Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 79–86

Embedding Problems with restricted Ramifications and the Class Number of Hilbert Class Fields

Akito Nomura

§1. 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 $(\varepsilon) : 1 \to A \to E \xrightarrow{j} G \to 1$ a group extension with an abelian kernel A. Then an embedding problem $(L/k, \varepsilon)$ is defined by the diagram

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

where φ is the canonical surjection. When (ε) is a central extension, we call $(L/k, \varepsilon)$ a central embedding problem. A solution of the embedding problem $(L/k, \varepsilon)$ is, by definition, a continuous homomorphism ψ of $\mathfrak{G}$ to E satisfying the conditions $j \circ \psi = \varphi$. We say the embedding problem $(L/k, \varepsilon)$ is solvable if it has a solution. The Galois extension over k corresponding to the kernel of any solution is called a solution field. A solution ψ is called a proper solution if it is surjective. The existence of a proper solution of $(L/k, \varepsilon)$ is equivalent to the existence of a Galois extension $M/L/k$ such that the canonical sequence $1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/k) \to \mathrm{Gal}(L/k) \to 1$ coincides with ε.

Let S be a finite set of primes of L. An embedding problem with ramification conditions $(L/k, \varepsilon, S)$ is defined by the diagram $(*)$, which is same to the case of $(L/k, \varepsilon)$. A solution ψ is called a solution of $(L/k, \varepsilon, S)$ if M/L is unramified outside S, where M is the solution field corresponding to ψ. We remark that these definitions are a little different from those in [3] and [8], but essentially of the same nature.

Received August 28, 1998.
Revised October 24, 1998.

§2. Central embedding problems

In this section, we quote some well-known results about central embedding problems without proofs. General studies on embedding problem are in Hoechsmann[5] and Neukirch[8].

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

Fact 1. If L/k is unramified or (ε) is split, then $(L/k,\varepsilon)$ is solvable.

Fact 2 (Ikeda[6]). If $(L/k,\varepsilon)$ is solvable, then $(L/k,\varepsilon)$ has a proper solution.

We remark that Fact 2 is always true in case A is abelian not necessary (ε) is central.

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

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

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.

Fact 3. Let $(\varepsilon): 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/k) \to 1$ be a central extension. If $(L_\mathfrak{q}/k_\mathfrak{q},\varepsilon_\mathfrak{q})$ is solvable for every prime $\mathfrak{q}$, then $(L/k,\varepsilon)$ is solvable.

Fact 4 (Neukirch[8]). Let $(\varepsilon): 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/k) \to 1$ 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 M 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.

By using this fact, we can construct a good solution of $(L/k,\varepsilon)$.

§3. Main theorem

Let L/K be a Galois extension of an algebraic number field K. 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). Let T be a finite set of primes of k, and denote by $B_k(T)$ the set $\{\alpha \in k^* | (\alpha) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ of k, and $\alpha \in {k_\mathfrak{q}}^p$ for every prime $\mathfrak{q}$ of $T\}$.

The following is a main theorem of this article.

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 $(\varepsilon) : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/k) \to 1$ be a non-split central extension. Assume that the following conditions* (C1), (C2) *and* (C3) *are satisfied.*

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

(C2) *For every 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 proper solution. That is to say, there exists a Galois extension M/k such that

(i) $1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/k) \to \mathrm{Gal}(L/k) \to 1$ *coincides with* (ε), *and*

(ii) *M/L is unramified outside S.*

Remark. (1) There does not always exist a non-split central extension $(\varepsilon) : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/k) \to 1$. The existence is equivalent to the non-vanishing of the cohomology group $\mathrm{H}^2(\mathrm{Gal}(L/k), \mathbf{Z}/p\mathbf{Z})$.

(2) If k is the rational number field $\mathbf{Q}$ and L/K is unramified, then the conditions (C1), (C2) and (C3) are satisfied.

As a simple case of the main theorem, we have the following. We treat the sketch of the proof of the following instead of the main theorem. For details, see [10] and [13].

Proposition 1. *Let p be an odd prime, and $L/K/\mathbf{Q}$ a Galois extension such that L/K is an unramified p-extension and that the degree $[K : \mathbf{Q}]$ is prime to p. Let $(\varepsilon) : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$ be a non-split central extension.*

Then there exists a Galois extension $M/\mathbf{Q}$ such that

(i) $1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/\mathbf{Q}) \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$ *coincides with* (ε), *and*

(ii) *M/L is unramified.*

(sketch of the proof.) In this case, by using the general theory of embedding problems, we can easily see that the problem $(L/\mathbf{Q}, \varepsilon)$ is solvable. By virtue of Fact 2 we can take a solution field $M_1/L/\mathbf{Q}$ such that every prime $\mathfrak{P}$ of L lying above p is unramified in M_1/L. Let $\mathfrak{Q}$ be a prime of L ramified in M_1/L, and q the prime number below $\mathfrak{Q}$. Then $q \equiv 1 \bmod p$. Hence there exists a field F such that $\mathbf{Q} \subset F \subset \mathbf{Q}(\zeta_q)$ and that $[F : \mathbf{Q}] = p$. Let M_2 be the inertia field of $\mathfrak{Q}$ in M_1F/L, then M_2 is also a solution field of $(L/\mathbf{Q}, \varepsilon)$. And the number of primes ramified in M_2/L is less than that of in M_1/L. By repeating this process, we can take a required extension.

§4. Applications

Let D be the group defined by

$$< x, y, z \,|\, x^p = y^p = z^p = 1, yxy^{-1} = xz, zx = xz, yz = zy > .$$

This is a non-abelian p-group of order p^3.

Proposition 2. *Let K be a quadratic field, and assume that the p-rank of the ideal class group of K is greater than or equal to 2. Then there exists a Galois extension M/K such that the Galois group is isomorphic to D and that M/K is unramified.*

(sketch of the proof.) Let L/K be an unramified extension such that the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Then the Galois group $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to

$$< a, b, c \,|\, a^p = b^p = c^2 = 1, ab = ba, cac^{-1} = a^{-1}, cbc^{-1} = b^{-1} > .$$

Let $E =< x, y, z, t \,|\, x^p = y^p = z^p = t^2 = 1, y^{-1}xy = xz, zx = xz, yz = zy, t^{-1}xt = x^{-1},\ t^{-1}yt = y^{-1}, tz = zt >$.

Then $1 \to < z > \to E \xrightarrow{j} \mathrm{Gal}(L/\mathbf{Q}) \to 1$ is a non-split central extension, where j is defined by $x \to a, y \to b, t \to c$.

Since the Sylow subgroup of E is isomorphic to D, then by applying Proposition 1, we can take a required extension.

Let K_1 be the Hilbert p-class field of K, and K_2 the central p-class field of K_1/K. The following proposition is obtained by Miyake.

Proposition 3 (Miyake[7]). *Let K be a quadratic field. Then the Galois group $\mathrm{Gal}(K_2/K_1)$ is isomorphic to $\mathrm{Gal}(K_1/K) \wedge \mathrm{Gal}(K_1/K)$,* *where* $\wedge$ *denotes the exterior square. Further assume that the p-Sylow subgroup of the ideal class group of K is isomorphic to* $\mathbf{Z}/p^{e_1}\mathbf{Z}\times\mathbf{Z}/p^{e_2}\mathbf{Z}\times\cdots\times\mathbf{Z}/p^{e_r}\mathbf{Z}$ $(1\le e_1\le e_2\le\cdots\le e_r)$.

Then the Galois group $\mathrm{Gal}(K_2/K)$ *is isomorphic to*

$$< a_i, c_{i,j} \mid i=1,2,\cdots,r,\ j=i+1,\cdots,r >;$$
$$a_i^{p^{e_i}} = c_{i,j}^{p^{e_i}} = 1,\ [a_i,a_j]=c_{i,j},\ [a_i,c_{m,n}]=[c_{i,j},c_{m,n}]=1,$$
$$i=1,2,\cdots,r, j=i+1,\cdots r, 1\le m<n\le r.$$

Let ϱ_p be the p-rank of the unit group of k and Cl_k the ideal class group of k.

Proposition 4 (Nomura[13]). *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* $\mathrm{H}^2(\mathrm{Gal}(L/k),\mathbf{Z}/p\mathbf{Z})$ *is greater than* ϱ_p*+p-rank* Cl_k*, then the class number of L is divisible by p.*

(sketch of the proof.) 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) $|S_0|=\varrho_p+p$-rank Cl_k.

Indeed, let $F = k(\sqrt[p]{\alpha};\alpha\in B_k(\emptyset))$. Then the Galois group $\mathrm{Gal}(F/k(\zeta_p))$ is an abelian p-group and isomorphic to $\left(\mathbf{Z}/p\mathbf{Z}\right)^m$, where $m=\varrho_p+p\text{-rank}Cl_k$. By Chevotarev's density theorem, there exist primes $\mathfrak{q}_1,\mathfrak{q}_2,\cdots,\mathfrak{q}_m$ such that the Frobenius automorphism of $\mathfrak{q}_i$ $(i=1,2,\cdots,m)$ generate $\mathrm{Gal}(F/k(\zeta_p))$. Then $S_0=\{\mathfrak{q}_1,\cdots,\mathfrak{q}_m\}$ is a required set.

Let S be the set of primes of L which is an extension of $\mathfrak{q}\in S_0$. For each $(\varepsilon): 1\to\mathbf{Z}/p\mathbf{Z}\to E\to\mathrm{Gal}(L/k)\to 1$, 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 the Galois group $\mathrm{Gal}(M/L)$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^m$, where m is equal to the p-rank of $\mathrm{H}^2(\mathrm{Gal}(L/k),\mathbf{Z}/p\mathbf{Z})$. For $\mathfrak{q}\in S_0$, denote by $M(\mathfrak{q})$ the inertia field of $\widehat{\mathfrak{q}}$ in M/L, where $\widehat{\mathfrak{q}}$ is an extension of $\mathfrak{q}$ to L. Since $\mathrm{Gal}(M/L)$ is contained in the center of $\mathrm{Gal}(M/k)$, $M(\mathfrak{q})/L/k$ is a Galois extension. Then every 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.

Proposition 5. *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* $(1+\sqrt{1+8\varrho_p})/2$*, then the class number of L is divisible by p.*

(proof.) Since $\mathrm{Gal}(L/k)$ is abelian, the p-rank of $\mathrm{H}^2(\mathrm{Gal}(L/k), \mathbf{Z}/p\mathbf{Z})$ is equal to $n(n+1)/2$, where n is the p-rank of the ideal class group of k. By using Proposition 4, we have thus proved the proposition.

We investigate an application to the Boston's question, which is related to the Fontaine-Mazur conjecture. For the Fontaine-Mazur conjecture, see [1], [2] and [4].

Conjecture (Fontaine-Mazur). Let K^{ur} be the maximal unramified extension of an algebraic number field K. For any K, positive integer n and representation $\rho : \mathrm{Gal}(K^{ur}/K) \to \mathrm{GL}_n(\mathbf{Q}_p)$, the image of ρ is finite.

Let p be an odd prime. A pro-p group G is called powerful if $G/\overline{G^p}$ is abelian, where the line denotes topological closure.

In [1] Boston introduced the following, which is equivalent to the above conjecture.

Conjecture (Fontaine-Mazur-Boston). For any algebraic number field K, there does not exist an unramified pro-p extension $\tilde{K}/K$ such that the degree $[\tilde{K} : K]$ is infinite and that the Galois group is powerful.

Boston pointed out that this conjecture is closely related to the existence of unramified p-extensions of a certain type, and introduced the following question.

Question (Boston). Let K be a number field, p an odd prime, and $K(p)$ its p-class field. Suppose that the class number of $K(p)$ is divisible by p. Then is there always an everywhere unramified extension M of degree p of $K(p)$ such that M is Galois over K and $exp(\mathrm{Gal}(M/K)) = exp(\mathrm{Gal}(K(p)/K))$? The "*exp*" stands for the exponent of the group.

Remark (Boston). (1) The truth of the Fontaine-Mazur conjecture implies an affirmative answer, when K has an infinite p-class field tower.

(2) Lemmermeyer noticed that the answer to this question is in the negative in general. He pointed out an example, due to Scholz and Taussky[14]. The Galois group of the maximal unramified 3-extension of $\mathbf{Q}(\sqrt{-4027})$ is isomorphic to $< x, y \,|\, y^{(x,y)} = y^{-2}, x^3 = y^3 >$. This group has a non-abelian subgroup of order 27 and exponent 9. Let K be the corresponding intermediate field, its 3-class field is an elementary abelian extension of degree 9 contained in no larger unramified extension with Galois group of exponent 3. Since the class field tower of K is finite, this is not a counter example of Fontaine-Mazur conjecture.

We produce some sufficient conditions for the answer to Boston's question for K and p is affirmative. For detail and other results, see [11] and [12].

Proposition 6. (1) *Let l and p be odd primes such that the order of p mod l is even. Assume that $K/\mathbf{Q}$ is an abelian l-extension and the class number of K is divisible by p. Then there exists an unramified non-abelian p-extension M/K such that the exponent of* $\mathrm{Gal}(M/K)$ *is p, and therefore the answer to Boston's question for K and p is affirmative.*

(2) *Let p be an odd prime, and K a quadratic field. Then the answer to Boston's question for K and p is affirmative.*

(sketch of the proof.) (1) There exists a Galois extension $L/K/\mathbf{Q}$ such that L/K is an unramified abelian p-extension of exponent p. Under the assumption of p and l, the cohomology group $\mathrm{H}^2(\mathrm{Gal}(L/\mathbf{Q}), \mathbf{Z}/p\mathbf{Z})$ is non-trivial. Hence there exists an non-split central extension $(\varepsilon) : 1 \to \mathbf{Z}/p\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$. By Proposition 1, there exists a Galois extension $M_1/L/\mathbf{Q}$ such that M_1 gives a proper solution of $(L/\mathbf{Q}, \varepsilon)$ and that M_1/L is unramified. By group theoretical considerations, the p-Sylow subgroup E_p of E is a non-abelian p-group of exponent p, and the Galois group of M_1/K is isomorphic to E_p. Then $M_1 \cdot K(p)$ gives an affirmative answer to Boston's question for K and p.

By using Proposition 2, we can easily prove (2).

References

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

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

[3] T. Crespo, Embedding problem with ramification conditions, Arch. Math., **53** (1989), 270–276.

[4] F. Hajir, On the growth of p-class groups in p-class field towers, J. Algebra, **188** (1996), 256–271.

[5] K. Hoechsmann, Zum Einbettungsproblem, J. reine angew. Math., **229** (1968), 81–106.

[6] M. Ikeda, Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem, Hamb. Abh., **24** (1960), 126–131.

[7] K. Miyake, On the Ideal Class Groups of the p-Class Fields of Quadratic Number Fields, Proc. Japan Acad., **68** Ser.A (1992), 62–67.

[8] J. Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math., **21** (1973), 59–116.

[9] A. Nomura, On the existence of unramified p-extensions, Osaka J. Math., **28** (1991), 55–62.

[10] A. Nomura, On the class number of certain Hilbert class fields, Manuscripta Math., **79** (1993), 379–390.

[11] A. Nomura, A Remark on Boston's Question Concerning the Existence of Unramified p-extensions, J.Number Theory, **58** (1996), 66–70.

[12] A. Nomura, A Remark on Boston's Question Concerning the Existence of Unramified p-extensions II, Proc. Japan Acad., **73** Ser.A (1997), 10–11.

[13] A. Nomura, On embedding problems with restricted ramifications, Arch. Math., **73** (1999), 199–204.

[14] A. Scholz and O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper; ihre rechnerische Bestimmung und ihr Einfluss auf den Klassenkörperturm, J. Reine Angew. Math., **171** (1934), 19–41.

Department of Mathematics, Kanazawa University,
Kanazawa 920-1192, Japan
E-mail address: `anomura@t.kanazawa-u.ac.jp`