A note on unramified quaternion extensions over quadratic number fields

By Akito Nomura

Department of Mathematics, Kanazawa University, Kakuma-machi, Kanazawa, Ishikawa 920-1192

(Communicated by Shokichi Iyanaga, M. J. A., June 11, 2002)

Abstract: The present note studies the existence of unramified quaternion extensions over quadratic fields, and give an alternative proof of Lemmermeyer's result. Our method is based on the theory of embedding problems with restricted ramification.

Key words: Embedding problems; inverse Galois problems; unramified quaternion extensions.

1. Introduction. The inverse Galois problem with unramified conditions is described as follows: For an algebraic number field K and a finite group G, to study whether there exists an unramified Galois extension M/K with the Galois group isomorphic to G. In case G is abelian, by class field theory, this problem is closely related to the ideal class group of K. Lemmermeyer [1] studied the existence of unramified quaternion extension over quadratic field and proved the following.

Theorem (Lemmermeyer)**.** *Let K be a quadratic field with discriminant d, and H_8 the quaternion group defined by $\langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = \sigma^2, [\sigma, \tau] = \tau^2 \rangle$. Then the following assertions are equivalent:*

(1) *There exists a Galois extension $M/K/\mathbf{Q}$ such that M/K is unramified at all finite primes and that $\mathrm{Gal}(M/K)$ is isomorphic to H_8.*

(2) *There is a factorization $d = d_1 d_2 d_3$ of d into three quadratic discriminants which are relatively prime and which satisfy the conditions $(d_1 d_2 / p_3) = (d_2 d_3 / p_1) = (d_3 d_1 / p_2) = +1$ for all primes $p_i \mid d_i$.*

The proof of (1) ⇒ (2) is elementary and short and is based on the Hilbert's theory of ramification and group theoretical considerations. But the proof of converse is long. First we shall study the embedding problem with restricted ramification. And as an application, we give an alternative proof of (2) ⇒ (1). If the computational group theory will advance, we hope our method will be applicable to many other cases.

2. Embedding problems. Let $\mathfrak{G}$ be the absolute Galois group of $\mathbf{Q}$, and $L/\mathbf{Q}$ a finite Galois extension with Galois group G. For a central extension $(\varepsilon) : 1 \to A \to E \xrightarrow{j} G \to 1$, the embedding problem $(L/\mathbf{Q}, \varepsilon)$ is defined by the diagram

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

where φ is the canonical surjection. A solution of the embedding problem $(L/\mathbf{Q}, \varepsilon)$ is, by definition, a continuous homomorphism ψ of $\mathfrak{G}$ to E such that $j \circ \psi = \varphi$. A field M is called a solution field of $(L/\mathbf{Q}, \varepsilon)$ if M is corresponding to the kernel of any solution. When $(L/\mathbf{Q}, \varepsilon)$ has a solution, we call $(L/\mathbf{Q}, \varepsilon)$ is solvable. A solution ψ is called a proper solution if it is surjective.

For each prime q of $\mathbf{Q}$, we denote by $\mathbf{Q}_q$ (resp. L_q) the completion of $\mathbf{Q}$ (resp. L) by q (resp. an extension of q to L). Then the local problem $(L_q/\mathbf{Q}_q, \varepsilon_q)$ of $(L/\mathbf{Q}, \varepsilon)$ is defined by the diagram

$$\begin{tikzcd}
 & & & \mathfrak{G}_q \arrow[d, "\varphi|_{\mathfrak{G}_q}"] & \\
(\varepsilon_q) : 1 \arrow[r] & A \arrow[r] & E_q \arrow[r, "j|_{E_q}"] & G_q \arrow[r] & 1
\end{tikzcd}$$

where G_q is the Galois group of $L_q/\mathbf{Q}_q$, which is isomorphic to the decomposition group of q in $L/\mathbf{Q}$, $\mathfrak{G}_q$ is the absolute Galois group of $\mathbf{Q}_q$, and E_q is the inverse of $\mathfrak{G}_q$ by j. In the same manner as the case of $(L/\mathbf{Q}, \varepsilon)$, solution and proper solution are defined for $(L_q/\mathbf{Q}_q, \varepsilon_q)$.

We need some lemmas, which are essential in the theory of embedding problems. Let $L/\mathbf{Q}$ be a 2-extension and $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$ a central extension.

2000 Mathematics Subject Classification. 12F12, 11R29.

Lemma 1 (Neukirch [2]). *$(L/\mathbf{Q}, \varepsilon)$ is solvable if and only if $(L_q/\mathbf{Q}_q, \varepsilon_q)$ are solvable for all prime q ramified in $L/\mathbf{Q}$.*

Remark. It is easy to see that if ε_q splits then $(L_q/\mathbf{Q}_q, \varepsilon_q)$ is solvable.

Lemma 2 (Nomura [3]). *If (ε) is a non-split extension, every solution of $(L/\mathbf{Q}, \varepsilon)$ is a proper solution.*

Lemma 3 (Neukirch [2]). *Assume that $(L/\mathbf{Q}, \varepsilon)$ is solvable. Let S be a finite set of primes of $\mathbf{Q}$ and $M(q)$ a solution field of $(L_q/\mathbf{Q}_q, \varepsilon)$ for q of S. Then there exists a solution field M of $(L/\mathbf{Q}, \varepsilon)$ such that the completion of M by q is equal to $M(q)$ for each q of S.*

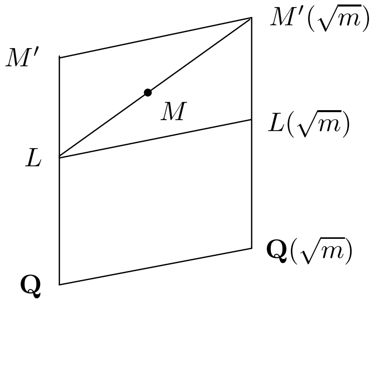
We denote by $Ram(L/\mathbf{Q})$ the set of all primes of $\mathbf{Q}$ which are ramified in $L/\mathbf{Q}$. The following is a key lemma in this note. A similar result can be found in my preprint [4]. For the convenience of readers, we shall prove the following.

Proposition 4. *Let $L/\mathbf{Q}$ be a 2-extension, S the union of $Ram(L/\mathbf{Q})$ and $\{2\}$, and $(\varepsilon) : 1 \to \mathbf{Z}/2\mathbf{Z} \to E \to \mathrm{Gal}(L/\mathbf{Q}) \to 1$ a non-split central extension. We assume that for any prime of S the local problem $(L_q/\mathbf{Q}_q, \varepsilon_q)$ has a solution field which is unramified over L_q. Then there exists a Galois extension $M/L/\mathbf{Q}$ satisfying the conditions*

(1) *M gives a proper solution of $(L/\mathbf{Q}, \varepsilon)$,*

(2) *M/L is unramified at all finite primes.*

Proof. By Lemma 1, the embedding problem $(L/\mathbf{Q}, \varepsilon)$ is solvable. By virtue of Lemma 2 and Lemma 3, there exists a Galois extension $M'/L/\mathbf{Q}$ such that M' gives a proper solution and that any prime of S is unramified in M'/L. Let p_i $(i = 1, 2, \ldots, t)$ be the all primes of $\mathbf{Q}$ which are ramified in M'/L. By the choice of M', p_i is odd for all i. Let $m = \pm p_1 p_2 \cdots p_t$, where the sign is determined by the condition $m \equiv 1 \pmod 4$. Then $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$ is unramified outside $\{p_1, \ldots, p_t\}$. Let M be the field such that $M'(\sqrt{m}) \supsetneqq M \supsetneqq L$, $M \neq L(\sqrt{m})$, $M \neq M'$.



By using the Hilbert's theory of ramification, it is easy to see M/L is unramified at all finite primes. Since (ε) is a central extension, M gives a proper solution of $(L/\mathbf{Q}, \varepsilon)$. We have thus proved this proposition. □

3. Proof of (2) ⇒ (1). Let $L = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ and take x, y, z such that

$$\mathrm{Gal}(L/\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})) = \langle x \rangle,$$
$$\mathrm{Gal}(L/\mathbf{Q}(\sqrt{d_2}, \sqrt{d_3})) = \langle y \rangle,$$
$$\mathrm{Gal}(L/\mathbf{Q}(\sqrt{d_1}, \sqrt{d_3})) = \langle z \rangle.$$

Let Γ be the group $\langle \rho, \sigma, \tau \mid \rho^4 = 1, \rho^2 = \sigma^2 = \tau^2, [\rho, \sigma] = [\rho, \tau] = 1, [\sigma, \tau] = \rho^2 \rangle$ and $(\varepsilon) : 1 \to \langle \rho^2 \rangle \to \Gamma \xrightarrow{j} \mathrm{Gal}(L/\mathbf{Q}) \to 1$ a central extension, where j is defined by $j(\sigma) = xz$, $j(\tau) = xy$, $j(\rho) = xyz$.

We claim that the local problem $(L_p/\mathbf{Q}_p, \varepsilon_p)$ is solvable for all p ramified in $L/\mathbf{Q}$. We first consider the case p is a finite prime dividing d_1. Denote by D_p the decomposition field of p in $L/\mathbf{Q}$. Since p is ramified in $\mathbf{Q}(\sqrt{d_1})$ and totally decomposed in $\mathbf{Q}(\sqrt{d_2 d_3})$, D_p is equal to $\mathbf{Q}(\sqrt{d_2}, \sqrt{d_3})$ or $\mathbf{Q}(\sqrt{d_2 d_3})$.

Case 1: $D_p = \mathbf{Q}(\sqrt{d_2}, \sqrt{d_3})$.

Then $\mathrm{Gal}(L_p/\mathbf{Q}_p) = \langle y \rangle$, and $\varphi^{-1}(\langle y \rangle) = \langle \sigma\rho, \rho^2 \rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Hence the local extension $(\varepsilon_p) : 1 \to \langle \rho^2 \rangle \to \varphi^{-1}(\langle y \rangle) \to \langle y \rangle \to 1$ splits. Therefore $(L_p/\mathbf{Q}_p, \varepsilon_p)$ is solvable.

Case 2: $D_p = \mathbf{Q}(\sqrt{d_2 d_3})$.

Then $\mathrm{Gal}(L_p/\mathbf{Q}_p) = \langle y, xz \rangle$, and $\varphi^{-1}(\langle y, xz \rangle) = \langle \sigma\rho, \sigma, \rho^2 \rangle = \langle \sigma\rho, \sigma \rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Let K_1 (resp. K_2) be the subfield of L_p corresponding to $\langle y \rangle$ (resp. $\langle xz \rangle$). Then $K_1/\mathbf{Q}_p$ is unramified and $K_2/\mathbf{Q}_p$ is ramified. We can take an unramified extension $N_p/\mathbf{Q}_p$ such that $N_p \supset K_1$ and that $\mathrm{Gal}(N_p/\mathbf{Q}_p) \cong \mathbf{Z}/4\mathbf{Z}$. Then $M_p = N_p K_2$ gives a solution of $(L_p/\mathbf{Q}_p, \varepsilon_p)$.

We omit the case p divides $d_2 d_3$, because the proof is similar to the case above.

Next we consider the case $p = \infty$. By the assumption of Legendre's symbol, it is easy to see that at most one of the d_i is negative. Then if $p = \infty$ is ramified in L, the decomposition field is $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathbf{Q}(\sqrt{d_2}, \sqrt{d_3})$ or $\mathbf{Q}(\sqrt{d_3}, \sqrt{d_1})$. In this case the local extension ε_p splits. Thus $(L_p/\mathbf{Q}_p, \varepsilon_p)$ is solvable. Hence we proved the claim.

By virtue of Proposition 4, there exists a Galois extension $M/L/\mathbf{Q}$ such that $\mathrm{Gal}(M/\mathbf{Q}) \cong \Gamma$ and that M/L is unramified at all finite primes. Then $\mathrm{Gal}(M/\mathbf{Q}(\sqrt{d})) = \langle \sigma, \tau \rangle \cong H_8$. We have thus proved (2) ⇒ (1).

References

[1] Lemmermeyer, F.: Unramified quaterinon extensions of quadratic number fields. J. Théor. Nombres Bordeaux, **9**, 51–68 (1997).

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

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

[4] Nomura, A.: Notes on the existence of certain unramified 2-extensions. (Preprint).