Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 107–121

A Survey of p-Extensions

Masakazu Yamagishi

This is a brief survey of what is known or unknown about the Galois group of the maximal pro-p-extension (p a fixed prime) of a number field which is unramified outside a given set of places. We are particularly interested in

- presentation in terms of generators and relations
- cohomological dimension

of the Galois group. The contents are as follows. In Section 1 we recall basic facts on pro-p-groups. In Section 2 we review the structure of the Galois group of the maximal pro-p-extension of a local field. In Section 3 we state some known facts and unsolved conjectures about the structure of the Galois group of the the maximal pro-p-extension of a number field which is unramified outside a given finite set of places. In Section 4 we introduce some topics in Iwasawa theory. In Section 5 we state some known facts about the structure of the Galois group of the maximal pro-p-extension of a number field. Finally, as an application of Sections 3 and 4, we give some examples of free pro-p-extensions of number fields in Section 6.

The author would like to thank the referee for valuable comments.

§1. Pro-p-groups

Main references are Serre [54, I §3–§4] and Koch [26, §5–§6]. Let G be a pro-p-group.

1.1. Generators and relations

We put $d(G) = \dim H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $r(G) = \dim H^2(G, \mathbb{Z}/p\mathbb{Z})$. $d(G)$ is the minimal number of generators of G, which we also call the rank of G, and $r(G)$ is the minimal number of relations of G.

Received September 1, 1998.
Revised November 26, 1998.

1.2. Cohomological dimension

The cohomological dimension and the strict cohomological dimension of G are defined by

$$\mathrm{cd}(G) = \inf\{n; H^q(G,A) = 0\ \forall q > n, \forall A : \text{discrete torsion } G\text{-module}\},$$
$$\mathrm{scd}(G) = \inf\{n; H^q(G,A) = 0\ \forall q > n, \forall A : \text{discrete } G\text{-module}\},$$

respectively. We know the following facts:

- $\mathrm{cd}(G) \leq n$ if and only if $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.
- $\mathrm{cd}(G) \leq \mathrm{scd}(G) \leq \mathrm{cd}(G) + 1$.
- If H is a closed subgroup of G, then $\mathrm{cd}(H) \leq \mathrm{cd}(G)$ and $\mathrm{scd}(H) \leq \mathrm{scd}(G)$.
- If G has non trivial torsion, then $\mathrm{cd}(G) = \mathrm{scd}(G) = \infty$.
- Suppose $\mathrm{cd}(G) = n < \infty$, then $\mathrm{scd}(G) = n$ if and only if $H^n(H, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ for all open subgroups H of G.

1.3. Euler-Poincaré characteristic

If $\mathrm{cd}(G)$ is finite and $H^i(G, \mathbb{Z}/p\mathbb{Z})$ is finite for all i, we define the Euler-Poincaré characteristic of G by

$$\chi(G) = \sum_{i=0}^{\infty} (-1)^i \dim H^i(G, \mathbb{Z}/p\mathbb{Z}).$$

If $\chi(G)$ is defined and H is an open subgroup of G, then $\chi(H)$ is also defined and $\chi(H) = [G : H]\chi(G)$.

1.4. Free pro-p-groups

G is called a free pro-p-group if and only if $r(G) = 0$, or equivalently, $\mathrm{cd}(G) \leq 1$. If G is a free pro-p-group and H is a closed subgroup of G, then H is also a free pro-p-group since $\mathrm{cd}(H) \leq \mathrm{cd}(G) \leq 1$. If, in addition, the rank of G is finite and H is open in G, then the rank of H is also finite and we have Schreier's formula:

$$d(H) - 1 = [G : H](d(G) - 1),$$

which follows from Subsection 1.3.

1.5. Demuškin groups

G is called a Demuškin group if it satisfies the following conditions:

(i) $d(G)$ is finite.
(ii) $r(G) = 1$.

(iii) The cup-product

$$H^1(G,\mathbb{Z}/p\mathbb{Z}) \times H^1(G,\mathbb{Z}/p\mathbb{Z}) \to H^2(G,\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$$

is a non-degenerate bilinear form.

The structure of Demuškin groups is known as follows. Suppose $p > 2$ for simplicity and let G be a Demuškin group. Then we see by (iii) that $d(G) = 2n$ is even and by (ii) that the maximal abelian quotient G^{ab} is isomorphic to $\mathbb{Z}_p^{2n-1} \times \mathbb{Z}_p/q\mathbb{Z}_p$, where q is either 0 or a power of p.

Theorem 1.1 (Demuškin [7]). *Let p be an odd prime and G a Demuškin group with n and q as above. Then there exist generators $x_1, x_2, \ldots, x_{2n}$ of G such that the single relation for G has the form :*

$$x_1^q[x_1,x_2][x_3,x_4]\cdots[x_{2n-1},x_{2n}] = 1,$$

where $[x,y] = x^{-1}y^{-1}xy$.

See Serre [53] and Labute [34] for the case $p = 2$.

§2. Local fields

Main reference is Serre [54, II §5]. Let k be a finite extension of $\mathbb{Q}_l$, $k(p)$ the maximal pro-p-extension of k, and $G = \mathrm{Gal}(k(p)/k)$ the Galois group. The structure of G is determined. We use the following notation:

- $N = \begin{cases} [k:\mathbb{Q}_p] & (l = p) \\ 0 & (l \neq p) \end{cases}.$
- $\bar{k}$: the algebraic closure of k.
- μ_p : the group of pth roots of unity in $\bar{k}$.
- $\delta = \begin{cases} 1 & (k \supset \mu_p) \\ 0 & (k \not\supset \mu_p) \end{cases}.$

Theorem 2.1. $d(G) = N + 1 + \delta,\ r(G) = \delta.$

Proof. By local class field theory $H^1(G,\mathbb{Z}/p\mathbb{Z})$ is dual to $k^\times/k^{\times p}$. The inflation homomorphism $H^2(G,\mathbb{Z}/p\mathbb{Z}) \to H^2(\mathrm{Gal}(\bar{k}/k),\mathbb{Z}/p\mathbb{Z})$ is an isomorphism and by the local duality theorem this last group is dual to $H^0(\mathrm{Gal}(\bar{k}/k),\mu_p)$. □

Corollary 2.2 (Šafarevič [47]). *If $\delta = 0$, then G is a free pro-p-group.*

Corollary 2.3. *If $\delta = 1$, then G is a Demuškin group.*

Proof. Since $k \supset \mu_p$, we have $H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong k^\times/k^{\times p}$ and the cup-product corresponds to the norm residue symbol, which is non-degenerate on $k^\times/k^{\times p}$. □

Remark 2.4. If $\delta = 1$ and $p > 2$, then, with the notation of Theorem 1.1, the invariant q is the maximal power of p such that k contains the group of qth roots of unity.

Theorem 2.5. $\mathrm{cd}(G) \leq 2$, $\mathrm{scd}(G) = 2$.

Proof. These follow from Corollaries 2.2 and 2.3. □

Corollary 2.6. $\chi(G) = -N$.

Remark 2.7. Let G be a pro-p-group. It is known that G is a free pro-p-group if and only if

$$d(H) - 1 = [G : H](d(G) - 1)$$

for all open subgroups H of G. It is also known that G is a Demuškin group if and only if

$$d(H) - 2 = [G : H](d(G) - 2)$$

for all open subgroups H of G (Dummit-Labute [8]). These characterization of free pro-p-groups and Demuškin groups give alternative proofs of Corollaries 2.2 and 2.3.

It would be an interesting problem to consider a pro-p-group G such that

$$d(H) - c = [G : H](d(G) - c)$$

for all open subgroups H of G, where $c \geq 3$ is a fixed positive integer. A trivial example is $G = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (c times). Are there any examples of such G which arise naturally in number theory? See Schmidt [50] for related topics.

§3. Global fields

Main references are Haberland [13] and Koch [26] (see also [28]). Let k be a finite extension of $\mathbb{Q}$, S a finite set of places of k, $k_S(p)$ the maximal pro-p-extension of k unramified outside S, and $G_S = \mathrm{Gal}(k_S(p)/k)$ the Galois group. Suppose that p is odd or that k is totally imaginary. Then since no archimedean place can ramify in a pro-p-extension of k, we may assume that S is disjoint from the set of the archimedean places of k. We use the following notation:

- r_1 : the number of real places of k.
- r_2 : the number of imaginary places of k.
- k_v : the completion of k with respect to a place v of k.
- μ_p : the group of pth roots of unity in the algebraic closure $\bar{k}$.
- $\delta = \begin{cases} 1 & (k \supset \mu_p) \\ 0 & (k \not\supset \mu_p) \end{cases}$.
- $\delta_v = \begin{cases} 1 & (k_v \supset \mu_p) \\ 0 & (k_v \not\supset \mu_p) \end{cases}$.
- S_p : the set of all places of k which are above p.
- $V_S = \{x \in k^\times; (x) = \mathfrak{A}^p, x \in k_v^{\times p}\ \forall v \in S\}/k^{\times p}$.
- $\theta = \begin{cases} 1 & (\delta = 1, S = \emptyset) \\ 0 & (\text{otherwise}) \end{cases}$.

Theorem 3.1 (Šafarevič [48]).

$$d(G_S) = \sum_{v \in S} \delta_v - \delta - (r_1 + r_2 - 1) + \sum_{v \in S \cap S_p} [k_v : \mathbb{Q}_p] + \dim V_S,$$

$$r(G_S) \leq \sum_{v \in S} \delta_v - \delta + \dim V_S + \theta.$$

Two cases are of particular interest to us: one is the case where S is empty, the other is the case where $S \supset S_p$.

3.1. Case $S = \emptyset$

It has been conjectured that every number field of finite degree can be embedded in a number field with class number one (the class field tower problem). In particular, $G_\emptyset$ has been conjectured to be finite. Golod and Šafarevič [11] showed that if G is a finite p-group then $r(G) > (d(G) - 1)^2/4$ holds (in fact $r(G) > d(G)^2/4$ holds, see, for example, Roquette [46, Remark 14]). Using this and Theorem 3.1, they gave examples of k (and p) with infinite $G_\emptyset$.

Presentation of $G_\emptyset$ in terms of generators and relations is not known in general; there seems no single example of infinite $G_\emptyset$ whose minimal relations are completely known.

Suppose $G_\emptyset \neq \{1\}$. It is known that $\mathrm{scd}(G_\emptyset) \geq 3$ and conjectured that $\mathrm{cd}(G_\emptyset) = \infty$ (cf. Kawada [22, p.111]). Note that this conjecture is trivial if $G_\emptyset$ is finite and $\neq \{1\}$.

Fontaine and Mazur [9, Conjecture 5b] conjectured that $G_\emptyset$ has no infinite p-adic analytic quotient. See Boston [3],[4], Hajir [14], Nomura [44],[45] for related topics.

If we allow the degree of the number field to be *infinite*, then interesting examples of unramified pro-p-extensions are known. See Asada [2, Supplement] for a construction of an unramified $\mathrm{SL}_2(\mathbb{Z}_p)$-extension (note that $\mathrm{SL}_2(\mathbb{Z}_p)$ itself is not a pro-p-group, but contains a pro-p-subgroup with finite index), and Wingberg [64] for the case where the Galois group of the maximal unramified pro-p-extension is a free pro-p-group.

3.2. Case $S \supset S_p$

In this case, the inequality for $r(G_S)$ in Theorem 3.1 is in fact an equality (Brumer [5]). For a proof by using the Poitou-Tate global duality theorem and a result of Neumann [39, Corollary 1], see Nguyen Quang Do [41, Proposition 11].

Example 3.2. k is called p-rational if G_{S_p} is a free pro-p-group. If $k \supset \mu_p$ and $S \supset S_p$, then

$$\begin{aligned} V_S \cong & \ker\{H^1(G_S, \mu_p) \\ & \to \prod_{v \in S} H^1(\mathrm{Gal}(k_v(p)/k_v), \mu_p)\} \cong \mathrm{Hom}(Cl_S, \mathbb{Z}/p\mathbb{Z}), \end{aligned}$$

where Cl_S denotes the S-ideal class group of k (see, for example, Neukirch [38, 7.3]). Hence if $k \supset \mu_p$, then k is p-rational if and only if $|S_p| = 1$ and $p \nmid |Cl_{S_p}|$ (see also [48, §4]). A typical example is $k = \mathbb{Q}(\mu_p)$ where p is a regular prime. See Movahhedi-Nguyen Quang Do [37], Movahhedi [36], Sauzet [49] for more examples of p-rational number fields and the arithmetic of such fields, and also G. Gras-Jaulent [12], Jaulent-Nguyen Quang Do [20] for related topics.

Wingberg [62] and [63] showed that in some cases G_S has a free pro-p product decomposition. Let $\mathcal{G}_v$ denote the decomposition subgroup of a place v in $k_S(p)/k$ (defined up to conjugate) and $\star$ the free pro-p product.

Theorem 3.3 ([62, Theorem A]). *Suppose $k \supset \mu_p$. Then*

$$G_S \cong \mathop{\bigstar}_{v \in S - \{v_0\}} \mathcal{G}_v \star \mathcal{F}$$

for some $v_0 \in S_p$ and for some free pro-p-group $\mathcal{F}$ if and only if v_0 does not split in $k_S(p)/k$ at all. If this is the case, then $d(\mathcal{F}) = [k_{v_0} : \mathbb{Q}_p] + 2 - |S| - r_2$.

Remark 3.4. Wingberg showed more: if G_S does not have a free pro-p product decomposition of this form, then G_S is a pro-p duality group of dimension 2 which is not Poincaré type. See also Schmidt [51].

If G_S has free pro-p product decomposition as in Theorem 3.3, then $\mathcal{G}_v$ coincides with $\mathrm{Gal}(k_v(p)/k_v)$ (Kuz'min [32]), which is a Demuškin group. Therefore we know the relations of G_S; in particular, they all come from local relations.

Example 3.5 (essentially due to Kuz'min [32]). Let $p = 3, k = \mathbb{Q}(\sqrt{-3}, \sqrt{15})$. Then G_{S_p} is a Demuškin group of rank 4.

For free pro-p product decomposition of G_S in a different setting, see Neumann [40], Movahhedi-Nguyen Quang Do [37], Jaulent-Nguyen Quang Do [20] and Jaulent-Sauzet [21].

For the case where G_S is a Demuškin group, see Tsvetkov [58], Arrigoni [1] and Sauzet [49].

In general, presentation of G_S in terms of generators and relations is not known. In some cases, the class two quotient $G_S/[G_S, [G_S, G_S]]$, where $[\ ,\ ]$ denotes the topological commutator, can be described in terms of generators and relations. See Fröhlich [10], Koch [27], Ullom-Watt [59] and Movahhedi-Nguyen Quang Do [37]. Komatsu [29] treated the case where there is a global relation (i.e. not coming from local relations). See also Koch [26, §11.4].

The cohomological dimension of G_S is known:

Theorem 3.6. $\mathrm{cd}(G_S) \leq 2$.

For proofs, see Brumer [5], Kuz'min [30],[31], Neumann [39] and Haberland [13, Proposition 7].

Corollary 3.7. $\chi(G_S) = -r_2$.

On the contrary, the strict cohomological dimension of G_S is not known:

Conjecture 3.8. $\mathrm{scd}(G_S) = 2$.

In the cases where the explicit structure of G_S is known (i.e. G_S is a free pro-p-group or a Demuškin group or G_S has a free pro-p product decomposition), this conjecture is true. See Corollary 4.3 for a relation with the Leopoldt conjecture.

The Galois group G_S is often compared to (the pro-p completion of) the fundamental group of a Riemann surface. For example, free pro-p product decomposition of G_S is an analogue of Riemann's existence theorem (Neumann [40]). See also [67].

§4. Iwasawa theory

We introduce some topics in Iwasawa theory which are deeply connected with G_S. Main reference is Wingberg [61]. See also Washington [60] for Iwasawa Theory. We keep the notation of the previous section and suppose that $S \supset S_p$.

4.1. The Leopoldt conjecture

The following is Iwasawa's formulation [17, 2.3] of the Leopoldt conjecture.

Conjecture 4.1. k has exactly $r_2 + 1$ independent $\mathbb{Z}_p$-extensions.

This conjecture has been verified in some cases; for example, $k/\mathbb{Q}$ is abelian (Ax-Brumer; see [60, 5.25]).

Proposition 4.2. *The Leopoldt conjecture is equivalent to* $H^2(G_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

For proofs, see, for example, Haberland [13, Proposition 18] and Nguyen Quang Do [41, Proposition 12]. See also [67, §4] for related topics.

Corollary 4.3. $\mathrm{scd}(G_S) = 2$ *if and only if the Leopoldt conjecture is true for all finite subfields of* $k_S(p)/k$.

Proof. By Subsection 1.2, Theorem 3.6 and Proposition 4.2. □

Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension of k and $H_S = \mathrm{Gal}(k_S(p)/k_\infty)$ the Galois group. The following is called the weak Leopoldt conjecture for k_∞.

Proposition 4.4. $H^2(H_S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

See Schneider [52, Lemma 7] and Wingberg [61, 5.1] for proofs, and also Nguyen Quang Do [42, §2] for related topics.

4.2. Iwasawa invariants

In addition to k_∞ and H_S as above, we use the following notation:

- $\Gamma = \mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p$.
- $\Lambda = \mathbb{Z}_p[[\Gamma]]$: completed group ring.
- $\mathcal{X}_S = H_S^{ab} = \mathrm{Gal}(M_S/k_\infty)$, where M_S is the maximal abelian pro-p-extension of k_∞ unramified outside S.
- $X = \mathrm{Gal}(L/k_\infty)$, where L is the maximal unramified abelian pro-p-extension of k_∞.

The Galois group Γ naturally acts on $\mathcal{X}_S$ and X by conjugation; therefore $\mathcal{X}_S$ and X are naturally Λ-modules. Concerning the Λ-module structure of $\mathcal{X}_S$ and X, we know the following facts:

- $\mathcal{X}_S$ and X are Noetherian Λ-modules.
- The Λ-rank of $\mathcal{X}_S$ is r_2.
- The Λ-rank of X is 0, i.e. X is a torsion Λ-module.
- The Iwasawa invariants $\mu(X)$ and $\lambda(X)$ for the Noetherian Λ-module X coincide with the usual Iwasawa invariants $\mu(k)$ and $\lambda(k)$ of k_∞/k, respectively.

Proposition 4.5. *The following two statements are equivalent:*
(i) *H_S is a free pro-p-group,*
(ii) $\mu(\mathcal{X}_S) = 0$.
If $k \supset \mu_p$, then these are equivalent to
(iii) $\mu(X) = 0$.

For proofs, see Iwasawa [19, Theorem 2] and Wingberg [61, 5.3 and 7.9]. It is conjectured that $\mu(X) = 0$ in general, and this has been verified in some cases; for example, $k/\mathbb{Q}$ is abelian (Ferrero and Washington; see [60, 7.15]).

For a CM-field k, let k^+ denote the maximal real subfield of k and $\lambda^-(k)$ the minus part of $\lambda(k)$. The following is an analogue of the Riemann-Hurwitz formula.

Theorem 4.6 (Kida [23]). *If k is a CM-field such that $k \supset \mu_p$ and $\mu(k) = 0$, and if K is a finite Galois p-extension of k which is also a CM-field, then we have $\mu(K) = 0$ and*

$$2(\lambda^-(K) - 1) = [K_\infty : k_\infty]\, 2\,(\lambda^-(k) - 1) + \sum_w (e_w - 1),$$

where w ranges over all finite places of K_∞ such that $w \nmid p$ and w splits in K_∞/K_∞^+, and e_w denotes the ramification index of w in K_∞/k_∞.

Proof. (Cf. [61, §7].) Take S large enough so that $k_S(p) \supset K$. It follows from 1.4 and Proposition 4.5 that $\mu(K) = 0$ (see also Iwasawa [18, Theorem 3]). The Galois group $H_S(k_\infty^+)$ is a free pro-p-group since $\mu(k^+) = 0$, and is finitely generated since it has Λ-rank 0. Applying Schreier's formula to $H_S(k_\infty^+) \supset H_S(K_\infty^+)$, we obtain a formula connecting λ-invariants of $\mathcal{X}_S(k_\infty^+)$ and $\mathcal{X}_S(K_\infty^+)$. Then by duality, we obtain a formula connecting λ^--invariants of $X(k_\infty)$ and $X(K_\infty)$. $\square$

For other proofs or generalization of this theorem, see, for example, Kuz'min [33], Iwasawa [19], Nguyen Quang Do [43] and Wingberg [65].

§5. The maximal pro-p-extension

Let the notation be as in Section 3 except that S is the set of *all* places of k (S was supposed to be a finite set in Section 3). We drop S in our notation. Hence $k(p)$ is the maximal pro-p-extension of k and $G = \mathrm{Gal}(k(p)/k)$.

Both $d(G)$ and $r(G)$ are countably infinite and a minimal presentation of G in terms of generators and relations is known (Koch [24, §3], [25] and Hoechsmann [15]; see also [26, §11.1] and [16]).

Theorem 5.1 (Serre [54, II.4.4]). $\mathrm{cd}(G) = 2$.

Theorem 5.2 (Brumer [6, 6.2]). $\mathrm{scd}(G) = 2$.

See also Haberland [13, Section 6] for proofs of these theorems.

Corollary 5.3 (see Serre [55, Theorem 4]). $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Theorem 5.4. *Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension of k. Then $\mathrm{Gal}(k(p)/k_\infty)$ is a free pro-p-group of countably infinite rank.*

For proofs, see Serre [54, II,Propositions 2 and 9] and Miyake [35].

§6. Free pro-p-extensions

We consider the following problem: how large free pro-p-groups can be realized as Galois groups? To be precise, let k be a finite extension of $\mathbb{Q}$, F_d a free pro-p-group of rank d (unique up to isomorphism). A Galois extension is called an F_d-extension if the Galois group is isomorphic to F_d. We define the invariant

$$\rho = \max\{d; k \text{ has an } F_d\text{-extension}\},$$

which depends on k and p. Since k always has the cyclotomic $\mathbb{Z}_p$-extension, we always have $\rho \geq 1$.

Lemma 6.1 ([66, 2.1]). *An F_d-extension ($d \geq 1$) of k is unramified outside p.*

Hence ρ is the maximal rank of free pro-p quotient of G_{S_p}. Considering abelianization, we see that if the Leopoldt conjecture is true for k, then we have $\rho \leq r_2 + 1$. Some examples with $\rho = r_2 + 1$ and $\rho < r_2 + 1$ are known as follows.

Example 6.2. If G_{S_p} itself is free (cf. Example 3.2), then $\rho = d(G_{S_p}) = r_2 + 1$.

Proposition 6.3 ([66, 4.6]). *With the notation and assumption of Theorem 3.3, if G_{S_p} has a free pro-p product decomposition as in the theorem, then we have*

$$\rho = r_2 + 1 - \frac{1}{2} \sum_{v \in S_p - \{v_0\}} [k_v : \mathbb{Q}_p].$$

Proof. It suffices to know the maximal rank of free pro-p quotient of the Demuškin group $\mathcal{G}_v$. Using a result of J. Sonn [56], which states that there exists a surjection from a Demuškin group G to F_d if and only if $d \leq d(G)/2$, we obtain the desired formula. □

In particular, if G_{S_p} is a Demuškin group and if k is not totally real, then we have $\rho < r_2 + 1$.

Example 6.4 (cf. Example 3.5). Let $p = 3$ and $k = \mathbb{Q}(\sqrt{-3}, \sqrt{15})$. We have $\rho = 2$ and $r_2 + 1 = 3$.

See also [69] and Jaulent-Sauzet [21, 2.8] for related topics.

References

[1] M. Arrigoni, *On Demuškin groups*, Sūrikaisekikenkyūsho Kōkyūroku, **971** (1996), 116–124.

[2] M. Asada, *Construction of certain non-solvable unramified Galois extensions over the total cyclotomic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **32** (1985), 397–415.

[3] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory, **42** (1992), 285–291.

[4] ———, *Some cases of the Fontaine-Mazur conjecture, II*, J. Number Theory, **75** (1999), 161–169.

[5] A. Brumer, *Galois groups of extensions of algebraic number fields with given ramification*, Michigan Math. J., **13** (1966), 33–40.

[6] ———, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra, **4** (1966), 442–470.

[7] S. P. Demuškin, *On the maximal p-extension of a local field*, Izv. Akad. Nauk SSSR Ser. Mat., **25** (1961), 329–346. (Russian)

[8] D. Dummit and J. P. Labute, *On a new characterization of Demuskin groups*, Invent. Math., **73** (1983), 413–418.

[9] J. M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[10] A. Fröhlich, *On fields of class two*, Proc. London Math. Soc., (3) **4** (1954), 235–256.

[11] E. S. Golod and I. R. Šafarevič, *On class field towers*, Izv. Akad. Nauk. SSSR. Ser. Mat., **28** (1964), 261–272 (Russian); Amer. Math. Soc. Transl. Ser. 2, **48** (1965), 91–102; I. R. Šafarevič Collected Mathematical Papers, 317–328.
[12] G. Gras and J. F. Jaulent, *Sur les coprs de nombres réguliers*, Math. Z., **202** (1989), 343–365.
[13] K. Haberland, *Galois cohomology of algebraic number fields*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
[14] F. Hajir, *On the growth of p-class groups in p-class field towers*, J. Algebra, **188** (1996), 256–271.
[15] K. Hoechsmann, *Über die Gruppe der maximalen l-Erweiterung eines globalen Körpers*, J. Reine Angew. Math., **222** (1966), 142–147.
[16] ———, *l-extensions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 297–304, Thompson, Washington, D.C., 1967.
[17] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math., (2) **98** (1973), 246–326.
[18] ———, *On the μ-invariants of $\mathbb{Z}_l$-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, 1–11, Kinokuniya, Tokyo, 1973.
[19] ———, *Riemann-Hurwitz formula and p-adic Galois representations for number fields*, Tôhoku Math. J., (2) **33** (1981), 263–288.
[20] J. F. Jaulent and T. Nguyen Quang Do, *Corps p-rationnels, corps p-reguliers, et ramification restreinte*, J. Théor. Nombres Bordeaux, **5** (1993), 343–363.
[21] J. F. Jaulent and O. Sauzet, *Pro-l-extensions de corps de nombres l-rationnels*, J. Number Theory, **65** (1997), 240–267.
[22] Y. Kawada, *Class formations*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., 20), 96–114, Amer. Math. Soc., Providence, R.I., 1971.
[23] Y. Kida, *l-extensions of CM-fields and cyclotomic invariants*, J. Number Theory, **12** (1980), 519–528.
[24] H. Koch, *l-Erweiterungen mit vorgegebenen Verzweigungsstellen*, J. Reine Angew. Math., **219** (1965), 30–61.
[25] ———, *Beweis einer Vermutung von Höchsmann aus der Theorie der l-Erweiterungen*, J. Reine Angew. Math., **225** (1967), 203–206.
[26] ———, *Galoissche Theorie der p-Erweiterungen*, Springer-Verlag, Berlin-Heidelberg-New York, 1970.
[27] ———, *Fields of class two and Galois cohomology*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975), 609–624, Academic Press, London, 1977.
[28] ———, *On p-extensions with given ramification*, Appendix 1 to [13], 89–126.
[29] K. Komatsu, *On the maximal p-extensions of real quadratic fields unramified outside p*, J. Algebra, **123** (1989), 240–247.

[30] L. V. Kuz'min, *Homology of profinite groups, Schur multipliers, and class field theory*, Izv. Akad. Nauk SSSR Ser. Mat., **33** (1969), 1220–1254. (Russian); Math. USSR-Izv., **3** (1969), 1149–1181.

[31] ———, *The Tate module for algebraic number fields*, Izv. Akad. Nauk. SSSR. Ser. Mat., **36** (1972), 267–327. (Russian); Math. USSR-Izv., **6** (1972), 263–321.

[32] ———, *Local extensions associated with l-extensions with given ramification*, Izv. Akad. Nauk. SSSR. Ser. Mat., **39** (1975), 739–772. (Russian); Math. USSR-Izv., **9** (1975), 693–726.

[33] ———, *Some duality theorems for cyclotomic Γ-extensions of algebraic number fields of CM type*, Izv. Akad. Nauk. SSSR. Ser. Mat., **43** (1979), 483–546. (Russian); Math. USSR-Izv., **14** (1980), 441–498.

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

[35] K. Miyake, *A fundamental theorem on p-extensions of algebraic number fields*, Japan. J. Math. (N.S.), **16** (1990), 307–315.

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

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

[38] J. Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math., **6** (1969), 296–314.

[39] O. Neumann, *On p-closed algebraic number fields with restricted ramification*, Izv. Akad. Nauk SSSR Ser. Mat., **39** (1975), 259–271,471. (Russian); Math. USSR-Izv., **9** (1975), 243–254.

[40] ———, *On p-closed number fields and an analogue of Riemann's existence theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975), 625–647, Academic Press, London, 1977.

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

[42] ———, *Formations de classes et modules d'Iwasawa*, Number Theory, Noordwijkerhout 1983, 167–185, Lecture Notes in Math., 1068, Springer, Berlin-New York, 1984.

[43] ———, *K_3 et formules de Riemann-Hurwitz p-adiques*, K-theory, **7** (1993), 429–441.

[44] A. Nomura, *A remark on Boston's question concerning the existence of unramified p-extensions*, J. Number Theory, **58** (1996), 66–70.

[45] ———, *A remark on Boston's question concerning the existence of unramified p-extensions II*, Proc. Japan Acad. Ser. A, **73** (1997), 10–11.

[46] P. Roquette, *On class field towers*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 231–249, Thompson, Washington, D.C., 1967.

[47] I. R. Šafarevič, *On p-extensions*, Mat. Sb. (N.S.), **20(62)** (1947), 351–363. (Russian); Amer. Math. Soc. Transl. Ser. 2, **4** (1956), 59–72; Collected Mathematical Papers, 6–19.

[48] ———, *Extensions with given points of ramification*, Inst. Hautes Études Sci. Publ. Math., **18** (1964), 295–319. (Russian); Amer. Math. Soc. Transl. Ser. 2, **59** (1966), 128–149; Collected Mathematical Papers, 295–316.

[49] O. Sauzet, *Théorie d'Iwasawa des corps p-rationnels et p-birationnels*, Manuscripta Math., **96** (1998), 263–273.

[50] A. Schmidt, *Bounded defect in partial Euler characteristics*, Bull. London Math. Soc., **28** (1996), 463–464.

[51] ———, *Extensions with restricted ramification and duality for arithmetic schemes*, Compositio Math., **100** (1996), 233–245.

[52] P. Schneider, *Über gewisse Galoiscohomologiegruppen*, Math. Z., **168** (1979), 181–205.

[53] J. P. Serre, *Structure de certains pro-p-groupes (d'après Demuškin)*, Séminaire Bourbaki 1962/63, no. 252; Collected Papers, II, 199–207.

[54] ———, *Cohomologie galoisienne*, Lecture Notes in Math., 5, Springer, Berlin-Heidelberg-New York, 1965; *Galois cohomology*, Springer, 1997.

[55] ———, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975), 193–268, Academic Press, London, 1977; Collected Papers, III, 293–367.

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

[57] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 288–295, Inst. Mittag-Leffler, Djursholm, 1963.

[58] V. M. Tsvetkov, *Examples of extensions with Demushkin group*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), **103** (1980), 146–149,160. (Russian); J. Soviet Math., **24** (1984), 480–482.

[59] S. V. Ullom and S. B. Watt, *Generators and relations for certain class two Galois groups*, J. London Math. Soc., (2) **34** (1986), 235–244.

[60] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Math., 83, Springer, New York-Berlin, 1996.

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

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

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

[64] ———, *On the maximal unramified p-extension of an algebraic number field*, J. Reine Angew. Math., **440** (1993), 129–156.

[65] ———, *A Riemann-Hurwitz formula for the p-rank of ideal class groups of CM-fields*, J. Number Theory, **56** (1996), 319–328.

[66] M. Yamagishi, *A note on free pro-p-extensions of algebraic number fields*, J. Théor. Nombres Bordeaux, **5** (1993), 165–178.
[67] ———, *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.
[68] ———, *On the number of Galois p-extensions of a local field*, Proc. Amer. Math. Soc., **123** (1995), 2373–2380.
[69] ———, *A note on free pro-p-extensions of algebraic number fields II*, Manuscripta Math., **91** (1996), 231–233.

Department of Intelligence & Computer Science
Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan
E-mail address: yamagisi@kyy.nitech.ac.jp