

ON FREE PRO- p -EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

山岸正和 (MASAKAZU YAMAGISHI)

東京大学大学院数理科学研究科・学振特別研究員
(Department of Mathematical Sciences, University of Tokyo)

INTRODUCTION

In number theory, there often appear free pro- p -extensions (p a prime), i.e. Galois extensions whose Galois groups are free pro- p -groups. For example:

- (1) The maximal pro- p -extension of a p -adic number field not containing a primitive p -th root of unity is free (Šafarevič [Š1], Theorem 1).
- (2) The maximal unramified pro- p -extension of an algebraic function field over an algebraically closed field of characteristic p is free (Šafarevič [Š1], Theorem 2).
- (3) The maximal pro- p -extension of the cyclotomic $\mathbb{Z}_p$ -extension of an algebraic number field is free (Iwasawa [I1]).
- (4) The maximal pro- p -extension unramified outside p of the cyclotomic $\mathbb{Z}_p$ -extension of an algebraic number field is free if and only if the associated Iwasawa μ -invariant vanishes (cf. [I3], Theorem 2), and this is conjecturally always true.
- (5) The freeness of the maximal unramified pro- p -extension of the cyclotomic $\mathbb{Z}_p$ -extension of a CM-field has been investigated by Wingberg [W1].

Now we are interested in the following problem:

How large free pro- p -extension can be realized over a fixed algebraic number field?

We denote by ρ the maximal rank of free pro- p -extensions of an algebraic number field k . Since the Leopoldt conjecture states that k has exactly $r_2 + 1$ independent $\mathbb{Z}_p$ -extensions, where r_2 denotes the number of complex places of k , we have an obvious inequality $\rho \leq r_2 + 1$ under this conjecture. Some examples of k and p with $\rho = r_2 + 1$ have been known. In [Y], the author gave an explicit formula for ρ in some special cases, and in particular, gave some examples of k and p with $\rho < r_2 + 1$. We shall briefly review the results of [Y] in §1.

Our main purpose of this talk is to report a simple remark on the uniqueness of a free pro- p -extension of rank $r_2 + 1$ (when it exists). Such a uniqueness has been already proved by Iwasawa under the assumption that the Leopoldt conjecture at p is true for any finite Galois p -extension of k which is unramified outside p (cf. [Y], Proposition 2.2). We claim

Supported in part by JSPS Fellowships for Japanese Junior Scientists.

that we have only to assume the validity of the Leopoldt conjecture for the ground field k , in order to conclude the uniqueness (Theorem 2.2). We shall prove this in §2.

Finally, in §3, we shall refer to a very recent result by Wingberg [W2] on the existence of free pro- p -extensions of rank $r_2 + 1$ in the case of CM-fields (Theorem 3.1).

Acknowledgements. This report was written while I stayed at the RIMS, Kyoto University. I would like to thank the institute for the hospitality. I also express my sincere gratitude to Professor Kay Wingberg, who kindly allowed me to refer to his newest, hottest result in my talk.

1 FREE PRO- p -EXTENSIONS

In this section, we review some known facts. See [Y] for the details. Let p be a prime and let F_d denote a free pro- p -group of rank d . In particular, $F_1 \cong \mathbb{Z}_p$ (the additive group of p -adic integers). Let k be an algebraic number field, i.e. a finite extension of the rational number field $\mathbb{Q}$.

Definition 1.1. An F_d -extension K of k is a Galois extension such that the Galois group $\text{Gal}(K/k)$ is isomorphic to F_d as a topological group.

We define the invariant

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

and would like to know the exact value of ρ . The following Lemma is basic in our study.

Lemma 1.2. An F_d -extension of an algebraic number field is unramified outside the primes above p .

Let S denote the set of the primes of k above p , k_S the maximal pro- p -extension of k which is unramified outside S , and let $G_S := \text{Gal}(k_S/k)$. By Lemma 1.2, k has an F_d -extension if and only if G_S has a quotient isomorphic to F_d . Concerning the structure of the maximal abelian quotient G_S^{ab} of G_S , it is known by class field theory that G_S^{ab} has $\mathbb{Z}_p$ -rank at least $r_2 + 1$, and there is the following famous

Conjecture 1.3. (The Leopoldt conjecture in the sense of [I2], page 254) The $\mathbb{Z}_p$ -rank of G_S^{ab} is equal to $r_2 + 1$;

$$G_S^{\text{ab}} \cong \mathbb{Z}_p^{r_2+1} \times (\text{finite}).$$

Hence we obviously have $\rho \leq r_2 + 1$ if the Leopoldt conjecture is true for k and p . Note that we always have $\rho \geq 1$ because k has the cyclotomic $\mathbb{Z}_p$ -extension. Some examples of k and p with $\rho = r_2 + 1$ and also with $\rho < r_2 + 1$ are known in the following way.

First, the case where G_S itself is free would be the simplest. Since an explicit formula for the minimal number of relations of G_S was given by Šafarevič ([Š2], Theorem 5, where one can replace “ $\leq$ ” by “ $=$ ” using Tate’s duality theorem when S contains all primes above p), a necessary and sufficient condition for G_S to be free is known. In particular, when k contains a primitive p -th root of unity, G_S is free if and only if the following two conditions hold:

- (1) p does not decompose in $k/\mathbb{Q}$,
- (2) p does not divide the order of the S -ideal class group of k .

Here, the S -ideal class group is, by definition, the quotient group of the usual ideal class group by the subgroup generated by the classes of prime ideals in S . Furthermore, it is known that if G_S is free then its rank must be equal to $r_2 + 1$, hence $\rho = r_2 + 1$ holds in this case.

Example 1.4. (cf. [Š2], §4) For $k =$ the p -th cyclotomic field $\mathbb{Q}(\mu_p)$, G_S is free if and only if p is a regular prime, i.e. p does not divide the class number of k .

On the other hand, based on a result by Wingberg about free-product decomposition of G_S , the author obtained an explicit formula for ρ in some special cases.

Theorem 1.5. ([Y], Corollary 4.6) Suppose that p is an odd prime, k contains a primitive p -th root of unity, and that there exists a prime v_0 of k which does not decompose in k_S at all (then v_0 must divide p). Then we have

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

where k_v denotes the completion of k at v . In particular, for such k and p , $\rho < r_2 + 1$ holds if and only if there exist more than one primes of k above p .

Example 1.6. ([Y], page 174) Let $p = 3$, $k = \mathbb{Q}(\sqrt{-3}, \sqrt{15})$ or $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-26})$. The assumptions of Theorem 1.5 are satisfied, and we have $\rho = 2$ while $r_2 + 1 = 3$.

In general, the existence of v_0 in Theorem 1.5 can be checked in finite steps, provided that we explicitly know a basis of the ideal class group and fundamental units of k . The author knows no other example with $\rho < r_2 + 1$ for which we can apply Theorem 1.5, but there should be many such examples.

2 UNIQUENESS OF F_{r_2+1} -EXTENSIONS

We keep the notation and, in addition, let $\text{LC}(k, p)$ denote the statement that the Leopoldt conjecture for k and p is true. All algebraic extensions of k appearing in this section are considered as subfields of k_S .

Proposition 2.1. (Remark by Iwasawa, cf. [Y], Proposition 2.2) Assume $\text{LC}(L, p)$ for any finite subfield L of k_S/k . If k has an F_{r_2+1} -extension K , then the following hold.

- (1) K is unique.
- (2) Any F_d -extension ($d \leq r_2 + 1$) of k is contained in K .

We shall show that the assumption of this proposition can be weakened as follows.

Theorem 2.2. If k has an F_{r_2+1} -extension K which contains the cyclotomic $\mathbb{Z}_p$ -extension of k , then K is unique. In particular, we can prove Proposition 2.1 (1) assuming only $\text{LC}(k, p)$.

Remark 2.3. There are few examples of k and p which satisfy the assumption of Proposition 2.1, while there are many examples with $\text{LC}(k, p)$.

Remark 2.4. When $\rho < r_2 + 1$, an F_ρ -extension is not necessarily unique. For example, $\rho(k, 2) = 1$ for $k = \mathbb{Q}(\sqrt{-7})$ (cf. [Y], page 174). Since $r_2 + 1 = 2$, k has infinitely many $F_\rho (= \mathbb{Z}_2)$ -extensions.

Remark 2.5. At present, the author knows no proof of Proposition 2.1 (2) under only $\text{LC}(k, p)$.

Proof of Theorem 2.2. Let K/k be an F_{r_2+1} -extension which contains the cyclotomic $\mathbb{Z}_p$ -extension k_∞ of k .

We first prove the uniqueness of $k_\infty^{\text{ab}} \cap K$, where $^{\text{ab}}$ means the maximal abelian extension. Let $\Gamma := \text{Gal}(k_\infty/k)$ and $X := \text{Gal}(k_\infty^{\text{ab}} \cap K/k_\infty) = \text{Gal}(K/k_\infty)^{\text{ab}}$. The exact sequence of pro- p -groups

$$1 \rightarrow \text{Gal}(K/k_\infty) \rightarrow \text{Gal}(K/k) \rightarrow \Gamma \rightarrow 1$$

induces a natural action of Γ on X , hence a Λ -module structure on X , where $\Lambda = \mathbb{Z}_p[[\Gamma]]$ is the completed group ring. Since $\text{Gal}(K/k)$ is a free pro- p -group of rank $r_2 + 1$, $\text{Gal}(K/k_\infty)$ is a free pro- p - Γ -operator group of rank r_2 , and we have $X \cong \Lambda^{r_2}$ (cf. [W1], Section I). We therefore have a surjection of Λ -modules

$$\text{Gal}(k_S/k_\infty)^{\text{ab}} \twoheadrightarrow X \cong \Lambda^{r_2}.$$

On the other hand, by Iwasawa theory, there exists an injection of Λ -modules

$$\text{Gal}(k_S/k_\infty)^{\text{ab}} \hookrightarrow \Lambda^{r_2} \oplus (\Lambda\text{-torsion})$$

(cf. [I2], Theorem 17). That k_∞ is cyclotomic is necessary only for this fact. Combining these two facts, we know that the kernel of the natural surjection

$$\text{Gal}(k_S/k_\infty)^{\text{ab}} \twoheadrightarrow X$$

is just the maximal Λ -torsion Λ -submodule of $\text{Gal}(k_S/k_\infty)^{\text{ab}}$, which is independent of K . Since $k_\infty^{\text{ab}} \cap K$ is the fixed field of this kernel, it also is independent of K .

Now let

$$k_\infty = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K$$

be the tower of subfields of K/k_∞ which corresponds to the derived series of $\text{Gal}(K/k_\infty)$. Since the intersection of the derived series of a pro- p -group reduces to the identity element, we have $\bigcup_{n \geq 0} K_n = K$. It therefore suffices to prove the uniqueness of each K_n . This is trivial

for $n = 0$. Assume the uniqueness of K_n . We have clearly $K_{n+1} = K_n^{\text{ab}} \cap K$, and writing $K_n = \bigcup L$, where L runs over all finite subfields of K_n/k , we have $K_{n+1} = \bigcup (L^{\text{ab}} \cap K)$. By Schreier's formula, $\text{Gal}(K/L)$ is a free pro- p -group of rank $[L : K]r_2 + 1 = r_2(L) + 1$ (cf. Lemma 1.2), and clearly K contains the cyclotomic $\mathbb{Z}_p$ -extension L_∞ of L , therefore $L_\infty^{\text{ab}} \cap K$ is independent of K by applying what we have proved above to L . Hence $L^{\text{ab}} \cap K = L^{\text{ab}} \cap (L_\infty^{\text{ab}} \cap K)$ is also independent of K , and thus K_{n+1} is unique. $\square$

3 A RECENT RESULT BY WINGBERG ON THE EXISTENCE OF F_{r_2+1} -EXTENSIONS

Recently, Wingberg obtained a remarkable result on the existence of F_{r_2+1} -extensions of CM-fields.

Notation.

- p : an odd prime,
- k : a CM field containing a primitive p -th root of unity,
- k^+ : the maximal totally real subfield of k ,
- k_n^+ : the n -th layer of the cyclotomic $\mathbb{Z}_p$ -extension k_∞^+ of k^+ ,
- $Cl_S(k_n^+)$: the S -ideal class group of k_n^+ , where S is the set of the primes of k_n^+ above p .

Theorem 3.1. (Wingberg, [W2], Theorem 2.4, Corollary 2.7)

(1) Assume that

- (a) the Iwasawa μ -invariant of the cyclotomic $\mathbb{Z}_p$ -extension of k is zero,
- (b) no prime of k^+ above p splits in k .

If p does not divide the order of $Cl_S(k_n^+)$ for all $n \gg 0$, then k has an F_{r_2+1} -extension.

(2) Conversely, assume that

- (c) the Leopoldt conjecture is true for k and p ,
- (d) the Greenberg conjecture is true for k^+ and p , i.e. the Iwasawa λ , μ -invariants of k_∞^+/k^+ are zero.

If k has an F_{r_2+1} -extension (i.e. $\rho = r_2 + 1$, because of (c)), then p does not divide the order of $Cl_S(k_n^+)$ for all $n \gg 0$.

Note that the assumptions (a) and (c) are known to be true when k is an abelian extension of $\mathbb{Q}$, and note also that when p does not split in $k^+/\mathbb{Q}$ the following are equivalent (Iwasawa):

- (1) p does not divide the order of $Cl_S(k^+)$,
- (2) p does not divide the order of $Cl_S(k_n^+)$ for all $n \gg 0$.

We therefore have the following interesting

Corollary 3.2. ([W2], Theorem in the introduction) Let $k = \mathbb{Q}(\mu_p)$ be the p -th cyclotomic field. Then the following are equivalent:

- (1) $\rho(k, p) = (p + 1)/2$ holds and the Greenberg conjecture is true for k^+ and p .
- (2) The Vandiver conjecture is true for p , i.e. p does not divide the class number of k^+ .

Finally, we give some examples with $\rho < r_2 + 1$ using Theorem 3.1.

Example 3.3. Let $p = 3$, $k = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$, where d is a square-free positive integer. Assumptions (a) and (c) are true as we mentioned above. Suppose, for simplicity, that 3 does not decompose in k , i.e. $d \equiv 2 \pmod{3}$ or $d \equiv 3 \pmod{9}$. Assuming the Greenberg conjecture at 3 for $k^+ = \mathbb{Q}(\sqrt{d})$, we see by Theorem 3.1, that $\rho(k) < 3$ if and only if the class number of k is divisible by 3. (In that case, the exact value of $\rho(k)$ is 2 because the

subfield $\mathbb{Q}(\sqrt{-3})$ has an F_2 -extension). Thus we have many examples with $\rho < r_2 + 1$. Here is the list of such d 's (except for the Greenberg conjecture) in the range $d < 1000$.

(1) $d \equiv 2 \pmod{3}$:

$$d = 254, 257, 326, 359, 443, 473, 506, 659, 761, 785, 839, 842, 899.$$

(2) $d \equiv 3 \pmod{9}$:

$$d = 786, 894, 993.$$

Among these, the Greenberg conjecture has been verified for

$$d = 257, 326, 359, 443, 506, 659, 761, 839, 842$$

as far as the author knows.¹

REFERENCES

- [I1] K. Iwasawa, *On solvable extensions of algebraic number fields*, Ann. of Math. **58** (1953), 548–572.
- [I2] K. Iwasawa, *On $\mathbb{Z}_\ell$ -extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.
- [I3] K. Iwasawa, *Riemann-Hurwitz formula and p -adic Galois representations for number fields*, Tôhoku Math. J. **33** (1981), 263–288.
- [Š1] I. R. Šafarevič, *On p -extensions*, Mat. Sb. **20** (**62**) (1947), 351–363 (Russian); English transl., Amer. Math. Soc. Transl. Ser. 2 **4** (1956), 59–72; see also, Collected Mathematical Papers, Springer-Verlag, Berlin Heidelberg New York, 1989, pp. 6–19.
- [Š2] I. R. Šafarevič, *Extensions with given ramification points*, Inst. Hautes Études Sci. Publ. Math. **18** (1964), 295–319 (Russian); English transl., Amer. Math. Soc. Transl. Ser. 2 **59** (1966), 128–149; see also, Collected Mathematical Papers, Springer-Verlag, Berlin Heidelberg New York, 1989, pp. 295–316.
- [W1] K. Wingberg, *On the maximal unramified p -extension of an algebraic number field*, J. reine angew. Math. **440** (1993), 129–156.
- [W2] K. Wingberg, *On free pro- p -extensions of algebraic number fields of CM-type*, preprint.
- [Y] M. Yamagishi, *A note on free pro- p -extensions of algebraic number fields*, Journ. Théor. Nombres Bordeaux **5** (1993), 165–178.

¹I am grateful to Hisao Taya for information about the Greenberg conjecture for real quadratic fields.