SMALL GALOIS GROUPS THAT ENCODE VALUATIONS

IDO EFRAT AND JÁN MINÁČ

ABSTRACT. Let $p$ be a prime number and let $F$ be a field containing a root of unity of order $p$. We prove that a certain relatively small canonical Galois group $(G_F)^3$ over $F$ encodes the valuations on $F$ whose value group is not $p$-divisible and which satisfy a variant of Hensel’s lemma.

1. Introduction

A repeated phenomena in Galois theory is that essential arithmetical information on a field is encoded in the group-theoretic structure of its canonical Galois groups. A prototype of this phenomena is the classical Artin–Schreier theorem: a field $F$ has an ordering if and only if its absolute Galois group $G_F = \text{Gal}(F_{\text{sep}}/F)$ contains a (non-trivial) involution.

As shown by Becker [Bec74], the same holds when $G = G_F$ is replaced by its maximal pro-$2$ quotient $G(2)$. Moreover, the second author and Spira [MS90, Th. 2.7] established a similar correspondence for an even smaller pro-$2$ Galois group of $F$, the $W$-group of $F$.

In this paper we consider a generalization of the $W$-group to the pro-$p$ context, and prove an analogous result for valuations. Here $p$ is an arbitrary fixed prime number, and we assume that $F$ contains a root of unity of order $p$ (in particular, char $F \neq p$). We set $G^{(2)} = G_p[G, G]$ and $G^{(3)} = G_{3p}[G^{(2)}, G]$, where $\delta = 1$ if $p > 2$, and $\delta = 2$ if $p = 2$. The pro-$p$ Galois group we consider is $G^{[3]} = G/G^{(3)}$. It has exponent $\delta p$, and when $p = 2$ it coincides with the $W$-group of $F$ [EM11, Remark 2.1(1)].

Of course, a field always carries the trivial valuation, so one is only interested in valuations $v$ satisfying certain natural requirements. In the pro-$p$ context, such requirements on $v$ are:

(i) $v(F^\times) \neq pv(F^\times)$;

(ii) $(F^\times)^p$-compatibility: $1 + m_v \leq (F^\times)^p$, where $1 + m_v$ is the group of $1$-units of $v$, i.e., all elements $x$ of $F$ with $v(x - 1) > 0$.

Thus (i) is a strong form of non-triviality, whereas (ii) is a variant of Hensel’s lemma. Indeed, when the residue field $F_v$ has characteristic not $p$, (ii) is

2010 Mathematics Subject Classification. Primary 12J10; Secondary 12E30.

Key words and phrases. valuations, Galois groups, Galois cohomology, Milnor $K$-theory, $W$-group, rigid elements.
equivalent to the validity of Hensel’s lemma relative to the maximal pro-$p$ extension $F(p)$ ([Wad83, Prop. 1.2], [Efr06, Prop. 18.2.4]).

Our main result (Corollary 6.4) is that, under a finiteness assumption and the hypothesis that $-1$ is a square if $p = 2$, there exists a valuation $v$ on $F$ satisfying (i) and (ii) above if and only if the center $Z(G_{[3]})$ has a nontrivial image in $G^{[2]} = G/G^{(2)}$.

Note that when char $\overline{F} \neq p$, conditions (i) and (ii) give a description of the full maximal pro-$p$ Galois group $G_F(p) = \text{Gal}(F(p)/F)$ of $F$ as a semi-direct product $\mathbb{Z}_p^m \rtimes G_{\overline{F}_v}(p)$ where $m = \dim_{\mathbb{F}_p}(v(F^\times)/pv(F^\times))$ and the action is given by the cyclotomic character [Efr06, Example 22.1.6].

The proof of the main theorem is based on two key ingredients. First, results of Villegas, Spira and the authors (see Theorems 2.1 and 2.2 below) give an explicit list $\mathcal{L}_p$ of small finite $p$-groups such that, for $G = G_F$ as above,

$$G_{[3]} = \bigcap \{N \leq G \mid G/N \in \mathcal{L}_p\}.$$

A second ingredient is the notion of $p$-rigid elements in $F$ (see §3 for the definition). In a series of works by Arason, Elman, Hwang, Jacob, Ware, and the first author (see [Jac81], [War81], [AEJ87], [HJ95], [Efr99], [Efr06, Ch. 26], [Efr07]) it was shown that there exist valuations satisfying (i) and (ii) if and only if $F$ has sufficiently many $p$-rigid elements. The dual notion in $G^{[2]}$ under the Kummer pairing can be interpreted, using certain Galois embedding problems, in terms of the groups in $\mathcal{L}_p$.

Connections between the group $G_{[3]}$ and valuations were earlier studied in [MMS04, §7–8] (for $p = 2$) and also announced in [Pop06b]. This is also related to works by Bogomolov, Tschinkel, and Pop ([Bog91], [Bog92], [BT08], [Pop06a]), showing that for function fields $F$ over algebraically closed fields, such “tame” valuations can be recovered from the larger Galois group $G/[[G, G], G]$. For a nice survey with more references see [BT10]. Some other connections between rigidity and small Galois groups were previously also investigated in [AGKM01] and [LS02], and in connection with absolute or maximal pro-$p$ Galois groups in, e.g., [Efr99], [Efr00], [EN94], and [Koc03].

Underlying our results is the fact, proved in [EM11] (extending earlier results in [CEM10]), that for $G = G_F$ with $F$ as above, $G_{[3]}$ determines the Galois cohomology ring $H^*(G, \mathbb{Z}/q)$, and is in fact the minimal Galois group of $F$ with this property.

For other works demonstrating the importance of the quotient $G_{[3]}$ in the Galois theory of algebraic number fields see, e.g., [Koc02], [Mor04], [Vog05].
2. Galois-theoretic preliminaries

We fix a prime number $p$. For $p > 2$ let

$$H_{p^3} = \langle r, s, t \mid r^p = s^p = t^p = [r, t] = [s, t] = [r, s] = 1 \rangle$$

be the nonabelian group of order $p^3$ and exponent $p$ (the Heisenberg group). Also let $D_4$ be the dihedral group of order 8. To make the discussion uniform, we set

$$(2.1) \quad \bar{G} = \begin{cases} H_{p^3} & p > 2 \\ D_4 & p = 2. \end{cases}$$

In both cases, the Frattini subgroup of $\bar{G}$ is its center $Z(\bar{G})$, and one has $\bar{G}/Z(\bar{G}) \cong (\mathbb{Z}/p)^2$. Moreover, this is the unique quotient of $\bar{G}$ isomorphic to $(\mathbb{Z}/p)^2$. Also, every proper subgroup of $\bar{G}$ is abelian.

From now on let $F$ be a field containing a fixed root of unity $\zeta_p$ of order $p$, and let $G = G_F$ be its absolute Galois group. The following theorem was proved in [EM11, Thm. D].

**Theorem 2.1.** Assume that $p > 2$. Then $G(3)$ is the intersection of all normal open subgroups $N$ of $G$ such that $G/N$ is isomorphic to $\{1\}$, $\mathbb{Z}/p$ or $H_{p^3}$.

The analog of this fact for $p = 2$ was proved by Villegas [Vil88] and Mináč–Spira [MS96, Cor. 2.18] (see also [EM08, Cor. 11.3 and Prop. 3.2]):

**Theorem 2.2.** Assume that $p = 2$. Then $G(3)$ is the intersection of all normal open subgroups $N$ of $G$ such that $G/N$ is isomorphic to $\{1\}$, $\mathbb{Z}/2$, $\mathbb{Z}/4$, or $D_4$.

Moreover, $\mathbb{Z}/2$ can be omitted from this list unless $F$ is Euclidean [EM08, Cor. 11.4].

Let $H^i(G) = H^i(G, \mathbb{Z}/p)$ be the $i$th profinite cohomology group with the trivial action of $G$ on $\mathbb{Z}/p$. Thus $H^1(G)$ is the group of all continuous homomorphisms $G \to \mathbb{Z}/p$. We write $\cup$ for the cup product $H^1(G) \times H^1(G) \to H^2(G)$. For $a \in F^\times$ let $(a)_F \in H^1(G)$ correspond to the coset $a(F^\times)^p$ under the Kummer isomorphism $F^\times/(F^\times)^p \xrightarrow{\sim} H^1(G)$. One has $(a)_F \cup (a)_F = (a)_F \cup (-1)_F$ [Ber10, Prop. III.9.15(5)].

Next for a finite group $K$, we call a Galois extension $E/F$ an $K$-extension if $\text{Gal}(E/F) \cong K$. We say that a $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$-extension $F(\sqrt{a}, \sqrt{b})/F$ embeds inside a $\bar{G}$-extension $E/F$ properly if either $p > 2$ or else $p = 2$ and $\text{Gal}(E/F(\sqrt{ab})) \cong \mathbb{Z}/4$.

We refer to [Led05, (6.1.8), (3.6.3), (3.6.2)] for the following well known facts; see also [GSS95] and [GS96].
Lemma 2.3. Let \( a, b \in F^\times \).

(a) When \((a)_F, (b)_F\) are \(\mathbb{F}_p\)-linearly independent, \(F(\sqrt[p]{a}, \sqrt[p]{b})/F\) embeds inside a \(G\)-extension properly if and only if \((a)_F \cup (b)_F = 0\).

(b) When \(p = 2\) and \((a)_F \neq 0\), the extension \(F(\sqrt{a})/F\) embeds inside a \(\mathbb{Z}/4\)-extension if and only if \((a)_F \cup (-1)_F = 0\).

3. Rigidity

The following key notion is a special case of [Efr06, Def. 23.3.1] and originates from [Szy77] and [War81]. Note however that our definition differs by sign from that of [War81].

Definition 3.1. An element \(a\) of \(F^\times\) is called \(p\)-rigid if \((a)_F \neq 0\) and there is no \(b \in F^\times\) such that \((a)_F \cup (b)_F = 0\) in \(H^2(G)\) and \((a)_F, (b)_F\) are \(\mathbb{F}_p\)-linearly independent.

To get an alternative description of \(p\)-rigid elements, we define subsets \(C, D\) of \(F^\times\) as follow.

When \((-1)_F = 0\) (resp., \((-1)_F \neq 0\)) let \(C\) be the set of all \(a \in F^\times\) for which there exists \(b \in F^\times\) such that \((a)_F \cup (b)_F = 0\) and \((a)_F, (b)_F\) (resp., \((a)_F, (b)_F, (-1)_F\)) are \(\mathbb{F}_p\)-linearly independent in \(H^1(G)\).

When \((-1)_F \neq 0\) (so \(p = 2\)) we set

\[
D = \{a \in F^\times \mid (a)_F \cup (-1)_F = 0\}.
\]

It is the subgroup of \(F^\times\).

Lemma 3.2. Let \(a \in F^\times\) such that \((a)_F \neq 0, (-1)_F\). The following conditions are equivalent:

(a) \(a\) is not \(p\)-rigid;

(b) either \(a \in C\) or both \((-1)_F \neq 0\) and \(a \in D\);

Proof. When \((-1)_F = 0\) this is immediate.

Next assume that \((a)_F \cup (-1)_F \neq 0\). Then \((-1)_F \neq 0, p = 2\) and \((a)_F \cup (a)_F \neq 0\). Thus, if \(b \in F^\times\) satisfies \((a)_F \cup (b)_F = 0\), then \((b)_F \neq (-1)_F, (a)_F\). Therefore \((-a)_F, (b)_F\) are \(\mathbb{F}_2\)-linearly independent if and only if \((a)_F, (b)_F, (-1)_F\) are \(\mathbb{F}_2\)-linearly independent. Conclude that in this case \(a\) is not 2-rigid if and only if \(a \in C\).

Finally, assume that \((-1)_F \neq 0\) but \((a)_F \cup (-1)_F = 0\) (i.e., \(a \in D\)). Then \(p = 2\) and, by the assumptions, \((-a)_F, (-1)_F\) are \(\mathbb{F}_2\)-linearly independent. Hence \(a\) is not 2-rigid.

Next let \(N_p\) be the subgroup of \(F^\times\) generated by all elements which are not \(p\)-rigid and by \(-1\).
We will need the following result of Berman and Cordes which simplifies the definition in the case \( p = 2 \) (see [War81, Example 2.5(i)], [Mar80, Ch. 5, Th. 5.18], and the related result [BCW80, Th. 1]):

**Proposition 3.3.** Let \( p = 2 \). Then \( N_2 \) is the set of all \( a \in F^\times \) such that \( a \) or \(-a\) is not \( 2\)-rigid.

**Corollary 3.4.** One of the following holds:

1. \( N_p = \langle (F^\times)^p, C, -1 \rangle \);
2. \( p = 2, \) \(-1\) is not \( p\)-rigid and \( N_2 = \langle D, -1 \rangle \).

**Proof.** If \((-1)_F = 0\), then (1) holds by Lemma 3.2.

Next suppose that \((-1)_F \neq 0\) (so \( p = 2 \)). By Lemma 3.2, \( a \in F^\times \setminus ((F^\times)^2 \cup -(F^\times)^2) \) is not \( 2\)-rigid if and only if it is in \( C \cup D \). Hence the subgroups \( \langle (F^\times)^2, C, -1 \rangle \) and \( \langle D, -1 \rangle \) of \( F^\times \) are contained in \( N_2 \). Conversely, by Proposition 3.3, \( N_2 \) is contained in the union of these two subgroups. Thus

\[
N_2 = \langle (F^\times)^2, C, -1 \rangle \cup \langle D, -1 \rangle.
\]

Since a group cannot be the union of two proper subgroups, (1) or (2) must hold. \( \square \)

**Remark 3.5.** Let \( K^*_M(F) \) be the Milnor \( K\)-ring of \( F \) ([Mil70], [Efr06, §24]). The Kummer isomorphism \( F^\times/(F^\times)^p \tilde\to H^1(G_F, a(F^\times)_F) \mapsto (a)_F \), induces the Galois symbol homomorphism \( K^*_M(F)/pK^*_M(F) \to H^*(G_F) \). By the Merkurjev–Suslin theorem ([MS82], [GS06, Ch. 8]), it is an isomorphism in degree 2 (in fact, by the more recent results of Rost and Voevodsky [Voe11], it is an isomorphism in all degrees, but we shall not need this very deep fact). Therefore, our notion of a \( p\)-rigid element \( a \) coincides with the notion of \( (F^\times)^p\)-rigidity of \( a(F^\times)^p \) in \( K^*_M(F)/pK^*_M(F) \) given in [Efr06, Def. 23.3.1]. Consequently \( N_p \) coincides with the subgroup \( N_{(F^\times)^p} \), defined \( K\)-theoretically in [Efr06, Def. 26.4.5].

4. **The Kummer pairing**

Let \( \mu_p \) be the group of \( p\)th roots of unity in \( F \) and recall that \( G = G_F \) is the absolute Galois group of \( F \). Consider the Kummer pairing

\[
(\cdot, \cdot) : \quad G \times F^\times \to \mu_p, \quad (\sigma, a) \mapsto \sigma(\sqrt[p]{a})/\sqrt[p]{a}.
\]

Its left kernel is \( G^{(2)} \) and its right kernel is \( (F^\times)^p \). We compute the annihilator of \( N_p \) under this pairing.

Let \( T = \bigcap_p \rho^{-1}(2\mathbb{Z}/4\mathbb{Z}) \), where \( \rho \) ranges over all epimorphisms \( \rho : G \to \mathbb{Z}/4 \), and \( 2\mathbb{Z}/4\mathbb{Z} \) is the subgroup of \( \mathbb{Z}/4 \) of order 2.
Lemma 4.1. Assume that \((-1)_F \neq 0\). The annihilator of \(D\) with respect to the Kummer pairing is \(T\).

Proof. Let \(\sigma \in G\). Then \(\sigma \in T\) if and only if \(\sigma\) fixes \(\sqrt{a}\) for every \(a \in F^\times \setminus (F^\times)^2\) such that \(F(\sqrt{a})/F\) embeds inside a \(\mathbb{Z}/4\)-extension of \(F\). By Lemma 2.3(b), this means that \((\sigma, a) = 1\) whenever \((a)_F \cup (-1)_F = 0\), i.e., whenever \(a \in D\).

We define a subgroup \(\tilde{G}\) of \(G\) by \(\tilde{G} = G\) if \(p > 2\), and \(\tilde{G} = G_{F(\sqrt{-1})}\) when \(p = 2\). Thus \(\tilde{G} = G\) when \((-1)_F = 0\). Also let \(\tilde{G}\) be as in (2.1).

Proposition 4.2. The following conditions on \(\sigma \in \tilde{G}\) are equivalent:

(a) for every \(\tau \in \tilde{G}\) the commutator \([\sigma, \tau]\) is in \(G_{(3)}\);
(b) for every \(\tau \in \tilde{G}\) and every \(\tilde{G}\)-extension \(L\) of \(F\), the restrictions \(\sigma|_L, \tau|_L\) commute;
(c) \((\sigma, a) = 1\) for every \(a \in C\).

Proof. (a)\(\Leftrightarrow\)(b): Let \(\tau \in \tilde{G}\). By Theorem 2.1 and Theorem 2.2, \([\sigma, \tau] \in G_{(3)}\) if and only if \(\sigma|_L, \tau|_L\) commute in \(\text{Gal}(L/F)\) for every Galois extension \(L/F\) with Galois group in \(\{1, \mathbb{Z}/p, H_{p^3}\}\), when \(p > 2\), or in \(\{1, \mathbb{Z}/2, \mathbb{Z}/4, D_4\}\), when \(p = 2\). When \(\text{Gal}(L/F)\) is abelian, the commutativity is trivial, so it is enough to consider \(\tilde{G}\)-extensions \(L/F\).

(b)\(\Rightarrow\)(c): Let \(a \in C\) and take \(b \in F^\times\) as in the definition of \(C\). Then when \((-1)_F = 0\) (resp., \((-1)_F \neq 0\)) the Kummer elements \((a)_F, (b)_F\) (resp., \((a)_F, (b)_F, (-1)_F\)) are \(\mathbb{F}_p\)-linearly independent. Hence there exists \(\tau \in \tilde{G}\) such that \(\tau(\sqrt{a}) = \sqrt{a}\) and \(\tau(\sqrt{b}) \neq \sqrt{b}\). Moreover, \((a)_F \cup (b)_F = 0\), so Lemma 2.3(a) yields a \(\tilde{G}\)-extension \(L/F\) with \(F(\sqrt{a}, \sqrt{b}) \subseteq L\). By assumption, the restrictions \(\sigma|_L, \tau|_L\) commute. But \(G\) is non-commutative, so these restrictions belong to a proper subgroup of \(\text{Gal}(L/F)\). By the Frattini argument, their restrictions \(\sigma_1, \tau_1\) to \(\text{Gal}(F(\sqrt{a}, \sqrt{b})/F) \cong (\mathbb{Z}/p)^2\) belong to a proper subgroup, which is necessarily cyclic of order \(p\). Thus \(\sigma_1 \in \langle \tau_1 \rangle\), whence \(\sigma(\sqrt{a}) = \sigma_1(\sqrt{a}) = \sqrt{a}\), as desired.

(c)\(\Rightarrow\)(b): Let \(\tau \in \tilde{G}\) and let \(L\) be a \(\tilde{G}\)-extension of \(F\). Take \(a, b \in F^\times\) such that \(L_0 = F(\sqrt{a}, \sqrt{b})\) is a \((\mathbb{Z}/p)^2\)-extension of \(F\) which embeds properly in \(L\). By Lemma 2.3(a), \((a)_F \cup (b)_F = 0\). In view of the structure of \(\tilde{G}\), the center \(Z(\text{Gal}(L/F))\) is \(\text{Gal}(L/L_0)\).

Case 1: \(\sigma|_{L_0}, \tau|_{L_0}\) do not generate \(\text{Gal}(L_0/F)\). Then \(\sigma|_L, \tau|_L\) generate a proper subgroup of \(\text{Gal}(L/F) \cong \tilde{G}\), which is necessary commutative. Thus \(\sigma|_L, \tau|_L\) commute, as required.
Case 2: \(a, b \in C\). By assumption, \((\sigma, a) = (\sigma, b) = 1\). Therefore \(\sigma|_L \in \text{Gal}(L/L_0) = Z(\text{Gal}(L/F))\), and we are done again.

Case 3: \(\sigma|_{L_0}, \tau|_{L_0}\) generate \(\text{Gal}(L_0/F)\) and at least one of \(a, b\) is not in \(C\). By construction, \((a)_F, (b)_F\) are \(\mathbb{F}_2\)-linearly independent. Hence necessarily \((-1)_F \neq 0, p = 2,\) and \((a)_F, (b)_F, (-1)_F\) are \(\mathbb{F}_2\)-linearly dependent. Without loss of generality, \((a)_F \neq (-1)_F\). We obtain that

\[
\text{Gal}(L/F(\sqrt{a}, \sqrt{-1})) = \text{Gal}(L/L_0) = Z(\text{Gal}(L/F)).
\]

If \(\sigma(\sqrt{a}) = \sqrt{a}\), then \((\sigma|_L) = Z(\text{Gal}(L/F)).\)

Similarly, if \(\tau(\sqrt{a}) = \sqrt{a}\), then \(\tau|_L \in Z(\text{Gal}(L/F))\), and in both cases we are done.

Finally, if \(\sigma(\sqrt{a}) = \tau(\sqrt{a}) = -\sqrt{a}\), then \(\sigma, \tau\) coincide on \(F(\sqrt{a}, \sqrt{-1}) = L_0\). Hence \(\sigma|_L, \tau|_L\) generate a proper subgroup of \(\text{Gal}(L/F) \cong \tilde{G}\), which is necessarily abelian. Therefore they commute. \(\square\)

Corollary 4.3. The annihilator of \(N_p\) in \(G\) with respect to the Kummer pairing is

\[
\tilde{Z} = \begin{cases} \{T \cap \tilde{G} \mid \forall \tau \in \tilde{G} : [\sigma, \tau] \in G^{(3)}\} & \text{if } (-1)_F \neq 0 \text{ and } N_2 = \langle D, -1 \rangle \\ \{\sigma \in \tilde{G}\} & \text{otherwise.} \end{cases}
\]

Proof. First we note that, since \(-1 \in N_p\), the annihilator of \(N_p\) is contained in \(\tilde{G}\). Now in case (1) (resp., (2)) of Corollary 3.4, the assertion follows from Proposition 4.2 (resp., Lemma 4.1). \(\square\)

Next let \(\tilde{Z}\) be the image of \(\tilde{Z}\) under the natural projection \(G \to G^{[2]} = G/G^{(2)}\). Then \(Z \cong \tilde{Z}/(G^{(2)} \cap \tilde{Z})\). Note that if \((-1)_F = 0\), then \(Z\) is just the image of \(Z(G^{(3)})\) in \(G^{[2]}\).

Corollary 4.4. The Kummer pairing induces a perfect pairing

\[
Z \times (F^\times/N_p) \to \mu_p.
\]

Proof. The Kummer pairing induces a perfect pairing

\[
G^{[2]} \times (F^\times/(F^\times)^p) \to \mu_p.
\]

By Corollary 4.3 the annihilator of \(N_p/(F^\times)^p\) is \(\tilde{Z}\). The assertion now follows from general Pontrjagin duality theory. \(\square\)
5. Rigid fields

The field $F$ is called $p$-rigid if all $a \in F^\times \setminus (F^\times)^p$ are $p$-rigid. The next result applies Corollary 4.4 to characterize these fields in terms of $G_{[3]}$. For $p > 2$ the equivalence $(a) \iff (e)$ was proved in [MN77, Th. 14]; see also [War92]. For $p = 2$ the equivalences $(a) \iff (c) \iff (d)$ where earlier proved in [MS90, Th. 3.13].

Theorem 5.1. Assume that $(-1)_F = 0$. The following conditions are equivalent:

(a) $F$ is $p$-rigid;
(b) $N_p = (F^\times)^p$;
(c) $G_{[3]}$ is abelian;
(d) When $p > 2$ (resp., $p = 2$), $G_{[3]} \cong (\mathbb{Z}/p)^I$ (resp., $G_{[3]} \cong (\mathbb{Z}/4)^I$) for some index set $I$;
(e) $F$ has no $\bar{G}$-extensions.

Proof. (a)$\iff$(b): Immediate.

(b)$\iff$(c): By Corollary 4.4, $N_p = (F^\times)^p$ if and only if $\bar{Z} \cong G^{[2]}$, i.e., the natural map $G_{[3]} \rightarrow G^{[2]}$ maps $Z(G_{[3]})$ surjectively. By the Frattini argument, this means that $G_{[3]} = Z(G_{[3]})$.

(c)$\Rightarrow$(d): When $p > 2$, we use that abelian profinite groups of exponent dividing $p$ always have the form $(\mathbb{Z}/p)^I$. Similarly, when $p = 2$ the group $G_{[3]}$ has exponent dividing 4, and by assumption is abelian. Moreover, since $(-1)_F = 0$, every $\mathbb{Z}/2$-extension embeds in a $\mathbb{Z}/4$-extension (Lemma 2.3(b)). Hence $G_{[3]}$ has the form $(\mathbb{Z}/4)^I$.

(d)$\Rightarrow$(c)$\Rightarrow$(e): Immediate.

(e)$\Rightarrow$(c): Use Theorem 2.1 (when $p > 2$) and Theorem 2.2 (when $p = 2$). \hfill $\Box$

Remark 5.2. An analogous result was proved in [EM08, Prop. 12.1 and Prop. 3.2] for the larger quotient $G/G^{(3)}$, where $G^{(3)} = (G^{(2)})^p[G^{(2)}, G]$ is the third subgroup in the descending $p$-central filtration of $G = G_F$: namely, when $p > 2$ (resp., $p = 2$) $G/G^{(3)}$ is abelian if and only if $F$ has no Galois extensions with Galois group $M_{p^3}$ (resp., $D_4$), where $M_{p^3}$ denotes the unique nonabelian group of odd order $p^3$ and exponent $p^2$. Note that indeed $G^{(3)} = G_{[3]}$ for $p = 2$, by [EM11, Remark 2.1(1)].
6. Valuations

Throughout this section we assume that \((-1)^{F} = 0\). As we mentioned earlier, existence of \((F^{\times})^p\)-compatible valuations \(v\) with \(v(F^{\times}) \neq pv(F^{\times})\) is related to \(p\)-rigid elements, and therefore to the group \(N_p\). Further, \(F^{\times}/N_p\) is dual to the image \(\tilde{Z}\) of \(Z(G^{[3]})\) in \(G^{[2]}\) (Corollary 4.4). Thus we can now detect these valuations from our Galois group \(G^{[3]}\) under some finiteness conditions discussed below.

Denote the exterior (graded) algebra of an \(R\)-module \(M\) by \(\bigwedge_{R}^* M\). There is a canonical graded ring epimorphism \(\bigwedge_{F_p}^*(F^{\times}/(F^{\times})^p) \rightarrow K^M_*(F)/pK^M_*(F)\).

We say that \((F^{\times})^p\) is totally rigid if this map is an isomorphism (see \[Efr06, \S 26.3 and Example 23.2.4\]).

Example 6.1. Suppose that \(F\) is equipped with an \((F^{\times})^p\)-compatible valuation \(v\) such that \(\bar{F}^{\times} = (\bar{F}^{\times})^p\) and such that the induced map \(F^{\times}/pv(F^{\times}) \rightarrow 0[v(F^{\times})/pv(F^{\times})]\) as graded rings \[Efr06, Example 23.2.4\]. Further, there is a natural isomorphism \(K^M_*(F)/pK^M_*(F) \rightarrow 0[v(F^{\times})/pv(F^{\times})]\) \[Efr06, Th. 26.1.2 and Example 26.1.1(2)\]. Hence \((F^{\times})^p\) is totally rigid. See also \[Efr06, \S 26.8\].

For a valuation \(v\) on \(F\) let \(\bar{F}_v\) be its residue field, and let \(O_v^{\times}\) be its group of \(v\)-units. We will need the following special cases of \[Efr06, Prop. 26.5.1, Th. 26.5.5(c), Th. 26.6.1\], respectively:

Proposition 6.2. (a) If \(v\) is an \((F^{\times})^p\)-compatible valuation on \(F\), then \(N_p \leq (F^{\times})^pO_v^{\times}\).

(b) If \((F^{\times})^p\) is not totally rigid, and either \(p = 2\) or \((F^{\times} : (F^{\times})^p) < \infty\), then there exists an \((F^{\times})^p\)-compatible valuation \(v\) on \(F\) with \(N_p = (F^{\times})^pO_v^{\times}\).

(c) If \((F^{\times})^p\) is totally rigid, then there exists an \((F^{\times})^p\)-compatible valuation \(v\) on \(F\) with \(((F^{\times})^pO_v^{\times} : N_p)/p\).

We obtain our main result:

Theorem 6.3. (a) If \(v\) is an \((F^{\times})^p\)-compatible valuation on \(F\), then \(v(F^{\times})/pv(F^{\times})\) is a quotient of the Pontrjagin dual \(\bar{Z}^{\times}\).
(b) Assume that \((F^\times)^p\) is not totally rigid, and that \(p = 2\) or \((F^\times : (F^\times)^p) < \infty\). Then there exists an \((F^\times)^p\)-compatible valuation \(v\) on \(F\) with \(v(F^\times)/pv(F^\times) \cong \hat{\mathbb{Z}}^v\).

(c) Assume that \((F^\times)^p\) is totally rigid. There exists an \((F^\times)^p\)-compatible valuation \(v\) on \(F\) and an epimorphism \(\hat{\mathbb{Z}}^v \to v(F^\times)/pv(F^\times)\) with kernel of order dividing \(p\).

Proof. By Corollary 4.4, \(\hat{\mathbb{Z}}^v \cong F^\times/N_p\). Every valuation \(v\) on \(F\) induces an isomorphism \(F^\times/(F^\times)^pO^\times_v \cong v(F^\times)/pv(F^\times)\). Now use Proposition 6.2 \(\square\)

From parts (a) and (b) we deduce:

**Corollary 6.4.** Assume that \((F^\times)^p\) is not totally rigid, and that \(p = 2\) or \((F^\times : (F^\times)^p) < \infty\). Then there exists an \((F^\times)^p\)-compatible valuation \(v\) on \(F\) with \(v(F^\times) \neq pv(F^\times)\) if and only if \(\hat{\mathbb{Z}} \neq \{1\}\).

**Remark 6.5.** The finiteness assumption for \(p \neq 2\) in Proposition 6.2(b) (and therefore in Theorem 6.3 and Corollary 6.4) originates from the chain argument in the proof of [Efr06, Prop. 26.5.4]. It is currently not known whether this assumption in Proposition 6.2(b) is actually necessary.

**Acknowledgements.** The first author was supported by the Israel Science Foundation (grant No. 23/09). The second author was supported in part by National Sciences and Engineering Council of Canada grant R0370A01. We also acknowledge the referee’s suggestions which we use in our exposition.

**References**

[AGKM01] A. Adem, W. Gao, D.B. Karagueuzian and J. Mináč, *Field theory and the cohomology of some Galois groups*, J. Algebra 235 (2001), 608–635.

[AEJ87] J.Kr. Arason, R. Elman and B. Jacob, *Rigid elements, valuations, and realization of Witt rings*, J. Algebra 110 (1987), 449–467.

[Bec74] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. reine angew. Math. 268/269 (1974), 41–52.

[Ber10] G. Berhuy, *An Introduction to Galois Cohomology and its Applications*, London Mathematical Society Lecture Notes, Vol. 377 (2010), Cambridge University Press, Cambridge.

[BCW80] L. Berman, C. Cordes, and R. Ware, *Quadratic forms, rigid elements, and power series fields*, J. Algebra 66 (1980), 123–133.

[Bog91] F.A. Bogomolov, *On two conjectures in birational algebraic geometry*, in: Algebraic Geometry and Analytic Geometry (Tokyo, 1990), ICM-90 Satell. Conf. Proc., Springer, Tokyo, 1991, 26–52.
[Bog92] F.A. Bogomolov, *Abelian subgroups of Galois groups*, Izv. Akad. Nauk SSSR Ser. Mat. 55 (1991), 32–67 (in Russian); English transl.: Math. USSR, Izv. 38 (1992), 27–67.

[BT08] F. Bogomolov and Y. Tschinkel, *Reconstruction of function fields*, Geom. Func. Anal. 18 (2008), 400–462.

[BT10] F. Bogomolov and Y. Tschinkel, *Introduction to birational anabelian geometry* (2010), preprint, available at arXiv:1011.0883v1

[CEM10] S.K. Chebolu, I. Efrat and J. Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology* (2010), to appear in Math. Ann., DOI: 10.1007/s00208-011-0635-6.

[Efr95] I. Efrat, *A Galois-theoretic characterization of p-adically closed fields*, Israel J. Math. 91 (1995), 273–284.

[Efr99] I. Efrat, *Construction of valuations from K-theory*, Math. Res. Lett. 6 (1999), 335–343.

[Efr00] I. Efrat, *The local correspondence over absolute fields: an algebraic approach*, Internat. Math. Res. Notices (2000), no. 23, 1213–1223.

[Efr06] I. Efrat, *Valuations, Orderings, and Milnor K-Theory*, Mathematical Surveys and Monographs 124, Amer. Math. Soc., Providence, RI, 2006.

[Efr07] I. Efrat, *Compatible valuations and generalized Milnor K-Theory*, Trans. Amer. Math. Soc. 359 (2007), 4695–4709.

[EM08] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups* (2008), Amer. J. Math. 133 (2011), 1503–1532.

[EM11] I. Efrat and J. Mináč, *Galois groups and cohomological functors* (2011), preprint, available at arXiv:1103.1508v1.

[EN94] A.J. Engler and J.B. Nogueira, *Maximal abelian normal subgroups of Galois pro-2-groups*, J. Algebra 166 (1994), 481–505.

[GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, Cambridge, 2006.

[GS96] H.G. Grundman and T.L. Smith, *Automatic realizability of Galois groups of order 16*, Proc. Amer. Math. Soc. 124 (1996), 2631–2640.

[GSS95] H.G. Grundman, T.L. Smith and J.R. Swallow, *Groups of order 16 as Galois groups*, Expo. Math. 13 (1995), 289–319.

[HJ95] Y.S. Hwang and B. Jacob, *Brauer group analogues of results relating the Witt ring to valuations and Galois theory*, Canad. J. Math. 47 (1995), 527–543.
I. EFRAT AND J. MINÁČ

[Bac81] B. Jacob, *On the structure of Pythagorean fields*, J. Algebra 68 (1981), 247–267.

[Koc02] H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin 2002.

[Koe03] J. Koenigsmann, *Encoding valuations in absolute Galois groups*, in: Valuation Theory and its Applications, Part II, Conference on Valuation Theory (University of Saskatchewan, 1999), F.-V. Kuhlmann et al. (eds.), Fields Institute Communications, Vol. 33, Amer. Math. Soc., Providence, RI, 2003, 107–132.

[Led05] A. Ledet, *Brauer Type Embedding Problems*, Fields Institute Monographs, Vol. 21, Amer. Math. Soc., Providence, RI, 2005.

[LS02] D.B. Leep and T.L. Smith, *Multiquadratic extensions, rigid fields and Pythagorean fields*, Bull. London Math. Soc. 34 (2002), 140–148.

[MMS04] L. Mahé, J. Mináč and T.L. Smith, *Additive structure of multiplicative subgroups of fields and Galois theory*, Doc. Math. 9 (2004), 301–355.

[Mar80] M. Marshall, *Abstract Witt rings*, Queen’s Papers in Pure and Applied Mathematics, Vol. 57, Queen’s University, Kingston, Ont., 1980.

[MN77] R. Massy and T. Nguyen-quang-do, *Plongement d’une extension de degré $p^2$ dans une surextension non abélienne de degré $p^3$: étude locale-globale*, J. reine angew. Math. 291 (1977), 149–161.

[MS82] A.S. Merkurjev and A.A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), 1011–1046 (in Russian); English transl.: Math. USSR Izv. 21 (1983), 307–340.

[Mil70] J. Milnor, *Algebraic K-theory and quadratic forms*, Invent. Math. 9 (1969/1970), 318–344.

[MS90] J. Mináč M. Spira, *Formally real fields, Pythagorean fields, C-fields and W-groups*, Math. Z. (205) (1990), 519–530.

[MS96] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. Math. 144 (1996), 35–60.

[Mor04] M. Morishita, *Milnor invariants and Massey products for prime numbers*, Compositio Math. 140 (2004), 69–83.

[Pop06a] F. Pop, *Almost commuting elements in small Galois groups*, Abstract in Mathematisches Forschungsinstitut Oberwolfach report 25/2006, “Pro-p Extensions of Global Fields and pro-p Groups”.
[Pop06b] F. Pop, *Galois theory of Zariski prime divisors*, in: “Groupes de Galois arithmétiques et différentiels, D. Bertrand et al. (eds.), Séminaires et Congrès, Vol. 1 (2006), Soc. Math. de France, 293–312.

[Szy77] K. Szymiczek, *Quadratic forms over fields*, Dissert. Math. Rozprawy Mat. 52 (1977).

[Vil88] F.R. Villegas, *Relations between quadratic forms and certain Galois extensions*, a manuscript, Ohio State University, 1988, [http://www.math.utexas.edu/users/villegas/osu.pdf](http://www.math.utexas.edu/users/villegas/osu.pdf).

[Voe11] V. Voevodsky, *On motivic cohomology with Z/l-coefficients*, Ann. Math. 174 (2011), 401–438.

[Vog05] D. Vogel, *On the Galois group of 2-extensions with restricted ramification*, J. reine angew. Math. 581 (2005), 117–150.

[Wad83] A.R. Wadsworth, *p-Henselian field: K-theory, Galois cohomology, and graded Witt rings*, Pacific J. Math. 105 (1983), 473–496.

[War81] R. Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. 33 (1981), 1338–1355.

[War92] R. Ware, *Galois groups of maximal p-extensions*, Trans. Amer. Math. Soc. 333 (1992), 721–728.

Mathematics Department, Ben-Gurion University of the Negev, P.O. Box 653, Be’er-Sheva 84105, Israel
E-mail address: efrat@math.bgu.ac.il

Mathematics Department, University of Western Ontario, London, Ontario, Canada N6A 5B7
E-mail address: minac@uwo.ca