Токуо Ј. Матн. Vol. 7, No. 2, 1984

Some Unramified Cyclic Cubic Extensions of Pure Cubic Fields

Yoshitaka ODAI

Tokyo Metropolitan University (Communicated by K. Ogiue)

Introduction

In [6], Ishida has explicitly constructed the genus field of an algebraic number field F of a certain type. Therefore it is of some interest to construct unramified abelian extensions, of F, which are not contained in the genus field. In this paper, we shall consider this problem in the case that F is a pure cubic field.

Let Q denote the field of rational numbers, and let Z be the ring of rational integers. Let $K=Q(\sqrt[3]{m})$ be a real pure cubic field, where m is a positive cubefree rational integer. Let $\zeta = \exp(2\pi i/3)$. Let $k = Q(\zeta)$ and $\tilde{K} = Kk$. Then \tilde{K} is the Galois closure of K. Let M (resp. M') be the genus field of K (resp. \tilde{K}) over Q (resp. k). The field M was given explicitly in [1]. We shall give some unramified cyclic cubic extensions, of K, which are not contained in M. Let $\operatorname{Re} \alpha$ denote the real part of a complex number α . Then such extensions are written in the form $K(\operatorname{Re}\sqrt[3]{\varepsilon_0})$, where ε_0 is a unit of \tilde{K} with some properties (cf. Theorems 1.3 and 3.1).

Notations: Let J be the complex conjugate map, and let σ be a generator of $\operatorname{Gal}(\tilde{K}/k)$ with $(\sqrt[3]{m})^{\sigma} = \sqrt[3]{m} \cdot \zeta$, Then $\operatorname{Gal}(\tilde{K}/Q)$ is generated by $\{J, \sigma\}$ with the relations $J^2 = \sigma^3 = 1$, $\sigma J = J\sigma^2$. For an algebraic number field F, let F'^* (resp. E_F) denote its multiplicative group (resp. its unit group).

§1. Preliminaries.

LEMMA 1.1. Let \mathscr{A} be the set of all the unramified cyclic cubic extensions of K and let \mathscr{B} be the set of all the unramified cyclic cubic extensions, of \tilde{K} , which are abelian over K. (We note from Kummer theory that any element of \mathscr{B} is written in the form $\tilde{K}(\sqrt[3]{\alpha})$, where

Received September 5, 1983 Revised November 4, 1983

 $\alpha \in \tilde{K}^*$.) Let ρ be the mapping $\tilde{K}(\sqrt[3]{\alpha}) \in \mathscr{B} \to K(\operatorname{Re}\sqrt[3]{\alpha})$. Then ρ is a bijection of \mathscr{B} onto \mathscr{A} .

PROOF. As $\widetilde{K}(\sqrt[3]{\alpha}) \in \mathscr{B}$ is cyclic sextic over K, the mapping $\widetilde{K}(\sqrt[3]{\alpha}) \to X$, where X is a unique cubic subfield of $\widetilde{K}(\sqrt[3]{\alpha})$ over K, is clearly a bijection of \mathscr{B} onto \mathscr{A} . Therefore it suffices to show that $K(\operatorname{Re}\sqrt[3]{\alpha})=X$. Clearly $K(\operatorname{Re}\sqrt[3]{\alpha})$ is X or K since $K(\operatorname{Re}\sqrt[3]{\alpha})\subset \mathbb{R}$. (\mathbb{R} is the field of real numbers.) As $\widetilde{K}(\sqrt[3]{\alpha})/K$ is abelian, we see from Kummer theory that $\alpha^{1+J} \in (\widetilde{K}^*)^3$. Hence $(\sqrt[3]{\alpha})^{1+J} \in \widetilde{K} \cap \mathbb{R} = K$, which implies that $\sqrt[3]{\alpha}$ is quadratic over $K(\operatorname{Re}\sqrt[3]{\alpha})$. As $\sqrt[3]{\alpha}$ is not quadratic over K, we have $K(\operatorname{Re}\sqrt[3]{\alpha})=X$.

LEMMA 1.2. Let \mathscr{B} , ρ be as in Lemma 1.1. Then, for $F \in \mathscr{B}$, we have that:

$$F \subset M' \longleftrightarrow \rho(F) \subset M$$
.

PROOF. The part " \leftarrow ": It is clear because $F = \rho(F) \cdot \tilde{K}$. The part " \Rightarrow ": Assume that $F \subset M'$. Then, as F is abelian over K and over k, we see that F/Q is a Galois extension. Moreover, since \tilde{K}/k is ramified, then $\operatorname{Gal}(F/k) \simeq (\mathbb{Z}/3\mathbb{Z})^2$. So an application of Lemma 2 in [7] to $\operatorname{Gal}(F/Q)$ proves that $\rho(F) \subset M$.

THEOREM 1.3. Any unramified cyclic cubic extension of K is obtained by adjoining Re $\sqrt[8]{\alpha}$ to K, where $\alpha \in \tilde{K}^*$ satisfies the following three conditions:

0. $\widetilde{K}(\sqrt[3]{\alpha})$ is cubic over \widetilde{K} , namely, $\alpha \notin (\widetilde{K}^*)^{s}$.

I. $\widetilde{K}(\sqrt[3]{\alpha})$ is unramified over \widetilde{K} , namely,

i) there exists an ideal \mathfrak{A} of \widetilde{K} such that $(\alpha) = \mathfrak{A}^s$,

ii) for any prime ideal l of \tilde{K} dividing 3, α is a 3rd power residue mod l^{se_0} , where e_0 is the ramification index of l over k.

II. $\widetilde{K}(\sqrt[3]{\alpha})$ is abelian over K, namely, $\alpha^{1+J} \in (\widetilde{K}^*)^3$. Moreover, when $\alpha \in \widetilde{K}^*$ satisfies the above conditions 0, I and II, we obtain that $K(\operatorname{Re}\sqrt[3]{\alpha}) \not\subset M$ if and only if

III. $\alpha^{\sigma-1} \notin (\widetilde{K}^*)^{\mathfrak{s}}$.

PROOF. The first assertion follows immediately from Lemma 1.1, the ramification theory in Kummer extensions (cf. [4], Ia, Satz 9) and Kummer theory. As \tilde{K}/k is abelian, we see from Kummer theory that $\tilde{K}(\sqrt[3]{\alpha}) \not\subset M' \leftrightarrow \tilde{K}(\sqrt[3]{\alpha})/k$ is not abelian $\Leftrightarrow \alpha^{\sigma-1} \notin (\tilde{K}^*)^s$. The second assertion follows at once from this fact and Lemma 1.2.

REMARK. One can easily know whether $\alpha \in \widetilde{K}^*$ satisfies the condition

CUBIC EXTENSIONS

I ii), by taking $\pi \in \widetilde{K}^*$ such that $I \parallel \pi$ and by calculating the π -expansion of α .

§2. Field associated with \mathcal{H}_1 .

Let \mathscr{H}_2 , \mathscr{H}_1 and \mathscr{H}_1^0 be the 3-elementary class group (i.e., the 3elementary part of the ideal class group) of \tilde{K} , the group of ambiguous ideal classes of \tilde{K}/k and the group of ideal classes represented by ambiguous ideals of \tilde{K}/k respectively. Then $\mathscr{H}_1^0 \subset \mathscr{H}_1 \subset \mathscr{H}_2$ as the class number of k is 1. Let $cl(\mathfrak{A})$ denote the ideal class represented by an ideal \mathfrak{A} of \tilde{K} .

For $\alpha \in \tilde{K}^*$, the field associated with α is defined as

$$p(\vec{K}(\sqrt[3]{\alpha})) = K(\operatorname{Re}\sqrt[3]{\alpha})$$
 if α satisfies the conditions 0, I and II in
Theorem 1.3,
 K otherwise.

Furthermore, for a subgroup H of \mathscr{H}_2 , the field associated with H is defined as the composite of all the fields associated with those $\alpha \in \tilde{K}^*$ such that $(\alpha) = \mathfrak{A}^{\mathfrak{s}}$ with $\operatorname{cl}(\mathfrak{A}) \in H$. We note that the condition I i) shows that any unramified cyclic cubic extension of K is contained in the field associated with \mathscr{H}_2 .

For a subgroup H of \mathscr{H}_2 such that $H^J \subset H$, we denote

$$H^{\pm} = \{h \in H | h^J = h^{\pm 1}\}$$
.

Then

$$H = H^+ \times H^-$$
 (direct).

In fact, for $h \in H$, we have $h = h^{2(1+J)} \times h^{2(1-J)}$ and $h^{2(1\pm J)} \in H^{\pm}$.

LEMMA 2.1. Let H be a subgroup of \mathscr{H}_2 such that $H^{J} \subset H$. Then the field associated with H is the same as the field associated with H^{-} .

PROOF. Let α be an element of \widetilde{K}^* such that $(\alpha) = \mathfrak{A}^*$ with $\operatorname{cl}(\mathfrak{A}) \in H$. We may assume that α satisfies the condition II. Then \mathfrak{A}^{1+J} is a principal ideal, since $(\alpha^{1+J}) = (\mathfrak{A}^{1+J})^*$ and $\alpha^{1+J} \in (\widetilde{K}^*)^*$. Therefore $\operatorname{cl}(\mathfrak{A})^{2(1+J)} = 1$, namely, $\operatorname{cl}(\mathfrak{A}) \in H^-$.

REMARK. If $H = \mathscr{H}_2$, \mathscr{H}_1 or \mathscr{H}_1^0 , then $H^j \subset H$. So Lemma 2.1 is applicable to these cases.

We shall consider the case $H = \mathscr{H}_1$ in this paper.

LEMMA 2.2. Let p_1, \dots, p_s be all the rational primes dividing m and

congruent to 1 mod 3. We write $p_i = \pi_i^{1+J}$ for $1 \leq i \leq s$, where π_i are prime elements in k congruent to 1 mod 3. Then

$$\int_{i=1}^{\bullet} \rho(\tilde{K}(\sqrt[3]{\pi_i^{1+2J}})) = K(\operatorname{Re}\sqrt[3]{\pi_1^{1+2J}}, \cdots, \operatorname{Re}\sqrt[3]{\pi_{\bullet}^{1+2J}}) = M.$$

PROOF. From Lemma 3.2 in [2] and the condition II, we see that $\tilde{K}(\sqrt[8]{\pi_1^{1+2J}}, \dots, \sqrt[8]{\pi_s^{1+2J}})$ is the maximal subfield, of M', which is abelian over K. The lemma follows at once from this fact and Lemmas 1.1 and 1.2.

THEOREM 2.3. Let L be the composite of all the fields associated with the units in \tilde{K} . (We note that L is the field associated with the identity subgroup {1} of \mathcal{H}_2 .) Then the field associated with \mathcal{H}_1 is the same as ML.

PROOF. From the proof of proposition 2 in [3], we see that $\mathscr{H}_1^- = \mathscr{H}_1^{0-}$. So an application of Lemma 2.1 to \mathscr{H}_1 and \mathscr{H}_1^0 implies that the field associated with \mathscr{H}_1 is the same as the field associated with \mathscr{H}_1^0 . Let $\mathfrak{P}_1, \dots, \mathfrak{P}_i$ be all the prime ideals of \widetilde{K} ramified over k. Then \mathscr{H}_1^0 is generated by these ideal classes as the class number of k is 1. We write $\mathfrak{P}_i^3 = (\pi_i')$ for $1 \leq i \leq t$, where π_i' are prime elements in k. Let s, π_i be as in Lemma 2.2. Then $2s \leq t$. We can take

$(\pi_i'=\pi_i)$	for	$1{\leq}i{\leq}s$,
$\pi'_{i=\pi_{i-s}}$		$s{+}1{\leq}i{\leq}2s$,
$(\pi'_i$ is a rational prime or $\sqrt{-3}$	for	$2s{<}i$.

Then the field associated with \mathscr{H}_1^{α} is the composite of all the fields associated with $\alpha = \varepsilon \prod_{i=1}^{t} \pi_i^{\prime \alpha_i}$, where $\varepsilon \in E_{\widetilde{K}}$, $\alpha_i \in \mathbb{Z}$. We may assume that α satisfies the conditions 0, I and II. By II, we have $\widetilde{K}(\sqrt[3]{\alpha}) = \widetilde{K}(\sqrt[3]{\alpha^{1+2J}})$, which is contained in

$$\widetilde{K}(\sqrt[3]{\pi_1'^{1+2J}}, \cdots, \sqrt[3]{\pi_t'^{1+2J}}, \sqrt[3]{\varepsilon^{1+2J}})$$

Since $\pi_i^{\prime_1+2J} \cdot \pi_{i+s}^{\prime_1+2J} \in (\tilde{K}^*)^s$ for $1 \leq i \leq s$ and since $\pi_i^{\prime_1+2J} \in (\tilde{K}^*)^s$ for 2s < i, we have

$$\widetilde{K}(\sqrt[9]{\alpha}) \subset \widetilde{K}(\sqrt[9]{\pi_1^{1+2J}}, \cdots, \sqrt[9]{\pi_1^{1+2J}}, \sqrt[9]{\varepsilon^{1+2J}}).$$

As α^{1+2J} and each $\pi_i^{j_1+2J}$ satisfy the conditions I and II, so does ε^{1+2J} . Let Y be $\rho(\tilde{K}(\sqrt[3]{\varepsilon^{1+2J}}))$ or K, according as ε^{1+2J} satisfies the condition 0 or not. Then, by Lemma 1.1, we have

$$\rho(\widetilde{K}(\sqrt[3]{\alpha})) \subset \prod_{i=1}^{\bullet} \rho(\widetilde{K}(\sqrt[3]{\pi_i^{1+2j}})) \cdot Y \text{ and } Y \subset L$$

So we see from Lemma 2.2 that $\rho(\tilde{K}(\sqrt[3]{\alpha})) \subset ML$. Conversely it is clear from this lemma that M is contained in the field associated with \mathscr{H}_1° .

This completes the proof of the theorem.

In the next section, we shall consider the field associated with a unit in \tilde{K} .

§3. Field associated with a unit.

Let $\{\varepsilon_1, \varepsilon_2\}$ be a system of the fundamental units of \tilde{K} . As the field associated with a unit is the same as the field associated with one of $\zeta^a \varepsilon_1^b \varepsilon_2^c$, where $a, b, c \in \{0, 1, 2\}$, we shall examine the conditions 0, I, II and III in Theorem 1.3 for $\zeta^a \varepsilon_1^b \varepsilon_2^c$. Clearly each $\zeta^a \varepsilon_1^b \varepsilon_2^c$ satisfies the conditions 0 and I i) unless a=b=c=0.

Now to examine the conditions II and III we use some results about $\{\varepsilon_1, \varepsilon_2\}$. Let *e* be a fundamental unit of *K* with norm 1. Then the following two cases occur (cf. [8]).

Case 1. $\{\varepsilon_1, \varepsilon_2\} = \{e, e^{\sigma}\}.$

Case 2. $\{\varepsilon_1, \varepsilon_2\} = \{\varepsilon, \varepsilon^o\}$, where ε is a unit in \widetilde{K} such that $\varepsilon^{1-\sigma} = e$.

Case 1. The condition II: Since $(e^{\sigma})^{1+J} = e^{-1}$, then $(\zeta^a e^{b+\sigma\sigma})^{1+J} = e^{2b-\sigma}$. Therefore only ζ^a and $\zeta^a e^{1+2\sigma}$ satisfy this condition. (We may delete $\zeta^a e^{2+\sigma}$ because $e^{1+2\sigma} e^{2+\sigma} \in (\tilde{K}^*)^3$.) The condition III: We have $(\zeta^a e^{1+2\sigma})^{\sigma-1} = e^{-8-3\sigma} \in (\tilde{K}^*)^3$. Hence in Case 1 there are no units in \tilde{K} satisfying the conditions II and III.

Case 2. The condition II: By Equality (4) in [5], $\varepsilon^{1+J} = \pm e$, and so $\varepsilon^{J} = \pm \varepsilon^{-\sigma}$. An easy calculation then shows that $(\zeta^{a}\varepsilon^{b+\sigma\sigma})^{1+J} = \varepsilon^{(b-\sigma)+(\sigma-b)\sigma}$. Thefore only ζ^{a} and $\zeta^{a}\varepsilon^{1+\sigma}$ satisfy this condition. (This time we may delete $\zeta^{a}\varepsilon^{2+2\sigma}$.) The condition III: We have $\varepsilon^{\sigma^{2}} = \xi\varepsilon^{-1-\sigma}$ with $\xi = \varepsilon^{1+\sigma+\sigma^{2}} \in E_{k}$, so $(\zeta^{a}\varepsilon^{1+\sigma})^{\sigma-1} = \xi\varepsilon^{-2-\sigma} \notin (\tilde{K}^{*})^{3}$. Hence in Case 2 it follows that only $\zeta^{a}\varepsilon^{1+\sigma}$, a=0, 1, 2, satisfy the conditions II and III. The condition I ii): This condition is easily examined (cf. Remark just following Theorem 1.3). In particular, at most one of $\zeta^{a}\varepsilon^{1+\sigma}$ satisfies this condition because ζ does not.

Hence we have the following

THEOREM 3.1. Let L be the composite of all the fields associated with the units in \tilde{K} . Let Case 1, Case 2 and ε be as above. Then we have that: Case 1. $L \subset M$.

Case 2. #U=0 or 1, where $U=\{\zeta^a\varepsilon^{1+\sigma}, a=0, 1, 2 | \zeta^a\varepsilon^{1+\sigma} \text{ satisfies the condition I ii} \text{ in Theorem 1.3.}\}.$

 $\begin{cases} If \quad U = \emptyset \ , \qquad then \quad L \subset M. \\ If \quad U = \{\varepsilon_0\} \ , \qquad then \quad ML = M \cdot K(\operatorname{Re} \sqrt[9]{\varepsilon_0}) \neq M \ . \end{cases}$

REMARK. Some effective methods to calculate a fundamental unit e of K have been known. (For example, there is a table for $m \leq 250$ in

[10]. Also if m is of particular form, e is given explicitly (cf. [9]).) Moreover, by easy arithmetic involving the unit e, we can know whether this is Case 2, and in Case 2 we can also calculate the unit ε (cf. [5]).

By Theorems 2.3 and 3.1, we have completely obtained the field associated with \mathcal{H}_1 . As was noted in section 2, in order to obtain all the unramified cyclic cubic extensions of K, it suffices to construct the field associated with \mathcal{H}_2 . But, as it seems somewhat complicated to treat the case $H = \mathcal{H}_2$, we shall consider this case elsewhere.

EXAMPLE. $K = Q(\sqrt[3]{m})$, where *m* is a positive cubefree rational integer. We consider the case

 $m=D^3+d$ with $D, d\in \mathbb{Z}$, D>0, $d|3D^2$.

This is Case 1 or Case 2 according as $d = \pm 1 \operatorname{except} (D, d) = (1, 1), (2, 1)$ or $d \neq \pm 1$. In the case $d \neq \pm 1 \operatorname{except} (D, d) = (1, 3), (2, -6), (5, -25), (2, -4),$ we have $\varepsilon = (\theta - D)/(\theta^{\sigma^2} - D)$ with $\theta = \sqrt[3]{m}$. (The above results have been obtained in [9] and [5].) Examining the condition I ii) for $\zeta^{\alpha} \varepsilon^{1+\sigma}$ (cf. Remark just following Theorem 1.3), we obtain the following

PROPOSITION 3.2. Let $K = Q(\sqrt[3]{m})$, where m is a positive cubefree rational integer written as

 $\begin{array}{rrrr} D^3+d & with & D, \, d\in \mathbb{Z} \ , & D>0 \ , & d \,|\, 3D^2 \ , & d\neq \pm 1 \ , \\ & (D,\,d)\!\neq\!(1,\,3) \ , & (2,\,-6) \ , & (5,\,-25) \ , & (2,\,-4) \ . \end{array}$ Then U in Theorem 3.1 is as follows:

Г

				U
	$m \equiv \pm 1 \mod 9$			Ø
34 <i>D</i>	$m \not\equiv \pm 1 \mod 9 \text{ and } 3 \not\mid m$	3łd	$m \equiv \pm 4 \mod 9$	$\{\zeta \varepsilon^{1+\sigma}\}$
			$m \equiv \pm 2 \mod 9$	$\{\varepsilon^{1+\sigma}\}$
		3 <i>d</i>		Ø
	3 <i>m</i>		Ø	
	0211	$m/9\equiv D \mod 3$		$\{\zeta^2 \varepsilon^{1+\sigma}\}$
	3²∥ <i>m</i>	$m/9 \equiv -D \mod 3$		$\{\zeta \varepsilon^{1+\sigma}\}$
3 <i>D</i>	3†m		$\{\zeta \varepsilon^{1+\sigma}\}$	
		$m/3 \equiv D/3 \mod 3$		$\{\zeta^2 \varepsilon^{1+\sigma}\}$
	3∥ <i>m</i>	$m/3 \equiv -D/3 \mod 3$		$\{\varepsilon^{1+\sigma}\}$
	3 ² <i>m</i>			Ø
$3^2 D$				$\{\zeta \varepsilon^{1+\sigma}\}$

396

CUBIC EXTENSIONS

Here $\varepsilon = (\theta - D)/(\theta^{\sigma^2} - D)$ with $\theta = \sqrt[8]{m}$.

NUMERICAL EXAMPLES: $K = Q(\sqrt[3]{m})$. Let h and g be the class number and the genus number of K respectively.

(1) m=30 (An example contained in Proposition 3.2.) As $30=3^3+3$, D=d=3. Since $3 \parallel D$, $3 \parallel m$ and $m/3 \equiv D/3 \mod 3$, then $U=\{\zeta^2 \varepsilon^{1+\sigma}\}$. Therefore

$$K(\operatorname{Re}\sqrt[8]{\zeta^{2}\varepsilon^{1+\sigma}}) = K(\operatorname{Re}\sqrt[8]{(\sqrt[8]{30}\zeta - 3)/(\sqrt[8]{30} - 3\zeta)})$$

is an unramified cyclic cubic extension, of K, which is not contained in M. Moreover, since it is known that g=1 and h=3, $K(\operatorname{Re}\sqrt[3]{\zeta^2}\varepsilon^{1+\sigma})$ is the field associated with \mathscr{H}_1 and also the absolute class field of K.

(2) m=34 (An example not contained in Proposition 3.2.) $e=334153+103146\theta+31839\theta^2$ (cf. [10]). Then, by the method described in [5], we know that this is Case 2 and

$$\varepsilon = 305 + 94\theta + 29\theta^2 - 52\zeta - 16\theta\zeta - 5\theta^2\zeta$$
.

Examining the condition I ii), we have $U = \{\varepsilon^{1+\sigma}\}$. Therefore $K(\operatorname{Re}\sqrt[3]{\varepsilon^{1+\sigma}})$ is an unramified cyclic cubic extension, of K, which is not contained in M. Moreover, since it is known that g=1 and h=3, $K(\operatorname{Re}\sqrt[3]{\varepsilon^{1+\sigma}})$ is the field associated with \mathscr{H}_1 and also the absolute class field of K.

References

- A. FRÖHLICH, The genus field and genus group in finite number fields, II, Mathematika, 6 (1959), 142-146.
- [2] F. GERTH, On 3-class groups of pure cubic fields, J. Reine Angew. Math., 278/279 (1975), 52-62.
- [3] G. GRAS, Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l a clôture galoisienne diédrale de degré 2l, J. Math. Soc. Japan, 26 (1974), 677-685.
- [4] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Physica-Verlag, Würzburg/Wien, 1970.
- [5] K. IIMURA, On the unit groups of certain sextic number fields, Abh. Math. Sem. Univ. Hamburg, 50 (1980), 32-39.
- [6] M. ISHIDA, The genus fields of algebraic number fields, Lecture Notes in Math., 555, Springer, Berlin-Heidelberg-New York, 1976.
- [7] 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.
- [8] A. SCHOLZ, Idealklassen und Einheiten in kubischen Körpern, Monatsh. Math. Phys., 40 (1933), 211-222.
- [9] H.-J. STENDER, Lösbare Gleichungen $ax^n by^n = c$ und Grundeinheiten für einige algebraische Zahlkörper vom Grade n=3, 4, 6, J. Reine Angew. Math., **290** (1977), 24-62.

[10] H. WADA, A table of fundamental units of purely cubic fields, Proc. Japan Acad., 46 (1970), 1135-1140.

Present Address: Department of Mathematics Faculty of Sciences Tokyo Metropolitan University Fukasawa, Setagaya-ku, Tokyo 158

398