$p$ groups were first introduced and studied in depth by M. Lazard [La65], and are now an object of research, both in group theory and number theory (see [dSMS00]).

Lazard found a beautiful group-theoretic characterization of $p$-adic analytic pro-$p$ group. This is the main result of the book [DdSMS03]. One variant of it is the following theorem.

**Theorem 4.17** ([DdSMS03, Chapter 8])**.** *The following statements are equivalent for a topological group $G$.*

(1) *$G$ is a compact $p$-adic analytic group.*
(2) *$G$ contains an open normal uniform pro-$p$ group of finite index.*
(3) *$G$ is a profinite group containing an open subgroup which is a pro-$p$ group of finite rank.*

Using this result and Theorem 4.16 we obtain the next theorem.

**Theorem 4.18.** *Assume that $\dim_{\mathbb{F}_p} \dot{F}/(\dot{F})^p < \infty$. Then $F$ is $p$-rigid if and only if $G_F(p)$ is a $p$-adic analytic pro-$p$ group.*

*Proof.* Assume first that $\dim_{\mathbb{F}_p} \dot{F}/(\dot{F})^p < \infty$ and $F$ is $p$-rigid. Then as we pointed out in Remark 4.13, $G$ itself is uniform and hence by previous result $G$ is $p$-adic analytic.

Assume now that $\dim_{\mathbb{F}_p} \dot{F}/(\dot{F})^p < \infty$ and $G_F(p)$ is $p$-adic analytic. Then there exists an open normal uniform subgroup $H$ of $G_F(p)$. Let $K$ be the fixed field of $H$. Then $H = G_K(p)$. Because $H$ is uniform, it is in particular powerful and by Proposition 3.8 we see that $K$ is $p$-rigid. Now by Theorem 4.16 we see that $F$ is $p$-rigid as well. □

For a (not necessarily pro-$p$) group $G$, its dimension subgroups $D_n = D_n(G)$ are defined as follows: $D_1 = G$, and for $n > 1$

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

where $\lceil n/p \rceil$ is the least integer $k$ such that $pk \geq n$. Dimension subgroups define the fastest descending series of $G$ such that $[D_i, D_j] \leq D_{i+j}$ and $D_i^p \leq D_{pi}$, for any $i, j \in \mathbb{N}^*$. Moreover, $D_n$ is the kernel of all the natural homomorphisms of $G$ into the unit group of $\kappa[G]/I^n$, i.e., $D_n \cong 1 + I^n$, where $\kappa$ is any field of characteristic $p$, and $I$ is the augmentation ideal of $\kappa[G]$ [DdSMS03, §11.1]. The following formula, due to Lazard, provides an explicit description for $D_n$ (see [DdSMS03, Theorem 11.2])

$$D_n(G) = \prod_{ip^h \geq n} \gamma_i(G)^{p^h}. \tag{4.8}$$

It is worth questioning how the dimension subgroups look when $G$ is the maximal pro-$p$ Galois group $G_F(p)$ of a $p$-rigid field $F$. This can be addressed using the following theorem.

**Theorem 4.19** ([DdSMS03, Thm. 11.4])**.** *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 $n$.*

Thus, by Corollary 3.22, the above theorem also holds for finitely generated $G_F(p)$ with $F$ a $p$-rigid field. However, in our calculation below we can assume that $G_F(p)$ is any Galois group of the maximal $p$-extension of a $p$-rigid field which is not necessarily finitely generated. Let $G = G_F(p)$ for such a field and $k \in \mathbb{N} \cup \{\infty\}$ and $\theta_F$ be as above, and set $N = \ker(\theta_F)$. Thus $N \cong \mathbb{Z}_p^{\mathcal{I}}$ as pro-$p$ subgroups – in particular, if $k = \infty$ then $N = G$. Then by (4.6) one has

$$[G, G] = N^{p^k} \quad \text{and} \quad \gamma_i(G) = N^{p^{k(i-1)}},$$

for $i > 1$. (We implicitly set $p^\infty = 0$. Thus in the case $k = \infty$, all commutators are trivial and the calculation below became very simple while still giving us the same result formally as below, independent of whether $k$ is finite or infinite.) Assume $p^{\ell-1} < n \leq p^\ell$, with $\ell \geq 1$, so that $\ell = \lceil \log_p(n) \rceil$, i.e., $\ell$ is the least integer such that $\ell \geq \log_p(n)$. Hence, by Lazard's formula (4.8), one has

$$D_n(G) = \gamma_1(G)^{p^\ell} \prod_{ip^h \geq n} \gamma_i(G)^{p^h} = G^{p^\ell} \prod_{ip^h \geq n} N^{p^{k(i-1)+h}}, \tag{4.9}$$

where $i \geq 2$.

We shall show that for every $i, h$ such that $i \geq 2$ and $ip^h \geq n$, one has the inequality

$$k(i-1) + h \geq \ell, \tag{4.10}$$

so that $N^{p^{k(i-1)+h}} \leq G^{p^\ell}$ and $D_n(G) = G^{p^\ell}$. If $h \geq \ell$, then (4.10) follows immediately. Otherwise, notice that $i > p^{\ell-h-1} \geq 1$, as $ip^h \geq n > p^{\ell-1}$, which implies

$$k(i-1) > k\left(p^{(\ell-h)-1} - 1\right). \tag{4.11}$$

Therefore, for $\ell - h \geq 2$, the inequality (4.11) implies $k(i-1) \geq \ell - h$, and thus (4.10), whereas for $\ell - h = 1$ (4.10) follows from the fact that $i \geq 2$.

Altogether, this shows that

$$D_n(G) = G^{p^\ell}, \quad \text{with } p^{\ell-1} < n \leq p^\ell,$$
$$\text{and} \quad \frac{D_n(G)}{D_{n+1}(G)} \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^{\mathcal{I}} & \text{for } n \text{ a } p\text{-power}, \\ 1 & \text{otherwise.} \end{cases}$$

## Acknowledgements

The authors thank A. Adem, D. Karagueuzian, and I. Efrat for working with the second author over the years on related topics which strongly influenced the way we think about rigidity and its unique place in Galois theory. Moreover, we thank E. Aljadeff, D. Neftin, J. Sonn, and N.D. Tan for their interest and helpful suggestions on this paper. Also the second author is grateful to J. Koenigsmann for calling his attention to Koenigsmann's paper with A. Engler that is quoted and used in our paper. We are grateful to Leslie Hallock for her passion for a proper and elegant use of English language and for her kind but forceful advice related to its use in our paper. We are also grateful to the referee for encouragement and for providing a number of valuable suggestions to improve the exposition of this paper. Last but not least, the second and third authors are very grateful to Th.S. Weigel who introduced them to each other.

## References


[AGKM01] Alejandro Adem, Wenfeng Gao, Dikran B. Karagueuzian, and Ján Mináč, *Field theory and the cohomology of some Galois groups*, J. Algebra **235** (2001), no. 2, 608–635, DOI 10.1006/jabr.2000.8481. MR1805473 (2001m:12011)

[AEJ87] Jón Kr. Arason, Richard Elman, and Bill Jacob, *Rigid elements, valuations, and realization of Witt rings*, J. Algebra **110** (1987), no. 2, 449–467, DOI 10.1016/0021-8693(87)90057-3. MR910395 (89a:11041)

[AT09] Emil Artin and John Tate, *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original. MR2467155 (2009k:11001)

[Be74] Eberhard Becker, *Euklidische Körper und euklidische Hüllen von Körpern* (German), J. Reine Angew. Math. **268/269** (1974), 41–52. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II. MR0354625 (50 #7103)

[Ca1545] G. Cardano, *Artis magnae, sive de regulis algebraicis liber unus*, Nuremberg 1545. Translated by T. Richard Witmer as Ars Magma, or the Rules of Algebra, MIT Press, 1968, reprinted, Dover Publications, 1993.

[CEM12] Sunil K. Chebolu, Ido Efrat, and Ján Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Math. Ann. **352** (2012), no. 1, 205–221, DOI 10.1007/s00208-011-0635-6. MR2885583

[dSMS00] Marcus du Sautoy, Dan Segal, and Aner Shalev (eds.), *New horizons in pro-p groups*, Progress in Mathematics, vol. 184, Birkhäuser Boston Inc., Boston, MA, 2000. MR1765115 (2001b:20001)

[DdSMS03] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999. MR1720368 (2000m:20039)

[Ef95] Ido Efrat, *Abelian subgroups of pro-2 Galois groups*, Proc. Amer. Math. Soc. **123** (1995), no. 4, 1031–1035, DOI 10.2307/2160698. MR1242081 (95e:12007)

[Ef98] Ido Efrat, *Small maximal pro-p Galois groups*, Manuscripta Math. **95** (1998), no. 2, 237–249, DOI 10.1007/s002290050026. MR1603329 (99e:12005)

[Ef99] Ido Efrat, *Construction of valuations from K-theory*, Math. Res. Lett. **6** (1999), no. 3-4, 335–343, DOI 10.4310/MRL.1999.v6.n3.a7. MR1713134 (2001i:12011)

[Ef06] Ido Efrat, *Valuations, orderings, and Milnor K-theory*, Mathematical Surveys and Monographs, vol. 124, American Mathematical Society, Providence, RI, 2006. MR2215492 (2007g:12006)

[EM11] Ido Efrat and Ján Mináč, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. **133** (2011), no. 6, 1503–1532, DOI 10.1353/ajm.2011.0041. MR2863369

[EM12] Ido Efrat and Ján Mináč, *Small Galois groups that encode valuations*, Acta Arith. **156** (2012), no. 1, 7–17, DOI 10.4064/aa156-1-2. MR2997568

[EM13] Ido Efrat and Ján Mináč, *Galois groups and cohomological functors*, Preprint, available at `arXiv:1103.1508`.

[EL72] Richard Elman and T. Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, Amer. J. Math. **94** (1972), 1155–1194. MR0314878 (47 #3427)

[EK98] Antonio José Engler and Jochen Koenigsmann, *Abelian subgroups of pro-p Galois groups*, Trans. Amer. Math. Soc. **350** (1998), no. 6, 2473–2485, DOI 10.1090/S0002-9947-98-02063-7. MR1451599 (98h:12004)

[GLMS03] Wenfeng Gao, David B. Leep, Ján Mináč, and Tara L. Smith, *Galois groups over nonrigid fields*, Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 33, Amer. Math. Soc., Providence, RI, 2003, pp. 61–77. MR2018550 (2005a:12007)

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR2266528 (2007k:16033)

[HJ95] Yoon Sung Hwang and Bill Jacob, *Brauer group analogues of results relating the Witt ring to valuations and Galois theory*, Canad. J. Math. **47** (1995), no. 3, 527–543, DOI 10.4153/CJM-1995-029-4. MR1346152 (97a:12004)

[Ja81] Bill Jacob, *On the structure of Pythagorean fields*, J. Algebra **68** (1981), no. 2, 247–267, DOI 10.1016/0021-8693(81)90263-5. MR608534 (82g:12020)

[JW89] Bill Jacob and Roger Ware, *A recursive description of the maximal pro-2 Galois group via Witt rings*, Math. Z. **200** (1989), no. 3, 379–396, DOI 10.1007/BF01215654. MR978598 (90b:11127)

[KS11] Benjamin Klopsch and Ilir Snopce, *Pro-p groups with constant generating number on open subgroups*, J. Algebra **331** (2011), 263–270, DOI 10.1016/j.jalgebra.2010.12.016. MR2774657 (2012d:20061)

[Ko95] Jochen Koenigsmann, *From p-rigid elements to valuations (with a Galois-characterization of p-adic fields),* with an appendix by Florian Pop, J. Reine Angew. Math. **465** (1995), 165–182, DOI 10.1515/crll.1995.465.165. MR1344135 (96m:12003)

[Ko01] Jochen Koenigsmann, *Solvable absolute Galois groups are metabelian*, Invent. Math. **144** (2001), no. 1, 1–22, DOI 10.1007/s002220000117. MR1821143 (2002a:12006)

[Ko03] Jochen Koenigsmann, *Encoding valuations in absolute Galois groups*, Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 33, Amer. Math. Soc., Providence, RI, 2003, pp. 107–132. MR2018554 (2004m:12012)

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003)

[La65] Michel Lazard, *Groupes analytiques p-adiques* (French), Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603. MR0209286 (35 #188)

[LS02] David B. Leep and Tara L. Smith, *Multiquadratic extensions, rigid fields and Pythagorean fields*, Bull. London Math. Soc. **34** (2002), no. 2, 140–148, DOI 10.1112/S0024609301008694. MR1874079 (2003a:11037)

[MSp96] Ján Mináč and Michel Spira, *Witt rings and Galois groups*, Ann. of Math. (2) **144** (1996), no. 1, 35–60, DOI 10.2307/2118582. MR1405942 (97i:11038)

[MS03] Ján Mináč and John Swallow, *Galois module structure of pth-power classes of extensions of degree p*, Israel J. Math. **138** (2003), 29–42, DOI 10.1007/BF02783417. MR2031948 (2004m:12008)

[MST] Ján Mináč, John Swallow, and Adam Topaz, *Galois module structure of* $(\ell^n)$*th classes of fields*, Bull. Lond. Math. Soc. **46** (2014), no. 1, 143–154, DOI 10.1112/blms/bdt082. MR3161770

[NSW] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000. MR1737196 (2000j:11168)

[Qu13] Claudio Quadrelli, *Bloch-Kato pro-p groups and locally powerful groups*, Forum Math. **26** (2014), no. 3, 793–814, DOI 10.1515/forum-2011-0069. MR3200350

[Se65] Jean-Pierre Serre, *Sur la dimension cohomologique des groupes profinis* (French), Topology **3** (1965), 413–420. MR0180619 (31 #4853)

[Se79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[SW00] Peter Symonds and Thomas Weigel, *Cohomology of p-adic analytic groups*, New horizons in pro-*p* groups, Progr. Math., vol. 184, Birkhäuser Boston, Boston, MA, 2000, pp. 349–410. MR1765127 (2001k:22025)

[Sz77] K. Szymiczek, *Quadratic forms over fields*, Dissertationes Math. (Rozprawy Mat.) **152** (1977), 63. MR0450199 (56 #8495)

[Vo11] Vladimir Voevodsky, *On motivic cohomology with* $\mathbf{Z}/l$*-coefficients*, Ann. of Math. (2) **174** (2011), no. 1, 401–438, DOI 10.4007/annals.2011.174.1.11. MR2811603 (2012j:14030)

[Wr78] Roger Ware, *When are Witt rings group rings? II*, Pacific J. Math. **76** (1978), no. 2, 541–564. MR0568320 (58 #27920)

[Wr81] Roger Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. **33** (1981), no. 6, 1338–1355, DOI 10.4153/CJM-1981-103-0. MR645230 (83i:10028)

[Wr92] Roger Ware, *Galois groups of maximal p-extensions*, Trans. Amer. Math. Soc. **333** (1992), no. 2, 721–728, DOI 10.2307/2154057. MR1061780 (92m:12008)

[We08] C. Weibel. The proof of the Bloch-Kato Conjecture. ICTP Lecture Notes Series 23 (2008), 1-28.

[We09] C. Weibel, *The norm residue isomorphism theorem*, J. Topol. **2** (2009), no. 2, 346–372, DOI 10.1112/jtopol/jtp013. MR2529300 (2011a:14039)

Department of Mathematics, Illinois State University, Campus box 4520, Normal, Illinois 61761

*E-mail address*: schebol@ilstu.edu

Department of Mathematics, University of Western Ontario, Middlesex College, London, Ontario N6A5B7, Canada

*E-mail address*: minac@uwo.ca

Dipartimento di Matematica, Università di Milano-Bicocca, Ed. U5, Via R.Cozzi 53, 20125 Milano, Italy

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