Tôhoku Math. Journ.
34 (1982), 311-317.

GALOIS GROUPS OF UNRAMIFIED SOLVABLE EXTENSIONS

KÔJI UCHIDA

(Received September 17, 1981)

Let $\boldsymbol{Q}$ and $\boldsymbol{Z}$ be the rational numbers and the rational integers, respectively. Let m be a positive integer. Let q be a prime number such that $q \equiv 1(\mathrm{mod}\, m)$. Let ζ_q be a primitive q-th root of unity. Then there exists an element η_q in $\boldsymbol{Q}(\zeta_q)$ such that $[\boldsymbol{Q}(\zeta_q): \boldsymbol{Q}(\eta_q)] = m$. Let $\boldsymbol{Q}^{(m)}$ be the field generated by η_q over $\boldsymbol{Q}$ for all prime numbers q such that $q \equiv 1(\mathrm{mod}\, m)$. Then $\boldsymbol{Q}^{(m)}$ depends only on m. We are interested in the structure of the Galois groups of maximal unramified (solvable) extensions of algebraic number fields containing $\boldsymbol{Q}^{(m)}$ for some integer m. "Unramified" means every finite or infinite prime is unramified. We will see below that cohomological dimensions of such Galois groups are at most one. We will also see the Galois groups of maximal unramified solvable extensions are free pro-solvable groups under some additional condition on the ground fields. We see p-extensions given by Reichardt and Shafarevich are unramified over $\boldsymbol{Q}^{(m)}$, and their methods are essential in the following.

LEMMA 1. *Let l be a prime number and let $\boldsymbol{Q}_l$ be the l-adic number field. Then $\boldsymbol{Q}_l^{(m)} = \boldsymbol{Q}^{(m)} \cdot \boldsymbol{Q}_l$ contains the maximal unramified extension of $\boldsymbol{Q}_l$.*

PROOF. Let p be any prime number and p^d be any power of p. It suffices to show that $\boldsymbol{Q}_l^{(m)}$ contains an unramified extension of $\boldsymbol{Q}_l$ whose degree is a multiple of p^d. We can assume d is sufficiently large. It is easily seen that any common factor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$ and $l^{mp^{d-1}} - 1$ is a power of p. Hence any prime factor of m except possibly p is not a factor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$ for sufficiently large d. If $d \geqq 2$ and if p is a factor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$, it must be $l^m \equiv 1(\mathrm{mod}\, p)$ and $l^{mp^{d-1}} - 1 = p^s a$, $(a, p) = 1$ for $s \geqq 2$. Then it is easy to see that $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$ is not divisible by p^2. Let $\Psi(X)$ be the defining polynomial of the primitive mp-th roots of unity over $\boldsymbol{Q}$. Then $\Phi(X) = \Psi(X^{p^{d-1}})$ is the defining polynomial of the primitive mp^d-th roots of unity. This shows $|\Phi(l)|$ is arbitrarily large for sufficiently large d. As $\Phi(l)$ is a divisor of $(l^{mp^d} - 1)/(l^{mp^{d-1}} - 1)$, $\Phi(l)$ has a prime factor q which is not a divisor of mpl. Then $\Phi(l) = \prod_\zeta (l - \zeta)$ shows (q) splits com-

pletely in $\boldsymbol{Q}(\zeta)$ where ζ is a primitive mp^d-th root of unity, i.e., $q \equiv 1 (\mathrm{mod}\, mp^d)$, and l has the order $mp^d \bmod q$. This shows $\boldsymbol{Q}_l(\zeta_q)$ is an unramified extension of degree mp^d over $\boldsymbol{Q}_l$. Then $\boldsymbol{Q}_l(\eta_q)$, which is a subfield of $\boldsymbol{Q}_l^{(m)}$, has the degree multiple of p^d.

Let K be an algebraic number field and let F be a finite p-extension of K for some prime number p. Let ζ_p be a primitive p-th root of unity. Let $K_1 = K(\zeta_p)$, $F_1 = F(\zeta_p)$ and $n = [F_1 : F]$. Then F_1 is a Galois extension of K whose Galois group is the direct product of $G(F_1/K_1) \simeq G(F/K)$ and $G(F_1/F) \simeq G(K_1/K)$. We fix a generator ρ of $G(F_1/F)$ and determine a rational integer r by $\zeta_p^\rho = \zeta_p^r$. We can choose r such that $r^n - 1 = ps$, $(p, s) = 1$. We define

$$T = \rho^{n-1} + r\rho^{n-2} + \cdots + r^{n-1}$$

in the integral group ring $\boldsymbol{Z}[G(F_1/F)]$. When $F_1 = F$, T is the identity. In general $(r - \rho)T = r^n - 1 = ps$.

LEMMA 2 [2]. *Let $\mu_1 \in F_1^\times$ be such that $\mu_1^{\sigma-1} = \lambda_\sigma^p$, $\lambda_\sigma \in F_1^\times$, for any $\sigma \in G(F_1/K_1)$. Then there exists an element $\mu_2 \in F_1^\times$ such that $\mu_2^{\sigma-1} = \lambda_\sigma^p$ for every σ, $\mu_2^{r-\rho} \in F_1^{\times p}$ and $\mu_2 = \nu^T \xi^p$ for some $\nu, \xi \in F_1^\times$.*

PROOF. As ρ commutes with σ and as $\alpha_{\sigma,\tau} = \lambda_\tau^\sigma \lambda_{\sigma\tau}^{-1} \lambda_\sigma$ is a p-th root of unity, $\{\lambda_\sigma^{r-\rho}\}$ is a 1-cocycle. Then there exists $\omega \in F_1^\times$ such that $\omega^{\sigma-1} = \lambda_\sigma^{r-\rho}$ for every σ. Hence

$$(\omega^T)^{\sigma-1} = \lambda_\sigma^{(r-\rho)T} = \lambda_\sigma^{ps} = \mu_1^{s(\sigma-1)}$$

for every σ, i.e., $a = \omega^T \mu_1^{-s} \in K_1^\times$. As $(p, s) = 1$, we can find integers t and u such that $st + pu = 1$. Let

$$\mu_2 = \mu_1 a^t = \mu_1^{st+pu} \omega^{Tt} \mu_1^{-st} = (\omega^t)^T (\mu_1^u)^p = \nu^T \xi^p .$$

Then $\mu_2^{\sigma-1} = \mu_1^{\sigma-1} = \lambda_\sigma^p$, and

$$\mu_2^{r-\rho} = \nu^{(r-\rho)T} \xi^{p(r-\rho)} = \nu^{ps} \xi^{p(r-\rho)} \in F_1^{\times p} .$$

THEOREM 1. *Let K be an algebraic number field containing $\boldsymbol{Q}^{(m)}$ for some m. Let L be the maximal unramified extension (or the maximal unramified solvable extension) of K. Then the cohomological dimension of the Galois group $G(L/K)$ is at most 1.*

PROOF. Let p be any prime number. Let M be the maximal unramified p-extension of K. If $\mathrm{cd}\, G(M/K) \leqq 1$, the same is true over any finite extension of K. Then a Sylow p-subgroup of $G(L/K)$ has the cohomological dimension at most 1, because it is a projective limit of such groups. Hence we only need to show $\mathrm{cd}\, G(M/K) \leqq 1$. Let F be a finite Galois extension of K contained in M. Let $H = G(F/K)$ and let

$\{\alpha_{\sigma,\tau}\}$ be any cocycle class in $H^2(H, \boldsymbol{Z}/p\boldsymbol{Z})$ which does not split. Let

$$1 \to \boldsymbol{Z}/p\boldsymbol{Z} \to E \xrightarrow{\pi} H \to 1$$

be the group extension corresponding to $\{\alpha_{\sigma,\tau}\}$. It suffices to show that this imbedding problem has a solution in M. Let $K_1 = K(\zeta_p)$, $F_1 = F(\zeta_p)$ and $n = [F_1: F]$. We identify $G(F_1/K_1)$ with H. Let ρ, r and T be as above. We consider $\alpha_{\sigma,\tau}$ to be a p-th root of unity. Class field theory shows

$$H^2(H, F_1^\times) \to \prod_v H^2(H_v, F_{1,v}^\times)$$

is injective, where H_v is the decomposition subgroup for a prime v of K_1. $H_v = 1$ for every archimedean prime, because F_v/K_v is unramified. $H_v = 1$ also for every finite prime v, because K_v contains the maximal unramified extension of $\boldsymbol{Q}_v$ by Lemma 1. Hence $H^2(H, F_1^\times) = 0$. Then $\{\alpha_{\sigma,\tau}\}$ is mapped to 0 under $H^2(H, \boldsymbol{Z}/p\boldsymbol{Z}) \to H^2(H, F_1^\times)$. This shows that there exists $\{\lambda_\sigma\} \subset F_1^\times$ such that

$$\alpha_{\sigma,\tau} = \lambda_\tau^\sigma \lambda_{\sigma\tau}^{-1} \lambda_\sigma \qquad \text{for every} \quad \sigma, \tau \in H .$$

As the 1-cocycle $\{\lambda_\sigma^p\}$ splits, there exists $\mu \in F_1^\times$ such that $\mu^{\sigma-1} = \lambda_\sigma^p$ for every $\sigma \in H$. Lemma 2 shows that we can assume $\mu = \nu^T \xi^p$ for some $\nu, \xi \in F_1^\times$. Then $F_1(\sqrt[p]{\mu})$ is a Galois extension of K containing a subfield which is a solution of the above imbedding problem [2]. But this solution is not necessarily contained in M. Galois extensions of K which are solutions of the same imbedding problem can also be obtained by substituting μa^T, $a \in K_1^\times$, for μ. Hence our problem is to find $a \in K_1^\times$ such that $F_1(\sqrt[p]{\mu a^T})$ is unramified over F_1.

We can find a subfield $\mathfrak{k}$ of K of finite degree over $\boldsymbol{Q}$ satisfying the following conditions.

(i) There exists a finite Galois extension $\mathfrak{f}$ of $\mathfrak{k}$ such that $\mathfrak{f} \cap K = \mathfrak{k}$, $\mathfrak{f} \cdot K = F$, i.e., $G(\mathfrak{f}/\mathfrak{k}) \simeq H$.

(ii) $\mathfrak{f}$ is unramified over $\mathfrak{k}$, and every prime divisor of (mp) in $\mathfrak{k}$ splits completely in $\mathfrak{f}$.

(iii) Let $\mathfrak{k}_1 = \mathfrak{k}(\zeta_p)$ and $\mathfrak{f}_1 = \mathfrak{f}(\zeta_p)$. Then $[\mathfrak{k}_1: \mathfrak{k}] = [\mathfrak{f}_1: \mathfrak{f}] = n$ and $\mathfrak{f}_1$ contains all of λ_σ, μ, ν, ξ.

We note that these conditions do not change when we replace $\mathfrak{k}$ by any finite extension of $\mathfrak{k}$ contained in K. We now consider an imbedding problem of $\mathfrak{f}/\mathfrak{k}$ by the same group extension $E \xrightarrow{\pi} H$. Then $\mathfrak{f}_1(\sqrt[p]{\mu})$ contains a Galois extension of $\mathfrak{k}$ which is a solution of this imbedding problem. As $\mu^{\sigma-1}$ is a p-th power in $\mathfrak{f}_1$ for every $\sigma \in H$, and as $\mathfrak{f}_1$ is unramified over $\mathfrak{k}_1$, the principal ideal (μ) must be of the form $(\mu) =$

$\mathfrak{m}\cdot\mathfrak{a}^p$, where $\mathfrak{m}$ is an ideal of $\mathfrak{k}_1$, and $\mathfrak{a}$ is an ideal of $\mathfrak{f}_1$. As $\mu^{r-\rho}$ is a p-th power in $\mathfrak{f}_1$, $\mathfrak{m}^{r-\rho}$ is a p-th power in $\mathfrak{f}_1$. As $\mathfrak{f}_1/\mathfrak{k}_1$ is unramified, $\mathfrak{m}^{r-\rho}=\mathfrak{m}_1^p$ for some ideal $\mathfrak{m}_1$ of $\mathfrak{k}_1$. Then $\mathfrak{m}^{s(r-\rho)}=\mathfrak{m}_1^{ps}=\mathfrak{m}_1^{(r-\rho)T}$, i.e., $(\mathfrak{m}_1^T\mathfrak{m}^{-s})^{r-\rho}=1$. Since $(r-\rho)T=ps\neq 0$, $\mathfrak{m}^s=\mathfrak{m}_1^T$. This shows $(\mu)=\mathfrak{n}^T\mathfrak{a}^p$ for some ideal $\mathfrak{n}$ of $\mathfrak{k}_1$ and $\mathfrak{a}$ of $\mathfrak{f}_1$.

Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be the prime divisors of (mp) in $\mathfrak{k}_1$. As $\{\mathfrak{p}_1,\cdots,\mathfrak{p}_r\}^\rho=\{\mathfrak{p}_1,\cdots,\mathfrak{p}_r\}$ and as n is prime to p, we can find prime divisors $\mathfrak{P}_i$ of $\mathfrak{p}_i$ in $\mathfrak{f}_1$ such that $\{\mathfrak{P}_1,\cdots,\mathfrak{P}_r\}^\rho=\{\mathfrak{P}_1,\cdots,\mathfrak{P}_r\}$. As $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ split completely in $\mathfrak{f}_1$, we can find an element a in $\mathfrak{k}_1^\times$ such that ν/a is a p-th power in every completion $\mathfrak{f}_{1,\mathfrak{P}_i}$. As $(\nu/a)^\rho$ is also a p-th power by our assumption, ν^T/a^T is a p-th power in every $\mathfrak{f}_{1,\mathfrak{P}_i}$. Then

$$(\nu^T/a^T)^\sigma=\nu^{T\sigma}/a^T=\nu^{T(\sigma-1)}\cdot\nu^T/a^T=\mu^{\sigma-1}\cdot\xi^{-p(\sigma-1)}\cdot\nu^T/a^T=(\lambda_\sigma/\xi^{\sigma-1})^p\cdot\nu^T/a^T$$

is also a p-th power in every $\mathfrak{f}_{1,\mathfrak{P}_i}$ for any $\sigma\in H$. That is, ν^T/a^T is a p-th power in every $\mathfrak{f}_{1,\mathfrak{P}_i\sigma}$. Hence every prime divisor of (mp) splits completely in $\mathfrak{f}_1(\sqrt[p]{\mu/a^T})$. The same argument shows that we can also assume ν/a is positive for every real prime of $\mathfrak{f}_1$.

We now assume that every prime divisor of (mp) and every real prime is unramified in $\mathfrak{f}_1(\sqrt[p]{\mu})$ over $\mathfrak{f}_1$. Then $\mathfrak{n}$ can be chosen relatively prime to mp. We can find a finite extension $\mathfrak{k}'$ of $\mathfrak{k}$ contained in K such that

$$\left(\frac{\mathfrak{k}_1'(\zeta_{mp})/\mathfrak{k}_1'}{\mathfrak{n}}\right)=1$$

where $\mathfrak{k}_1'=\mathfrak{k}'(\zeta_p)$, because

$$\left(\frac{\mathfrak{k}_1'(\zeta_{mp})/\mathfrak{k}_1'}{\mathfrak{n}}\right)=\left(\frac{\mathfrak{k}_1(\zeta_{mp})/\mathfrak{k}_1}{\mathfrak{n}}\right)^{[\mathfrak{k}_1':\mathfrak{k}_1]}$$

and $[\mathfrak{k}_1':\mathfrak{k}_1]=[\mathfrak{k}':\mathfrak{k}]$. The density theorem shows that there exists a prime ideal $\mathfrak{q}$ of $\mathfrak{k}_1'$ unramified of degree one over $\boldsymbol{Q}$ such that $\mathfrak{q}$ and $\mathfrak{n}$ are in the same ray class mod p^2m_∞, where p^2m_∞ means the product of a divisor (p^2m) and all real primes in $\mathfrak{k}_1'$.

Then a prime divisor of $\mathfrak{q}$ is of degree one in $\mathfrak{k}_1'(\zeta_{mp})$ because $\mathfrak{q}$ splits completely in $\mathfrak{k}_1'(\zeta_{mp})/\mathfrak{k}_1'$. Let q be the prime number contained in $\mathfrak{q}$. Then $q\equiv 1(\mathrm{mod}\ mp)$ because a prime divisor of q is unramified of degree one in $\boldsymbol{Q}(\zeta_{mp})$. Then the ramification index of q in $\boldsymbol{Q}(\eta_q)$ is a multiple of p. Let $\beta\in\mathfrak{k}_1'$ be such that $(\beta)=\mathfrak{q}/\mathfrak{n}$, $\beta\equiv 1(\mathrm{mod}\ mp^2)$ and β is positive for every real prime of $\mathfrak{k}_1'$. Then only prime divisors of $\mathfrak{q}^T$ are ramified in $\mathfrak{f}_1\cdot\mathfrak{k}'(\sqrt[p]{\mu\beta^T})/\mathfrak{f}_1\cdot\mathfrak{k}'$. Let $\mathfrak{k}''=\mathfrak{k}'(\eta_q)\subset K$. Then the ramification index of every prime divisor of $\mathfrak{q}^T$ in $\mathfrak{k}_1''=\mathfrak{k}_1'(\eta_q)$ is a multiple of p over $\mathfrak{k}_1'$, because every conjugate of $\mathfrak{q}$ over $\mathfrak{k}'$ is unramified in $\mathfrak{k}_1'$. This shows $\mathfrak{f}_1\cdot\mathfrak{k}''(\sqrt[p]{\mu\beta^T})$

is unramified over $\mathfrak{f}_1 \cdot \mathfrak{k}''$. That is, $F_1(\sqrt[p]{\mu\beta^T})$ is unramified over F_1, and contains a solution of the given imbedding problem. This completes the proof of Theorem 1.

We next show that the Galois group of the maximal unramified solvable extension is free under some additional condition on K.

LEMMA 3 [1]. *Let G be a pro-solvable group with at most countable open subgroups. Then G is a free pro-solvable group with countable generators, if it satisfies the following conditions:*

(i) $\operatorname{cd} G \leqq 1$.

(ii) *Let U be any open normal subgroup and let p be any prime number. Let $H = G/U$, and let*

$$1 \to (\boldsymbol{Z}/p\boldsymbol{Z})H \to E \xrightarrow{\pi} H \to 1$$

be a split group extension with the natural action of H on the additive group of the group ring $(\boldsymbol{Z}/p\boldsymbol{Z})H$. Then there exists an open normal subgroup V of G contained in U such that $G/V \simeq E$ and the natural projection $G/V \to G/U$ coincides with π.

PROOF. In fact, [1] requires conditions (i) and

(ii)′ Let U, p and H be as above. Let

$$1 \to \sum_{i=1}^{m} (\boldsymbol{Z}/p\boldsymbol{Z})H \to E \xrightarrow{\pi} H \to 1$$

be a split group extension with the natural action of H. Then there exists an open normal subgroup V of G contained in U such that $G/V \simeq E$ and $G/V \to G/U$ coincides with π. But we get (ii)′ from (ii), because

$$1 \to (\boldsymbol{Z}/p\boldsymbol{Z})H \to E \to F \to 1$$

is a homomorphic image of

$$1 \to (\boldsymbol{Z}/p\boldsymbol{Z})F \to E' \to F \to 1\ ,$$

where F' is the extension

$$1 \to \sum_{i=1}^{m-1} (\boldsymbol{Z}/p\boldsymbol{Z})H \to F \to H \to 1\ .$$

THEOREM 2. *Let K be an algebraic number field containing $\boldsymbol{Q}^{(m)}$ for some integer m. We further assume that K contains a subfield K_0 of finite degree over $\boldsymbol{Q}$ such that K is a subfield of the maximal nilpotent extension of K_0. Let L be the maximal unramified solvable extension of K. Then the Galois group $G(L/K)$ is a free pro-solvable group with countable generators.*

PROOF. We see $G(L/K)$ has at most countable open subgroups and $\mathrm{cd}\, G(L/K) \leqq 1$ by Theorem 1. Let F be any finite Galois extension of K contained in L. Let

$$1 \to (\boldsymbol{Z}/p\boldsymbol{Z})H \to E \xrightarrow{\pi} H \to 1$$

be a split group extension of $H = G(F/K)$ as in Lemma 3. We have to show this imbedding problem has a solution in L. Let ζ_p be a primitive p-th root of unity. Let $F_1 = F(\zeta_p)$ and $n = [F_1: F]$. Let ρ be a generator of $G(F_1/F)$. Let r be an integer such that $\zeta_p^{\rho} = \zeta_p^{r}$, and let

$$T = \rho^{n-1} + r\rho^{n-2} + \cdots + r^{n-1}$$

as before. We can find a subfield $\mathfrak{k}$ of K finite over Q satisfying the following conditions.

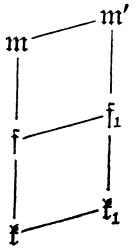
(i) There exists a finite unramified Galois extension $\mathfrak{f}$ of $\mathfrak{k}$ such that $F = \mathfrak{f}\cdot K$, $\mathfrak{f} \cap K = \mathfrak{k}$, i.e., $G(\mathfrak{f}/\mathfrak{k}) \simeq H$.

(ii) Let $\mathfrak{f}_1 = \mathfrak{f}(\zeta_p)$. Then $n = [\mathfrak{f}_1: \mathfrak{f}]$.

(iii) $\mathfrak{k}$ contains a subfield $\mathfrak{k}_0$ which is an extension of K_0 such that $\mathfrak{k}$ is a proper Galois extension of $\mathfrak{k}_0$ of degree prime to p.

We consider an imbedding problem of $\mathfrak{f}/\mathfrak{k}$ by the group extension $E \xrightarrow{\pi} H$.

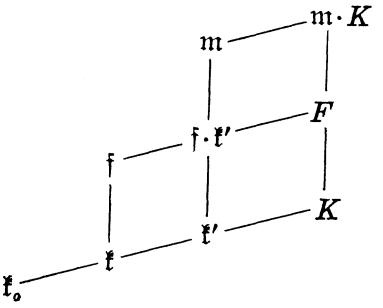
Let $\mathfrak{l}_1 = (\lambda)$ be a principal prime ideal of $\mathfrak{f}_1$ which is unramified and of degree one over $\boldsymbol{Q}$ such that $\lambda \equiv 1 (\mathrm{mod}\, p^2 m_\infty)$. Then $l = N\mathfrak{l}_1 = N\lambda$ is a prime number congruent to $1 \,\mathrm{mod}\, p^2 m$. We now consider a field $\mathfrak{m}' = \mathfrak{f}_1(\sqrt[p]{\lambda^T}, \sqrt[p]{\lambda^{T\sigma}}, \cdots, \sqrt[p]{\lambda^{T\tau}})$, where $H = \{1, \sigma, \cdots, \tau\}$. In the above, σ also means an automorphism of $\mathfrak{f}_1$ which is an extension of $\sigma \in H$. As $T\rho^i\sigma \equiv Tr^i\sigma (\mathrm{mod}\, p)$ for any other extension $\rho^i\sigma$ of σ, $\mathfrak{f}_1(\sqrt[p]{\lambda^{T\sigma}})$ does not depend on the choice of the extension. Then $\mathfrak{m}'$ is a Galois extension of $\mathfrak{k}$, and is an abelian extension of $\mathfrak{f}$. Let $\mathfrak{m}$ be the maximal p-extension of $\mathfrak{f}$ contained in $\mathfrak{m}'$. Then $\mathfrak{m}$ is a Galois extension of $\mathfrak{k}$.



Let $\mathfrak{l} = \mathfrak{l}_1 \cap \mathfrak{k}$. As $\mathfrak{l}$ splits completely in $\mathfrak{f}_1$, (λ^T), $(\lambda^{T\sigma})$, $\cdots$, $(\lambda^{T\tau})$ are relatively prime to one another. Hence $\mathfrak{m}$ is a solution of the imbedding

problem. Every prime ideal which is ramified in $\mathfrak{m}/\mathfrak{f}$ is a prime divisor of $\mathfrak{l}$. The ramification index in $\mathfrak{f}(\eta_l)/\mathfrak{f}$ of any prime divisor of $\mathfrak{l}$ is a multiple of p because $l \equiv 1 (\mathrm{mod}\, p^2 m)$. Then $\mathfrak{m}(\eta_l)$ is unramified over $\mathfrak{f}(\eta_l)$. That is, $\mathfrak{m} \cdot K$ is unramified over K.

We assume $\mathfrak{m} \cap K \neq \mathfrak{k}$. Then $[\mathfrak{m} \cap K : \mathfrak{k}]$ is a power of p because $\mathfrak{f} \cap K = \mathfrak{k}$. Then $\mathfrak{m} \cap K$ contains a Galois extension $\mathfrak{k}'$ of $\mathfrak{k}$ of degree p because $\mathfrak{m} \cap K$ is contained in a nilpotent extension. As $[\mathfrak{k} : \mathfrak{k}_0]$ is relatively prime to p, and as $\mathfrak{k}'$ is contained in a nilpotent extension of $\mathfrak{k}_0$, $\mathfrak{k}'$ must be a Galois extension of $\mathfrak{k}_0$.



Let $\mathfrak{l}_0$ be the restriction of $\mathfrak{l}$ to $\mathfrak{k}_0$. As $\mathfrak{l}_0$ splits completely in $\mathfrak{k}$, there exists a prime ideal $\mathfrak{l}'$ different from $\mathfrak{l}$ which is conjugate to $\mathfrak{l}$ over $\mathfrak{k}_0$. As $\mathfrak{m}$ does not contain an unramified extension of $\mathfrak{f}$, $\mathfrak{l}$ must be ramified in $\mathfrak{k}'$. But this is a contradiction, as $\mathfrak{l}'$ is unramified in $\mathfrak{k}'$, and as $\mathfrak{l}$ and $\mathfrak{l}'$ must have the same ramification index in the Galois extension $\mathfrak{k}'/\mathfrak{k}_0$. This shows $\mathfrak{m} \cap K = \mathfrak{k}$. Then $\mathfrak{m} \cdot K$ is a subfield of L which is a solution of our imbedding problem.

REFERENCES

[1] K. IWASAWA, On solvable extensions of algebraic number fields, Ann. of Math. 58 (1953), 548-572.

[2] H. REICHARDT, Konstrunktion von Zahlkörpern mit gegebener Galois-gruppe von Primzahlpotenzordnung, J. für Math. 177 (1937), 1-5.

[3] I. R. SHAFAREVICH, On the construction of fields with given Galois group of order l^a, Izv. Akad. Nauk SSSR 18 (1954), AMS Translation 4 (1956), 107-142.

DEPARTMENT OF MATHEMATICS
COLLEGE OF GENERAL EDUCATION
TÔHOKU UNIVERSITY
SENDAI, 980
JAPAN