JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

MASAKAZU YAMAGISHI

A note on free pro-p-extensions of algebraic number fields

Journal de Théorie des Nombres de Bordeaux, tome 5, n° 1 (1993), p. 165-178

<http://www.numdam.org/item?id=JTNB_1993__5_1_165_0>

Journal de Théorie des Nombres
de Bordeaux **5** *(1993), 165–178*

A note on free pro-p-extensions of algebraic number fields

par MASAKAZU YAMAGISHI

ABSTRACT. For an algebraic number field k and a prime p, define the number ρ to be the maximal number d such that there exists a Galois extension of k whose Galois group is a free pro-p-group of rank d. The Leopoldt conjecture implies $1 \leq \rho \leq r_2 + 1$, (r_2 denotes the number of complex places of k). Some examples of k and p with $\rho = r_2 + 1$ have been known so far. In this note, the invariant ρ is studied, and among other things some examples with $\rho < r_2 + 1$ are given.

Introduction

In this note we shall consider free pro-p-extensions (i.e. Galois extensions whose Galois groups are free pro-p-groups) of algebraic number fields. This is a natural generalization of $\mathbb{Z}_p$-extensions since $\mathbb{Z}_p$ is a free pro-p-group of rank one. It would be of interest to generalize some deep results in Iwasawa's theory on $\mathbb{Z}_p$-extensions to the case of free pro-p-extensions of arbitrary ranks. (For local fields, some results have been obtained by T. Nguyen Quang Do [11, §8].)

Our guiding problem in this note, however, is to determine the *maximal rank* ρ of free pro-p Galois groups over a fixed algebraic number field k for a fixed prime p. If the Leopoldt conjecture is true for k and p, then by class field theory we have $\rho \leq r_2 + 1$, where r_2 denotes the number of complex places of k (cf. (1.5) below). Some examples of k and p for which the equality $\rho = r_2 + 1$ hold are known. The main results of this note are the following:

(1) We shall prove $\rho \leq r_2 + 1$ under the assumption that the "weak Leopoldt conjecture" is true for all $\mathbb{Z}_p$-extensions of k (Proposition 3.5).
(2) If p is odd, k contains a primitive p-th root of unity, and if there exists

Mots-clés : Algebraic number field, $\mathbb{Z}_p$-extension, free pro-p-group.
Manuscrit reçu le 22 septembre 1992, version définitive le 31 juillet 1993.

a prime v_0 of k which does not decompose at all in the maximal pro-p-extension of k unramified outside p, then ρ is explicitly given by

$$\rho = r_2 + 1 - \frac{1}{2} \sum_{\substack{v|p \\ v \neq v_0}} [k_v : \mathbb{Q}_p],$$

where k_v denotes the completion of k at v. This is a special case of Corollary 4.6. Using this formula, we shall give examples of k and p such that $\rho < r_2 + 1$ is a *strict inequality.*

For the proof of (2), we use K. Wingberg's "free product decomposition" of Galois groups ([20], [21]).

The assumption of the existence of v_0 in (2) seems quite strong. For example this implies the validity of the Leopoldt conjecture for k and p. We think that we are far from the complete determination of ρ in general.

Acknowledgement. The author wishes to express his hearty thanks to Professor Shōichi Nakajima, under whose guidance this work was done, to Professor Mamoru Asada for the proof of Lemma 2.1, and to other members of the Number Theory Seminar at Komaba, Tokyo, especially to Professor Kenkichi Iwasawa, for valuable advice and comments. The author is also grateful to the referee for useful comments on the bibliography.

1. Formulation of the problem

Free pro-p-groups (cf. [15]). Let p be a prime, which will be fixed throughout this note. For any set I of indices, the free pro-p-group $F(I)$ generated by $\{x_i\}_{i \in I}$ is defined ([15, I-1.5]), and $F(I) \cong F(J)$ if and only if $\sharp I = \sharp J$, ($\sharp$ denotes the cardinality of a set). The cardinality of I is called the *rank* of $F(I)$, which we denote by $\mathrm{rk}(F(I))$. (For a general pro-p-group G, $\mathrm{rk}(G)$ is defined to be the cardinality of a minimal generating subset of G. This is equal to $\dim_{\mathbb{Z}/p\mathbb{Z}} H^1(G, \mathbb{Z}/p\mathbb{Z})$, cf. [15, I-4.2].) In all cases of interest to us, the rank will be finite. We shall write F_d instead of $F(I)$ when $d = \sharp I$ is finite. In particular, $F_1 = \mathbb{Z}_p$ (the additive group of p-adic integers).

As in the case of abstract free groups, any closed subgroup of a free pro-p-group is again free ([15, I-37, Cor. 3]). Furthermore, let F be a free pro-p-group of finite rank and U be an open subgroup of F. Then U is also of finite rank, which is given by Schreier's formula, (cf. [15, I-38]):

$$\mathrm{rk}(U) - 1 = [F : U](\mathrm{rk}(F) - 1). \tag{1.1}$$

F_d-extensions. By a G-extension, where G is a profinite group, we mean a Galois field extension whose Galois group is isomorphic to G as a topological group. As a generalization of $\mathbb{Z}_p$-extensions ([4]), we consider F_d-extensions, and we introduce the following invariant: for a field k and a prime p, define

$$\rho_p(k) := \sup\{d \geq 0 \ ; \ k \text{ has an } F_d\text{-extension}\}. \tag{1.2}$$

We shall write ρ instead of $\rho_p(k)$ if the reference to k and p is clear from the context.

Examples.
(1) If k is a finite field, then $\rho_p(k) = 1$ for all p.
(2) If k is a local number field, then we can give an explicit formula for $\rho_p(k)$. See Proposition 4.9 below.

Leopoldt conjecture. From now on, let k be an algebraic number field (i.e. a finite extension of the rational number field $\mathbb{Q}$). Let us recall the Leopoldt conjecture (cf. [4, 2.3]). Embed the group of global units E of k diagonally into the direct product $\prod_{v|p} U_v$, where U_v denotes the group of local units of the completion k_v of k at v, and let $\overline{E}$ be the closure of the image of E with respect to the natural topology on $\prod_{v|p} U_v$. Define the non-negative integer $\delta_p(k)$ as

$$\begin{aligned} \delta_p(k) &:= \mathrm{rk}_{\mathbb{Z}} E - \mathrm{rk}_{\mathbb{Z}_p} \overline{E} \\ &:= \dim_{\mathbb{Q}}(E \otimes \mathbb{Q}) - \dim_{\mathbb{Q}_p}(\overline{E} \otimes \mathbb{Q}_p). \end{aligned} \tag{1.3}$$

Then the Leopoldt conjecture is stated as follows.

CONJECTURE 1.4 (THE LEOPOLDT CONJECTURE). $\delta_p(k) = 0$ *holds.*

In other words, $\delta_p(k)$ measures the *defect* of the Leopoldt conjecture. We often write δ instead of $\delta_p(k)$ when there is no risk of confusion. Conjecture 1.4 is known to be true for all p if k is an abelian extension over $\mathbb{Q}$ or over an imaginary quadratic field (Ax, Brumer). Several equivalent formulations of Conjecture 1.4 or equivalent definitions of δ are known. They are of much interest in their own, but the one that we need is the following: *there exist exactly $r_2 + 1 + \delta$ independent $\mathbb{Z}_p$-extensions over k, where r_2 denotes the number of complex places of k.*

Let us return to F_d-extensions. Since an F_d-extension contains a $\mathbb{Z}_p^d$-extension as a subextension, we have an inequality:

$$1 \leq \rho \leq r_2 + 1 + \delta. \tag{1.5}$$

In particular, $\rho \leq r_2 + 1$ holds if the Leopoldt conjecture is valid for k and p.

Examples with $\rho = r_2 + 1$.

Example 1.6 (I. R. Šafarevič [14, §4]). Let $k = \mathbb{Q}(\mu_p)$ be the p-th cyclotomic field and assume that p is regular (i.e. p does not divide the class number of k). Then the Galois group of the maximal pro-p-extension of k unramified outside p is a free pro-p-group of rank $(p+1)/2 = r_2 + 1$. Since the Leopoldt conjecture is true for k and p, we find, by (1.5), that $\rho = r_2 + 1$.

Let G_{S_p} denote the Galois group of the maximal pro-p-extension of k which is unramified outside p. A necessary and sufficient condition on k and p for G_{S_p} to be free pro-p has been known (cf., for example, [9, 2.1], [21, Cor.]). In this case, the rank of G_{S_p} is equal to $r_2 + 1$. Since the Leopoldt conjecture at p is valid for such k, we find that $\rho = r_2 + 1$ holds for such k and p. (Alternatively, use Lemma 2.1 instead of the validity of the Leopoldt conjecture to conclude $\rho = r_2 + 1$.)

A. Movahhedi and T. Nguyen Quang Do [9] (see also [8]) define such an algebraic number field k (i.e. for which G_{S_p} is free pro-p) to be *p-rational*, and they investigate interesting arithmetic properties of p-rational fields. Simultaneously, G. Gras and J.-F. Jaulent [2] introduced the notion of *p-regular* number field. This notion is, in a sense, a natural generalization of the regularity of primes. We refer the reader to [5] concerning these topics.

Example 1.7 (cf. [8, p. 166]). For a prime $p \geq 5$, an imaginary quadratic field k is p-rational if p does not divide the class number of k. The converse is not true in general.

Other examples of p-rational fields are found in [8] and [5].

On the other hand, by a result of K. Wingberg [18, Kor. 3.3], we can see the existence of non p-rational k with $\rho = r_2 + 1$.

Problems. A complete determination of ρ seems to be difficult. In this note, we shall focus on the following two problems, in view of the inequality (1.5) and known examples.

Problem 1.8. *Prove $\rho \leq r_2 + 1$ without assuming the Leopoldt conjecture.*

Problem 1.9. *Can it happen that $\rho < r_2 + 1$?*

As we mentioned in the introduction, we shall give partial answers to these problems in what follows.

2. Unramifiedness outside p of F_d-extensions

The aim of this section is to prove the following

LEMMA 2.1. *An F_d-extension over a finite algebraic number field is unramified outside primes above p.*

Remark. This is well known when $d = 1$, ([4, 2.2]).

Proof. We shall give two proofs.

First Proof: archimedean primes do not ramify in an F_d-extension since F_d has no non-trivial torsion element. Let K be an F_d-extension over an algebraic number field k, $\mathfrak{L}$ (resp. $\mathfrak{l}$) be a non-archimedean prime of K (resp. of k), such that $\mathfrak{L} \mid \mathfrak{l} \nmid p$. Consider the localization $K_{\mathfrak{L}}/k_{\mathfrak{l}}$. This is also a free pro-p-extension because $\mathrm{Gal}(K_{\mathfrak{L}}/k_{\mathfrak{l}})$ may be considered as a closed subgroup of $\mathrm{Gal}(K/k)$. But by the assumption $\mathfrak{l} \nmid p$, $k_{\mathfrak{l}}$ possesses a unique $\mathbb{Z}_p$-extension, namely the maximal unramified pro-p-extension $k_{\mathfrak{l}}^{ur}$ (cf. [4, 12.1]), and consequently $k_{\mathfrak{l}}^{ur}$ is also the unique non-trivial free pro-p-extension of $k_{\mathfrak{l}}$. Therefore $K_{\mathfrak{L}}$ coincides either with $k_{\mathfrak{l}}^{ur}$ or with $k_{\mathfrak{l}}$, hence is unramified over $k_{\mathfrak{l}}$. □

Second Proof (due to M. Asada): as we mentioned above, the case $d = 1$ is well known, which we admit in the following. Therefore a multiple $\mathbb{Z}_p$-extension (i.e. a $\mathbb{Z}_p^e$-extension for some $e < \infty$) over a finite algebraic number field is unramified outside p. Let K/k be as in the first proof with its Galois group $G \cong F_d$. Put $G_1 = G$, and inductively $G_{n+1} = G_n^p \cdot \overline{[G_n, G_n]}$ (the Frattini subgroup of G_n). Then the descending series of closed subgroups

$$G = G_1 \supset G_2 \supset \cdots \supset G_n \supset \cdots$$

has the following properties (cf. [15, I-38]):

(1) G_n is an open normal subgroup of G for all $n \geq 1$,
(2) G_n/G_{n+1} is abelian for all $n \geq 1$,
(3) $\bigcap_{n=1}^{\infty} G_n = \{1\}$.

Let k_n be the fixed field of G_n. Corresponding to (1)–(3), the tower of fields

$$k = k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots$$

satisfies the following properties:

(1)' k_n/k is a finite normal extension for all $n \geq 1$,

(2)' k_{n+1}/k_n is an abelian extension for all $n \geq 1$,

(3)' $\bigcup_{n=1}^{\infty} k_n = K$.

Since $\mathrm{Gal}(k_{n+1}/k_n)$ is a quotient of the maximal abelian quotient

$$\mathrm{Gal}(K/k_n)^{ab} = G_n^{ab},$$

and since G_n^{ab} is isomorphic to $\mathbb{Z}_p^e$ for some $e < \infty$, k_{n+1}/k_n is embeddable in a multiple $\mathbb{Z}_p$-extension, hence is unramified outside p. By virtue of (3)', K/k is unramified outside p. □

As is clear from the second proof, any filtration of G satisfying (1)–(3) will suffice. For example, the descending p-central series defined by $G_{n+1} = G_n^p \cdot \overline{[G, G_n]}$. The one that we used, however, has an additional property:

(4) G_n/G_{n+1} is the maximal abelian quotient of G_n with exponent p,

and this enables us to prove the following

PROPOSITION 2.2. [1] *Let k be an algebraic number field. Assume that the Leopoldt conjecture with respect to p is true for any finite p-extension over k which is unramified outside p. If $\rho = r_2 + 1$ holds, then k possesses a unique F_ρ-extension K/k, and any F_d-extension ($d \leq \rho$) over k is contained in K.*

Proof. Let K be an arbitrary F_ρ-extension over k with Galois group G. Then, with the same notation as in the second proof of Lemma 2.1, the extension k_{n+1}/k_n is characterized as the maximal abelian extension with exponent p which is embeddable in a multiple $\mathbb{Z}_p$-extension. Indeed, the maximality can be seen as follows:

$$\begin{aligned}
\mathrm{rk}_{\mathbb{Z}/p\mathbb{Z}} \mathrm{Gal}(k_{n+1}/k_n) &= \mathrm{rk}_{\mathbb{Z}_p} G_n^{ab} && \text{by (4)} \\
&= \mathrm{rk}(G_n) \\
&= [k_n : k](\mathrm{rk}(G) - 1) + 1 && \text{Schreier's formula (1.1)} \\
&= [k_n : k] r_2(k) + 1 \\
&= r_2(k_n) + 1,
\end{aligned}$$

[1] Professor Kenkichi Iwasawa has kindly informed the author of this application.

and note that the Leopoldt conjecture for k_n and p is true. Thus K is unique. Let K' be an F_d-extension ($d \leq \rho$) and define k'_n in the same way as we defined k_n for K. Then we can show $k'_n \subset k_n$ for all $n \geq 0$. □

3. Weak Leopoldt conjecture

In this section we recall the weak Leopoldt conjecture and apply it to our problem. Let k be an algebraic number field, k_∞/k be a $\mathbb{Z}_p$-extension, and for each $n \geq 0$ let k_n be the n-th layer of k_∞/k, (i.e. k_n is the unique subfield such that $[k_n : k] = p^n$).

CONJECTURE 3.1 (THE WEAK LEOPOLDT CONJECTURE).

$\delta_p(k_n)$ is bounded as $n \to \infty$.

Note that $\{\delta_p(k_n)\}_{n=1}^{\infty}$ is a non-decreasing sequence of non-negative integers.

For the importance of Conjecture 3.1 in Iwasawa theory, see [3]. See also [12, §2], [13, §3], or [19, §5] for Galois cohomological treatment. An application is found in [22].

We abbreviate "the Leopoldt conjecture for k" to LC(k), and "the weak Leopoldt conjecture for k_∞" to WLC(k_∞), (note that whether Conjecture 3.1 is true or not depends only on k_∞ but not on the ground field k). We omit the reference to p since it is fixed. The following facts are known concerning WLC.

(3.2) WLC(k_∞) is true for the cyclotomic $\mathbb{Z}_p$-extension k_∞/k.
(3.3) If LC(k) is true, then WLC(k_∞) is true for any $\mathbb{Z}_p$-extension k_∞/k.
(3.4) Consider the set $\mathcal{E}$ of all $\mathbb{Z}_p$-extensions of k, and let $\mathcal{E}'$ denote the subset of $\mathcal{E}$ consisting of those $\mathbb{Z}_p$-extensions k_∞/k such that WLC(k_∞) is true. Then $\mathcal{E}'$ is an open dense subset of $\mathcal{E}$ with respect to the natural topology on $\mathcal{E}$ ([1, Thm. 3], [12, Thm. 2.11]. See also [3, §3]).

Our result in this section is the following

PROPOSITION 3.5. *If K/k is an F_d-extension with the condition $d > r_2 + 1$, then WLC(k_∞) is false for any $\mathbb{Z}_p$-extension k_∞/k contained in K. In particular, the following assertions hold.*
(1) If WLC(k_∞) is true for all k_∞/k, then $\rho \leq r_2 + 1$.
(2) If $\delta > 0$ (i.e. the Leopoldt conjecture is false for k and p), then $\rho < r_2 + 1 + \delta$ (strict inequality) holds.

Remark. (1) is a refinement of (1.5) in view of (3.3).

Proof. For any finite subfield L of K/k, K/L is also a free pro-p-extension, and the rank is given by Schreier's formula (1.1):

$$\begin{aligned} \mathrm{rk}((\mathrm{Gal}(K/L))) &= [L:k](d-1)+1 \\ &\geq [L:k](r_2+1)+1 \\ &= r_2(L)+1+[L:k]. \end{aligned}$$

The last equality follows from unramifiedness at archimedean primes, (see Lemma 2.1). Then it is clear that $\delta_p(L) \geq [L:k]$, and this proves the first statement. (1) follows from this. For (2) use (3.2). □

Question. *Can we improve this by using (3.4) ?*

4. Application of a theorem of K. Wingberg

In this section we compute ρ explicitly in a special case (Corollary 4.6) by using K. Wingberg's "free product decomposition" of Galois groups (Theorem 4.5).

First we extend the definition (1.2) of the invariant ρ to a pro-p-group G as follows:

$$\rho(G) := \sup\{d \geq 0 \ ; \ G \text{ has a quotient isomorphic to } F_d\}. \tag{4.1}$$

(We may allow d to be a cardinal number, but in the following G will always be finitely generated.) Then, for a field k, we have

$$\rho(k) = \rho(\mathrm{Gal}(k(p)/k)), \tag{4.2}$$

where $k(p)$ denotes the maximal pro-p-extension of k. Furthermore, if k is an algebraic number field, then by Lemma 2.1 we have

$$\rho(k) = \rho(G_{S_p}), \tag{4.3}$$

where G_{S_p} is the Galois group of the maximal pro-p-extension of k which is unramified outside p (this notation is consistent with that introduced below). Thus some information on G_{S_p} may be useful in determining ρ. The pro-p-group G_{S_p} has been extensively studied by many people, and among their works we shall apply a result of K. Wingberg to our problem.

We fix the notation.

p is a prime,

k is an algebraic number field (we assume p is odd or k is totally imaginary, therefore an archimedean prime does not ramify in a p-extension),
S_∞ is the set of archimedean primes of k,
S_p is the set of primes of k above p,
S is a finite set of primes of k such that $S \supset S_\infty \cup S_p$,
$k_S(p)$ is the maximal pro-p-extension of k unramified outside S,
$G_S := \mathrm{Gal}(k_S(p)/k)$,
$\mathcal{G}_v := \mathrm{Gal}(k_v(p)/k_v)$, where k_v is the completion of k at a prime v, and $k_v(p)$ is the maximal pro-p-extension of k_v,
μ_p is the group of p-th roots of unity,
$\delta(F) = 1$ or 0 according as $F \supset \mu_p$ or $F \not\supset \mu_p$ for a field F of characteristic 0 (this is irrelevant to (1.3)),
S_0 is a maximal subset of $S \setminus S_\infty$ satisfying

$$\sum_{v \in S_0} \delta(k_v) = \delta(k), \tag{4.4}$$

$V_{S_0}^S := \{a \in k^\times \ ; \ a \in k_v^{\times p} \ \forall v \in S_0 \text{ and } p \mid \mathrm{ord}_v(a) \ \forall v \notin S\}/k^{\times p}$.

THEOREM 4.5 (K. Wingberg [20], [21]). *With the notation and assumption as above, if there exists S_0 such that $V_{S_0}^S = 0$, then*

$$G_S \cong \underset{v \in S \setminus S_0}{*} \mathcal{G}_v * \mathcal{F},$$

where $*$ denotes free pro-p product (cf. [10]) *and $\mathcal{F}$ is a free pro-p-group with*

$$\mathrm{rk}(\mathcal{F}) = 1 + \sum_{v \in S_p \cap S_0} [k_v : \mathbb{Q}_p] - \sharp(S \setminus S_0).$$

Remark. In addition to above, K. Wingberg proves that if $V_{S_0}^S \neq 0$ for any S_0, then G_S is a pro-p duality group (or strict Cohen-Macaulay in the terminology of [15]) of dimension 2. We shall not treat this case in this note.

Our result is the following

COROLLARY 4.6. *With the same notation as above, if $V_{S_0}^S = 0$ for some S_0, then*

$$\rho = r_2 + 1 - \frac{1}{2}\left(\sum_{v \in S_p \setminus S_0} [k_v : \mathbb{Q}_p] + \varepsilon_v\right),$$

where $\varepsilon_v = 1$ or 0 according as $[k_v : \mathbb{Q}_p]$ is odd or even.

Remark. The formula for ρ stated in the introduction is a special case of this by virtue of [21, Lemma 2].

Examples.
(1) $p = 2$, $k = \mathbb{Q}(\sqrt{-\ell})$, where $\ell > 0$ is a rational prime such that $\ell \equiv 7 \pmod 8$. In this case $\rho = 1$, while $r_2 + 1 = 2$.
(2) $p = 3$, $k = \mathbb{Q}(\sqrt{-3}, \sqrt{15})$ or $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-26})$. In this case $\rho = 2$, while $r_2 + 1 = 3$.
In each case, S_p consists of two elements, say, $S_p = \{v_0, v_1\}$. Take $S = S_\infty \cup S_p$ and $S_0 = \{v_0\}$. The condition $V_{S_0}^S = 0$ was checked by V. M. Tsvetkov [17] in case (1), and by L. V. Kuz'min [6], V. M. Tsvetkov [17] respectively in case (2).

Proof of Corollary 4.6.

LEMMA 4.7. *Let $G_1, \cdots, G_m$ be finitely generated pro-p-groups. Then*

$$\rho(\overset{m}{\underset{i=1}{*}} G_i) = \sum_{i=1}^{m} \rho(G_i)$$

holds.

LEMMA 4.8 (J. Sonn [16], cf. [11, p. 102]). *Let G be a (pro-p) Demuškin group. Then $\rho(G) = \frac{1}{2}(\mathrm{rk}(G) - \varepsilon)$, where $\varepsilon = 1$ or 0 according as $\mathrm{rk}(G)$ is odd or even.*

We shall prove these lemmas in §5.
Recall the structure of the local Galois group $\mathcal{G}_v$ (cf. [15, II-5.6]):

$$\mathcal{G}_v = \begin{cases} \text{free pro-}p\text{-group of rank 1}, & \text{if } k \not\supset \mu_p \text{ and } v \nmid p\infty, \\ \text{free pro-}p\text{-group of rank } [k_v : \mathbb{Q}_p] + 1, & \text{if } k \not\supset \mu_p \text{ and } v \mid p, \\ \text{Demuškin group of rank 2}, & \text{if } k \supset \mu_p \text{ and } v \nmid p\infty, \\ \text{Demuškin group of rank } [k_v : \mathbb{Q}_p] + 2, & \text{if } k \supset \mu_p \text{ and } v \mid p, \\ \{1\}, & \text{if } v \mid \infty. \end{cases}$$

Combining this with the preceding lemmas, we can compute ρ. □

Remark. If we assume that $S = S_\infty \cup S_p$, $k \supset \mu_p$ and k is a Galois extension over $\mathbb{Q}$, then $V_{S_0}^S = 0$ implies either

(1) $S_p = S_0 = \{v_0\}$ and G_S is a free pro-p-group of rank $r_2 + 1$, or
(2) $S_p = \{v_0, v_1\}$, $S_0 = \{v_0\}$ and $G_S = \mathcal{G}_{v_0} = \mathcal{G}_{v_1}$ is a Demuškin group of rank $r_2 + 2$ (so that $\rho = 1 + [r_2/2]$ where $[x]$ = the greatest integer not exceeding x). This is the case with the examples given above.

Proof of Remark. First note that S_0 consists of a single element if $k \supset \mu_p$. Assume $V_{S_0}^S = 0$. Then the formula for $\mathrm{rk}(\mathcal{F})$ in Theorem 4.5 becomes: $\mathrm{rk}(\mathcal{F}) = (2-g) + (1/g - 1)r_1 + (2/g - 1)r_2$, where $g = \sharp S_p$ and r_1 denotes the number of real places of k. Since $\mathrm{rk}(\mathcal{F})$ must be non-negative, we have either (1) $g = 1$ or (2) $g = 2$ and $r_1 = 0$. This completes the proof. □

From this point of view, we cannot expect more interesting phenomena as long as we restrict ourselves to the case $k \supset \mu_p$ and $k/\mathbb{Q}$ is Galois ($S = S_\infty \cup S_p$ is no restriction in the light of Lemma 2.1). In particular, under these assumptions (including $V_{S_0}^S = 0$), we cannot find any example with $\rho = r_2 + 1$ other than the case that G_S itself is free.

Finally, combining (4.2), Lemma 4.8 and the known structure of the Galois groups of the maximal pro-p-extensions of local fields, we can compute ρ for local fields.

PROPOSITION 4.9. *Let k be a local field, (in the sense that it is obtained as the completion of an algebraic number field with respect to a non-archimedean prime) with residue characteristic ℓ. Then*

$$\rho_p(k) = \begin{cases} 1, & \text{if } \ell \neq p, \\ [k:\mathbb{Q}_p] + 1, & \text{if } \ell = p \text{ and } k \not\supset \mu_p, \\ \frac{1}{2}([k:\mathbb{Q}_p] - \varepsilon) + 1, & \text{if } \ell = p \text{ and } k \supset \mu_p, \end{cases}$$

where $\varepsilon = 1$ or 0 according as $[k:\mathbb{Q}_p]$ is odd or even. □

Remark. For another proof based on a viewpoint of embedding problem, see [11, §5].

5. Proof of the lemmas

Proof of Lemma 4.7. Firstly, if there exist surjective homomorphisms $\varphi_i : G_i \twoheadrightarrow F_{d_i}$ $(1 \leq i \leq m)$, then we can construct a surjective homomorphism

$$\overset{m}{\underset{i=1}{*}} \varphi_i : \overset{m}{\underset{i=1}{*}} G_i \twoheadrightarrow \overset{m}{\underset{i=1}{*}} F_{d_i} = F_d,$$

where $d = \sum_{i=1}^{m} d_i$ (cf. [10, Satz 1.2]). Hence we have $\rho(\overset{m}{\underset{i=1}{*}} G_i) \geq \sum_{i=1}^{m} \rho(G_i)$. In order to obtain the inverse inequality, we claim that if there exists a surjective homomorphism $\varphi : \overset{m}{\underset{i=1}{*}} G_i \twoheadrightarrow F_d$, then there exist a partition $d = \sum_{i=1}^{m} d_i$, $(d_i \geq 0)$, and surjective homomorphisms $\varphi_i : G_i \twoheadrightarrow F_{d_i}$, $(1 \leq i \leq m)$. We may assume $m = 2$. Let us consider each G_i as a closed subgroup of $G_1 * G_2$. Then φ induces a homomorphism $\psi : G_1 * G_2 \to \varphi(G_1) * \varphi(G_2)$. On the other hand, there exists a natural (surjective) homomorphism $h : \varphi(G_1) * \varphi(G_2) \twoheadrightarrow F_d$, and it is clear that $\varphi = h \circ \psi$. The images $\varphi(G_i)$ $(i = 1, 2)$ are free pro-p-groups, and we have

$$\mathrm{rk}(\varphi(G_1)) + \mathrm{rk}(\varphi(G_2)) = \mathrm{rk}(\varphi(G_1) * \varphi(G_2)) \geq d$$

since h is surjective. Starting from the natural surjections $G_i \twoheadrightarrow \varphi(G_i)$, $(i = 1, 2)$, and taking quotients if necessary, we obtain a desired partition $d = d_1 + d_2$ and surjective homomorphisms $G_i \twoheadrightarrow F_{d_i}$, $(i = 1, 2)$. □

Proof of Lemma 4.8. Let G be a Demuškin group. We must show that there exists a surjective homomorphism from G to F_d if and only if $d \leq \frac{1}{2}\,\mathrm{rk}(G)$. This is a part of a theorem of J. Sonn [16, Thm. 7], but in the case $q(G) = 2$, he only stated this and gave no proof. We therefore prove this along his idea, for completeness. Note that the "if" part is obvious from the canonical form of the "Demuškin relation" (cf. [7]). In the proof of the "only if" part, the key point is that Lemma 5.1 below holds even in characteristic 2. Now let $G \twoheadrightarrow F_d$ be a surjective homomorphism. Put $M = H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $N = H^1(F_d, \mathbb{Z}/p\mathbb{Z})$, where $\mathbb{Z}/p\mathbb{Z}$ is acted trivially. Both M and N are $\mathbb{Z}/p\mathbb{Z}$-vector spaces, and we identify N with its image in M under the inflation map. Then the following diagram is commutative:

$$\begin{array}{ccc} M \times M & \xrightarrow{\text{cup product}} & H^2(G, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} \\ \cup\uparrow & & \uparrow\text{infl.} \\ N \times N & \xrightarrow{\text{cup product}} & H^2(F_d, \mathbb{Z}/p\mathbb{Z}) = 0. \end{array}$$

Thus N is an "isotropic" subspace of the "symplectic" space M. Therefore it suffices to prove the following

LEMMA 5.1. *Let $\mathfrak{k}$ be a field, M be a finite dimensional vector space over $\mathfrak{k}$ equipped with a non-degenerate, anti-symmetric bilinear form $M \times M \to \mathfrak{k}$,*

and N be an isotropic subspace of M with respect to this pairing (i.e. $a \cdot b = 0$ for all $a, b \in N$). Then $\dim(N) \leq \frac{1}{2}\dim(M)$.

Proof. Put $r = \dim(N)$. Then, by an induction on r, we can choose linearly independent vectors $a_1, b_1, \cdots, a_r, b_r \in M$ such that $\{a_1, \cdots, a_r\}$ is a basis of N, and $a_i \cdot b_j = 1$ if $i = j$, 0 otherwise. □ □

Remark. If $\mathfrak{k}$ is not of characteristic 2, we can impose $b_i \cdot b_j = 0$, i.e. we can choose $\{a_1, b_1, \cdots, a_r, b_r\}$ which forms a part of a *symplectic basis* of M (cf. [16, Prop. 3]).

References

[1] V. A. Babaĭcev, *On some questions in the theory of Γ-extensions of algebraic number fields*, Izv. Akad. Nauk. SSSR. Ser. Mat. **40** (1976), 477–487; English transl. in Math. USSR-Izv. **10** (1976), 453–462.

[2] G. Gras et J.-F. Jaulent, *Sur les corps de nombres réguliers*, Math. Z. **202** (1989), 343–365.

[3] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978), 85–99.

[4] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[5] J.-F. Jaulent et T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers, et ramification restreinte*, Séminaire de Théorie des Nombres de Bordeaux, (1987–1988), Exposé 10, 10-01–10-26.

[6] L. V. Kuz'min, *Local extensions associated with ℓ-extensions with given ramification*, Izv. Akad. Nauk. SSSR. Ser. Mat. **39** (1975), 739–772; English transl. in Math. USSR-Izv. **9** (1975), 693–726.

[7] J. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106–132.

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

[9] A. Movahhedi et T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987-88, Progr. Math., 81, Birkhäuser Boston, MA, 1990, 155–200.

[10] J. Neukirch, *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie*, Archiv der Math. **22** (1971), 337–357.

[11] T. Nguyen Quang Do, *Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa*, Compositio Math. **46** (1982), 85–119.

[12] T. Nguyen Quang Do, *Formations de classes et modules d'Iwasawa*, Number Theory Noordwijkerhout 1983, Lecture Notes in Math. **1068** (1984), 167–185.

[13] T. Nguyen Quang Do, *Sur la torsion de certains modules galoisiens II*, Séminaire de Théorie des Nombres, Paris 1986-87, Progr. Math., 75, Birkhäuser Boston, MA, 1988, 271–297.

[14] I. R. Šafarevič, *Extensions with given points of ramification*, Inst. Hautes Études Sci. Publ. Math. **18** (1964), 295–319; English transl. in Amer. Math. Soc. Transl. Ser. 2 **59** (1966), 128–149; see also Collected Mathematical Papers, 295–316.

[15] J. -P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. **5** (1964).

[16] J. Sonn, *Epimorphisms of Demushkin groups*, Israel J. Math. **17** (1974), 176–190.

[17] V. M. Tsvetkov, *Examples of extensions with Demushkin group*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **103** (1980), 146–149; English transl. in J. Soviet Math. **24–4** (1984), 480–482.

[18] K. Wingberg, *Freie Produktzerlegungen von Galoisgruppen und Iwasawa-Invarianten für p-Erweiterungen von* $\mathbb{Q}$, J. Reine Angew. Math. **341** (1983), 111–129.

[19] K. Wingberg, *Duality theorems for Γ-extensions of algebraic number fields*, Compositio Math. **55** (1985), 333–381.

[20] K. Wingberg, *On Galois groups of p-closed algebraic number fields with restricted ramification*, J. Reine Angew. Math. **400** (1989), 185–202.

[21] K. Wingberg, *On Galois groups of p-closed algebraic number fields with restricted ramification II*, J. Reine Angew. Math. **416** (1991), 187–194.

[22] M. Yamagishi, *On the center of Galois groups of maximal pro-p extensions of algebraic number fields with restricted ramification*, J. Reine Angew. Math. **436** (1993), 197–208.

Masakazu Yamagishi
Department of Mathematical Sciences,
University of Tokyo,
Hongo, Tokyo 113, JAPON