K. Miyake
Nagoya Math. J.
Vol. 93 (1984), 133-148

ON CENTRAL EXTENSIONS OF A GALOIS EXTENSION OF ALGEBRAIC NUMBER FIELDS

KATSUYA MIYAKE

Introduction

Let k be an algebraic number field of finite degree, and K a finite Galois extension of k. A central extension L of K/k is an algebraic number field which contains K and is normal over k, and whose Galois group over K is contained in the center of the Galois group $\mathrm{Gal}(L/k)$. We denote the maximal abelian extensions of k and K in the algebraic closure of k by k_{ab} and K_{ab} respectively, and the maximal central extension of K/k by $\mathrm{MC}_{K/k}$. Then we have $K_{ab}\supset \mathrm{MC}_{K/k}\supset k_{ab}\cdot K$.

Put $\mathfrak{g}=\mathrm{Gal}(K/k)$, and let $\mathfrak{S}(K/k)$ be the dual group of the Schur multiplicator $H^2(\mathfrak{g}, \boldsymbol{Q}/\boldsymbol{Z})$ of $\mathfrak{g}$. It is known as was explained in [5] for example, that there exists a canonical isomorphism

$$\varphi_{K/k} : \mathfrak{S}(K/k) \xrightarrow{\sim} \mathrm{Gal}(\mathrm{MC}_{K/k}/k_{ab}\cdot K).$$

Therefore, especially, $\mathrm{MC}_{K/k}$ is a finite extension of $k_{ab}\cdot K$. For a central extension L of K/k, this $\varphi_{K/k}$ induces a surjective homomorphism $\mathrm{rest}_L\circ\varphi_{K/k}$ of $\mathfrak{S}(K/k)$ onto $\mathrm{Gal}(L/L\cap k_{ab}\cdot K)$. It is also known that there exists a finite central extension L of K/k such that $\varphi_{K/k}$ induces an isomorphism of $\mathfrak{S}(K/k)$ onto $\mathrm{Gal}(L/L\cap k_{ab}\cdot K)$. Such an L is said to be an abundant central extension of K/k for convenience in [5], where we posed the following problem:

PROBLEM. Is there an abundant central extension M of K/k such that $M\cap k_{ab}\cdot K=K$? If not, then what determines the structure of $\mathrm{Gal}(M\cap k_{ab}\cdot K/K)$ for an abundant central extension M of minimum degree?

In this paper, we give a couple of sufficient conditions under which $M\cap k_{ab}\cdot K$ coincides with K, and examine some cases for which the conditions hold. We also give an upper bound for $[M:K]$ in the final section.

Received September 27, 1982.
Revised January 28, 1983.

There is a certain kind of important central extensions which were introduced by Opolka [6] and others as a substitute for the Hasse norm theorem in K/k. Let $\mathfrak{K}(K/k)$ be Scholz's number knot of K/k, that is the quotient group of

$$\{a \in k^\times | a \text{ is a norm locally everywhere in } K\}$$

by its subgroup $\{a \in k^\times | a \text{ is a global norm in } K\}$. There exists a canonical surjective homomorphism $\psi_{K/k}$ of $\mathfrak{S}(K/k)$ onto $\mathfrak{K}(K/k)$. (See [5] for example.) A central solution of $\mathfrak{K}(K/k)$ is, according to Opolka, a finite central extension L of K/k such that an element a of $k^\times$ is a global norm in K if a is a norm locally everywhere in L. For a finite central extension L of K/k to be a solution of $\mathfrak{K}(K/k)$, it is necessary and sufficient that there exists a homomorphism $\psi : \mathrm{Gal}(L/L \cap k_{\mathrm{ab}} \cdot K) \to \mathfrak{K}(K/k)$ such that $\psi_{K/k} = \psi \circ \mathrm{rest}_L \circ \varphi_{K/k}$.

In this paper, we also show the result of Opolka [7] which gives an upper bound of $[L:K]$ for a minimal central solution L of $\mathfrak{K}(K/k)$, and improve his sufficient condition for such an L to satisfy that $L \cap k_{\mathrm{ab}} \cdot K = K$.

1. Notation and Preliminaries

Let K/k be a finite Galois extension of algebraic number fields of finite degree with $\mathfrak{g} = \mathrm{Gal}(K/k)$. Put $\mathfrak{S}(K/k)$ = the dual group of $H^2(\mathfrak{g}, \boldsymbol{Q}/\boldsymbol{Z})$, as was in Introduction. Let $K_A^\times$ be the idele group of K, and $\mathfrak{a}_K : K_A^\times \to \mathrm{Gal}(K_{\mathrm{ab}}/K)$ the Artin map of class field theory with $K^\# = \mathrm{Ker}\, \mathfrak{a}_K$. Throughout this paper, we consider the idele group $k_A^\times$ naturally imbedded into $K_A^\times$. Define a closed subgroup of $K_A^\times$ by

$$K_A^{\Delta\mathfrak{g}} = \langle x^{1-\sigma} | x \in K_A^\times, \sigma \in \mathfrak{g} \rangle$$

under the natural action of $\mathfrak{g}$ on $K_A^\times$. Then $\mathfrak{a}_K$ induces an isomorphism $\bar{\mathfrak{a}}_K : K_A^\times / K_A^{\Delta\mathfrak{g}} \cdot K^\# \xrightarrow{\sim} \mathrm{Gal}(\mathrm{MC}_{K/k}/K)$. (See [5] for example.) Let $N_{K/k} : K_A^\times \to k_A^\times$ be the norm map. Then Scholz's number knot is given as

$$\mathfrak{K}(K/k) = k^\times \cap N_{K/k}(K_A^\times) / N_{K/k}(K^\times)$$

where $k^\times$ and $K^\times$ are the multiplicative groups of k and K respectively. From the divisibility properties of $k^\# / k^\times$ and $K^\# / K^\times$, we easily see that $\mathfrak{K}(K/k)$ is isomorphic to $k^\# \cap N_{K/k}(K_A^\times) / N_{K/k}(K^\#)$. Therefore we have

$$\mathfrak{K}(K/k) \simeq N_{K/k}^{-1}(k^\#) / N_{K/k}^{-1}(1) \cdot K^\#.$$

(Cf. [3] for example.) Since $\mathfrak{a}_K$ induces an isomorphism of $N_{K/k}^{-1}(k^\#)/K^\#$ onto $\mathrm{Gal}(K_{\mathrm{ab}}/k_{\mathrm{ab}}\cdot K)$, we have the following commutative diagram:

$$(*)\qquad \begin{array}{ccccccc} \mathrm{Gal}(\mathrm{MC}_{K/k}/K) & \hookleftarrow & \mathrm{Gal}(\mathrm{MC}_{K/k}/k_{ab}\cdot K) & \xleftarrow[\varphi_{K/k}]{\sim} & \mathfrak{S}(K/k) & & \\ \uparrow \wr\ \vec{\mathfrak{a}}_K & & \uparrow \wr & & & \searrow^{\psi_{K/k}} & \\ K_A^\times/K_A^{\Delta g}\cdot K^\# & \hookleftarrow & N_{K/k}^{-1}(k^\#)/K_A^{\Delta g}\cdot K^\# & \xrightarrow[\mathrm{proj.}]{} & N_{K/k}^{-1}(k^\#)/N_{K/k}^{-1}(1)\cdot K^\# & \xrightarrow[N_{K/k}]{\sim} & \mathfrak{K}(K/k). \end{array}$$

Let $\pi: K_A^\times \to K_A^\times/K_A^{\Delta g}\cdot K^\#$ be the natural projection, and put

$$\mathscr{C} = \{L \mid \text{a finite central extension of } K/k\},$$
$$\mathfrak{U} = \{U \mid \text{an open subgroup of } \pi(K_A^\times)\}.$$

Then we have a perfect correspondence between $\mathscr{C}$ and $\mathfrak{U}$ assigning $U = \pi(N_{L/K}(L_A^\times))$ to $L \in \mathscr{C}$. If L is a finite abelian extension of K, then $L \in \mathscr{C}$ if and only if $N_{L/K}(L_A^\times)\cdot K^\times \supset K_A^{\Delta g}\cdot K^\#$. Therefore, for $L \in \mathscr{C}$, we have a surjective homomorphism of $\mathfrak{S}(K/k)(\simeq N_{K/k}^{-1}(k^\#)/K_A^{\Delta g}\cdot K^\#)$ onto $N_{K/k}(L_A^\times)\cdot N_{K/k}^{-1}(k^\#)/N_{L/K}(L_A^\times)\cdot K^\times$ which is naturally isomorphic to $N_{K/k}^{-1}(k^\#)/N_{L/K}(L_A^\times)\cdot K^\times \cap N_{K/k}^{-1}(k^\#)$. Because the last isomorphism corresponds to the isomorphism

$$\mathrm{Gal}(L\cdot k_{\mathrm{ab}}/k_{\mathrm{ab}}\cdot K) \xrightarrow{\sim} \mathrm{Gal}(L/L\cap k_{\mathrm{ab}}\cdot K)$$

by the Artin map $\mathfrak{a}_K$, the surjection is the idelic version of $\mathrm{rest}_L \circ \varphi_{K/k}$ of $\mathfrak{S}(K/k)$ onto $\mathrm{Gal}(L/L\cap k_{\mathrm{ab}}\cdot K)$, which was stated in Introduction. Therefore we have:

A member L of $\mathscr{C}$ is abundant

$\iff \mathrm{Gal}(L/L\cap k_{\mathrm{ab}}\cdot K) \simeq \mathfrak{S}(K/k)$

$\iff N_{L/K}(L_A^\times)\cdot K^\times \cap N_{K/k}^{-1}(k^\#) = K_A^{\Delta g}\cdot K^\#$.

It is also clear that:

A member L of $\mathscr{C}$ is a solution of $\mathfrak{K}(K/k)$

$\iff N_{L/K}(L_A^\times)\cdot K^\times \cap N_{K/k}^{-1}(k^\#) \subset N_{K/k}^{-1}(1)\cdot K^\#$

$\iff$ There exists a homomorphism $\psi: \mathrm{Gal}(L/L\cap k_{\mathrm{ab}}\cdot K) \longrightarrow \mathfrak{K}(K/k)$ such that $\psi_{K/k} = \psi \circ \mathrm{rest}_L \circ \varphi_{K/k}$.

The following proposition is now almost obvious:

PROPOSITION 1. *There exists an abundant central extension M of K/k such that $M\cap k_{\mathrm{ab}}\cdot K = K$ if and only if there exists a member U of $\mathfrak{U}$ such that $U\cap \pi(N_{K/k}^{-1}(k^\#)) = 1$ and $U\cdot\pi(N_{K/k}^{-1}(k^\#)) = \pi(K_A^\times)$.*

Now, let $\mathfrak{p}$ and $\mathfrak{P}$ be prime divisors of k and K, respectively, with the completion $k_{\mathfrak{p}}$ and $K_{\mathfrak{P}}$. We denote the maximal order of k or the ring of integers of $k_{\mathfrak{p}}$ by $O(k)$ or $O(k_{\mathfrak{p}})$, respectively, and the unit groups by $O^{\times}(k)$ or $O^{\times}(k_{\mathfrak{p}})$. We also denote $O^{\times}(k_A) = k_{\infty}^{\times} \cdot \prod_{\mathfrak{p}} O^{\times}(k_{\mathfrak{p}})$ where $k_{\infty}^{\times}$ is the Archimedean part of $K_A^{\times}$. For an Archimedean prime divisor $\mathfrak{p}$, let us write $O^{\times}(k_{\mathfrak{p}}) = k_{\mathfrak{p}}^{\times}$ where $k_{\mathfrak{p}}$ is the completion of k by $\mathfrak{p}$. Then $O^{\times}(k_A) = \prod_{\mathfrak{p}} O^{\times}(k_{\mathfrak{p}})$ where $\prod_{\mathfrak{p}}$ is the direct product over all prime divisors of k. We naturally identify $(K \otimes_k k_{\mathfrak{p}})^{\times}$ with $\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^{\times}$, and denote the norm map $(K \otimes k_{\mathfrak{p}})^{\times} \to k_{\mathfrak{p}}^{\times}$ by $N_{K/k}^{(\mathfrak{p})}$. For a prime divisor $\mathfrak{P}$ of K, the norm map $K_{\mathfrak{P}}^{\times} \to k_{\mathfrak{p}}^{\times}$ is simply denoted by $N_{\mathfrak{P}}$ if $\mathfrak{p} = \mathfrak{P}|_k$. Let $\mathfrak{g}(\mathfrak{P})$ be the decomposition group of $\mathfrak{P}$, and put

$$K_{\mathfrak{P}}^{\Delta\mathfrak{g}(\mathfrak{P})} = \langle x^{1-\sigma} \,|\, x \in K_{\mathfrak{P}}^{\times}, \sigma \in \mathfrak{g}(\mathfrak{P}) \rangle.$$

We also put

$$(K \otimes k_{\mathfrak{p}})^{\Delta\mathfrak{g}} = \langle x^{1-\sigma} \,|\, x \in (K \otimes k_{\mathfrak{p}})^{\times}, \sigma \in \mathfrak{g} \rangle.$$

The following three propositions are well known:

PROPOSITION 2. *Let $\mathfrak{P}$ and $\mathfrak{P}'$ be prime divisors of K such that $\mathfrak{P}|_k = \mathfrak{P}'|_k = \mathfrak{p}$. Then there exists an element $\sigma \in \mathfrak{g}$ such that $N_{\mathfrak{P}}^{-1}(1) = N_{\mathfrak{P}'}^{-1}(1)^{\sigma}$ in $(K \otimes k_{\mathfrak{p}})^{\times}$. Especially, we have $(N_{K/k}^{(\mathfrak{p})})^{-1}(1) = (K \otimes k_{\mathfrak{p}})^{\Delta\mathfrak{g}} \cdot N_{\mathfrak{P}}^{-1}(1)$ for any $\mathfrak{P}$ dividing $\mathfrak{p}$.*

PROPOSITION 3. $N_{\mathfrak{P}}^{-1}(1)/K_{\mathfrak{P}}^{\Delta\mathfrak{g}(\mathfrak{P})} \simeq$ *the dual of* $H^2(\mathfrak{g}(\mathfrak{P}), \boldsymbol{Q}/\boldsymbol{Z})$.

Remark. This is the local version of the isomorphism of $\mathfrak{S}(K/k) \simeq N_{K/k}^{-1}(k^{\#})/K_A^{\Delta\mathfrak{g}} \cdot K^{\#}$ in the diagram (*).

PROPOSITION 4. *If $K_{\mathfrak{P}}$ is cyclic over $k_{\mathfrak{p}}$ for a prime divisor $\mathfrak{P}$ dividing $\mathfrak{p}$, then $N_{\mathfrak{P}}^{-1}(1) = K_{\mathfrak{P}}^{\Delta\mathfrak{g}(\mathfrak{P})}$ and $(N_{K/k}^{(\mathfrak{p})})^{-1}(1) = (K \otimes k_{\mathfrak{p}})^{\Delta\mathfrak{g}}$.*

If $\mathfrak{p}$ is unramified in K/k, then $K_{\mathfrak{P}}$ is cyclic over $k_{\mathfrak{p}}$ for any $\mathfrak{P}|\mathfrak{p}$. Put

$$D = \{\mathfrak{p} \,|\, \text{a prime divisor of } k \text{ ramified in } K/k\}.$$

PROPOSITION 5. *For each $\mathfrak{p} \in D$, take a prime divisor $\tilde{\mathfrak{p}}$ of K dividing $\mathfrak{p}$. Then we have*

$$N_{K/k}^{-1}(1) = K_A^{\Delta\mathfrak{g}} \cdot \prod_{\mathfrak{p} \in D} N_{\tilde{\mathfrak{p}}}^{-1}(1).$$

Here each $N_{\tilde{\mathfrak{p}}}^{-1}(1)$ is considered to be naturally imbedded in $K_A^{\times}$.

2. The condition $C(m)$ and the key theorem

For a positive integer m, let us consider a few conditions on K/k.

$C(m): \{u \in N_{K/k}(K_A^\times)\cdot k^\times \mid u^m = 1\} \subset N_{K/k}(\{z \in K_A^\times \mid z^m \in K_A^{\Delta\mathfrak{g}}\})\cdot\{\zeta \in k^\times \mid \zeta^m = 1\}$;
$C'(m): \{u \in N_{K/k}(K_A^\times)\cdot k^\times \mid u^m = 1\} \subset N_{K/k}(K_A^\times)\cdot\{\zeta \in k^\times \mid \zeta^m = 1\}$;
$C_1(m): u \in N_{K/k}(K_A^\times)\cdot k^\times$ and $u^m = 1 \Longrightarrow \exists\zeta \in k^\times \forall\mathfrak{p} \in D\ ((u\zeta)_\mathfrak{p} = 1)$.

Here for an idele $x \in k_A^\times$ and a prime divisor $\mathfrak{p}$, $x_\mathfrak{p}$ is the $\mathfrak{p}$-component of x, i.e. $x = (\cdots, x_\mathfrak{p}, \cdots) \in k_A^\times = \prod'_\mathfrak{p} k_\mathfrak{p}^\times$.

Remark. It is obvious that $C_1(m)$ implies $C_1(\mu)$ for every $\mu | m$.

PROPOSITION 6. $C_1(m) \Rightarrow C(m) \Rightarrow C'(m)$.

Proof. It is obvious that $C(m)$ implies $C'(m)$. We show that $C_1(m)$ implies $C(m)$. Let u be an element of $N_{K/k}(K_A^\times)\cdot k^\times$ such that $u^m = 1$. Choose $\zeta \in k^\times$ for u by $C_1(m)$. Then in $k_\mathfrak{p}$, we have $\zeta^{-1} = u_\mathfrak{p}$. Therefore, especially, $\zeta^m = 1$. Since $(u\zeta)^m = 1$, we have $u\zeta \in O^\times(k_A)$. For each prime divisor $\mathfrak{p}$ of k, fix a prime divisor $\tilde{\mathfrak{p}}$ of K dividing $\mathfrak{p}$. For a prime divisor $\mathfrak{P}$ of K, put $z_\mathfrak{P} = 1$ if either $\mathfrak{P}|_k \in D$ or $\mathfrak{P} \neq \tilde{\mathfrak{p}}$ for $\mathfrak{p} = \mathfrak{P}|_k$. If $\mathfrak{P} = \tilde{\mathfrak{p}}$ for $\mathfrak{p} \notin D$, then $K_\mathfrak{P}$ is unramified over $k_\mathfrak{p}$. Therefore there is an element $z_\mathfrak{P}$ in $O^\times(K_\mathfrak{P})$ such that $N_\mathfrak{P}(z_\mathfrak{P}) = (u\zeta)_\mathfrak{p}$. Let $z = (\cdots, z_\mathfrak{P}, \cdots)$ be the idele of $K_A^\times$ with $z_\mathfrak{P}$ determined in this way as the $\mathfrak{P}$-component. Then we have $N_{K/k}(z) = u\zeta$. Since $N_{K/k}(z^m) = (u\zeta)^m = 1$, z^m belongs to $N_{K/k}^{-1}(1)$. Then by Proposition 4, we have $z^m \in K_A^{\Delta\mathfrak{g}}$ because of the choice of $z_\mathfrak{P}$'s for $\mathfrak{P}|_k \in D$. This shows that $u = (u\zeta)\cdot\zeta^{-1} = N_{K/k}(z)\cdot\zeta^{-1}$ belongs to the set at the right hand side of $C(m)$. Q.E.D.

PROPOSITION 7. *Suppose that* $m = q\cdot r$ *and* $(q, r) = 1$. *Then* $C(m)$ *implies* $C(q)$ *and* $C(r)$.

Proof. Take μ and ν in Z so that $\mu q + \nu r = 1$. Let u be an element of $N_{K/k}(K_A^\times)\cdot k^\times$ such that $u^q = 1$. Then by $C(m)$, we can find $z \in K_A^\times$ and $\zeta \in k^\times$ such that $z^m \in K_A^{\Delta\mathfrak{g}}$, $\zeta^m = 1$ and $N_{K/k}(z)\cdot\zeta = u$. Therefore we have

$$u = u^{\mu q + \nu r} = u^{\nu r} = N_{K/k}(z^{\nu r})\cdot\zeta^{\nu r}.$$

Because we have $(z^{\nu r})^q = (z^m)^\nu \in K_A^{\Delta\mathfrak{g}}$ and $(\zeta^{\nu r})^q = (\zeta^m)^\nu = 1$, we have seen that $C(m)$ implies $C(q)$. Q.E.D.

PROPOSITION 8. *Suppose that* $m = q\cdot r$ *and* $(q, r) = 1$. *Then* $C'(m)$ *implies* $C'(q)$ *and* $C'(r)$.

The proof is similar to the one of Proposition 7.

Now, define a set of prime numbers $\mathscr{P}$ and a positive integer $m(\mathfrak{g})$ by

$$\mathscr{P} = \{p \mid \text{a prime number, } p \mid |\mathfrak{S}(K/k)|\};$$
$$m(\mathfrak{g}) = \text{the exponent of } \mathfrak{S}(K/k).$$

Then $m(\mathfrak{g})$ divides the order $|\mathfrak{g}|$. (See the proof of Proposition 10.) Note that $\mathfrak{S}(K/k) \cong H^2(\mathfrak{g}, \boldsymbol{Q}/\boldsymbol{Z})$.

THEOREM 1. *Suppose that the condition* $C(m)$ *is satisfied for every* $m \mid m(\mathfrak{g})$ *by the Galois extension* K/k, *and that* $k^\times \cap k_A^{\times m(\mathfrak{g})} = k^{\times m(\mathfrak{g})}$. *Then there exists an abundant central extension* M *of* K/k *such that* $M \cap k_{ab} \cdot K = K$. *Especially,* $\mathrm{Gal}(M/K)$ *is isomorphic to* $\mathfrak{S}(K/k)$.

Remark. As is well known, $[k^\times \cap k_A^{\times m(\mathfrak{g})} : k^{\times m(\mathfrak{g})}] \leq 2$. If $k(\zeta_{2^t})$ is cyclic over k, then the index is equal to 1 where ζ_{2^t} is a primitive 2^t-th root of 1 for $2^t \| m(\mathfrak{g})$. (See Artin-Tate [1, Ch. 10, § 1].)

We prove the theorem by showing the existence of an open subgroup U of $\pi(K_A^\times) = K_A^\times / K_A^{\Delta_\mathfrak{g}} \cdot K^\#$ which satisfies the condition of Proposition 1.

LEMMA 1. *Suppose that the condition* $C(q)$, $q = p^e$ *for a prime number* p, *is satisfied. If* $p = 2$, *we assume that* $k^\times \cap k_A^{\times q} = k^{\times q}$. *Let* $\bar{x}$ *be an element of* $\pi(N_{K/k}^{-1}(k^\#))$. *If* $\bar{x}$ *belongs to* $\pi(K_A^\times)^q \cdot U$ *for every open subgroup* U *of* $\pi(K_A^\times)$ *such that* $U \cap \langle \bar{x} \rangle = 1$, *then* $\bar{x}$ *belongs to* $\pi(N_{K/k}^{-1}(k^\#))^q$.

Proof. Because $\pi(K_A^\times)^q = \{\bar{z}^q \mid \bar{z} \in \pi(K_A^\times)\}$ is a closed subgroup of $\pi(K_A^\times)$, we have $\bigcap_U \pi(K_A^\times)^q \cdot U = \pi(K_A^\times)^q$ where $\bigcap_U$ is the intersection over all the open subgroup U of $\pi(K_A^\times)$ such that $U \cap \langle \bar{x} \rangle = 1$. (Remember that $\pi(N_{K/k}^{-1}(k^\#))$ is isomorphic to $\mathfrak{S}(K/k)$, and finite. Therefore $\langle \bar{x} \rangle - \{1\}$ is a closed subset of $\pi(K_A^\times)$.) By the assumption, therefore, $\bar{x}$ belongs to $\pi(K_A^\times)^q$. Take $x \in N_{K/k}^{-1}(k^\#)$ and $y \in K_A^\times$ so that $\bar{x} = \pi(x) = \pi(y)^q$. Then $x = y^q wa$ with $w \in K_A^{\Delta_\mathfrak{g}}$ and $a \in K^\#$. Therefore $N_{K/k}(xa^{-1}) \in k^\# \cap K_A^{\times q}$. We have $k^\# = k^\times \cdot k^{\# q}$ by the divisibility property of $k^\#/k^\times$ (see [3] for example), and $k^\times \cap k_A^{\times q} = k^{\times q}$ (by the assumption if $p = 2$). Therefore there exists $b \in K^\#$ such that $N_{K/k}(xa^{-1}) = b^q$. Then we have $N_{K/k}(y) = u \cdot b$ with $u \in N_{K/k}(K_A^\times) \cdot k^\# = N_{K/k}(K_A^\times) \cdot k^\times$ such that $u^q = 1$. By $C(q)$, take $z \in K_A^\times$ and $\zeta \in k^\times$ such that $z^q \in K_A^{\Delta_\mathfrak{g}}$, $\zeta^q = 1$ and $N_{K/k}(z) \cdot \zeta = u$. Then $N_{K/k}(yz^{-1}) = \zeta \cdot b \in k^\#$, i.e. $yz^{-1} \in N_{K/k}^{-1}(k^\#)$. Since $\pi(z)^q = 1$, we finally have $\bar{x} = \pi(x) = \pi(y)^q = \pi(yz^{-1})^q \in \pi(N_{K/k}^{-1}(k^\#))^q$. Q.E.D.

LEMMA 2. *Let* A *be a finite abelian* p-*group, and* B *be a subgroup of* A. *Suppose that* $A^q \cap B \subset B^q$ *for each* q $(1 \leq q \leq \exp(B))$, *then there exists a subgroup* C *of* A *such that* $B \cdot C = A$ *and* $B \cap C = 1$.

Proof. Choose a set of generators $\{b_1, \cdots, b_\mu\}$ of B such that B is the direct product $\langle b_1\rangle \times \cdots \times \langle b_\mu\rangle$. Then $B^q = \langle b_1^q, \cdots, b_\mu^q\rangle$. Among the subsets $\{c_1, \cdots, c_\nu\}$ of A such that $A = \langle b_1, \cdots, b_\mu, c_1, \cdots, c_\nu\rangle$, take $\{c_1, \cdots, c_\nu\}$ so that $|\langle c_1\rangle| + \cdots + |\langle c_\nu\rangle|$ is minimum. Put $C = \langle c_1, \cdots, c_\nu\rangle$. Assume that $B \cap C \neq \{1\}$, and let x be an element of $B \cap C$ different from 1. Then $x = \prod_{i=1}^{\nu} c_i^{q_i \cdot r_i}$ where q_i is a power of p and $(r_i, p) = 1$. Put $q = \min\{q_i | c_i^{q_i \cdot r_i} \neq 1\}$. Then x belongs to B^q since this contains $A^q \cap B$. Take $u \in B$ such that $u^q = x$. Put $s_i = q_i \cdot r_i / q$ for i such that $c_i^{q_i \cdot r_i} \neq 1$, and $c = u^{-1} \cdot \prod' c_i^{s_i}$ where $\prod'$ is the product over all such i that $c_i^{q_i \cdot r_i} \neq 1$. Then we have $c^q = 1$. Let j be one of the indices such that $q_j = q$ (and $c_j^{q_j \cdot r_j} \neq 1$). Replacing c_j by c, we have a set of generators $\{b_1, \cdots, b_\mu, c_1, \cdots, c, \cdots, c_\nu\}$ of A. Since $c_j^q \neq 1$, we also have $|\langle c\rangle| < |\langle c_j\rangle|$. This contradicts the choice of $\{c_1, \cdots, c_\nu\}$. The proof is completed.

Proof of the theorem. Put $X = \pi(N_{K/k}^{-1}(k^\#))$. This is finite. Take $p \in \mathscr{P}$, and let $p^t \| m(\mathfrak{g})$. Then for each $q = p^e$ $(p \leq q \leq p^t)$, the condition $C(q)$ is satisfied. By Lemma 1, we see that, for every $x \in X - X^p$, there exists and open subgroup U_x of $\pi(K_A^\times)$ such that $U_x \cap X = \{1\}$ and $\pi(K_A^\times)^p \cdot U_x \not\ni x$. Put $U_1 = \bigcap_{x \in X - X^p} U_x$. Then we have

$$\pi(K_A^\times)^p \cdot U_1 \cap X \subset X^p.$$

Next, for every $y \in X^p - X^{p^2}$, take an open subgroup V_y of $\pi(K_A^\times)$, by Lemma 1, such that $V_y \cap X = \{1\}$ and $\pi(K_A^\times)^{p^2} \cdot V_y \not\ni y$. Put $U_2 = (\bigcap_{y \in X^p - X^{p^2}} V_y) \cap U_1$. Then we have

$$\begin{cases} \pi(K_A^\times)^p \cdot U_2 \cap X \subset X^p, \\ \pi(K_A^\times)^{p^2} \cdot U_2 \cap X \subset X^{p^2}. \end{cases}$$

Continue the process and obtain an open subgroup U of $\pi(K_A^\times)$ such that $U \cap X = \{1\}$ and

$$\pi(K_A^\times)^q \cdot U \cap X \subset X^q \quad \text{for} \quad q = p^e \ (p \leq q \leq p^t).$$

Let $X^{(p)}$ be the p-primary part of X and X_1 be the p-complementary part of X. Let A be the p-primary part of $\pi(K_A^\times)/U$ and put $B = X^{(p)} \cdot U/U$. Then A is a finite abelian p-group and B is its subgroup. By the choice of U, we can apply Lemma 2 to A and B. Therefore we can find an open subgroup W of $\pi(K_A^\times)$ containing U and X_1 such that $\pi(K_A^\times) = W \cdot X^{(p)}$ and $W \cap X^{(p)} = \{1\}$. Take another prime factor p_1 of $m(\mathfrak{g})$ and proceed the similar process to the above for W and X_1 in place of $\pi(K_A^\times)$ and X respectively. In this way, we can finally find an open subgroup of $\pi(K_A^\times)$ which satisfies the conditions of Proposition 1, and complete the proof.

In the following Sections 3∼6, we see examples to which Theorem 1 is applicable. Therefore, we assume there that the following condition is satisfied by K/k:

ASSUMPTION. $k^\times \cap k_A^{\times m(\mathfrak{g})} = k^{\times m(\mathfrak{g})}$.

Note that this implies $k^\times \cap k_A^{\times m} = k^{\times m}$ for every $m|m(\mathfrak{g})$. (See Artin-Tate [1, Ch. 10, Theorem 1].)

3. The case of unramified extensions

Suppose that K/k is unramified. Then by Proposition 5, we have $N_{K/k}^{-1}(1) = K_A^{\Delta\mathfrak{g}}$ in this case. Then it is easily seen that the conditions $C(m)$ and $C'(m)$ coincides for each m. It follows, moreover, from the commutative diagram (*) at once that $\mathfrak{S}(K/k)$ is isomorphic to $\mathfrak{K}(K/k)$. We also easily see that the following condition $C_1'(m)$ holds for any m in this case, that implies $C'(m)$ immediately:

$$C_1'(m) : \{u \in k_A^\times | u^m = 1\} \subset N_{K/k}(K_A^\times).$$

Hence we have

THEOREM 2. *Suppose that K/k is a finite (not necessarily abelian) unramified extension. Then there exists an abundant central extension M of K/k such that $M \cap k_{\mathrm{ab}} \cdot K = K$. Furthermore, $\mathfrak{S}(K/k)$ is isomorphic to $\mathfrak{K}(K/k)$, and also to* Gal(M/K) *for such an M.*

4. The case that k is either Q or an imaginary quadratic field

In this section, let k be either the rational number field $\boldsymbol{Q}$ or an imaginary quadratic field. In this case, the units of k are roots of 1, and very few. Therefore, for almost every ray class field K of k, the condition $C_1(m(\mathfrak{g}))$ holds.

Let $D_{k/\boldsymbol{Q}}$ be the discriminant of k over $\boldsymbol{Q}$, and $\mathfrak{f}$ be the conductor of K/k. Suppose that the following conditions are satisfied:

(1) If $2 \nmid D_{k/\boldsymbol{Q}}$, then $\mathfrak{p}|(2, \mathfrak{f}) \Longrightarrow \mathfrak{p}^2|\mathfrak{f}$;
(2) If $2 | D_{k/\boldsymbol{Q}}$, then $\mathfrak{p}|(2, \mathfrak{f}) \Longrightarrow \mathfrak{p}^3|\mathfrak{f}$;
(3) If $k = \boldsymbol{Q}(\sqrt{-3})$, then $\mathfrak{p}|(\sqrt{-3}, \mathfrak{f}) \Longrightarrow \mathfrak{p}^2|\mathfrak{f}$.

Now, put $U(\mathfrak{f}) = \{x \in O^\times(k_A) | x \equiv 1 \bmod \mathfrak{f}\}$. Then $N_{K/k}(K_A^\times) \cdot k^\times = U(\mathfrak{f}) \cdot k^\times$. Let u be an element of this group such that $u^m = 1$ for $m = m(\mathfrak{g})$. Then

u belongs to $O^\times(k_A)\cap U(\mathfrak{f})\cdot k^\times = U(\mathfrak{f})\cdot O^\times(k)$. Since $O^\times(k)$ consists of roots of 1, we easily see the condition $C_1(m(\mathfrak{g}))$ holds if the conditions (1)~(3) are satisfied. Hence we have

THEOREM 3. *Let K be a ray class field of k, and suppose that the conducor $\mathfrak{f}$ satisfies the conditions* (1)~(3). *Then there exists an abundant central extension M of K/k such that $M\cap k_{\mathrm{ab}}\cdot K = K$.*

Remark. Shirai [8] gave an M of Theorem 3 more explicitly in the case that $k = \boldsymbol{Q}$ and $\mathfrak{f} = \mathfrak{f}_0\cdot\mathfrak{p}_\infty$ unless $(\mathfrak{f}_0, 16) = 8$. Note that, if $k = \boldsymbol{Q}$, the condition (1) is automatically satisfied by any *conductor* $\mathfrak{f}$. Furthermore we have $\boldsymbol{Q}^\times\cap\boldsymbol{Q}_A^{\times m} = \boldsymbol{Q}^{\times m}$ for every m.

5. The case of ray class fields, I

If $\mathrm{Gal}(K/k)$ is a nilpotent group, $\mathrm{Gal}(L/k)$ is also nilpotent for any central extension L of K/k. Therefore it is essential to study the case of p-extensions for a prime p as far as K/k is nilpotent at most.

In this section and in the next, we consider the maximal p-extension K of k contained in a ray class field of k. Let $\mathfrak{f}$ be the conductor of K/k. Then K is also the maximal p-extension contained in the ray class field modulo $\mathfrak{f}$ of k.

For a positive integer q, let ζ_q be a primitive q-th root of 1. We define an integer $i = i(\mathfrak{p}) \geq 0$ for a prime divisor $\mathfrak{p}$ of k by the condition that $\zeta_{p^i}\in k_\mathfrak{p}$ and $\zeta_{p^{i+1}}\notin k_\mathfrak{p}$. For a prime divisor $\mathfrak{p}$ of p, let $\ell = \ell(\mathfrak{p})$ be the minimal positive integer among those for which $\zeta_p \not\equiv 1 \bmod \mathfrak{p}^\ell$ if $i(\mathfrak{p}) > 0$, and put $\ell(\mathfrak{p}) = 1$ if $i(\mathfrak{p}) = 0$. Then $\ell = \ell(\mathfrak{p})$ is the minimal positive integer such that $1 + \mathfrak{p}^\ell\cdot O(k_\mathfrak{p})$ does not contain any p-power root of 1 except 1 itself.

Let $\varepsilon_0, \varepsilon_1, \cdots, \varepsilon_r$ be a set cf generators of $O^\times(k)$ such that $\langle\varepsilon_0\rangle$ is finite, and that $\varepsilon_1, \cdots, \varepsilon_r$ are $\boldsymbol{Z}$-free.

THEOREM 4. *Suppose that $\mathfrak{p}^{\ell(\mathfrak{p})}|\mathfrak{f}$ for each prime divisor $\mathfrak{p}$ of $(p, \mathfrak{f})$. If there is a positive integer m such that $(m, p) = 1$ and $\varepsilon_i^m \equiv 1 \bmod \mathfrak{f}$ $(i = 1, \cdots, r)$, then there exists an abundant central extension M satisfying $M\cap k_{\mathrm{ab}}\cdot K = K$.*

Proof. It is sufficient to show that the condition $C_1(m(\mathfrak{g}))$ is satisfied. Put $q = m(\mathfrak{g})$ and $U(\mathfrak{f}) = \{x\in O^\times(k_A)\,|\,x\equiv 1 \bmod \mathfrak{f}\}$. Then the order of $N_{K/k}(K_A^\times)\cdot k^\times/U(\mathfrak{f})\cdot k^\times$ is relatively prime to p. Therefore an element u of

$N_{K/k}(K_A^\times)\cdot k^\times$ belongs to $U(\mathfrak{f})\cdot k^\times$ if $u^q = 1$. Then $u \in U(\mathfrak{f})\cdot O^\times(k) = U(\mathfrak{f})\cdot k^\times \cap O^\times(k_A)$. It follows from the assumption that the exponent of the quotient group $U(\mathfrak{f})\cdot O^\times(k)/U(\mathfrak{f})\cdot\langle\varepsilon_0\rangle$ is relatively prime to p. Therefore u has to be in $U(\mathfrak{f})\cdot\langle\varepsilon_0\rangle$. Let ζ be an element of $\langle\varepsilon_0\rangle$ such that $u\zeta \in U(\mathfrak{f})$. Because $\zeta^q = (u\zeta)^q$ belongs to $U(\mathfrak{f})$, we may assume that ζ is a p-power root of 1 adjusting ζ with an element of $\langle\varepsilon_0\rangle \cap U(\mathfrak{f})$. Then by the condition on $\mathfrak{f}$, we have $\zeta^q = 1$. Therefore $(u\zeta)^q = 1$. Since $u\zeta \in U(\mathfrak{f})$, we have $(u\zeta)_\mathfrak{p} = 1$ for each $\mathfrak{p}$ dividing $\mathfrak{f}$ by the same reason. Q.E.D.

6. The case of ray class fields, II

Let K/k be same as in the previous section. In this section, we suppose that Leopoldt's conjecture on the units of k for p is valid. (See [4] for example.) Now put $\mathfrak{q} = \prod_{\mathfrak{p}|p}\mathfrak{p}$, and

$$U(\mathfrak{q}) = \{x \in O^\times(k_A) \mid x \equiv 1 \mod \mathfrak{q}\}.$$

By Leopoldt's conjecture for p, we show

PROPOSITION 9. *For each $q = p^t$ $(t \geq 1)$, there exists a positive integer κ such that*

$$O^\times(k) \cap U(\mathfrak{q}^\kappa) \subset (O^\times(k) \cap U(\mathfrak{q}))^q.$$

Proof. Let $\ell = \max\{\ell(\mathfrak{p}) \mid \mathfrak{p}|p\}$, and put $E = O^\times(k) \cap U(\mathfrak{q}^\ell)$. Then E is a free Z-module. Let $e_1, \cdots, e_r$ be a set of generators of E over Z ($r = \operatorname{rank} E$). We imbed E into $\prod_{\mathfrak{p}|p}(1 + \mathfrak{p}\cdot O(k_\mathfrak{p}))$ diagonally, and take the closure $\bar{E}$ of E. Then the ring of p-adic integers Z_p naturally acts on $\bar{E}$ as powers. It follows, furthermore, from Leopoldt's conjecture that $\bar{E}$ is a free Z_p-module of rank r. In other words, the elements $e_1, \cdots, e_r$ of E are free over Z_p in $\bar{E}$ and generate $\bar{E}$ over Z_p. (See [4] for example.)

Now, assume that there exists $q = p^t$ such that $O^\times(k) \cap U(q^\kappa)$ is not contained in $(O^\times(k) \cap U(\mathfrak{q}))^q$ for any positive integer κ. For each $n = 1, 2, 3, \cdots$, take $x_n \in O^\times(k) \cap U(\mathfrak{q}^{\ell+n}) - (O^\times(k) \cap U(\mathfrak{q}))^q$. Then in $\bar{E}$, $\{x_n\}_{n=1}^{+\infty}$ converges to 1. Each x_n determines an element $\nu_n = (i_1(n), \cdots, i_r(n))$ in $Z\times\cdots\times Z$ (r copies) by $x_n = \prod_{\mu=1}^r e_\mu^{i_\mu(n)}$. Because $x_n \notin E^q$, we have $\nu_n \not\equiv (0, \cdots, 0) \mod q\cdot Z$. Since $Z_p\times\cdots\times Z_p$ (r copies) is compact, we may assume that $\{\nu_n\}_{n=1}^{+\infty}$ converges to an element $\nu = (i_1, \cdots, i_r)$ in $Z_p\times\cdots\times Z_p$, replacing $\{\nu_n\}$ by a suitable subsequence if necessary. This ν is not equal to $(0, \cdots, 0)$ because $\nu_n \not\equiv (0, \cdots, 0) \mod q\cdot Z$. But we have $\prod_{\mu=1}^r e_\mu^{i_\mu} = \lim x_n = 1$. This contradicts the fact that $e_1, \cdots, e_r$ are free over Z_p. Hence the proposition is proved.

Remark. Leopoldt's conjecture for p is actually equivalent to Proposition 9.

By Proposition 9, we define $\kappa(q)$ for each $q = p^t$ as the minimal κ that satisfies the condition of the proposition for q.

Now, decompose the conductor $\mathfrak{f}$ in such way as, $\mathfrak{f} = \mathfrak{f}' \cdot \mathfrak{f}_p$, $(\mathfrak{f}', p) = 1$ and $\mathfrak{f}_p = \prod_{\mathfrak{p}|p} \mathfrak{p}^{c(\mathfrak{p})}$, and define $q = q(\mathfrak{f}', p)$ to be the minimum such that

$$\begin{cases} q \geq p^{i(\mathfrak{p})} & \text{for every, } \mathfrak{p}|\mathfrak{f}', \\ (1 + \mathfrak{p} \cdot O(k_\mathfrak{p}))^q \subset 1 + \mathfrak{p}^{\ell(\mathfrak{p})} \cdot O(k_\mathfrak{p}) & \text{for every } \mathfrak{p}|\mathfrak{f}_p. \end{cases}$$

THEOREM 5. *If* $c(\mathfrak{p}) \geq \max\{\kappa(m(\mathfrak{g})q), \ell(\mathfrak{p})\}$ *for each* $\mathfrak{p}|p$, *then there exists an abundant central extension* M *of* K/k *such that* $M \cap k_{\text{ab}} \cdot K = K$.

Proof. We show that the condition $C_1(m(\mathfrak{g}))$ holds. Put $m = m(\mathfrak{g})$. Let u be an element of $N_{K/k}(K_A^\times) \cdot k^\times$ satisfying $u^m = 1$. As in the first step of the proof of Theorem 4, we see $u \in U(\mathfrak{f}) \cdot O^\times(k)$. Let $u = v \cdot \varepsilon$ with $v \in U(\mathfrak{f})$ and $\varepsilon \in O^\times(k)$. Then $\varepsilon^m = v^{-m} \in U(\mathfrak{f})$. Therefore ε^m belongs to $U(\mathfrak{q}^{\kappa(mq)})$. Take $\alpha \in O^\times(k) \cap U(\mathfrak{q})$ so that $\varepsilon^m = \alpha^{mq}$. Then $\alpha^q = \varepsilon \cdot \zeta$ with $\zeta \in k^\times$, $\zeta^m = 1$. Therefore $u\zeta = v\varepsilon\zeta = v\alpha^q$. Now, $v \in U(\mathfrak{f})$. Therefore, for $\mathfrak{p}|\mathfrak{f}'$, we have $(u\zeta)_\mathfrak{p} \equiv (\alpha)_\mathfrak{p}^q \bmod \mathfrak{p}$, and so, $(u\zeta)_\mathfrak{p} = 1$ because $q \geq p^{i(\mathfrak{p})}$. For $\mathfrak{p}|p$, $(u\zeta)_\mathfrak{p} \equiv (\alpha)_\mathfrak{p}^q \bmod \mathfrak{p}^{\ell(\mathfrak{p})}$. By the choice of q, we have $(\alpha)_\mathfrak{p}^q \equiv 1 \bmod \mathfrak{p}^{\ell(q)}$. Then by the choice of $\ell(\mathfrak{p})$, we conclude that $(u\zeta)_\mathfrak{p} = 1$. Therefore $C_1(m)$ is certainly satisfied. The proof is completed.

7. On solutions of the number knot $\mathfrak{K}(K/k)$

An abundant central extension M of K/k is a solution of $\mathfrak{K}(K/k)$ itself. But we can always find such a subfield L of M that L is a solution of $\mathfrak{K}(K/k)$, and that $\mathrm{Gal}(L/L \cap k_{\text{ab}} \cdot K)$ is isomorphic to $\mathfrak{K}(K/k)$. Therefore, if $M \cap k_{\text{ab}} \cdot K = K$, then we have $L \cap k_{\text{ab}} \cdot K = K$, and $\mathrm{Gal}(L/K) \simeq \mathfrak{K}(K/k)$. In this section, we see sufficient conditions for such a central solution L of $\mathfrak{K}(K/k)$ to exist.

Now, let $\pi' : K_A^\times \to K_A^\times / N_{K/k}^{-1}(1) \cdot K^\#$ be the natural projection, and put

$$m'(K/k) = \text{the exponent of } \mathfrak{K}(K/k).$$

Then replacing $\pi : K_A^\times \to K_A^\times / K_A^{\Delta_\mathfrak{g}} \cdot K^\#$ by this π', and $m(\mathfrak{g})$ by $m'(K/k)$, we can prove the following theorem in the same way as we did for Theorem 1.

THEOREM 6. *Suppose that the condition* $C'(m)$ *is satisfied for every*

https://doi.org/10.1017/S0027763000020766 Published online by Cambridge University Press

$m|m'(K/k)$ by the Galois extension K/k and that $k^\times \cap k_A^{\times m'(K/k)} = k^{\times m'(K/k)}$. Then there exists a central solution L of $\mathfrak{K}(K/k)$ such that $L \cap k_{ab}\cdot K = K$ and $\mathrm{Gal}(L/K) \simeq \mathfrak{K}(K/k)$.

Here we give an application of this theorem. As before, let D be the set of prime divisors of k which ramify in K/k, and fix a prime divisor $\tilde{\mathfrak{p}}$ of $\mathfrak{p}$ in K for each $\mathfrak{p} \in D$. Let $\mathfrak{g}(\mathfrak{p})$ be the decomposition group of $\tilde{\mathfrak{p}}$, $\bar{\mathfrak{g}}(\mathfrak{p}) = \mathfrak{g}(\mathfrak{p})/[\mathfrak{g}(\mathfrak{p}), \mathfrak{g}(\mathfrak{p})]$, and $\bar{\mathfrak{t}}(\mathfrak{p})$ the inertial group of $\tilde{\mathfrak{p}}$ in $\bar{\mathfrak{g}}(\mathfrak{p})$. For a prime number p, let $\bar{\mathfrak{t}}(\mathfrak{p})^{(p)}$ be the p-Sylow group of $\bar{\mathfrak{t}}(\mathfrak{p})$. Define a subset $\mathscr{P}'$ of $\mathscr{P}$ by

$$\mathscr{P}' = \{p \in \mathscr{P} \mid p \,|\, |\bar{\mathfrak{t}}(\mathfrak{p})| \text{ for some } \mathfrak{p} \in D\},$$

and positive integers $e(p)$ and $e'(p)$ for $p \in \mathscr{P}'$ and $\nu(K/k)$ by

$$\begin{aligned} p^{e(p)} &= \text{the } p\text{-factor of } m'(K/k), \text{ i.e. } p^{e(p)} \| m'(K/k), \\ p^{e'(p)} &= \max\{\text{the exponent of } \bar{\mathfrak{t}}(\mathfrak{p})^{(p)} \mid \mathfrak{p} \in D\}, \\ \nu(K/k) &= \prod_{p \in \mathscr{P}'} p^{e(p)+e'(p)}. \end{aligned}$$

PROPOSITION 10. $\nu(K/k) \,|\, |\mathfrak{g}| = [K:k]$.

Proof. It is obvious that $\nu(K/k)$ divides $\exp(\mathfrak{g})\cdot\exp(\mathfrak{S}(K/k))$. Since $\exp(\mathfrak{S}(K/k)) = \exp(H^2(\mathfrak{g}, \boldsymbol{Q}/\boldsymbol{Z}))$, we have the proposition by Huppert [2, Ch. V, The proof of 24.5, pp. 640–641] at once.

Remark. If $\mathfrak{g}$ is abelian, then

$$\mathscr{P} = \{p \mid \text{prime; } \mathfrak{g}^{(p)} \text{ is not cyclic}\}.$$

If $\mathfrak{g}^{(p)}$ is not cyclic, $\exp(\mathfrak{g}^{(p)})\cdot\exp(H^2(\mathfrak{g}^{(p)}, \boldsymbol{Q}/\boldsymbol{Z})) \| \, |\mathfrak{g}|$ if and only if $\mathfrak{g}^{(p)}$ is a direct product of two cyclic groups.

THEOREM 7. *If k contains a primitive $\nu(K/k)$-th root of* 1, *then $C'(m)$ holds for every $m|m'(K/k)$. Therefore there exists a central solution L of $\mathfrak{K}(K/k)$ such that $L \cap k_{ab}\cdot K = K$ and* $\mathrm{Gal}(L/K) \simeq \mathfrak{K}(K/k)$.

Proof. If $2^3|m'(K/k)$, then $\sqrt{-1}$ is contained in k. Therefore we have $k^\times \cap k_A^{\times m'(K/k)} = k^{\times m'(K/k)}$ in any case.

For a prime divisor $\mathfrak{p}$, let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}$ in K. Let F be the maximal abelian extension of $k_\mathfrak{p}$ in $K_\mathfrak{P}$, and $N_F: F^\times \to k_\mathfrak{p}^\times$ the norm map. Then $N_\mathfrak{P}(K_\mathfrak{P}^\times) \cap O^\times(k_\mathfrak{p}) = N_F(O^\times(F))$. Furthermore, the quotient group $O^\times(k_\mathfrak{p})/N_F(O^\times(F))$ is isomorphic to $\bar{\mathfrak{t}}(\mathfrak{p})$. Therefore, if p is not in $\mathscr{P}'$, then every p-power root of 1 in $k_\mathfrak{p}$ is contained in $N_F(O^\times(F))$, and so in $N_\mathfrak{P}(K_\mathfrak{P}^\times)$.

Let p belong to $\mathscr{P}'$. By the assumption, we see that a primitive $p^{e(p)+e'(p)}$-th root ζ of 1 belongs to $k_{\mathfrak{p}}$. Since the exponent of $O^{\times}(k_{\mathfrak{p}})/N_F(O^{\times}(F))$ is at most $p^{e'(p)}$, the primitive $p^{e(p)}$-th root $\zeta^{p^{e'(p)}}$ of 1 has to be in $N_F(O^{\times}(F))$, and so, in $N_{\mathfrak{P}}(K_{\mathfrak{P}}^{\times})$. Thus we have seen that the condition $C_1'(m'(K/k))$ holds. Therefore $C'(m)$ is certainly satisfied for every $m|m'(K/k)$. The proof is completed.

Remark. Opolka [6] showed the existence of a central solution L of $\mathfrak{R}(K/k)$ satisfying that $L \cap k_{\mathrm{ab}}\cdot K = K$ and $\mathrm{Gal}(L/K) \simeq \mathfrak{R}(K/k)$ in the case that k contains a primitive $[K:k]$-th root of 1.

8. An upper bound for the degree of a small abundant central extension

Put $n = [K:k]$ and let d be the minimal number of generators of $\mathfrak{S}(K/k)$. In this section, we give a positive number $\lambda = \lambda(K/k)$ for the Galois extension K/k such that there exists an abundant central extension M of K/k whose Galois group $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of $(Z/2\lambda nZ)\times\cdots\times(Z/2\lambda nZ)$ (d copies).

PROPOSITION 11. $\pi(K_A^{\times})^n \subset \pi(N_{K/k}(K_A^{\times}))$.

The proposition is clear because we have, for $x \in K_A^{\times}$,

$$x^n = N_{K/k}(x)\cdot\prod_{\sigma\in\mathfrak{g}} x^{1-\sigma} \in N_{K/k}(K_A^{\times})\cdot K_A^{\Delta_{\mathfrak{g}}}.$$

PROPOSITION 12. $[\pi(N_{K/k}(K_A^{\times})\cdot N_{K/k}^{-1}(1)) \cap \pi(N_{K/k}^{-1}(k^{\#})) : \pi(N_{K/k}^{-1}(1))] \leq 2$.

Proof. Let x be an element of $N_{K/k}^{-1}(k^{\#})$, and suppose that $x = y\cdot z$ with $y \in N_{K/k}(K_A^{\times})$ and $z \in N_{K/k}^{-1}(1)$. Then $y^n = N_{K/k}(y) = N_{K/k}(x) \in k^{\#} = k^{\times}\cdot k^{\#n}$. Take $a \in k^{\times}$ and $b \in k^{\#}$ so that $y^n = ab^n$. As is well known (cf. Artin-Tate [1], Ch. 10, § 1), we have $[k^{\times} \cap k_A^{\times n} : k^{\times n}] \leq 2$. If we can choose b to have $a = 1$, then $y = ub$, $u \in k_A^{\times}$, $u^n = 1$. Since $u^n = N_{K/k}(u)$, we have $x = yz = (uz)\cdot b$ with $uz \in N_{K/k}^{-1}(1)$ and $b \in k^{\#} \subset K^{\#}$. Therefore $\pi(x) \in \pi(N_{K/k}^{-1}(1))$ in this case. Suppose now that there exists an x_0 such that a_0 corresponding to it does not belong to $k^{\times n}$. Then $[k^{\times} \cap k_A^{\times n} : k^{\times n}] = 2$. Therefore, for each x, we can choose b so that a is either a_0 or 1. Then according to the cases, either $\pi(xx_0)$ belongs to $\pi(N_{K/k}^{-1}(1))$ or $\pi(x)$ does. The proposition is now clear.

Remark. If $[k^{\times} \cap k_A^{\times n} : k^{\times n}] = 1$, then the index of the proposition is also equal to 1.

https://doi.org/10.1017/S0027763000020766 Published online by Cambridge University Press

LEMMA 3. *For a positive integer m, we have*

$$\pi(N_{K/k}(K_A^\times))^{2m} \cap \pi(N_{K/k}^{-1}(k^\sharp)) \subset \pi(\{u \in (N_{K/k}(K_A^\times)^2 \cdot k^\times)^m \mid u^n = 1\}).$$

Proof. Let x be an element of $N_{K/k}(K_A^\times)$, and suppose $x^{2m} \in N_{K/k}^{-1}(k^\sharp)$. Then $N_{K/k}(x^{2m}) = x^{2mn} \in k^\sharp = k^\times \cdot k^{\sharp 2mn}$. Because $k^\times \cap k_A^{\times 2mn} \subset k^{\times mn}$ (cf. Artin-Tate [1], Ch. 10), we have an element a of $k^\sharp$ such that $x^{2mn} = a^{mn}$. Put $u = (x^2 \cdot a^{-1})^m$. Then $u \in (N_{K/k}(K_A^\times)^2 \cdot k^\sharp)^m$ and $u^n = 1$. Since $k^\sharp = k^\times \cdot k^{\sharp 2n} = k^\times \cdot N_{K/k}(k^\sharp)^2$, $\pi(x)^{2m} = \pi(u)$ belongs to the set at the right hand side of the lemma. Q.E.D.

LEMMA 4. *For a positive integer m, we have*

$$\pi(\{u \in (N_{K/k}(K_A^\times)^2 \cdot k^\times)^m \mid u^n = 1\}) \subset \pi(\prod_{\mathfrak{p} \in D} \{u \in k_\mathfrak{p}^{\times m} \mid u^{n(\mathfrak{p})} = 1\}),$$

where D is the set of prime divisors of k which ramify in K/k, and $n(\mathfrak{p}) = [K_\mathfrak{P} : k_\mathfrak{p}]$.

Proof. For $u \in k_A^\times$, we have $N_{K/k}(u) = u^n$. Therefore

$$\{u \in k_A^{\times m} \mid u^n = 1\} = k_A^{\times m} \cap N_{K/k}^{-1}(1).$$

It is easy to see, by Propositions 4 and 5,

$$N_{K/k}^{-1}(1) \cap k_A^{\times m} \subset K_A^{\Delta\mathfrak{g}} \cdot \prod_{\mathfrak{p} \in D} \{u \in k_\mathfrak{p}^{\times m} \mid u^{n(\mathfrak{p})} = 1\}.$$

Because $\pi(K_A^{\Delta\mathfrak{g}}) = 1$, we have shown the lemma.

Remark. Throughout this paper, we consider $k_A^\times$ a subset of $K_A^\times$ by the natural imbedding. But each factor $\{u \in k_\mathfrak{p}^{\times m} \mid u^{n(\mathfrak{p})} = 1\}$ for $\mathfrak{p} \in D$ in this lemma is a subset of the $\mathfrak{P}$-component $K_\mathfrak{P}^\times$ of $K_A^\times$, and is equal to $k_\mathfrak{p}^{\times m} \cap N_\mathfrak{P}^{-1}(1)$.

Now, for $\mathfrak{p} \in D$, let $\mathfrak{g}(\mathfrak{p}) = \mathrm{Gal}(K_\mathfrak{P} \cap k_{\mathfrak{p},\mathrm{ab}}/k_\mathfrak{p})$, and $\mathfrak{g}(\mathfrak{p})^{(p)}$ be the p-Sylow group of $\mathfrak{g}(\mathfrak{p})$. Put

$$\mathscr{P}_1 = \{p \mid \text{prime},\ p \mid |\mathfrak{g}(\mathfrak{p})| \text{ for some } \mathfrak{p} \in D\},$$

and determine $i = i(p, \mathfrak{p})$ by the condition that $\zeta_{p^i} \in k_\mathfrak{p}$ and $\zeta_{p^{i+1}} \notin k_\mathfrak{p}$, and $j = j(p, \mathfrak{p})$ so that p^j is the exponent of $\mathfrak{g}(\mathfrak{p})^{(p)}$. Put

$$\mu(p) = \mu_{K/k}(p) = \max(\{0\} \cup \{i(p, \mathfrak{p}) - j(p, \mathfrak{p}) \mid \mathfrak{p} \in D\}),$$
$$\lambda = \lambda(K/k) = \prod_{p \in \mathscr{P}_1} p^{\mu(p)}.$$

LEMMA 5. $\{u \in k_\mathfrak{p}^{\times \lambda} \mid u^{n(\mathfrak{p})} = 1\} \subset K_\mathfrak{P}^{\Delta\mathfrak{g}(\mathfrak{p})}$ *for each* $\mathfrak{p} \in D$.

Proof. Let u be an element of $k_{\mathfrak{p}}^{\times\lambda}$ such that $u^{n(\mathfrak{p})}=1$. Take $v \in k_{\mathfrak{p}}^{\times}$ satisfying $v^{\lambda}=u$. Then v is a root of 1 in $k_{\mathfrak{p}}$. By the choice of $j(p, \mathfrak{p})$, $K_{\mathfrak{P}}$ contains a cyclic extension of $k_{\mathfrak{p}}$ of degree $\prod_{p\in\mathscr{P}_1} p^{j(p,\mathfrak{p})}$. Put

$$q=\prod_{p\in\mathscr{P}_1} p^{\min(i(p,\mathfrak{p}),\, j(p,\mathfrak{p}))},$$

and let ζ be a primitive q-th root of 1. Then $\zeta\in k_{\mathfrak{p}}$. Therefore, $K_{\mathfrak{P}}$ contains a Kummer extension of $k_{\mathfrak{p}}$ of degree q. Hence we have $\zeta\in K_{\mathfrak{P}}^{\Delta\mathfrak{g}(\mathfrak{p})}$. We easily see that

$$\mu(p)+\min\{i(p, \mathfrak{p}), j(p, \mathfrak{p})\}\geq i(p, \mathfrak{p}).$$

Therefore, we have $\lambda q\geq \prod_{p\in\mathscr{P}_1} p^{i(p,\mathfrak{p})}$. Then by the choice of $i(p, \mathfrak{p})$, we see $u^q=v^{\lambda q}=1$, and $u\in\langle\zeta\rangle\subset K_{\mathfrak{P}}^{\Delta\mathfrak{g}(\mathfrak{p})}$. Q.E.D.

PROPOSITION 13. $\pi(K_A^{\times})^{2\lambda n}\cap\pi(N_{K/k}^{-1}(k^{\#}))=1$.

Proof. We have $\pi(K_A^{\times})^{2\lambda n}=(\pi(K_A^{\times})^{n})^{2\lambda}\subset\pi(N_{K/k}(K_A^{\times}))^{2\lambda}$ by Proposition 11. Then by Lemmas 3~5, we have

$$\pi(N_{K/k}(K_A^{\times}))^{2\lambda}\cap\pi(N_{K/k}^{-1}(k^{\#}))=1.$$

Therefore $\pi(K_A^{\times})^{2\lambda n}\cap\pi(N_{K/k}^{-1}(k^{\#}))=1$. Q.E.D.

THEOREM 8. *Let d and $\lambda=\lambda(K/k)$ be as above. Then there exists an abundant central extension M of K/k such that* Gal(M/K) *is isomorphic to a subgroup of the direct product of d copies of $Z/2\lambda nZ$.*

Proof. The subgroup $\pi(K_A^{\times})^{2\lambda n}$ of $\pi(K_A^{\times})$ is compact and closed. Therefore we easily see by Proposition 13 that there is an open subgroup U_1 of $\pi(K_A^{\times})$ such that $U_1\supset\pi(K_A^{\times})^{2\lambda n}$ and $U_1\cap\pi(N_{K/k}^{-1}(k^{\#}))=1$. Then by the fundamental theorem of finite abelian groups applied to $\pi(K_A^{\times})/U_1$ and its subgroup $\pi(N_{K/k}^{-1}(k^{\#}))\cdot U_1/U_1$, we can find an open subgroup U of $\pi(K_A^{\times})$ such that $U\supset U_1$, $U\cap\pi(N_{K/k}^{-1}(k^{\#}))=1$ and $\pi(K_A^{\times})/U$ is generated by d elements. Since U contains $\pi(K_A^{\times})^{2\lambda n}$, $\pi(K_A^{\times})/U$ is certainly isomorphic to a subgroup of $(Z/2\lambda nZ)\times\cdots\times(Z/2\lambda nZ)$ (d copies). Let M be the abelian extension of K corresponding to the open subgroup $\pi^{-1}(U)$ of $K_A^{\times}$. Then it is obvious that this M is a desired one.

Using Proposition 12 and Lemma 3 for $m=1$, we can prove the following theorem by the same way as in the proof of Theorem 8.

THEOREM 9. *Let d_1 be the minimal number of generators of $\mathfrak{K}(K/k)$. Then there exists a central solution L of $\mathfrak{K}(K/k)$ such that* Gal$(L/L\cap k_{\mathrm{ab}}\cdot K)$

https://doi.org/10.1017/S0027763000020766 Published online by Cambridge University Press

$\simeq \mathfrak{K}(K/k)$ *and* Gal(L/K) *is isomorphic to a subgroup of the direct product of* d_1 *copies of* $Z/2nZ$.

It is also obvious that we can show the following result of Opolka [7] by the same way using Proposition 12 on account of Remark just after the proposition.

THEOREM (Opolka). *Suppose that the index* $[k^\times \cap k_A^{\times n} : k^{\times n}]$ *is equal to* 1. *Then there exists a central solution* L *of* $\mathfrak{K}(K/k)$ *such that* Gal(L/K) *is isomorphic to a subgroup of the direct product of* d_1 *copies of* Z/nZ.

REFERENCES

[1] E. Artin and J. Tate, Class field theory, W. A. Benjamin, Inc., New York·Amsterdam, 1967.
[2] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin·Heidelberg·New York, 1967.
[3] K. Miyake, On the structure of the idele group of an algebraic number field, Nagoya Math. J., **80** (1980), 117–127.
[4] ——, On the units of an algebraic number field, J. Math. Soc. Japan, **34** (1982), 515–525.
[5] ——, Central extensions and Schur's multiplicators of Galois groups, Nagoya Math. J., **90** (1983), 137–144.
[6] H. Opolka, Zur Auflösung zahlentheoretischer Knoten, Math. Z., **173** (1980), 95–103.
[7] ——, Some remarks on the Hasse norm theorem, Proc. Amer. Math. Soc., **84** (1982), 464–466.
[8] S. Shirai, On the central class field mod $\mathfrak{m}$ of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.

Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464
Japan

https://doi.org/10.1017/S0027763000020766 Published online by Cambridge University Press