On embedding problems with restricted ramifications

著者	Nomura Akito, 野村 明人
journal or publication title	Archiv der Mathematik
volume	73
number	3
page range	199-204
year	1999-01-01
URL	http://hdl.handle.net/2297/1722

doi: <https://doi.org/10.1007/s000130050028>

On embedding problems with restricted ramifications

Akito Nomura

Department of Mathematics, Kanazawa University,
Kanazawa 920-1192, Japan

(abstract) Let L/k be a Galois extension with Galois group G , and $(\varepsilon) : 1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$ a central extension. We study the existence of the Galois extension $M/L/k$ such that the Galois group $\text{Gal}(M/k)$ is isomorphic to E and that M/L is unramified outside S , where S is a finite set of primes of L . As an application, we also study the class number of the Hilbert p -class field.

MSC Number : 11R29, 12F12

INTRODUCTION

Let k be an algebraic number field of finite degree, and $\mathfrak{G}$ its absolute Galois group. Let L/k be a finite Galois extension with Galois group G , and $(\varepsilon) : 1 \rightarrow A \rightarrow E \xrightarrow{j} G \rightarrow 1$ a group extension with an abelian kernel A , and S a set of primes of L . Then an embedding problem $(L/k, \varepsilon, S)$ is defined by the diagram

$$\begin{array}{ccccccc} & & & & \mathfrak{G} & & \\ & & & & \downarrow \varphi & & (*) \\ (\varepsilon) : 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G \longrightarrow 1 \end{array}$$

where φ is the canonical surjection. A solution of the embedding problem $(L/k, \varepsilon, S)$ is, by definition, a continuous homomorphism ψ of $\mathfrak{G}$ to E satisfying the conditions: (1) $j \circ \psi = \varphi$, (2) M/L is unramified outside S , where M is the Galois extension over k corresponding to the kernel of ψ . A solution ψ is called a proper solution if it is surjective. In case S is the set of all primes of L , the embedding problem $(L/k, \varepsilon, S)$ is denoted by $(L/k, \varepsilon)$. The Galois extension over k corresponding to the kernel of any solution is called a solution field.

Neukirch[3] and Crespo[1] studied the sufficient conditions for $(L/k, \varepsilon, S)$ to have a solution under the assumption that S contains all primes which are ramified in L/k and are the divisors of the cardinality of A . In the previous paper [5], we studied some sufficient conditions for $(L/k, \varepsilon, \emptyset)$ to have a proper solution in the case that p is an odd prime, (ε) is a non-split central extension of kernel isomorphic to $\mathbf{Z}/p\mathbf{Z}$, and k is either the rational number field $\mathbf{Q}$ or an imaginary quadratic field with the class number prime to p (p is not equal to 3 when $k = \mathbf{Q}(\sqrt{-3})$). In the present paper, we shall study the case that k is any finite number field and S is not necessary empty. And, as an application, we shall give some sufficient conditions for the class number divisible by p .

Acknowledgements. The author would like to thank P.Roquette and E.Lamprecht for valuable advices.

1. Some lemmas

In this section, we quote some lemmas without proofs.

Let k be an algebraic number field, and $(L/k, \varepsilon)$ an embedding problem defined by the diagram $(*)$ with a finite abelian group A of odd order.

For each prime $\mathfrak{q}$ of k , we denote by $k_{\mathfrak{q}}$ (resp. $L_{\mathfrak{q}}$) the completion of k (resp. L) by $\mathfrak{q}$ (resp. an extension of $\mathfrak{q}$ to L). Then the local problem $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ of $(L/k, \varepsilon)$ is defined by the diagram

$$\begin{array}{ccccccc} & & & & \mathfrak{G}_{\mathfrak{q}} & & \\ & & & & \downarrow \varphi|_{\mathfrak{G}_{\mathfrak{q}}} & & \\ (\varepsilon_{\mathfrak{q}}) : 1 & \longrightarrow & A & \longrightarrow & E_{\mathfrak{q}} & \xrightarrow{j|_{E_{\mathfrak{q}}}} & G_{\mathfrak{q}} \longrightarrow 1 \end{array}$$

where $G_{\mathfrak{q}}$ is the Galois group of $L_{\mathfrak{q}}/k_{\mathfrak{q}}$, which is isomorphic to the decomposition group of $\mathfrak{q}$ in L/k , $\mathfrak{G}_{\mathfrak{q}}$ is the absolute Galois group of $k_{\mathfrak{q}}$, and $E_{\mathfrak{q}}$ is the inverse of $G_{\mathfrak{q}}$ by j .

In the same manner as the case of $(L/k, \varepsilon)$, solutions, solution fields etc. are defined for $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$.

Let p be an odd prime.

Lemma 1 (Neukirch[3]) *Let $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(L/k) \rightarrow 1$ be a central extension, and assume that $(L/k, \varepsilon)$ has a solution. Let T be a finite set of primes of k , and $M(\mathfrak{q})$ be a solution field of $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ for $\mathfrak{q}$ of T . Then there exists a solution field of $(L/k, \varepsilon)$ such that the completion of M by $\mathfrak{q}$ is equal to $M(\mathfrak{q})$ for each $\mathfrak{q}$ of T .*

Lemma 2 (Nomura[5]) *Let $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(L/k) \rightarrow 1$ be a non-split central extension. Then every solution of $(L/k, \varepsilon)$ is a proper solution.*

For a finite set T of primes of k , let $B_k(T) = \{\alpha \in k^* | (\alpha) = \mathfrak{a}^p \text{ for some ideal } \mathfrak{a} \text{ of } k, \text{ and } \alpha \in k_{\mathfrak{q}}^p \text{ for any prime } \mathfrak{q} \text{ of } T\}$. We shall denote by $\sigma(T)$ the dimension of $B_k(T)/k^{*p}$ over $\mathbf{Z}/p\mathbf{Z}$.

Lemma 3 (Shafarevich[7;Theorem 1]) *Let T be a set of primes of k , and k_T/k the maximal p -extension unramified outside T . The number of generators*

$d(T)$ of $\text{Gal}(k_T/k)$ is given by

$$d(T) = t(T) + \lambda(T) + \sigma(T) - \varrho_p,$$

where $t(T)$ is the number of $\mathfrak{q} \in T$ for which $\zeta_p \in k_{\mathfrak{q}}$,

$$\lambda(T) = \sum_{\mathfrak{q}|p, \mathfrak{q} \in T} n(\mathfrak{q}), n(\mathfrak{q}) = [k_{\mathfrak{q}} : \mathbf{Q}_q], \mathfrak{q}|q$$

and ϱ_p is the p -rank of the unit group of k .

(sketch of the proof) Let J be the idele group of k , and $\mathfrak{U}_T$ (resp. $\mathfrak{U}$) be the T -idele group (resp. unit idele group) of k . We shall write $H_T = J/\mathfrak{U}_T \cdot J^p \cdot k$, then $d(T) = \dim_{\mathbf{Z}/p\mathbf{Z}} H_T$. Then the sequence

$$1 \rightarrow B_k(T)/k^p \xrightarrow{f_4} B_k(\emptyset)/k^p \xrightarrow{f_3} \mathfrak{U}/\mathfrak{U}_T \mathfrak{U}^p \xrightarrow{f_2} H_T \xrightarrow{f_1} H_{\emptyset} \rightarrow 1$$

is exact, where $f_i (i = 1, 2, 3, 4)$ are defined as follows;

f_1 is the natural map onto the factor group $H_{\emptyset} = H_T/(\mathfrak{U} \cdot J^p \cdot k/\mathfrak{U}_T J^p k)$.

$f_2(\mathfrak{a}) = \mathfrak{a}\mathfrak{U}_T J^p k$, for $\mathfrak{a} \in \mathfrak{U}$.

$f_3(\alpha) = \alpha\alpha^{-p}\mathfrak{U}_T \mathfrak{U}^p$, where $\mathfrak{a}^p = \alpha$.

f_4 is the natural injection.

We can easily proved that

$$\dim_{\mathbf{Z}/p\mathbf{Z}} \mathfrak{U}/\mathfrak{U}_T \mathfrak{U} = t(T) + \lambda(T), \quad \dim_{\mathbf{Z}/p\mathbf{Z}} B_k(\emptyset)/k^p = \dim_{\mathbf{Z}/p\mathbf{Z}} H_{\emptyset} + \varrho_p.$$

By the exactness of above sequence, we have thus proved.

2. Main theorem and applications

We denote by $P_1(L/K)$ (resp. $P_2(L/K)$) the set of primes of L which is ramified in L/K and not lying above p (resp. lying above p). Moreover, let ϱ_p be the p -rank of the unit group of k and Cl_k the ideal class group of k .

The following is a main theorem of the present paper.

Theorem *Let p be an odd prime, and $L/K/k$ a Galois extension such that L/K is a p -extension and that the degree $[K : k]$ is prime to p . Let S be a finite set of primes of L , which contains the set $P_1(L/K)$ and disjoint to $P_2(L/K)$, and $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(L/k) \rightarrow 1$ be a non-split central extension. Assume that the following conditions (C1) (C2) (C3) are satisfied.*

(C1) *The embedding problem $(L/k, \varepsilon)$ has a solution.*

(C2) *For any prime $\mathfrak{p}$ of k lying above p , the local problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \varepsilon_{\mathfrak{p}})$ has a solution $\psi_{\mathfrak{p}}$ such that $M_{\mathfrak{p}}/L_{\mathfrak{p}}$ is unramified, where $M_{\mathfrak{p}}$ is a solution field corresponding to $\psi_{\mathfrak{p}}$.*

(C3) *$B_k(S_0) = k^{*p}$, where S_0 is the set of prime $\mathfrak{q}$ of k such that $\mathfrak{q}$ is the restriction of some prime contained in S .*

Then, $(L/k, \varepsilon, S)$ has a solution, which is necessarily proper by Lemma 2. That is to say, there exists a Galois extension M/k such that

- (i) $1 \rightarrow \text{Gal}(M/L) \rightarrow \text{Gal}(M/k) \rightarrow \text{Gal}(L/k) \rightarrow 1$ coincides with (ε) , and
- (ii) M/L is unramified outside S .

Remark (1) By using the theory of embedding problems, we can easy to see the following. (Cf. Neukirch[3; Theorem 2.2, Theorem 3.2], Nomura[5; Theorem 8]). If any prime lying above p is unramified in L/K , then the conditions (C2) hold. If L/K is

locally cyclic, and the exponent of the p -Sylow subgroup of E is p then the conditions (C1) hold. In particular, if L/K is unramified, then (C1) (C2) hold.

(2) If k is either the rational number field $\mathbf{Q}$ or an imaginary quadratic field with the class number prime to p ($p \neq 3$ when $k = \mathbf{Q}(\sqrt{-3})$), then $B_k(\emptyset) = k^{*p}$ and therefore $B_k(S_0) = k^{*p}$ for any S_0 .

(3) There exists a finite set S_0 of primes of k satisfying the following conditions: (i) S_0 does not contain any prime lying above p , (ii) $B_k(S_0) = k^{*p}$, (iii) $|S_0| = \varrho_p + p\text{-rank}Cl_k$.

Indeed, let $F = k(\sqrt[p]{\alpha}; \alpha \in B_k(\emptyset))$. Then the Galois group $\text{Gal}(F/k(\zeta_p))$ is an abelian p -group and isomorphic to $(\mathbf{Z}/p\mathbf{Z})^m$, where $m = \varrho_p + p\text{-rank}Cl_k$. By Chebotarev's density theorem, there exist primes $q_1, q_2, \dots, q_m$ such that the Frobenius of q_i ($i = 1, 2, \dots, m$) generate $\text{Gal}(F/k(\zeta_p))$. Then $S_0 = \{q_1, \dots, q_m\}$ is a required set.

(4) There does not always exist a non-split central extension $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(L/k) \rightarrow 1$. It is well-known that there is one-one correspondence between the element of $H^2(\text{Gal}(L/k), \mathbf{Z}/p\mathbf{Z})$ and the equivalent class of central extensions of $\text{Gal}(L/k)$ with kernel isomorphic to $\mathbf{Z}/p\mathbf{Z}$. For example, let l and p be distinct odd primes, and assume that the least positive integer f that satisfies the condition $p^f \equiv 1 \pmod{l}$ is even. Let $L/K/k$ be a Galois extension such that L/K is a p -extension and that K/k is an abelian l -extension. Then $H^2(\text{Gal}(L/k), \mathbf{Z}/p\mathbf{Z}) \neq 0$. (Cf. Nomura[5]).

Proof of Theorem By Lemma 1 and the assumption (C1) (C2), there exists a solution field M_1/k of $(L/k, \varepsilon)$ such that any prime of L lying above p is unramified in M_1/L . By Lemma 2, M_1/k gives a proper solution. If M_1/L is unramified outside S , then M_1/k is a required Galois extension. Suppose that M_1/L is not unramified outside S , and take a prime $\hat{q}$ of L ramified in M_1/L and not contained in S . Let $\tilde{q}$ be an extension of $\hat{q}$ to M_1 , and q the restriction to k . Now we consider the local extension $M_{1\tilde{q}}/k_q$. Let J be a subgroup of $\text{Gal}(L_{\tilde{q}}/k_q)$ such that the index of J in $\text{Gal}(L_{\tilde{q}}/k_q)$ is equal to $[L_{\tilde{q}} : K_q]$, and F be the fixed field of J in $L_{\tilde{q}}/k_q$. Thus $M_{1\tilde{q}}/F$ is a split central extension of L_q/F . Let q_0 be the restriction of $\tilde{q}$ to F . Then q_0 is ramified in a cyclic extension over F of degree p . Therefore $N(q_0) \equiv 1 \pmod{p}$, where N denotes the absolute norm. Since F/k_q is a p -extension, there exists a nonnegative integer r such that $N(q_0) = N(q)^{p^r}$. Hence $N(q) \equiv 1 \pmod{p}$. By Lemma 3, $d(S_0 \cup \{q\}) = d(S_0) + 1$, hence there exists a cyclic extension $k(q)/k$ of degree p which is unramified outside $S_0 \cup \{q\}$ and q is ramified.

Let $\bar{q}$ be an extension of q to $M_1 \cdot k(q)$, and M_2 denotes the inertia field of $\bar{q}$ in $M_1 \cdot k(q)/L$. Since q is prime to p , $M_1 \cdot k(q)/M_2$ is a cyclic extension. Since $\hat{q}$ is ramified in M_1/L and $L \cdot k(q)/L$, M_2 is not equal to anyone of L, M_1 , and $M_1 \cdot k(q)$. Since $\text{Gal}(M_1 \cdot k(q)/L)$ is contained in the center of $\text{Gal}(M_1 \cdot k(q)/k)$, M_2/k is a Galois extension and the Galois group $\text{Gal}(M_2/k)$ is isomorphic to $\text{Gal}(M_1/k)$. Hence M_2/k gives a proper solution of $(L/k, \varepsilon)$. By the choice of $k(q)$ and M_2 , every prime of L which is not contained in S and unramified in M_1/L is unramified in M_2/L , and $\tilde{q}$ is also unramified in M_2/L . By repeating this process, we can take a required extension M/k . This proves the theorem.

Corollary 1. *Assume the same conditions as Theorem. If the exponent of the p -Sylow subgroup of E is equal to p , then $(L/k, \varepsilon, S - P_1(L/K))$ has a proper solution.*

Proof. Let $M/L/k$ be a Galois extension corresponding to a proper solution of $(L/k, \varepsilon, S)$. Let $\mathfrak{q}$ be a prime of L contained in $P_1(L/K)$, and $K(\mathfrak{q})$ the inertia field of $\mathfrak{q}$ in L/K . Since the exponent of $\text{Gal}(M/K(\mathfrak{q}))$ is p , $\text{Gal}(M/K(\mathfrak{q}))$ is isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. By using the Hilbert's theory of ramification, $\mathfrak{q}$ can not be ramified in M/L .

Corollary 2. *Let p be an odd prime, and $L/K/k$ a Galois extension such that L/K is an unramified p -extension and that the degree $[K : k]$ is prime to p . If p -rank of the cohomology group $H^2(\text{Gal}(L/k), \mathbf{Z}/p\mathbf{Z})$ is greater than $\varrho_p + p\text{-rank } Cl_k$, then the class number of L is divisible by p .*

Proof. By Remark (3), there exists a finite set S_0 of primes of k satisfying the conditions: (i) S_0 does not contain any prime lying above p , (ii) $B_k(S_0) = k^{*p}$, (iii) $|S_0| = \varrho_p + p\text{-rank } Cl_k$. Let S be the set of primes of L which is an extension of $\mathfrak{q} \in S_0$. For each $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow \text{Gal}(L/k) \rightarrow 1$, let M_ε be a Galois extension corresponding to a proper solution of $(L/k, \varepsilon, S)$. Let M be the composite field of M_ε for all ε . Then by Remark (4), the Galois group $\text{Gal}(M/L)$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^m$, where m is equal to the p -rank of $H^2(\text{Gal}(L/k), \mathbf{Z}/p\mathbf{Z})$. For $\mathfrak{q} \in S_0$, denote by $M(\mathfrak{q})$ the inertia field of $\hat{\mathfrak{q}}$ in M/L , where $\hat{\mathfrak{q}}$ is an extension of $\mathfrak{q}$ to L . Since $\text{Gal}(M/L)$ is contained in the center of $\text{Gal}(M/k)$, $M(\mathfrak{q})/L/k$ is Galois. Then any prime of L lying above $\mathfrak{q}$ is unramified in $M(\mathfrak{q})/L$. Let M^* be the intersection of $M(\mathfrak{q})$ for all $\mathfrak{q}$ of S_0 . If $m > |S_0|$, then M^*/L is a non-trivial p -extension. Hence the class number of L is divisible by p .

The idea of the above proof is similar to that of Lamprecht[2].

And the following Corollary is well-known, which has been proved by Golod-Shafarevich. (Cf. Roquette[6]) We shall consider from the viewpoint of the theory of central extensions.

Corollary 3. *Let p be an odd prime, and L/k an unramified p -extension. Assume that the p -rank of the ideal class group of k is greater than or equal to $2 + 2\sqrt{\varrho_p + 1}$. Then the class number of L is divisible by p , and therefore the p -class field tower is infinite.*

Proof. Let k_1 be the Hilbert p -class field of k . If k_1 is not contained in L , then $k_1 \cdot L/L$ is unramified abelian p -extension. Hence, in this case, the class number of L is divisible by p . For this reason, we assume that k_1 is contained in L . It is well known that $r(G) > \frac{1}{4}d(G)^2$, where G is a finite p -group, $d(G)$ is the generator rank, $r(G)$ is the relation rank which is equal to the p -rank of $H^2(G, \mathbf{Z}/p\mathbf{Z})$. By class field theory, $d(\text{Gal}(L/k))$ is equal to the p -rank of Cl_k . Then the condition $\frac{1}{4}d(\text{Gal}(L/k))^2 \geq \varrho_p + p\text{-rank } Cl_k$ is equivalent to $p\text{-rank } Cl_k \geq 2 + 2\sqrt{\varrho_p + 1}$. By applying Corollary 2 we can complete the proof of Corollary 3.

Corollary 4. *Let p be an odd prime, and L the Hilbert p -class field of k . Assume that the p -rank of the ideal class group of k is greater than $\frac{1}{2}(1 + \sqrt{1 + 8\varrho_p})$, then the class number of L is divisible by p .*

Proof. Since $\text{Gal}(L/k)$ is abelian, the p -rank of $H^2(\text{Gal}(L/k), \mathbf{Z}/p\mathbf{Z})$ is equal to $\frac{n(n+1)}{2}$, where n is the p -rank of the ideal class group of k . By using Corollary 2, we have thus proved.

Example Let p be an odd prime and $m(k, p) = \frac{1}{2}(1 + \sqrt{1 + 8\varrho_p})$.

If k is imaginary (resp. real) quadratic field ($\neq \mathbf{Q}(\sqrt{-3})$), then $m(k, p)$ is equal to 1 (resp. 2). And if $k/\mathbf{Q}$ is cyclic of degree 3, then $m(k, p)$ is $2.56 \dots$.

Remark In the previous paper [4], we have proved the following. Let p be an odd prime and k a quadratic field. If p -rank $Cl_k \geq 2$, then there exists an unramified Galois extension M/k such that $\text{Gal}(M/k)$ is isomorphic to the group $\langle x, y | x^p = y^p = z^p = 1, x^{-1}yx = yz, xz = zx, yz = zy \rangle$.

REFERENCES

1. T.Crespo, Embedding problem with ramification conditions, Arch.Math. **53** (1989), 270-276.
2. E.Lamprecht, Existenz von Zahlkörpern mit nicht abbrechendem Klassenkörperturm, Arch. Math.(Basel) **43** (1967), 140-152.
3. J.Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent.Math. **21** (1973), 59-116.
4. A.Nomura, On the existence of unramified p -extensions, Osaka J. Math. **28** (1991), 55-62.
5. A.Nomura, On the class number of certain Hilbert class fields, Manuscripta Math. **79** (1993), 379-390.
6. P.Roquette, On class field towers, in "Algebraic Number Theory" ed. J.Cassels, A.Fröhlich, Academic Press, 1980.
7. I.R.Shafarevich, Extensions with given points of ramification, AMS Translation, Ser.2 **59** (1966), 128-149.