Nomura, A.
Osaka J. Math.
28 (1991), 55–62

ON THE EXISTENCE OF UNRAMIFIED p-EXTENSIONS

AKITO NOMURA

(Received July 25, 1989)

Introduction

Let p be an odd prime. Let K be an algebraic number field of finite degree, and let L/K be a p-extension. Throughout this paper, a p-extension means a finite Galois extension whose Galois group is a p-group. In this paper, we study the existence of a p-extension $M/L/K$ such that M/L is unramified.

One of our results is the following.

Let k be the rational number field or an imaginary quadratic field with the class number prime to p (p is not equal to 3 when $k=\boldsymbol{Q}(\sqrt{-3})$). Let $L/K/k$ be a Galois tower satisfying the conditions (1), (2) and (3) in Theorem 1 below, and E be a non-split central extension of $\mathrm{Gal}(L/k)$ by $\boldsymbol{Z}/p\boldsymbol{Z}$. Then there exists a Galois extension M/k such that M/K is unramified and $\mathrm{Gal}(M/k)$ is isomorphic to E.

We try to proceed by means of the theory of central imbedding problems. In §**1**, we explain about the central imbedding problems. In §**2**, we study the existence of unramified p-extensions, and in §**3** and §**4**, we have an application of results proved in §**2**. In §**5**, we study the central imbedding problem of exponent p.

1. Central imbedding problems

Let k be an algebraic number field of finite degree, $\mathfrak{G}$ its absolute Galois group, and let L/k be a finite Galois extension with Galois group G. Let (ε): $1\to A\to E\xrightarrow{j} G\to 1$ be a central extension of finite groups. Then a central imbedding problem $(L/k, \varepsilon)$ is defined by the diagram

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

where φ is the canonical surjection. A solution of the imbedding problem $(L/k,\varepsilon)$ is, by definition, a continuous homomorphism ψ of $\mathfrak{G}$ to E with $j\circ\psi=\varphi$. 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 $(L/k,\mathcal{E})$ is equivalent to the existence of a Galois extension $M\supset L\supset k$ with Galois group $\mathrm{Gal}(M/k)$ which is isomorphic to E and the canonical projection $\mathrm{Gal}(M/k)\rightarrow\mathrm{Gal}(L/k)$ coincides with the given homomorphism $j\colon E\rightarrow G$. We say the imbedding problem $(L/k, \mathcal{E})$ is solvable (resp. properly solvable) if it has a solution (resp. proper solution). Now, we quote some results of central imbedding problems without proofs. For details, see Neukirch [1].

Let $(L/k,\mathcal{E})$ be a central imbedding problem defined by the diagram $(*)$.

Lemma 1. *If L/k is unramified or $\mathcal{E}$ is split, then $(L/k, \mathcal{E})$ is solvable.*

For any prime number p, denote by $G(p)$ one of the p-Sylow subgroups of G. Let $k^{(p)}$ be the fixed field of $G(p)$. Then the central imbedding problem $(L/k, \mathcal{E})$ induces the p-Sylow problem $(L/k^{(p)}, \mathcal{E}(p))$, which is defined by the diagram

$$\begin{tikzcd} & & & \mathfrak{G}(p) \arrow[d, "\varphi|_{\mathfrak{G}(p)}"] & \\ \mathcal{E}(p)\ :\ 1 \arrow[r] & A \arrow[r] & E(p) \arrow[r, "j|_{E(p)}"] & G(p) \arrow[r] & 1 \end{tikzcd}$$

where $E(p)$ (resp. $\mathfrak{G}(p)$) is the inverse of $G(p)$ by j (resp. φ).

The following reduction holds.

Lemma 2. *If p-Sylow problems $(L/k^{(p)}, \mathcal{E}(p))$ are solvable for any prime number p, then $(L/k, \mathcal{E})$ is solvable.*

REMARK. Lemma 2 holds for general imbedding problems, For example, let L/k be a Galois extension of a local field k and $\mathfrak{G}$ the Galois group of $\tilde{L}$ over k, where $\tilde{L}$ is the maximal unramified extension of L. Then an imbedding problem $(L/k, \mathcal{E})$ is defined, and Lemma 2 holds for this.

For any prime $\mathfrak{p}$ of k, denote by $k_{\mathfrak{p}}$(resp. $L_{\mathfrak{p}}$) the completion of k (resp. L) by $\mathfrak{p}$ (resp. an extension of $\mathfrak{p}$ to L). Then the local problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$ of $(L/k, \mathcal{E})$ is defined by the diagram

$$\begin{tikzcd} & & & \mathfrak{G}_{\mathfrak{p}} \arrow[d] & \\ (\mathcal{E}_{\mathfrak{p}})\colon 1 \arrow[r] & A \arrow[r] & E_{\mathfrak{p}} \arrow[r, "j|_{E_{\mathfrak{p}}}"] & G_{\mathfrak{p}} \arrow[r, "\varphi|_{\mathfrak{G}_{\mathfrak{p}}}"] & 1 \end{tikzcd}$$

where $\mathfrak{G}_{\mathfrak{p}}$ is the absolute decomposition group of $\mathfrak{p}$ which is isomorphic to the absolute Galois group of $k_{\mathfrak{p}}$, and $E_{\mathfrak{p}}$ is the inverse of $G_{\mathfrak{p}}$ by j. Similary to the case of $(L/k, \mathcal{E})$, we define a solution and a solution field of local problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$.

The following lemma is a generalization of Grunwald-Wang-Hasse's Theorem by Neukirch.

Lemma 3. (Neukirch [1; Example 1, Corollary 6.4]) *Assume that $(L/k, \mathcal{E})$ is solvable. Let S be a finite set of primes of k. Let $M_{\mathfrak{p}}$ be a solution field of $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$ for $\mathfrak{p}$ of S. Then there exists a solution field M of $(L/k, \mathcal{E})$ such that the completion of M by $\mathfrak{p}$ is equal to $M_{\mathfrak{p}}$ for any $\mathfrak{p}$ of S.*

For a finite set S of primes of k, let $B_k(S)=\{\alpha\in k^* \mid (\alpha)=\mathfrak{a}^p$ for some ideal $\mathfrak{a}$ of k, and $\alpha\in k_{\mathfrak{q}}{}^p$ for any $\mathfrak{q}$ of $S\}$. Then the following lemma is well-known.

Lemma 4. (Safarevic [2; Theorem 1]) *Assume that $B_k(S)=k^{*p}$. Let $\mathfrak{q}$ be a prime of k, not contained in S. If $N(\mathfrak{q})$, the absolute norm of $\mathfrak{q}$, is congruent to* 1 (mod. p), *then there exists a cyclic extension $k(\mathfrak{q})/k$ of degree p which is unramified outside $S\cup\{\mathfrak{q}\}$, and in which $\mathfrak{q}$ is ramified.*

REMARK. Let k be either the rational number field or an imaginary quadratic field with the class number prime to p ($p\neq 3$, when $k=\boldsymbol{Q}(\sqrt{-3})$). In this case, $B_k(\phi)=k^{*p}$, and hence $B_k(S)=k^{*p}$ for any S.

2. On unramified extensions

In this section, let p be an odd prime and let k denote either the rational number field or an imaginary quadratic field with the class number prime to p ($p\neq 3$, when $k=\boldsymbol{Q}(\sqrt{-3})$).

The following theorem is our main result.

Theorem 1. *Let $L/K/k$ be a Galois tower satisfying the following conditions.*

(1) *The degree of K/k is prime to p.*

(2) *L/K is an unramified p-extension.*

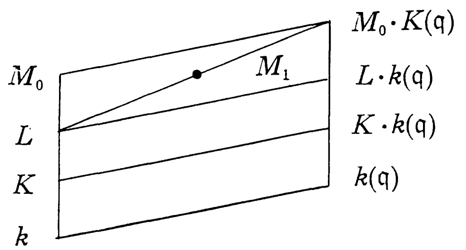
(3) *For any prime $\mathfrak{q}$ of k ramified in K/k, the inertia degree of $\mathfrak{q}$ in K/k is equal to* 1 *or $L_{\mathfrak{q}}/k_{\mathfrak{q}}$ is cyclic.*

Put $G=Gal(L/k)$, and let $(\mathcal{E})$: $1\to\boldsymbol{Z}/p\boldsymbol{Z}\to E\to G\to 1$ be a non-split central extension. Then there exists a Galois extension M/k such that

(i) *M/k gives a proper solution of the central imbedding problem $(L/k, \mathcal{E})$,*

(ii) *M/K is unramified.*

Proof. By Lemma 1 and Lemma 2, it is easy to see that $(L/k, \mathcal{E})$ is solvable. Now, we consider the local problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$ for any prime $\mathfrak{p}$ of k lying above p. By the remark of Lemma 2, as a solution field of $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$, we can take an unramified extension $M_{\mathfrak{p}}/K_{\mathfrak{p}}$. By Lemma 3, there exists a solution field M_0/k of $(L/k, \varepsilon)$ such that its localization is equal to $M_{\mathfrak{p}}$ for any prime $\mathfrak{p}$ lying above p. Let $\psi: \mathfrak{G}\to E$ be a solution of $(L/k, \varepsilon)$ corresponding to the solution field M_0/k. Since ε is non-split, the central extension $\varepsilon(p)$: $1\to \boldsymbol{Z}/p\boldsymbol{Z}\to E(p)\to G(p)\to 1$ of finite p-groups which is induced by ε, is also non-split. It is clear that the generator rank of $E(p)$ is equal to that of $G(p)$. Then the restriction $\psi|_{\mathfrak{G}(p)}: \mathfrak{G}(p)\to E(p)$ is surjective, and then $\psi: \mathfrak{G}\to E$ is surjective. Hence ψ is a proper solution of $(L/k, \varepsilon)$. By the choice of M_0/k, any prime of L lying above p is unramified in M_0/L. If M_0/L is unramified, then M_0/k is a required Galois extension. Suppose that M_0/L is not unramified, and take a prime $\tilde{\mathfrak{q}}$ of M_0 ramified in M_0/L. Let $\mathfrak{q}$ be a prime of k that is the restriction of $\tilde{\mathfrak{q}}$ to k. We claim that $N(\mathfrak{q})\equiv 1$ (mod.p). If $\mathfrak{q}$ is ramified in K/k and the inertia degree in K/k is equal to 1, then $N(\tilde{\mathfrak{q}})=N(\mathfrak{q})^{p^r}\equiv 1$ (mod.p) for some integer r. Hence $N(\tilde{\mathfrak{q}})\equiv 1$ (mod.p). Assume that $\mathfrak{q}$ is not as above. We consider the extension $M_{0\tilde{\mathfrak{q}}}/k_{\mathfrak{q}}$ which is the localization of M_0/k with respect to $\tilde{\mathfrak{q}}$. Then $M_{0\tilde{\mathfrak{q}}}/k_{\mathfrak{q}}$ is abelian since $L_{\tilde{\mathfrak{q}}}/k_{\mathfrak{q}}$ is cyclic and $M_{0\tilde{\mathfrak{q}}}/k_{\mathfrak{q}}$ is a central extension of $L_{\tilde{\mathfrak{q}}}/k_{\mathfrak{q}}$. Thus $\tilde{\mathfrak{q}}$ is ramified in a p-extension over $k_{\mathfrak{q}}$. Hence $N(\mathfrak{q})\equiv 1$ (mod.p). This proves the claim. By Lemma 4, there exists a cyclic extension $k(\mathfrak{q})/k$ of degree p whcih is unramified outside $\mathfrak{q}$ and in which $\mathfrak{q}$ is totally ramified. Then $k(\mathfrak{q})\cap M_0=k$ because $\mathfrak{q}$ is unramified in L/K and the generator rank of $\mathrm{Gal}(M_0/K)$ is equal to that of $\mathrm{Gal}(L/K)$. Let $\mathfrak{q}$ be an extension of $\mathfrak{q}$ to $M_0\cdot k(\mathfrak{q})$, and let M_1 be the inertia field of $\mathfrak{q}$ in $M_0\cdot k(\mathfrak{q})/L$.



Then M_1 is not equal to L, M_0 and $M_0\cdot k(\mathfrak{q})$ by the Hilbert theory of ramification. Since $\mathrm{Gal}(M_0\cdot k(\mathfrak{q})/L)$ is contained in the center of $\mathrm{Gal}(M_0\cdot k(\mathfrak{q})/k)$, M_1/k is a Galois extension. Moreover, $\mathrm{Gal}(M_0/k)$ is isomorphic to $\mathrm{Gal}(M_1/k)$ and M_1/k gives a proper solution of $(L/k, \varepsilon)$. By the choice of M_1, any prime of L which is unrmaified in M_0/L is also unramified in M_1/L, and $\tilde{\mathfrak{q}}$ is unramified in M_1/L. By continuing this procedure, we can take a required extension M/k. This proves the theorem.

3. An application to quadratic extensions

As in §2, let p be an odd prime, and let k be either the rational number field or an imaginary quadratic field with the class number prime to p ($p\neq 3$

when $k=\boldsymbol{Q}(\sqrt{-3})$). Let K be a quadratic extension over k. We first prove the following lemma.

Lemma 5. *Let K_1/K be an unramified cyclic extension of degree p, and $\mathfrak{p}$ a prime of k lying above p. Then we have the following.*

(1) *K_1 is a Galois extension over k, and the Galois group is isomorphic to the group $\langle\sigma, \tau \mid \sigma^p=\tau^2=1, \tau\sigma\tau^{-1}=\sigma^{-1}\rangle$.*

(2) *If $\mathfrak{p}$ is ramified in K/k, the inertia degree of $\mathfrak{p}$ in K_1/k is equal to* 1.

Proof. (1) Suppose that K_1/k is non-Galois. Let K_2 be a conjugate field of K_1 over k, which is distinct from K_1, and put $\mathrm{Gal}(K_1\cdot K_2/K_1)=\langle x\rangle$ and $\mathrm{Gal}(K/k)=\langle y_0\rangle$. Let y be an extension of y_0 to $K_1\cdot K_2$. Then $\mathrm{Gal}(K_1\cdot K_2/K_2)=\langle yxy^{-1}\rangle$ and $\mathrm{Gal}(K_1\cdot K_2/k)$ is generated by x and y. The fixed field of $\langle yxy^{-1}x^{-1}\rangle$ is an abelian extension over k of degree $2p$. By considering the ramification index, we see that there exists an unramified cyclic extension over k of degree p. This is a contradiction. And it is easy to see that $\mathrm{Gal}(K_1/k)$ is isomorphic to the group $\langle\sigma, \tau \mid \sigma^p=\tau^2=1, \tau\sigma\tau^{-1}=\sigma^{-1}\rangle$. (2) Let $\tilde{\mathfrak{p}}$ be an extension of $\mathfrak{p}$ to K, and put $G=\langle\sigma, \tau \mid \sigma^p=\tau^2=1, \tau\sigma\tau^{-1}=\sigma^{-1}\rangle$. Suppose that $\tilde{\mathfrak{p}}$ is also prime of K_1. Then the inertia group of $\mathfrak{p}$ in K_1/k is a normal subgroup of G, which is of order 2. But G has no normal subgroup of order 2. This is a contradiction.

Let H be a group of order p^3 defined by

$$\langle x, z \mid x^p = y^p = z^p = 1, z^{-1}xz = xy, y^{-1}xy = x, y^{-1}zy = z\rangle.$$

Let $Cl_K(p)$ be the p-Sylow subgroup of the ideal class group of K. Denote by d_pCl_K, the p-rank of $Cl_K(p)$.

Then we have the following.

Theorem 2. *If $d_pCl_K\geq 2$, then there exists an unramified Galois extension M/K with Galois group $Gal(M/K)$ isomorphic to H.*

Proof. Let K_1/K, K_2/K be unramified cyclic extensions of degree p such that $K_1\cap K_2=K$. Then by Lemma 5, $K_1\cdot K_2$ is a Galois extension over k, whose Galois group is isomorphic to the group

$G:=\langle u, v, w \mid u^p=v^p=w^2=1, w^{-1}uw=u^{-1}, w^{-1}vw=v^{-1}, v^{-1}uv=u\rangle.$

Now, we take a following group E of order $2p^3$,

$$E = \left\langle x, z, t \,\middle|\, \begin{matrix} x^p = y^p = z^p = t^2 = 1, z^{-1}xz = xy, y^{-1}xy = x, \\ y^{-1}zy = z, t^{-1}xt = x^{-1}, t^{-1}yt = y, t^{-1}zt = z^{-1} \end{matrix} \right\rangle.$$

Then,

$$1\to\langle y\rangle\to E\xrightarrow{j} G\to 1$$

is a non-split central extension, where j is defined by $x\to u$, $z\to v$, $t\to w$. By Theorem 1, there exists a Galois extension M/k such that $M/K_1\cdot K_2$ is unramified and that the Galois group $\mathrm{Gal}(M/k)$ is isomorphic to E. Since the p-Sylow subgroup of E is isomorphic to H, $\mathrm{Gal}(M/K)$ is isomorphic to H. This proves the theorem.

From the proof of Theorem 2, we have,

Corollary. *Assume that L/K is unramified extension with Galois group isomorphic to $\boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/p\boldsymbol{Z}$. Then the class number of L is divisible by p.*

4. An application to cubic extensions

Let p be an odd prime which is congruent to -1 (mod.3), and k be the same as in §3. Let K/k be a cyclic extension of degree 3. In this section, we prove the following.

Theorem 3. *Assume that the class number of K is divisible by p. Then there exists an unramified Galois extension M/K with the Galois group isomorphic to H, where H is the same group as in* §3.

First we prove the following lemma.

Lemma 6. (1) *Let K_1/K be an unramified cyclic extension of degree p. Then K_1/k is non-Galois.* (2) *Let L/k be the Galois closure of K_1/k. Then $\mathrm{Gal}(L/k)$ is isomorphic to the group*

$$G:=\langle u, v, w \mid u^p = v^p = w^3 = 1, w^{-1}uw = v, w^{-1}vw = u^{-1}v^{-1}, u^{-1}vu = v\rangle.$$

Proof. (1) Assume that K_1/k is Galois. Since p is congruent to -1 (mod. 3), the group of order $3p$ is abelian, so K_1/k is an abelian extension. Then it is easy to see that there exists an unramified cyclic extension of degree p. This is a contradiction. (2) The order of $\mathrm{Gal}(L/k)$ is either $3p^2$ or $3p^3$. We notice that a p-Sylow subgroup of $\mathrm{Gal}(L/k)$ is normal subgroup which is isomorphic to an elementary abelian p-group, and $\mathrm{Gal}(L/k)$ does not have a normal subgroup of order 3. The group of order $3p^2$ or $3p^3$ with this property is isomorphic to G (see Western [3]).

Proof of Theorem 3. By Lemma 6, there exists a Galois extension $L/K/k$ such that L/K is unramified and $\mathrm{Gal}(L/k)$ is isomorphic to G. Now, we take a following group E of order $3p^3$.

$$E=\left\langle x, z, t \;\middle|\; \begin{array}{l} x^p = y^p = z^p = t^3 = 1,\ x^{-1}zx = yz,\ x^{-1}yx = y,\ y^{-1}zy = z \\ t^{-1}xt = z,\ t^{-1}zt = x^{-1}z^{-1},\ y^{-1}ty = t \end{array}\right\rangle.$$

Then,

$$1 \to \langle y\rangle \to E \xrightarrow{j} G \to 1$$

is a non-split central extension, where j is defined by $x\to u$, $z\to v$, $t\to w$. In the same manner of the proof of Theorem 2, we can take a required extension M/k.

5. On central imbedding problems of exponent p

Let p be an odd prime and L/k a Galois extension of an algebraic number field k with Galois group G. In this section, we asusme that G is of exponent p (not necessary abelian). Let S_0 be the set of primes of k which are ramified in L and prime to p.

We prove the following.

Theorem 4. *Assume that $B_k(S_0)=k^{*p}$, and that $L_{\mathfrak{q}}/k_{\mathfrak{q}}$ is cyclic for any prime $\mathfrak{q}$ of k. Let E be a p-group of exponent p and $(\mathcal{E})$: $1\to \boldsymbol{Z}/p\boldsymbol{Z}\to E\xrightarrow{j} G\to 1$ a non-sprit central extension. Then there exists a Galois extension M/k such that*

(i) *M/k gives a proper solution of the central imbedding problem $(L/k, \mathcal{E})$,*

(ii) *M/L is unramified.*

Proof. For any prime $\mathfrak{q}$ of k, $\mathcal{E}_{\mathfrak{q}}$ is split by the assumption, so $(L_{\mathfrak{q}}/k_{\mathfrak{q}}, \mathcal{E}_{\mathfrak{q}})$ is solvable. Then $(L/k, \mathcal{E})$ is solvable. Now, we consider the local problem $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$ for any prime $\mathfrak{p}$ of k lying above p. It is clear we can take $L_{\mathfrak{p}}/k_{\mathfrak{p}}$ as a solution field of $(L_{\mathfrak{p}}/k_{\mathfrak{p}}, \mathcal{E}_{\mathfrak{p}})$. Then, by Lemma 3, there exists a Galois extension $M_1/L/k$ such that any prime $\mathfrak{p}$ lying above p is unramified in M_1/L and that M_1/k gives a proper solution of $(L/k, \mathcal{E})$. Let S_1 be the set of primes of k which are ramified in M_1. Let $\mathfrak{q}$ be a prime of S_1 not contained in $S_0\cup\{p\}$. Then, in the same manner of the proof of Theorem 1, we can take a Galois extension M_2/k that is unramified outside $S_1-\{\mathfrak{q}\}$, and can take a Galois extension M/k that is unramified outside $S_0\cup\{p\}$.

Let $\mathfrak{q}$ be a prime contained in S_0 and $\tilde{\mathfrak{q}}$ a prime of L which is an extension of $\mathfrak{q}$. Since E is of exponent p, $\tilde{\mathfrak{q}}$ is unramified in M by the Hilbert theory of ramification. Then M/L is unramified, therefore M/k is a required extension.

Let H be the same group as in §3. As a corollary of Theorem 4, we have

Corollary. *Let L/k be a Galois extension with the Galois group isomorphic to $\boldsymbol{Z}/p\boldsymbol{Z}\times \boldsymbol{Z}/p\boldsymbol{Z}$. Assume that $B_k(S_0)=k^{*p}$. Then the following conditions* (i) (ii) *are equivalent.*

(i) *There exists a Galois extension $M/L/k$ such that $Gal(M/k)$ is isomorphic to H and that M/L is unramified.*

(ii) *Any prime of k which is ramified in L/k is decomposed in L/k.*

Proof. (ii)→(i) is clear by Theorem 4. We prove (i)→(ii). Assume that there exists a prime $\mathfrak{q}$ of k which is ramified in L/k and is not decomposed in L/k. Let $\tilde{\mathfrak{q}}$ be a prime of M which is an extension of $\mathfrak{q}$. Since H is of exponent p, the decomposition group of $\tilde{\mathfrak{q}}$ in M/k is of order p^2. Then the decomposition group is normal subgroup of H, so the decomposition field is a cyclic extension over k of degree p. Therefore it is contained in L/k. This is a contradiction.

References

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

[2] I.R. Safarevic: *Extensions with given points of ramification*, AMS. Translation Ser. 2, vol. **59** (1966), 128–149.

[3] A.E. Western: *Groups of order p^3q*, Proc. London Math. Soc. Ser. 1, vol. **30** (1899), 209–263.

Department of Mathematics
Kanazawa University
Kanazawa 920
Japan