Notes on the minimal number of ramified primes in some $\mathbb{I}$ -extensions of $\mathbb{Q}$

著者	Nomura Akito
journal or publication title	Archiv der Mathematik
volume	90
number	6
page range	501-510
year	2008-06-01
URL	http://hdl.handle.net/2297/10951

doi: 10.1007/s00013-008-2586-z

Notes on the minimal number of ramified primes in some l -extensions of $\mathbf{Q}$

Akito Nomura

Abstract. For a finite l -group G , let $\text{ram}^t(G)$ denote the minimal integer such that G can be realized as the Galois group of a tamely ramified extension of $\mathbf{Q}$ ramified only at $\text{ram}^t(G)$ finite primes. We study the upper bound of $\text{ram}^t(G)$ and give an improvement of the result of Plans. We also give the best bound of $\text{ram}^t(G)$ for all 3-groups G of order less than or equal to 3^5 .

Mathematics Subject Classification (2000). Primary 12F12; Secondary 11R29.

Keywords. Inverse Galois Problem, class number, bounded ramification.

1. Introduction

Let l be an odd prime number. Scholz[11] and Reichardt[9] proved that every l -group G can be realized as the Galois group of some extension M of the rational number field $\mathbf{Q}$. We are interested in the number of primes which are ramified in $M/\mathbf{Q}$.

For a finite l -group G , let $\text{ram}^t(G)$ denote the minimal integer such that G can be realized as the Galois group of a tamely ramified extension of $\mathbf{Q}$ ramified only at $\text{ram}^t(G)$ finite primes.

We denote by $d(G)$ the minimal number of generators of a finite l -group G . Then it is well-known $d(G) \leq \text{ram}^t(G) \leq n$, where l^n is the order of G (cf. [10, Chapter 2]). Cueto-Hernández and Villa-Salvador[1] claimed that $\text{ram}^t(G) = d(G)$, but Plans[8, Remark 2.10] pointed out an error in the proof. Plans[8] also proved a better upper bound for $\text{ram}^t(G)$ (See Theorem A in the section 3 below). In this article we prove a little improvement of the result of [8, Proposition 2.5]. We also prove that $\text{ram}^t(G) = d(G)$ for any 3-group G of order less than or equal to 3^5 .

We use GAP Version 4.4 for calculations of 3-groups.

This research was partially supported by the Grants-in-Aid for Scientific Research (C), the Japan Society for the Promotion of Science.

2. Preliminary from embedding problems

In this section, we quote some results about embedding problems over the rational number field $\mathbf{Q}$. General studies on embedding problems can be found in [3] and [5].

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 $\varepsilon : 1 \rightarrow A \rightarrow E \xrightarrow{j} G \rightarrow 1$, the embedding problem $(L/\mathbf{Q}, \varepsilon)$ is defined by the diagram

$$\begin{array}{c} \mathfrak{G} \\ \varphi \downarrow \\ \varepsilon : 1 \longrightarrow A \longrightarrow E \xrightarrow{j} G \longrightarrow 1, \end{array}$$

where φ is the canonical surjection. A continuous homomorphism ψ of $\mathfrak{G}$ to E is called a solution of $(L/\mathbf{Q}, \varepsilon)$ if it satisfies the condition $j \circ \psi = \varphi$. When $(L/\mathbf{Q}, \varepsilon)$ has a solution, we say that $(L/\mathbf{Q}, \varepsilon)$ is solvable. A solution ψ is called a proper solution if it is surjective. A field M is also called a solution (resp. proper solution) of $(L/\mathbf{Q}, \varepsilon)$ if M corresponds to the kernel of any solution (resp. proper solution).

We first recall the so-called Scholz's condition for an l -extension of $\mathbf{Q}$. For a prime $\mathfrak{p}$ of L , we denote by $Z_{\mathfrak{p}}$ (resp. $T_{\mathfrak{p}}$) the decomposition group (resp. the inertia group) of $\mathfrak{p}$ in $L/\mathbf{Q}$.

Definition 2.1. Let l be an odd prime number and N a positive integer. An l -extension $L/\mathbf{Q}$ is said to be a Scholz extension of type (S_N) if, for any prime number p ramified in $L/\mathbf{Q}$, the following conditions hold:

- (1) $p \equiv 1 \pmod{l^N}$;
- (2) $Z_{\mathfrak{p}} = T_{\mathfrak{p}}$, where $\mathfrak{p}$ is a fixed prime of L lying above p .

An l -extension $L/\mathbf{Q}$ is simply said to be a Scholz extension if $L/\mathbf{Q}$ is a Scholz extension of type (S_N) for some positive integer N .

We need some lemmas, which are essential in the embedding problems. Let l be an odd prime and $L/\mathbf{Q}$ an l -extension. Let $\varepsilon : 1 \rightarrow A \rightarrow E \xrightarrow{j} \text{Gal}(L/\mathbf{Q}) \rightarrow 1$ be a central extension of l -groups. We denote by $\text{Ram}(L/\mathbf{Q})$ the set of all prime numbers which are ramified in $L/\mathbf{Q}$.

Lemma 2.2. [10, Proposition 2.1.7, Corollary 2.1.8] *Assume that $(L/\mathbf{Q}, \varepsilon)$ is solvable. Then $(L/\mathbf{Q}, \varepsilon)$ has a solution which is unramified outside $\text{Ram}(L/\mathbf{Q})$.*

Lemma 2.3. [3, Satz 2.3] *If $d(E) = d(\text{Gal}(L/\mathbf{Q}))$, then every solution of $(L/\mathbf{Q}, \varepsilon)$ is a proper solution.*

Lemma 2.4. [10, Theorem 2.1.3] *Let l^N be the exponent of the l -group E . Assume that $L/\mathbf{Q}$ is a Scholz extension of type (S_N) . Then $(L/\mathbf{Q}, \varepsilon)$ is solvable.*

3. Minimal number of ramified primes in l -extensions

In this section, we study $\text{ram}^t(G)$ for an l -group G , and gave a little improvement of the result of [8, Proposition 2.5]. We first recall some results in [8].

Notation Let $C_i(G)$ be the i -th higher commutator subgroup of an l -group G , which is defined inductively by $C_1(G) = G$ and $C_{i+1}(G) = [C_i(G), G]$. The smallest integer n such that $C_{n+1} = \{1\}$ is the nilpotency class of G . We denote $d_i(G) = d(C_i(G)/C_{i+1}(G))$. Further we denote by $Z(G)$ the center of G .

Theorem A. [8, Proposition 2.5] *Let l be an odd prime number and n the nilpotency class of an l -group G . Then:*

$$\text{ram}^t(G) \leq d(G) + \sum_{2 \leq i \leq n-1} d_i(G),$$

where the sum is assumed to be 0 in case $n \leq 2$.

Theorem B. [8, Proposition 2.4] *Let l be an odd prime number and $L/\mathbf{Q}$ an l -extension. Let $\varepsilon : 1 \rightarrow A \rightarrow E \xrightarrow{j} \text{Gal}(L/\mathbf{Q}) \rightarrow 1$ be a central extension of l -groups. Assume the conditions:*

- (C1) $L/\mathbf{Q}$ is a Scholz extension of type (S_N) ;
- (C2) A is a cyclic group;
- (C3) the exponent of E is at most l^N ;
- (C4) ε is split or A is contained in the Frattini subgroup of E .

Then the embedding problem $(L/\mathbf{Q}, \varepsilon)$ has a proper solution $M/\mathbf{Q}$ satisfying the conditions:

- (1) $M/\mathbf{Q}$ is a Scholz extension of type (S_N) ;
- (2) $\sharp \text{Ram}(M/\mathbf{Q}) \leq \sharp \text{Ram}(L/\mathbf{Q}) + 1$.

The following theorem is a key lemma in this article. This is easily proved from Theorem B, thus we omit the proof.

Theorem C. *Let l be an odd prime number and n the nilpotency class of an l -group G . Let N be a positive integer such that the exponent of G is at most l^N . Then there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:*

- (1) $\text{Gal}(L/\mathbf{Q})$ is isomorphic to G ;
- (2) $L/\mathbf{Q}$ is a Scholz extension of type (S_N) ;
- (3) $\sharp \text{Ram}(L/\mathbf{Q}) \leq d(G) + \sum_{2 \leq i \leq n} d_i(G)$, where the sum is assumed to be 0 in

case $n \leq 1$.

The following theorem is a little improvement of Theorem A.

Theorem 3.1. *Let l be an odd prime and G an l -group. Let $H = G/(Z(G) \cap [G, G])$ and m the nilpotency class of H . Then:*

$$\text{ram}^t(G) \leq d(G) + \sum_{2 \leq i \leq m} d_i(H),$$

where the sum is assumed to be 0 in case $m \leq 1$.

Proof. Let N be a positive integer such that the exponent of G is at most l^N , then the exponent of H is also at most l^N . By Theorem C, there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:

- (1) $\text{Gal}(L/\mathbf{Q})$ is isomorphic to H ;
- (2) $L/\mathbf{Q}$ is a Scholz extension of type (S_N) ;
- (3) $\sharp \text{Ram}(L/\mathbf{Q}) \leq d(H) + \sum_{2 \leq i \leq m} d_i(H)$.

We consider the central extension $\varepsilon : 1 \rightarrow Z(G) \cap [G, G] \rightarrow G \rightarrow H \rightarrow 1$. By Lemma 2.4, the embedding problem $(L/\mathbf{Q}, \varepsilon)$ is solvable. Since $Z(G) \cap [G, G] \subset [G, G]$, then $d(H) = d(G)$. By Lemmas 2.2 and 2.3, the embedding problem $(L/\mathbf{Q}, \varepsilon)$ has a proper solution which is unramified outside $\text{Ram}(L/\mathbf{Q})$. Hence

$$\text{ram}^t(G) \leq \sharp \text{Ram}(L/\mathbf{Q}) \leq d(G) + \sum_{2 \leq i \leq m} d_i(H).$$

□

Remark 3.2. Assume that G is a non-abelian l -group. Let $H = G/(Z(G) \cap [G, G])$ and n the nilpotency class of G . Then:

- (1) $d_i(H) \leq d_i(G)$ ($i = 2, 3, \dots, n$);
- (2) the nilpotency class of H is equal to $n - 1$.

We give a sketch of this proof. Put $D = Z(G) \cap [G, G]$, then $H = G/D$ and $C_i(H) = C_i(G)D/D$. Since there is a canonical surjection $C_i(G)/C_{i+1}(G) \rightarrow C_i(H)/C_{i+1}(H)$, $d_i(H) \leq d_i(G)$. Since D is a subgroup of the center of G , the nilpotency class of H is equal to n or $n - 1$. (See e.g. [12, Chapter 4 (2.6) Corollary 4].) The condition $C_{n+1}(G) = [C_n(G), G] = 0$ implies $C_n(G) \subset D$. Then $C_n(H) = C_n(G)D/D = 0$. Hence the nilpotency class of H is $n - 1$.

Example. Let G be the group of order 729 whose library number in GAP is (729, 290). By using the commutator notation $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$, the generator-relator notation of G is described as follows:

$$\langle x, y, z, u, v, w \mid [y, u], [y, z], [y, v], [z, u], [u, v], [x, v], [x, w], [z, v], [z, w], [u, w], [v, w], [y, w], v[x, z], w[x, u], u^2[y, x] \rangle.$$

Then $H = G/(Z(G) \cap [G, G])$ is the group of order 81 whose library number in GAP is (81, 12). The nilpotency class of G (resp. H) is 3 (resp. 2). Further $C_2(G)/C_3(G) \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ and $C_2(H) \cong \mathbf{Z}/3\mathbf{Z}$. Then,

$$d(G) + \sum_{2 \leq i \leq n-1} d_i(G) = d(G) + d_2(G) = 3 + 2 = 5,$$

$$d(G) + \sum_{2 \leq i \leq m} d_i(H) = d(G) + d_2(H) = 3 + 1 = 4.$$

This example shows that Theorem 3.1 is an improvement of Theorem A.

4. Minimal number of ramified primes in some 3-extensions

In this section, we prove that if G is any 3-group of order less than or equal to 3^5 then $\text{ram}^t(G) = d(G)$.

Notation In the rest of this article, we write $\Gamma(i, j)$ for the group whose library number in GAP is equal to (i, j) , where i is equal to the order of its group.

$$\Gamma(3^3, 3) = \langle x, y, z | x^3, y^3, z^3, z[y, x], [x, z], [y, z] \rangle,$$

$$\Gamma(3^3, 4) = \langle x, y | x^9, y^3, x^3[y, x] \rangle,$$

$$\Gamma(3^4, 4) = \langle x, y | x^9, y^9, x^3[y, x] \rangle,$$

$$\Gamma(3^4, 9) = \langle x, y, z | y[z, x], x^9, y^3, z^3, x^3[y, z], [x, y] \rangle,$$

$$\Gamma(3^5, 2) = \langle x, y, z, u, v | z[x, y], x^3u^{-1}, y^3v^{-1}, z^3, u^3, v^3, [x, z], [y, z], [y, u], [x, v] \rangle,$$

$$\Gamma(3^5, 22) = \langle x, y, z, u, v | u^3, v^3, x^3u^{-1}, y^3z^{-1}, z^3v^{-1}, [z, u], [x, v], [y, v], z[x, y] \rangle.$$

Definition 4.1. Let G be a non-trivial 3-group of order less than or equal to 3^5 . We classify these groups in six types (G1) $\sim$ (G6) as follows.

(G1) G is abelian.

(G2) The nilpotency class of G is 2.

(G3) The nilpotency class of G is greater than 2, the 3-rank of G is 2 and there exists a non-trivial central subgroup A of G such that G/A is isomorphic to $\Gamma(3^3, 3)$.

(G4) The nilpotency class of G is greater than 2 and the 3-rank of G is 2. Further the order of $Z(G)$ is 3 and $G/Z(G)$ is isomorphic to $\Gamma(3^4, 4)$.

(G5) The nilpotency class of G is greater than 2 and the 3-rank of G is 2. Further the order of $Z(G)$ is 3 and $G/Z(G)$ is isomorphic to $\Gamma(3^4, 9)$.

(G6) The nilpotency class of G is greater than 2, and the 3-rank of G is 3.

Remark 4.2. By using GAP, we can count the number of 3-groups satisfying the conditions in Definition 4.1. We list the number of the 3-group of each type (G1), (G2), $\dots$, (G6).

	(G1)	(G2)	(G3)	(G4)	(G5)	(G6)	total
number of groups	18	36	19	1	6	10	90

(1) We can check that any 3-group of order less than or equal to 3^5 satisfies exactly one condition of (G1), (G2), $\dots$, (G6).

(2) If G satisfies a condition of (G3) $\sim$ (G6), then the exponent of G is less than or equal to 27. In particular, if G satisfies the condition (G5) then the exponent of G is equal to 9.

(3) If G satisfies the condition (G4), then G is isomorphic to $\Gamma(3^5, 22)$.

(4) Assume that G satisfies the condition (G6). Then there exists a central subgroup A of G such that G/A is isomorphic to $\Gamma(3^3, 3) \times \mathbf{Z}/3\mathbf{Z}$.

(5) If the nilpotency class of G is greater than 2, there exists a central subgroup A such that $d(G) = d(G/A)$ and that G/A is isomorphic to one of $\Gamma(3^3, 3)$, $\Gamma(3^3, 3) \times \mathbf{Z}/3\mathbf{Z}$, $\Gamma(3^4, 4)$ and $\Gamma(3^4, 9)$.

Next we prepare some lemmas.

Lemma 4.3. *Let l be an odd prime number and G an l -group. If the nilpotency class of G is 1 or 2, then $\text{ram}^t(G) = d(G)$.*

This lemma is a special case of Theorem A (or Theorem 3.1).

Lemma 4.4. [6, Theorem 5.5, Proposition 7.1] *Let p and q be prime numbers such that $p \equiv q \equiv 1 \pmod{3}$. Let F_{pq} and F'_{pq} denote the two cyclic cubic fields of conductor pq .*

(1) *The class number of F_{pq} is divisible by 27 if and only if the class number of F'_{pq} is divisible by 27.*

(2) *Assume that the class number of F_{pq} is divisible by 27. Then there exists a Galois extension $L/F_{pq}/\mathbf{Q}$ satisfying the conditions:*

(a) *$\text{Gal}(L/\mathbf{Q})$ is isomorphic to $\Gamma(3^3, 3)$;*

(b) *L/F_{pq} is unramified;*

(c) *Any prime of F_{pq} lying above p or q splits completely in L/F_{pq} .*

(3) *Assume that the class number of F_{pq} is divisible by 81. Then there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:*

(a) *$\text{Gal}(L/\mathbf{Q})$ is isomorphic to $\Gamma(3^4, 9)$;*

(b) *L/F_{pq} is unramified;*

(c) *Any prime of F_{pq} lying above p or q splits completely in L/F_{pq} .*

This is a direct consequence of [6, Theorem 5.5] and the proof of [6, Proposition 7.1(2)(3)].

Remark 4.5. (1) Lemma 4.4(1) was first proved in [4]. The similar result on the divisibility by 81 does not hold. Let $p = 37, q = 991$. By the example bellow, the class number of F_{pq} is divisible by 81 but the one of F'_{pq} is not divisible by 81.

(2) The Galois extensions $L/\mathbf{Q}$ in Lemma 4.4(2) and (3) are Scholz extensions unramified outside pq .

Example. Let $h(F)$ denote the class number of the number field F .

p	q	$h(F_{pq})$	$h(F'_{pq})$
37	991	243	27
163	3889	171	9
433	2161	108	513
433	3889	27	27
487	2269	27	27
487	2917	9	36

Lemma 4.6. (1) *Assume that G is isomorphic to $\Gamma(3^3, 3)$ or $\Gamma(3^3, 3) \times \mathbf{Z}/3\mathbf{Z}$. Then there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:*

- (a) $\text{Gal}(L/\mathbf{Q})$ is isomorphic to G ;
 - (b) $\sharp\text{Ram}(L/\mathbf{Q}) = d(G)$;
 - (c) $L/\mathbf{Q}$ is a Scholz extension of type (S_3) .
- (2) There exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:
- (a) $\text{Gal}(L/\mathbf{Q})$ is isomorphic to $\Gamma(3^4, 9)$;
 - (b) $\sharp\text{Ram}(L/\mathbf{Q}) = d(\Gamma(3^4, 9)) (= 2)$;
 - (c) $L/\mathbf{Q}$ is a Scholz extension of type (S_2) .

Proof. (1) Let $p = 487$, $q = 2269$, then $p \equiv q \equiv 1 \pmod{3^4}$. By the example above the class number of a cyclic cubic field of conductor pq is divisible by 27. By Lemma 4.4(2), there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:

- $\text{Gal}(L/\mathbf{Q})$ is isomorphic to $\Gamma(3^3, 3)$;
- $L/\mathbf{Q}$ is unramified outside pq ;
- $L/\mathbf{Q}$ is a Scholz extension of type (S_4) .

This $L/\mathbf{Q}$ is a required extension for $G = \Gamma(3^3, 3)$. By applying Theorem B to the split extension

$$1 \rightarrow \mathbf{Z}/3\mathbf{Z} \rightarrow \Gamma(3^3, 3) \times \mathbf{Z}/3\mathbf{Z} \rightarrow \Gamma(3^3, 3) \rightarrow 1,$$

we can get the required extension for $G = \Gamma(3^3, 3) \times \mathbf{Z}/3\mathbf{Z}$.

(2) Let $p = 37$, $q = 991$, then $p \equiv q \equiv 1 \pmod{3^2}$. By the example above the class number of a cyclic cubic field of conductor pq is divisible by 81. By Lemma 4.4(3), there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:

- $\text{Gal}(L/\mathbf{Q})$ is isomorphic to $\Gamma(3^4, 9)$;
- $L/\mathbf{Q}$ is unramified outside pq ;
- $L/\mathbf{Q}$ is a Scholz extension of type (S_2) .

This $L/\mathbf{Q}$ is a required extension for $\Gamma(3^4, 9)$. □

Lemma 4.7. *Let p and q be primes satisfying the conditions: (1) $p \equiv q \equiv 1 \pmod{9}$, (2) $p^{\frac{q-1}{9}} \equiv 1 \pmod{q}$, (3) $q^{\frac{p-1}{9}} \equiv 1 \pmod{p}$. Assume that a cyclic cubic field of conductor pq is divisible by 27. Then there exists a Galois extension $L/\mathbf{Q}$ satisfying the conditions:*

- (a) $\text{Gal}(L/\mathbf{Q})$ is isomorphic to $\Gamma(3^4, 4)$;
- (b) $L/\mathbf{Q}$ is unramified outside pq ;
- (c) $L/\mathbf{Q}$ is a Scholz extension.

Proof. Let k_p (resp. k_q) be the cyclic extension of degree 9 which is unramified outside p (resp. q). Let F_{pq} be a cyclic cubic field of conductor pq . By Lemma 4.4(2), there exists a Galois extension $L_0/\mathbf{Q}$ satisfying the conditions:

- $\text{Gal}(L_0/\mathbf{Q})$ is isomorphic to $\Gamma(3^3, 3)$;
- L_0/F_{pq} is unramified;
- Any prime of F_{pq} lying above p or q splits completely in L_0/F_{pq} .

Let $\Gamma = \text{Gal}(L_0 k_p k_q / \mathbf{Q})$. Then Γ satisfies the conditions:

- the order is 243;
- the 3-rank is 2;
- the abelian quotient $\Gamma/[\Gamma, \Gamma]$ is isomorphic to $\mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$;
- Γ has a normal subgroup H such that Γ/H is isomorphic to $\Gamma(3^3, 3)$.

The group satisfying these conditions is unique and isomorphic to $\Gamma(3^5, 2)$. $\Gamma(3^5, 2)$ has a normal subgroup N such that $\Gamma(3^5, 2)/N$ is isomorphic to $\Gamma(3^4, 4)$. Let L be the field corresponding to N . Since $L_0 k_p k_q / \mathbf{Q}$ is a Scholz extension, $L/\mathbf{Q}$ is also a Scholz extension. Then L is a required field. $\square$

Remark 4.8. Let $p = 487, q = 2269$, then $p \equiv q \equiv 1 \pmod{3^4}$ and satisfy the conditions (1), (2), and (3) in Lemma 4.7.

Theorem 4.9. *Let G be a 3-group of order less than or equal to 3^5 . Then $\text{ram}^t(G) = d(G)$.*

Proof. If the nilpotency class of G is at most 2, then $\text{ram}^t(G) = d(G)$ by Lemma 4.3. Assume that the nilpotency class of G is greater than 2. Then, by the Remark 4.2, there exists a central subgroup A such that $d(G) = d(G/A)$ and that G/A is isomorphic to one of $\Gamma(3^3, 3)$, $\Gamma(3^3, 3) \times \mathbf{Z}/3\mathbf{Z}$, $\Gamma(3^4, 4)$ and $\Gamma(3^4, 9)$. Let 3^N be the exponent of G . By Lemma 4.6 and 4.7, there exists a Galois extension $L_0/\mathbf{Q}$ satisfying the conditions:

- (1) $L_0/\mathbf{Q}$ is a Scholz extension of type (S_N) ;
- (2) $\text{Gal}(L_0/\mathbf{Q})$ is isomorphic to G/A ;
- (3) $\sharp \text{Ram}(L_0/\mathbf{Q}) = d(G)$.

Let $\varepsilon : 1 \rightarrow A \rightarrow G \rightarrow \text{Gal}(L_0/\mathbf{Q}) \rightarrow 1$ be the canonical central extension. By applying Lemma 2.2, 2.3 and 2.4 to the problem $(L_0/\mathbf{Q}, \varepsilon)$, we can prove the existence of a Galois extension satisfying the conditions:

- (a) $\text{Gal}(L/\mathbf{Q})$ is isomorphic to G ;
- (b) $\sharp \text{Ram}(L/\mathbf{Q}) = d(G)$.

We have thus proved the theorem. $\square$

References

- [1] A. Cueto-Hernández and G.D. Villa-Salvador, *Nilpotent extensions of number fields with bounded ramification*, Pacific J. Math. **196** (2000), 297–316.
- [2] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4, 2005. (<http://www.gap-system.org>)
- [3] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.
- [4] H. Naito, *On l^3 -divisibility of class numbers of l -cyclic extensions*, pp. 87–92 in Algebraic number theory (Kyoto, 1986), Proc. Symp. RIMS (Kokyuroku) **603**, 1987.
- [5] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.
- [6] A. Nomura, *Unramified 3-extensions over cyclic cubic fields*, Pacific J. Math. **230** (2007), 167–182.
- [7] The Pari Group, PARI/GP, Bordeaux, 2004. (<http://pari.math.u-bordeaux.fr/>).
- [8] B. Plans, *On the minimal number of ramified primes in some solvable extensions of $\mathbf{Q}$* , Pacific J. Math. **215** (2004), 381–391.
- [9] H. Reichardt, *Konstruktion vom Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math. **177** (1937), 1–5.
- [10] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.
- [11] A. Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*, Math. Z. **42** (1936), 161–188.
- [12] M. Suzuki, *Group Theory II*, Grundlehren der Math. Wissenschaften **248**, Springer, New York, 1986.

Acknowledgment

I should like to express my gratitude to the referee for her/his careful reading and the advices.

Akito Nomura

Mathematics Section, Division of Innovative Technology and Science,
Graduate School of Natural Science and Technology, Kanazawa University,
Kanazawa 920-1192, Japan

e-mail: anomura@t.kanazawa-u.ac.jp