Y. Odai
Nagoya Math. J.
Vol. 107 (1987), 135-146

ON UNRAMIFIED CYCLIC EXTENSIONS OF DEGREE l OF ALGEBRAIC NUMBER FIELDS OF DEGREE l

YOSHITAKA ODAI

Introduction

Let l be an odd prime number and let K be an algebraic number field of degree l. Let M denote the genus field of K, i.e., the maximal extension of K which is a composite of an absolute abelian number field with K and is unramified at all the finite primes of K. In [4] Ishida has explicitly constructed M. Therefore it is of some interest to investigate unramified cyclic extensions of K of degree l, which are not contained in M. In the preceding paper [6] we have obtained some results about this problem in the case that K is a pure cubic field. The purpose of this paper is to extend those results.

Let $\boldsymbol{Q}$ denote the field of rational numbers and let $\boldsymbol{Z}$ be the ring of rational integers. Let ζ be a primitive l-th root of unity. Let $k = \boldsymbol{Q}(\zeta)$ and $L = K(\zeta)$. In Section 1 we see how an unramified cyclic extension N of K of degree l is obtained from an element α of L. Here α satisfies some conditions, one of which is that there exists an ideal $\mathfrak{A}$ of L such that $(\alpha) = \mathfrak{A}^l$. In Section 2, assuming that L is a ramified Galois extension of k, we give a criterion for N to be contained in M by means of α (see Theorem 1). In Section 3, assuming that l is regular, we define F_1 (resp. F_0) as the composite of all those N, for which $\mathfrak{A}$ are ambigious over k (resp. principal) (see Definition). Theorem 2 proves that $F_1 = F_0M$. In Section 4 F_0 is investigated and Theorem 4 gives infinitely many examples of N not contained in M.

Notations. $G = \mathrm{Gal}(L/K)$ is a cyclic group of order $l-1$. Let τ be a generator of G and let $\dot{r}$ be the element of $\boldsymbol{Z}/l\boldsymbol{Z}$ such that $\zeta^{\tau} = \zeta^{\dot{r}}$. Let $\boldsymbol{Z}/l\boldsymbol{Z}[G]$ denote the group ring of G over $\boldsymbol{Z}/l\boldsymbol{Z}$. We define

$$\dot{e}_i = -\sum_{j=0}^{l-2} \dot{r}^{-ij}\tau^j \qquad \text{for } 1 \leqq i \leqq l-1\,.$$

Received May 16, 1986.

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

Then $\dot{e}_i$ are mutually orthogonal idempotent elements of $\boldsymbol{Z}/l\boldsymbol{Z}[G]$. For a $\boldsymbol{Z}/l\boldsymbol{Z}[G]$-module A, let

$$A(i) = A^{\dot{e}_i} = \{a^{\dot{e}_i};\ a \in A\},$$

then $A(i) = \{a \in A;\ a^{\dot{e}_i} = a\} = \{a \in A;\ a^{\tau} = a^{\dot{r}^i}\}$ and $A = \prod_{i=1}^{l-1} A(i)$ (direct product). We take r (resp. e_i) as an element of $\boldsymbol{Z}$ (resp. $\boldsymbol{Z}[G]$) congruent to $\dot{r}$ (resp. $\dot{e}_i$) modulo l. For an algebraic number field F, let F^* (resp. E_F) denote its multiplicative group (resp. its unit group).

§ 1. Preliminaries

In this section, let K be an algebraic number field (not necessarily of degree l) such that $K \cap k = \boldsymbol{Q}$. The main idea of this section is due to G. Gras [1].

Let $\mathscr{K}$ be the set of all the cyclic extensions of K of degree l and let $\mathscr{L}$ be the set of all the cyclic extensions of L of degree l, which are abelian over K. We note that any element of $\mathscr{L}$ is written in the form $L(\sqrt[l]{\alpha})$, where $\alpha \in L^*$. For $1 \leqq \lambda \leqq l$, let

$$P_\lambda = \{(t_1, \cdots, t_\lambda) \in \{1, \cdots, l-1\}^\lambda;\ \textstyle\sum_{i=1}^{\lambda} r^{t_i} \equiv 0 \pmod{l}\}.$$

Let us define that $(t_1, \cdots, t_\lambda)$ and $(t'_1, \cdots, t'_\lambda)$ are equivalent if $t_1 - t'_1 \equiv \cdots \equiv t_\lambda - t'_\lambda \pmod{l-1}$ and let T_λ be a complete system of representatives of the equivalence classes. For $(t) = (t_1, \cdots, t_\lambda) \in P_\lambda$, we can take $\Gamma(t) \in \boldsymbol{Z}[G]$ such that $e_1 \cdot \sum_{i=1}^{\lambda} \tau^{t_i} = l\Gamma(t)$ since $e_1\tau \equiv e_1 r \pmod{l\boldsymbol{Z}[G]}$. Let $\mathrm{Tr}_{L/K}$ denote the trace map from L to K.

LEMMA 1. *For $L(\sqrt[l]{\alpha}) \in \mathscr{L}$, let*

$$A_\lambda = \begin{cases} 0 & \text{if } T_\lambda \text{ is empty,} \\ l\sum_{(t)\in T_\lambda} \mathrm{Tr}_{L/K}(\alpha^{\Gamma(t)}) & \text{otherwise,} \end{cases}$$

$$a_1 = -A_1, \quad a_\lambda = -\lambda^{-1}\Big(A_\lambda + \sum_{i=1}^{\lambda-1} a_i A_{\lambda-i}\Big) \quad \text{for } 2 \leqq \lambda \leqq l.$$

Let x be a root of $f(X) = X^l + \sum_{\lambda=1}^{l} a_\lambda X^{l-\lambda} = 0$. Let ρ be the mapping $L(\sqrt[l]{\alpha}) \to K(x)$. Then ρ is a bijection of $\mathscr{L}$ onto $\mathscr{K}$.

Proof. Let $N' = L(\sqrt[l]{\alpha})$. N' is a cyclic extension of K of degree $l(l-1)$. Let N be a unique subfield of N', of degree l over K. Then the mapping $N' \to N$ is clearly a bijection of $\mathscr{L}$ onto $\mathscr{K}$. Therefore it suffices to show that $N = K(x)$. The generator τ of G can be extended to be a generator of $\mathrm{Gal}(N'/N)$. Let ν be the generator of $\mathrm{Gal}(N'/L)$

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

such that ${}^l\sqrt{\alpha}^{\nu} = {}^l\sqrt{\alpha}\cdot\zeta$.

1st step. Let $y = \mathrm{Tr}_{N'/N}({}^l\sqrt{\alpha}) = \sum_{i=1}^{l-1} {}^l\sqrt{\alpha}^{\tau^i}$. Assume that $y \in K$. Then $y^{\nu^j} = y$ for $1 \leqq j \leqq l-1$, i.e.,

$$\sum_{i=1}^{l-1} \zeta^{jr^i}\cdot {}^l\sqrt{\alpha}^{\tau^i} = \sum_{i=1}^{l-1} {}^l\sqrt{\alpha}^{\tau^i} \qquad \text{for } 1 \leqq j \leqq l-1 .$$

This implies that the matrix $(\zeta^{jr^i} - 1)_{1\leqq i,j \leqq l-1}$ is not regular. It is a contradiction. Therefore $y \notin K$ and $N = K(y)$.

2nd step. We see from Kummer theory that $\alpha^{\tau-r} \in L^{*l}$, which implies that $\alpha^{e_1} \equiv \alpha \pmod{L^{*l}}$. Since $L({}^l\sqrt{\alpha^{e_1}}) = L({}^l\sqrt{\alpha})$, we have that $N = K(z)$ where $z = \mathrm{Tr}_{N'/N}({}^l\sqrt{\alpha^{e_1}})$ (cf. 1st step). Let $B_\lambda = \mathrm{Tr}_{N/K}(z^\lambda)$ for $1 \leqq \lambda \leqq l$. If $B_\lambda = A_\lambda$, we see from Newton relations for elementary symmetric forms that the minimal polynomial of z over K is $f(X)$. This implies $N = K(x)$. Therefore it suffices to show that $B_\lambda = A_\lambda$.

3rd step.

$$\begin{aligned} B_\lambda &= \sum_{j=1}^{l} \Big(\sum_{i=1}^{l-1} \zeta^{jr^i}\cdot {}^l\sqrt{\alpha^{e_1}}^{\tau^i}\Big)^\lambda \\ &= \sum_{j=1}^{l} \sum_{(t)} \zeta^{jR(t)}\cdot {}^l\sqrt{\alpha^{e_1}}^{S(t)} , \end{aligned}$$

where (t) runs over $\{1, \cdots, l-1\}^\lambda$ and $R(t) = \sum_{i=1}^{\lambda} r^{t_i}$, $S(t) = \sum_{i=1}^{\lambda} \tau^{t_i}$. As $\sum_{j=1}^{l} \zeta^{jR(t)} = l$ or 0 according as $R(t) \equiv 0 \pmod l$ or not, we have that

$$B_\lambda = \begin{cases} 0 & \text{if } P_\lambda \text{ is empty,} \\ l\sum_{(t)\in P_\lambda} {}^l\sqrt{\alpha^{e_1}}^{S(t)} = l\sum_{(t)\in T_\lambda} \mathrm{Tr}_{N'/N}({}^l\sqrt{\alpha^{e_1}}^{S(t)}) & \text{otherwise.} \end{cases}$$

It follows from $e_1S(t) = l\Gamma(t)$ that

$$({}^l\sqrt{\alpha^{e_1}}^{S(t)})^l = (\alpha^{\Gamma(t)})^l \quad \text{and} \quad ({}^l\sqrt{\alpha^{e_1}}^{S(t)})^{e_1} = (\alpha^{\Gamma(t)})^{e_1} .$$

Noting that $\zeta^{e_1} = \zeta$, we have that

$${}^l\sqrt{\alpha^{e_1}}^{S(t)} = \alpha^{\Gamma(t)} .$$

This implies $B_\lambda = A_\lambda$ and completes the proof of the lemma.

Let $\mathscr{K}^\circ$ (resp. $\mathscr{L}^\circ$) be the set of all the elements of $\mathscr{K}$ (resp. $\mathscr{L}$) which are unramified over K (resp. L).

COROLLARY. *The restriction of ρ on $\mathscr{L}^\circ$ is a bijection of $\mathscr{L}^\circ$ onto $\mathscr{K}^\circ$.*

Proof. Let $N' \in \mathscr{L}$ and $N = \rho(N') \in \mathscr{K}$. Then N'/L and N/K are cyclic extensions of degree l. As $[L:K] = l-1$, we see that N/K is unramified if and only if N'/L is unramified.

EXAMPLE. Let T denote $\mathrm{Tr}_{L/K}$.
In the case $l=3$: If we take $r=-1$ and $e_1=-1+\tau$, then

$$f(X)=X^3-3X-T(\alpha^{1-\tau}).$$

In the case $l=5$: If we take $r=2$ and $e_1=-1+2\tau+\tau^2-2\tau^3$, then

$$\begin{aligned}f(X)=X^5-10X^3-5T(\alpha^{-1+\tau^2})X^2\\ +(5-5T(\alpha^{-1-\tau+\tau^2+\tau^3}))X-T(\alpha^{-2-\tau+2\tau^2+\tau^3}).\end{aligned}$$

§ 2. Criterion to be contained in the genus field

Hereafter we assume that K is an algebraic number field of degree l such that L is a Galois extension of k. (Then L/k is a cyclic extension of degree l.) Let σ be a generator of $\mathrm{Gal}(L/k)$. Then L is a Galois extension of $\boldsymbol{Q}$, in fact, $\mathrm{Gal}(L/\boldsymbol{Q})$ is generated by σ and τ.

Let M' denote the genus field of L over k, i.e., the maximal extension of L which is a composite of an abelian extension of k with L and is unramified at all the finite primes of L.

LEMMA 2. *Let $L(\sqrt[l]{\alpha})$ and $K(x)$ be as in Lemma 1. If L is ramified over k, then we have that*

$$L(\sqrt[l]{\alpha})\subset M'\Longleftrightarrow K(x)\subset M.$$

Proof. Let $N'=L(\sqrt[l]{\alpha})$ and $N=K(x)$. Assume that $N'\subset M'$. Then, as N' is abelian over K and over k, we see that N' is a Galois extension of $\boldsymbol{Q}$. Moreover, since L is ramified over k, then $\mathrm{Gal}(N'/k)\simeq(\boldsymbol{Z}/l\boldsymbol{Z})^2$. If K is not Galois over $\boldsymbol{Q}$, then an application of Lemma 2 in [5] to $\mathrm{Gal}(N'/\boldsymbol{Q})$ proves that $N\subset M$. If K is cyclic over $\boldsymbol{Q}$, then so is L. We see from Kummer theory that N' is abelian over $\boldsymbol{Q}$, which implies that $N\subset M$. The converse is clear.

THEOREM 1. *Let K be an algebraic number field such that $K\cap k=\boldsymbol{Q}$. Let α be an element of L^* satisfying the following conditions*:

0. $\alpha\notin L^{*l}$.

I. $\alpha^{\tau-r}\in L^{*l}$.

II. (i) *There exists an ideal $\mathfrak{A}$ of L such that $(\alpha)=\mathfrak{A}^l$,*
(ii) *α is a l-th power residue modulo $(1-\zeta)^l$.*

Let x be as in Lemma 1. Then $K(x)$ is an unramified cyclic extension of K of degree l. Conversely any unramified cyclic extension of K of degree

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

l is obtained as above.

Moreover, if K is an algebraic number field of degree l such that L is a ramified Galois extension of k, we obtain that $K(x) \not\subset M$ if and only if

III. $\alpha^{\sigma-1} \notin L^{*l}$.

Proof. The first assertion follows from Lemma 1, its corollary and the ramification theory in Kummer extensions (cf. [3] Ia Satz 9). The secnod assertion follows at once from Lemma 2 and the fact that

$$L(\sqrt[l]{\alpha}) \not\subset M' \Longleftrightarrow L(\sqrt[l]{\alpha}) \text{ is not abelian over } k \Longleftrightarrow \alpha^{\sigma-1} \notin L^{*l}.$$

§ 3. The fields F_2 and F_1

In this section, let l be a regular odd prime number and let K be an algebraic number field of degree l such that L is a Galois extension of k. Then L is ramified over k.

Let $\mathscr{H} = \{c \in \text{the ideal class group of } L;\ c^l = 1\}$ and let $\mathscr{H}_0$ denote the identity subgroup $\{1\}$ of $\mathscr{H}$. Let $\mathscr{H}_2$ (resp. $\mathscr{H}_1$) denote the Sylow l-subgroup of the group of ambiguous ideal classes (resp. ideal classes represented by ambigious ideals) of L over k. As the class number of k is not divisible by l, we see easily that

$$\mathscr{H}_0 \subset \mathscr{H}_1 \subset \mathscr{H}_2 \subset \mathscr{H}.$$

So these are $Z/lZ[G]$-modules. Let N be an unramified cyclic extension of K of degree l. By Theorem 1, N is obtained from $\alpha \in L^*$ such that $(\alpha) = \mathfrak{A}^l$ where $\mathfrak{A}$ is an ideal of L. The condition I of the theorem implies that the ideal class $\mathrm{cl}(\mathfrak{A})$ represented by $\mathfrak{A}$ belongs to $\mathscr{H}(1)$. We see from Lemma 1 that $\mathrm{cl}(\mathfrak{A})$ is uniquely determined. For $i \in \{0, 1, 2\}$, we say that N is *associated with* $\mathscr{H}_i$ if $\mathrm{cl}(\mathfrak{A}) \in \mathscr{H}_i(1)$.

Definition. *For $i \in \{0, 1, 2\}$, F_i is defined as the composite of all the unramified cyclic extensions of K of degree l, which are associated with $\mathscr{H}_i$.*

Remark. We see that F_0 is the same as the composite of all the unramified cyclic extensions of K of degree l, which are obtained from the units of L.

To investigate F_i $(i = 0, 1, 2)$, we first consider the genus field M of K. Let $p_1, \cdots, p_s$ be all the rational primes congruent to 1 modulo l and totally ramified in K. Then $(p_i) = \mathfrak{p}_i^{1+\tau+\cdots+\tau^{l-2}}$ for $1 \leqq i \leqq s$, where $\mathfrak{p}_i$ are

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

prime ideals of k. Let h denote the class number of k. We write

$$\mathfrak{p}_i^h = (\pi_i) \quad \text{for } 1 \leqq i \leqq s, \text{ where } \pi_i \in k^*.$$

LEMMA 3. *Let* $U = \{\alpha \in k^*; (\alpha, 1-\zeta) = 1\}$ *and* $U' = \{\alpha \in U; \alpha \equiv 1 \pmod{(1-\zeta)^l}\}$. *Then*:

(i) *For any* $\alpha \in U$, *there exists a rational integer* m *such that* $(\alpha\zeta^m)^{e_1} \in U'U^l$.

(ii) *Let* ρ *be as in Lemma* 1 *and put* $\rho(L) = K$. *Let us take* π_i *so that* $\pi_i^{e_1} \in U'U^l$ *for* $1 \leqq i \leqq s$; *then*

$$M = \begin{cases} M_0 \cdot \rho(L(\sqrt[l]{\zeta})) & \text{if } L(\sqrt[l]{\zeta})/L \text{ is unramified,} \\ M_0 & \text{otherwise,} \end{cases}$$

where $M_0 = \prod_{i=1}^{s} \rho(L(\sqrt[l]{\pi_i^{e_1}}))$. *(If* $s = 0$, *we define* $M_0 = K$).

Proof. (i) Let $V = U/U'U^l$. V is a $Z/lZ[G]$-module. Let $\pi = 1-\zeta$; then $\{1-\pi^i\}_{1 \leqq i \leqq l-1}$ is a Z/lZ-basis of V. As $(1-\pi^i)^{e_i} \notin U'U^l$, we have that $\dim_{Z/lZ} V(i) = 1$ for $1 \leqq i \leqq l-1$. As $\zeta^{e_1} = \zeta$, $V(1)$ is generated by ζ. This completes the proof of (i).

(ii) Let $k_i = k(\sqrt[l]{\pi_i^{e_1}})$ and $L_i = L(\sqrt[l]{\pi_i^{e_1}})$. Let $F(p_i)$ (resp. $F(l^2)$) denote a unique subfield, of degree l, of the p_i-th (resp. l^2-th) cyclotomic field. As $\pi_i^{e_1} \in U'U^l$, only the prime ideals above p_i are ramified in k_i/k. As k_i is a cyclic extension of $\boldsymbol{Q}$ of degree $l(l-1)$, we see that $k_i = kF(p_i)$. Therefore $\rho(L_i) = KF(p_i)$. Similarly, if $L(\sqrt[l]{\zeta})/L$ is unramified, we see that $\rho(L(\sqrt[l]{\zeta})) = KF(l^2)$. Therefore Theorem of [4] completes the proof of (ii).

THEOREM 2. *Let* l *be a regular odd prime number and let* K *be an algebraic number field of degree* l *such that* L *is a Galois extension of* k. *Let notations be as above. Then we have that*

$$F_1 = F_0 M.$$

In particular, if $\mathscr{H}_2(1) = \mathscr{H}_1(1)$, *then*

$$F_2 = F_0 M.$$

Proof. Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_t$ be all the prime ideals of L, which are (totally) ramified over k. As $(h, l) = 1$, we have

$$\mathscr{H}_1 = \langle \mathrm{cl}(\mathfrak{P}_1^h), \cdots, \mathrm{cl}(\mathfrak{P}_t^h) \rangle .$$

We write

$$(\mathfrak{P}_i^h)^l = (\pi_i') \quad \text{for } 1 \leqq i \leqq t, \quad \text{where } \pi_i' \in k^*.$$

Let π_i $(1 \leqq i \leqq s)$ be as in Lemma 3. Then $(l-1)s \leqq t$ and we can take

$$\pi_i' = \pi_b^{\tau^a} \text{ for } i = as + b, \text{ where } a = 0, \cdots, l-2 \text{ and } b = 1, \cdots, s.$$

For $i > (l-1)s$, observing the decomposition groups of the prime ideals $\mathfrak{P}_i^l$ of k over $\boldsymbol{Q}$, we see that there exist divisers $d(i) \neq l-1$ of $l-1$ such that $\pi_i'^{\tau^{d(i)}-1} \in E_k$. To obtain F_1, we may consider only $\alpha \in L^*$ such that $(\alpha) = \mathfrak{A}^l$ and $\mathrm{cl}(\mathfrak{A}) \in \mathscr{H}_1(1)$. Then

$$\alpha \equiv \varepsilon \prod_{i=1}^{t} (\pi_i'^{e_1})^{a(i)} \pmod{L^{*l}} \text{ where } \varepsilon \in E_L \text{ and } a(i) \in \boldsymbol{Z}.$$

Here

$$\begin{cases} \pi_i'^{e_1} \equiv (\pi_b^{e_1})^{\tau^a} \pmod{L^{*l}} & \text{for } i = as + b \leqq (l-1)s\,, \\ \pi_i'^{e_1} \in E_k L^{*l} & \text{for } i > (l-1)s, \text{ because } e_1 \in (\tau^{d(i)} - 1, l)Z[G]\,. \end{cases}$$

Therefore

$$\alpha \equiv \varepsilon' \prod_{i=1}^{s} (\pi_i^{e_1})^{b(i)} \pmod{L^{*l}} \quad \text{where } \varepsilon' \in E_L \text{ and } b(i) \in \boldsymbol{Z}.$$

Then Lemma 3 proves that $F_1 = F_0 M$. It is clear that $\mathscr{H}_2(1) = \mathscr{H}_1(1) \Rightarrow F_2 = F_1$. The proof is complete.

COROLLARY. *Let notations and assumptions be as in Theorem* 2.

(i) *In the case that K is cyclic*: *Let f be the conductor of K. If $f = l^2$ or there exists a prime divisor $p \neq l$ of f such that $p \not\equiv 1 \pmod{l^2}$, then $F_2 = F_0 M$.*

(ii) *In the case that K is not cyclic*: *If K is totally real, then $F_2 = F_0 M$.*

Proof. Let N denote the norm map from L to k. Let $A = \mathscr{H}_2/\mathscr{H}_1$ and $B = (E_k \cap NL^*)/NE_L$. For $\mathrm{cl}(\mathfrak{A}) \in \mathscr{H}_2$, there exists $\alpha \in L^*$ such that $\mathfrak{A}^{\sigma-1} = (\alpha)$. Let ϕ be the mapping $\mathrm{cl}(\mathfrak{A}) \pmod{\mathscr{H}_1} \to N\alpha \pmod{NE_L}$. It is well known that ϕ is a group isomorphism of A onto B. Both A and B are $Z/lZ[G]$-modules. As k is Galois over $\boldsymbol{Q}$, we can write $\tau\sigma\tau^{-1} = \sigma^{r^x}$ where $x \in \{1, \cdots, l-1\}$. Then $A(1) \simeq B(l-x)$, because $\phi(a^\tau) = (\phi(a)^\tau)^{r^x}$ for $a \in A$. Let $B^+ = (E_{k^+} \cap NL^*)NE_L/NE_L$ and $B_W = (W_k \cap NL^*)NE_L/NE_L$, where k^+ is the maximal real subfield of k and W_k is the group of roots of unity in k. Then $B = B^+ \times B_W$ (direct product). Since the elements of E_{k^+} are invariant by $\tau^{(l-1)/2}$, we see that $B^+ = \prod_{i.\text{even}} B(i)$ (direct product)

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

and $B_W = B(1)$.

(i) $x = l - 1$. Namely $A(1) = B(1) = B_W = (W_k \cap NL^*)/(W_k \cap NE_L)$. It is clear that $\zeta \in NE_L$ if $f = l^2$. Using the properties of Hilbert norm residue symbols (cf. [3] II Section 11) in k, we see that $\zeta \notin NL^*$ if there exists a prime divisor $p \neq l$ of f such that $p \not\equiv 1 \pmod{l^2}$. Therefore $A(1) = \{1\}$.

(ii) If K is totally real, then $\sigma^{-1}\tau^{(l-1)/2}\sigma = \tau^{(l-1)/2}$, i.e., x is even. Hence $l - x$ is odd. $l - x \neq 1$ as K is not cyclic. Therefore $A(1) = B(l - x) = \{1\}$.

§ 4. The field F_0

In this section l is not necessarily regular. The definition of F_0 in Section 3 is still valid.

THEOREM 3. *Let K be a totally real algebraic number field of degree l such that L is a ramified Galois extension of k. Then*

$$F_0 \subset M.$$

Proof. Let k^+ (resp. L^+) be the maximal real subfield of k (resp. L). As $L^+ = Kk^+$, L^+ is totally real when K is totally real. Then it follows that $E_L/E_L^l \simeq (W_L E_{L^+})/(W_L E_{L^+})^l$ (as $\boldsymbol{Z}/l\boldsymbol{Z}[\mathrm{Gal}(L/\boldsymbol{Q})]$-modules) where W_L is the group of roots of unity in L (cf. Theorem 4.12 of [9]). For $\varepsilon \in E_{L^+}$, noting that ε is invariant by $\tau^{(l-1)/2}$, we have that

$$\varepsilon^{\tau - r} \in L^{*l} \Longrightarrow \varepsilon \in L^{*l} \Longrightarrow \varepsilon^{\sigma - 1} \in L^{*l}.$$

On the other hand $W_L^{\tau - r}, W_L^{\sigma - 1} \in L^{*l}$, since W_L is generared by $-\zeta$ or $-\sqrt[l]{\zeta}$. Therefore $W_L E_{L^+}$ has no elements satisfying the conditions I and III of Theorem 1, and so does E_L. The proof is complete by Remark just following Definition in Section 3.

Next we consider the case that K is not totally real.

LEMMA 4. *Let H be a cyclic group of order l and let σ be a generator of H. Let $g(\sigma)$ be the element of $\boldsymbol{Z}[H]$ such that $(1 - \sigma)^{l-1} = 1 + \sigma + \cdots + \sigma^{l-1} + lg(\sigma)$. Then $g(\sigma)$ is invertible in $\boldsymbol{Z}[H]$.*

Proof. We see that the ring homomorphism

$$\boldsymbol{Z}[H] \ni f(\sigma) \longrightarrow f(1) \times f(\zeta) \in \boldsymbol{Z} \times \boldsymbol{Z}[\zeta] \text{ (direct product)}$$

is injective, because $(X - 1) \cap (X^{l-1} + X^{l-2} + \cdots + 1) = (X^l - 1)$ in $\boldsymbol{Z}[X]$. We note that $g(1) = -1$ and $g(\zeta) = (1 - \zeta)^{l-1}/l = \prod_{i=1}^{l-1}(1 + \zeta + \cdots + \zeta^{i-1})^{-1}$.

Let $g'(\sigma) = \prod_{i=1}^{l-1}(1 + \sigma + \cdots + \sigma^{i-1}) - l^{-1}(1 + (l-1)!)(1 + \sigma + \cdots + \sigma^{l-1}) \in Z[H]$; then $g'(1) = g(1)^{-1}$ and $g'(\zeta) = g(\zeta)^{-1}$. This proves $g'(\sigma) = g(\sigma)^{-1}$.

Let K be a pure algebraic number field of degree l, i.e., $K = \boldsymbol{Q}(\sqrt[l]{m})$ where $m \neq 1$ is a l-th power-free natural number. Then it is well known that L is a ramified Galois extension of k.

THEOREM 4. *Let $K = \boldsymbol{Q}(\sqrt[l]{m})$ where $m \neq 1$ is a l-th power-free natural number written as*

$$D^l + d \text{ with } D, d \in Z,\ D > 0,\ d \mid D^l,\ d \neq \pm 1,\ l \mid D,\ l \nmid d.$$

Let σ be the generator of $\mathrm{Gal}(L/k)$ *such that $\sqrt[l]{m}^{\sigma} = \sqrt[l]{m} \cdot \zeta$. We define $\eta = (\sqrt[l]{m} - D)^{1-\sigma}$ and*

$$\varepsilon_0 = \zeta \cdot \prod_{i=1}^{l-2} \eta^{a(i)\sigma^i}$$

where $a(i)$ is a rational integer congruent to $\sum_{j=1}^{i} j^{-1}$ modulo l. Then ε_0 is a unit of L satisfying the conditions 0, I, II *and* III *of Theorem* 1. *Therefore we have*

$$F_0 \not\subset M.$$

Proof. We note that $\mathrm{Gal}(L/\boldsymbol{Q})$ is generated by σ and τ with the relations $\sigma^l = \tau^{l-1} = 1$, $\sigma\tau = \tau\sigma^r$. Let E_0 be the subgroup of E_L generated by E_k and the conjugates of E_K. Then $E_0 \supset E_L^l$ (cf. [8]). Let $\theta = (\sqrt[l]{m} - D)^l/d$, then $\theta \in E_K$ (cf. [2]). As $\eta^l = \theta^{1-\sigma}$, we have that $\eta \in E_L$ and $\varepsilon_0 \in E_L$.

1*st step*. We note that $m = d(D^l d^{-1} + 1)$ where $D^l d^{-1} \in Z$. Therefore d is l-th power-free and $(d, D^l d^{-1} + 1) = 1$. $D^l d^{-1} + 1 \neq \pm 1$ follows from $l \mid D$. We see that

$$\begin{aligned} (d, D^l d^{-1} + 1) = 1 \quad &\text{with } d \neq \pm 1,\ D^l d^{-1} + 1 \neq \pm 1 \\ &\Longrightarrow d \notin K^l \Longrightarrow \theta \notin E_K^l \Longrightarrow \theta \notin E_0^{1-\sigma}. \end{aligned}$$

Let $g(\sigma)$ be as in Lemma 4; then $\theta^{g(\sigma)} \notin E_0^{1-\sigma}$ follows from this lemma. As $g(1) = -1$, we have that

$$\eta^{(1-\sigma)^{l-2}} = (\sqrt[l]{m} - D)^{(1-\sigma)^{l-1}} = d(\sqrt[l]{m} - D)^{l g(\sigma)} = \theta^{g(\sigma)}. \tag{1}$$

Therefore $\eta^{(1-\sigma)^{l-3}} \notin E_0$ and $\eta^{(1-\sigma)^{l-2}} \in E_0$, which implies that

$$\langle \eta, \eta^{\sigma}, \cdots, \eta^{\sigma^{l-3}} \rangle E_0/E_0 = \langle \eta, \eta^{1-\sigma}, \cdots, \eta^{(1-\sigma)^{l-3}} \rangle E_0/E_0 \simeq (Z/lZ)^{l-2}. \tag{2}$$

We define

$$\mathscr{E} = \langle \eta, \eta^{\sigma}, \cdots, \eta^{\sigma^{l-3}}, \eta^{\sigma^{l-2}} \rangle \subset E_L .$$

The equation (1) implies $\eta^{\sigma^{l-2}} \equiv \theta \pmod{\langle \eta, \eta^{\sigma}, \cdots, \eta^{\sigma^{l-3}} \rangle \mathscr{E}^l}$, since $\theta^{\tau} \equiv \theta \pmod{\mathscr{E}^l}$. As $\theta \notin E_L^l$, we see from (2) that

$$\mathscr{E} \cap E_L^l = \mathscr{E}^l \quad \text{and} \quad \mathscr{E}/\mathscr{E}^l \simeq (\boldsymbol{Z}/l\boldsymbol{Z})^{l-1}. \tag{3}$$

2nd step. We shall prove that ε_0 satisfies the conditions I, II and III (0 follows from III). The condition III: Since $\eta^{\sigma^{l-1}} = \eta^{-1-\sigma-\cdots-\sigma^{l-2}}$ and $a(l-2) \equiv 1 \pmod{l}$, we see that $\varepsilon_0^{\sigma-1} \in \mathscr{E} \backslash \mathscr{E}^l$. Therefore (3) implies that ε_0 satisfies III. The condition I: For $j \in (\boldsymbol{Z}/l\boldsymbol{Z})^*$, we define

$$\eta_{(j)} = \eta^{1+\sigma+\cdots+\sigma^{j'-1}}$$

where j' is a positive rational integer congruent to j modulo l. This definition does not depend on the choice of j' because $\eta^{1+\sigma+\cdots+\sigma^{l-1}} = 1$. As $(\boldsymbol{Z}/l\boldsymbol{Z})^* = \langle \dot{r} \rangle$, it is clear that

$$\mathscr{E} = \langle \eta_{(1)}, \eta_{(\dot{r})}, \cdots, \eta_{(\dot{r}^{l-2})} \rangle .$$

Since $\eta^{\tau} = \eta^{1+\sigma+\cdots+\sigma^{r'-1}}$, we have that $\eta_{(j)}{}^{\tau} = \eta_{(j\dot{r})}$. Therefore we see from (3) that

$$\{\varepsilon \in \mathscr{E};\ \varepsilon \text{ satisfies I.}\} = \langle \varepsilon_1 \rangle \mathscr{E}^l \qquad \text{where } \varepsilon_1 = \prod_{i=0}^{l-2} \eta_{(\dot{r}^i)}{}^{r^{l-1-i}} .$$

If $\dot{r}^i = j$, then $r^{l-1-i} \pmod{l} = \dot{r}^{-i} = j^{-1}$. Hence

$$\varepsilon_1 \equiv \prod_{j=1}^{l-1} (\eta^{1+\sigma\cdots+\sigma^{j-1}})^{b(j)} \pmod{\mathscr{E}^l}$$

where $b(j)$ is a rational integer congruent to j^{-1} modulo l,

$$\equiv \prod_{i=0}^{l-2} \eta^{(b(i+1)+\cdots+b(l-1))\sigma^i} \pmod{\mathscr{E}^l}$$

$$\equiv \prod_{i=1}^{l-2} \eta^{-a(i)\sigma^i} \equiv (\zeta^{-1}\varepsilon_0)^{-1} \pmod{\mathscr{E}^l} .$$

Therefore $\zeta^{-1}\varepsilon_0$ satisfies I, and so does ε_0 as $\zeta^{\tau-r} = 1$. The condition II: Clearly ε_0 satisfies II(i). We note that $l \nmid m$ as $l \mid D$ and $l \nmid d$. Then $\eta = (\sqrt[l]{m} - D)/\zeta(\sqrt[l]{m} - D\zeta^{-1}) \equiv \zeta^{-1} \pmod{(1-\zeta)^l}$ because $(\sqrt[l]{m}, 1-\zeta) = 1$ and $(1-\zeta)^l \mid D(\zeta^{-1} - 1)$. Hence $\varepsilon_0 \equiv \zeta \cdot \prod_{i=1}^{l-2} \zeta^{-a(i)} \equiv 1 \pmod{(1-\zeta)^l}$ because $\sum_{i=1}^{l-2} a(i) \equiv 1 \pmod{l}$. Therefore ε_0 satisfies II(ii). The proof of the theorem is complete.

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

Remark. For a fixed l, there exist infinitely many pure algebraic number fields of degree l, satisfying the assumption of Theorem 4. For example, let $D = 2lD'$, $d = 2$ with $D' \in \boldsymbol{Z}, > 0$; then it is known that $D^l + d$ is l-th power-free for infinitely many D' (cf. [7]).

EXAMPLE. Let $f(X)$ be as in Example of Section 1. Let μ denote $\sqrt[l]{m}$.

(1) In the case $l = 3$: We can take

$$\varepsilon_0 = \zeta\eta^{\sigma} \quad \text{(cf. [6])}.$$

For $\alpha = \varepsilon_0$, we have

$$f(X) = X^3 - 3X - d^{-2}((9D^6 + 12D^3 d + 2d^2) + (-18D^5 - 12D^2 d)\mu + 9D^4\mu^2).$$

For example, let $D = 6$ and $d = 2$; then $m = 218 = 2\cdot 109$ and

$$f(X) = X^3 - 3X - 106274 + 35208\mu - 2916\mu^2.$$

(2) In the case $l = 5$: We can take

$$\varepsilon_0 = \zeta\eta^{\sigma - \sigma^2 + \sigma^3}.$$

For $\alpha = \varepsilon_0$, we have

$$\begin{aligned} f(X) = X^5 - 10X^3 & \\ & - 5d^{-4}(\mu - D)^4\Big(5 \sum_{\substack{i,j,k \in \boldsymbol{Z}/5\boldsymbol{Z} \\ i+2j+4k=2}} [2, i][8, j][6, k] - (\mu - D)^{16}\Big)X^2 \\ & + \Big\{5 - 5d^{-6}(\mu - D)^6\Big(5 \sum_{\substack{i,j,k \in \boldsymbol{Z}/5\boldsymbol{Z} \\ 2i+3j+4k=1}} [8, i][4, j][12, k] - (\mu - D)^{24}\Big)\Big\}X \\ & - d^{-8}(\mu - D)^8\Big(5 \sum_{\substack{i,j,k \in \boldsymbol{Z}/5\boldsymbol{Z} \\ 2i+3j+4k=3}} [14, i][2, j][16, k] - (\mu - D)^{32}\Big), \end{aligned}$$

where

$$[n, i] = \sum_{\substack{0 \leq j \leq n \\ j\,(\mathrm{mod}\ 5) = i}} \frac{n!}{j!(n-j)!}(-D)^{n-j}\mu^j \qquad \text{for } n \in \boldsymbol{Z}, > 0 \text{ and } i \in \boldsymbol{Z}/5\boldsymbol{Z}.$$

For example, let $D = 10$ and $d = 2$; then $m = 100002 = 2\cdot 3\cdot 7\cdot 2381$ and

$$\begin{aligned} f(X) = X^5 - 10X^3 & \\ & + (214851250061249942499980 - 78129531319062698750000\mu \\ & \quad - 27344625006531250000000\mu^2 - 7812546873062497500 0\mu^3 \\ & \quad + 2148500000350000000 0\mu^4)X^2 \\ & + (-6103955090097800313125937395000015 \\ & \quad - 6103784183457054922033750417500000\mu \\ & \quad - 48829453125156113437500000 0\mu^2 \end{aligned}$$

https://doi.org/10.1017/S0027763000002580 Published online by Cambridge University Press

$$
\begin{aligned}
&\qquad + 122076171962305053906100000050000\,\mu^3 \\
&\qquad + 4883050784218754125000000\,\mu^4)X \\
&+ 30518981892208452083260233579397181299849996 \\
&- 762838737035955369712416353069835632947500\,\mu \\
&- 76315308577887392315028065784834125000000\,\mu^2 \\
&+ 305206910252698725568190329921282625025000\,\mu^3 \\
&- 45779296903685893555340950587494680000000\,\mu^4\,.
\end{aligned}
$$

References

[1] G. Gras, Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, Bull. Soc. Math. France, **100** (1972), 177–193.

[2] F. Halter-Koch und H.-J. Stender, Unabhängige Einheiten für die Körper $K = \boldsymbol{Q}(\sqrt[n]{D^n \pm d})$ mit $d \mid D^n$, Abh. Math. Sem. Univ. Hamburg, **42** (1974), 33–40.

[3] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Physica-Verlag, Würzburg/Wien, 1970.

[4] M. Ishida, On the genus field of an algebraic number field of odd prime degree, J. Math. Soc. Japan, **27** (1975), 289–293.

[5] S. Kobayashi, On the l-dimension of the ideal class groups of Kummer extensions of a certain type, J. Fac. Sci. Univ. Tokyo Sec. IA, **18** (1971), 399–404.

[6] Y. Odai, Some unramified cyclic cubic extensions of pure cubic fields, Tokyo J. Math., **7** (1984), 391–398.

[7] G. Ricci, Ricerche aritmetiche sui polinomi, Rend. Circ. Mat. Palermo, **57** (1933), 433–475.

[8] C. Walter, A class number relation in Frobenius extension of number field, Mathematika, **24** (1977), 216–225.

[9] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1982.

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Fukasawa Setagaya-ku, Tokyo 158