TOKYO J. MATH.
VOL. 4, NO. 1, 1981

On the Genus Fields of Pure Number Fields II

Makoto ISHIDA

Tokyo Metropolitan University

In the preceding paper [3], we have investigated the genus fields K^* of pure number fields $K=\boldsymbol{Q}(\sqrt[n]{a})$. But there we could not decide K^* in the case where $2^3|n$ and $a\equiv -1 \pmod{2^4}$ and so our table in [3] was incomplete. Now, in the present paper, we shall treat this remaining open case and, consequently, shall determine the genus field K^* and the genus number g_K for any pure number field K explicitly. As for the definitions and the notations, see Ishida [2] and [3].

§1. Remaining case.

Let $K=\boldsymbol{Q}(\sqrt[n]{a})$ with $a\in \boldsymbol{Z}$ $(a\neq \pm 1)$ be a pure number field, where, as before, a has the property

$$(*)\qquad p^v \| a \Longrightarrow (v, n)=1$$

for any prime divisor p of a.

First, in §1, §2 and §3, as is stated in the introduction, we consider the remaining open case:

$$n=2^s \ (s\geqq 2 \text{ and so } n\geqq 4)$$
$$\text{and} \quad a\equiv -1 \pmod 4$$

(cf. [3]). We fix them in §1, §2, §3. Note that, in this case, 2 is totally ramified in K: $(2)=\mathfrak{l}^n$ ($\mathfrak{l}$ is a prime ideal of K). Let k^* be the maximal abelian subfield of the genus field K^* of K and k_2^* the maximal subfield of k^* such that $k_2^*\subset \boldsymbol{Q}(\zeta_{2^M})$ for some M. (ζ_{2^M} denotes a primitive 2^M-th root of unity.) In other words, k_2^* is the maximal absolute abelian number field such that k_2^*K is unramified over K (in narrow sense) and $k_2^*\subset \boldsymbol{Q}(\zeta_{2^M})$ for some M. As is well known, $\boldsymbol{Q}(\zeta_4)\boldsymbol{Q}(\sqrt{a})$ is unramified over $\boldsymbol{Q}(\sqrt{a})$ and so $\boldsymbol{Q}(\zeta_4)K$ is unramified over K. Hence $\boldsymbol{Q}(\zeta_4)\subset k_2^*$ and, as $\boldsymbol{Q}(\zeta_{2^M})/\boldsymbol{Q}(\zeta_4)$ is a cyclic extension, we have

Received June 28, 1980

$$k_2^* = \boldsymbol{Q}(\zeta_{2^d}) \qquad \text{for some} \quad d \in \boldsymbol{Z}\,.$$

Now we consider the two cases separately and prove the following assertions:

Case A. $a \equiv -1 (\mathrm{mod}\, 2^{s+1})$. Then we have

$$k_2^* = \boldsymbol{Q}(\zeta_{2^{s+1}})\,.$$

Case B. $a \not\equiv -1 (\mathrm{mod}\, 2^{s+1})$. Take such $r \in \boldsymbol{Z}(1 \leqq r < s)$ that $a \equiv -1$ $(\mathrm{mod}\, 2^{r+1})$ but $a \not\equiv -1 (\mathrm{mod}\, 2^{r+2})$. Then we have

$$k_2^* = \boldsymbol{Q}(\zeta_{2^{r+1}})\,.$$

For $s=2$ (i.e. $n=4$), we have just proved them in [3]:

$$\begin{cases} a \equiv -1 (\mathrm{mod}\, 8) \Longrightarrow k_2^* = \boldsymbol{Q}(\zeta_8)\,, \\ a \equiv 3 (\mathrm{mod}\, 8) \quad \Longrightarrow k_2^* = \boldsymbol{Q}(\zeta_4)\,. \end{cases}$$

Hence we shall prove these two assertions by using the induction on s.

Then we shall see that, if $2^N \| a+1$,

$$k_2^* = \boldsymbol{Q}(\zeta_{2^d}) \qquad \text{with} \quad d = \mathrm{Min}\,(N, s+1)\,.$$

§2. Proof in the case *B*.

We assume that

$$a \equiv -1 (\mathrm{mod}\, 2^{r+1}) \qquad \text{but} \quad a \not\equiv -1 (\mathrm{mod}\, 2^{r+2}) \quad \text{with} \quad 1 \leqq r < s\,.$$

Let $K_0 = \boldsymbol{Q}((\sqrt[n]{a})^{n/2^r}) \subset K$. Since $a \equiv -1 (\mathrm{mod}\, 2^{r+1})$, we see that, by the assumption of the induction, $\boldsymbol{Q}(\zeta_{2^{r+1}})K_0$ is unramified over K_0. Accordingly $\boldsymbol{Q}(\zeta_{2^{r+1}})K$ is also unramified over K and so $k_2^* \supset \boldsymbol{Q}(\zeta_{2^{r+1}})$. Suppose that $k_2^* \supsetneqq \boldsymbol{Q}(\zeta_{2^{r+1}})$. Then we have $k_2^* \supset \boldsymbol{Q}(\zeta_{2^{r+2}})$ and so $\boldsymbol{Q}(\zeta_{2^{r+2}})K$ is unramified over K; and, by the 'Verschiebungssatz', for any totally positive number γ in K, prime to 2, we have $N_{K/\boldsymbol{Q}}\gamma \equiv 1 (\mathrm{mod}\, 2^{r+2})$. Take $\gamma = \gamma_2 = 1 + \alpha^2 + \alpha$ $(\alpha = \sqrt[n]{a})$ in §3 of [3], for which we have $N_{K/\boldsymbol{Q}}\gamma_2 = 1 + a + a^2$. Then $N_{K/\boldsymbol{Q}}\gamma_2 \equiv 1 (\mathrm{mod}\, 2^{r+2})$ implies $a(1+a) \equiv 0 (\mathrm{mod}\, 2^{r+2})$ i.e., $a \equiv -1 (\mathrm{mod}\, 2^{r+2})$, which is a contradiction. Therefore we have

$$k_2^* = \boldsymbol{Q}(\zeta_{2^{r+1}})$$

and our assertion in case B is verified.

§3. Proof in the case A.

We assume that

$$a \equiv -1 (\mathrm{mod}\ 2^{s+1}) .$$

For the sake of simplicity, we use the following notations:

$$\alpha = \sqrt[2^s]{a} , \qquad \eta = \zeta_{2^s} , \qquad K_1 = \boldsymbol{Q}(\alpha^2)$$

and

$$F = \boldsymbol{Q}(\eta)K = K(\eta) , \qquad E = \boldsymbol{Q}(\zeta_{2^{s+1}})K = F(\sqrt{\eta}) .$$

Here, as an odd prime divisor p of a ramifies totally in K, we have $\boldsymbol{Q}(\zeta_{2^{s+1}}) \cap K = \boldsymbol{Q}$ (cf. the property $(*)$) and so $[E : K] = [\boldsymbol{Q}(\zeta_{2^{s+1}}): \boldsymbol{Q}] = 2^s$. Since $a \equiv -1 (\mathrm{mod}\ 2^{(s-1)+1})$, we see that, by the assumption of the induction, $\boldsymbol{Q}(\eta)K_1$ is unramified over K_1. Accordingly $F = \boldsymbol{Q}(\eta)K$ is also unramified over K.

Now we shall prove that any prime divisor of 2 in F is unramified in E (and so, that E is unramified over F). Then, by considering the ramification indices of 2 in K and $\boldsymbol{Q}(\zeta_{2^{s+1}})$, we see $k_2^* = \boldsymbol{Q}(\zeta_{2^{s+1}})$.

As is stated in §1, we have $(2) = \mathfrak{l}^n$ in K and so

$$(2) = (\mathfrak{L}_1 \mathfrak{L}_2 \cdots \mathfrak{L}_g)^n \qquad \text{in} \quad F ,$$

where $\mathfrak{L}_1, \mathfrak{L}_2, \cdots, \mathfrak{L}_g$ are distinct prime ideals of F. Take anyone of $\mathfrak{L}_j$'s and denote it by $\mathfrak{L}$. We have

$$X^{2^s} - 1 = (X^{2^{s-1}} - 1)(X^{2^{s-1}} + 1) = \prod_{i=0}^{2^s-1} (X - \eta^i)$$

and so

$$X^{2^{s-1}} + 1 = \prod_{i=0\,(\mathrm{odd})}^{2^s-1} (X - \eta^i) .$$

Hence we have

$$a + 1 = \alpha^{2^s} + 1 = \prod_{i=0\,(\mathrm{odd})}^{2^s-1} (\alpha^2 - \eta^i) .$$

Let N be the highest exponent of 2 in $a+1$ i.e., $2^N \| a+1$; so our assumption is equivalent to the inequality

$$N \geqq s+1 .$$

Then we have

$$\mathfrak{L}^{nN} \| \prod_{i=0\,(\mathrm{odd})}^{2^s-1} (\alpha^2 - \eta^i) .$$

Also, let e be the maximal value of the highest exponents of $\mathfrak{L}$ in $\alpha^2 - \eta^i$ for $i = 1, 3, \cdots, 2^s - 1 (\mathfrak{L}^e \| \alpha^2 - \eta^{i_0})$. As i_0 is odd, we may replace η by η^{i_0}

$(E=F(\sqrt{\eta})=F(\sqrt{\eta^{i_0}}))$ and so we may suppose $\mathfrak{L}^e \| \alpha^2-\eta$. Then, as $2^{s-1}e \geqq nN=2^s N$ i.e., $e \geqq 2N \geqq 2$, we can choose $t \in Z (t \geqq 0)$ such that

$$2^{t+1} \leqq e < 2^{t+2} .$$

Let $\mathfrak{L}^{e_i} \| \alpha^2-\eta^i$ for $i=1, 3, \cdots, 2^s-1 (e=e_1)$. For odd $i=1+2^{f_i}c$ $(2 \nmid c)$, we see that

$$\alpha^2-\eta^i=(\alpha^2-\eta)+\eta(1-\eta^{2^{f_i}c})$$

and $\mathfrak{L}^e \| \alpha^2-\eta$, $\mathfrak{L}^{2^{f_i+1}} \| 1-\eta^{2^{f_i}c}$ in F. Consequently we have

$$f_i \leqq t \Longrightarrow 2^{f_i+1} \leqq 2^{t+1} \leqq e \quad \text{and so} \quad e_i=2^{f_i+1}$$
$$(f_i=t,\ 2^{t+1}=e \Longrightarrow e_i \geqq e \text{ and so } e_i=e=2^{t+1} \text{ (the maximality of } e)) ,$$
$$f_i>t \Longrightarrow 2^{f_i+1} \geqq 2^{t+2}>e \quad \text{and so} \quad e_i=e .$$

Suppose that the inequality $t<s$ i.e., $t \leqq s-1$ holds and note that $1<i=1+2^{s-1} \leqq 2^s-1$. The number of such i that $f_i=1$ (resp. $2, 3, \cdots, t$) is 2^{s-2} (resp. $2^{s-3}, 2^{s-4}, \cdots, 2^{s-t-1}$). Hence we have

$$\begin{aligned} 2^s(s+1) \leqq 2^s N = nN = & \sum_{i=0(\text{odd})}^{2^s-1} e_i \\ & = 2^{s-2}\cdot 2^2+2^{s-3}\cdot 2^3+\cdots+2^{s-t-1}\cdot 2^{t+1} \\ & \quad +\{2^{s-1}-(2^{s-2}+\cdots+2^{s-t-1})\}e \\ & = t\cdot 2^s+2^{s-t-1}\cdot e<(s-1)2^s+2^{s-t-1}\cdot 2^{t+2} \\ & = 2^s(s+1) , \end{aligned}$$

which is a contradiction. Accordingly we must have $t \geqq s$ and so the inequality

$$e \geqq 2^{t+1} \geqq 2^{s+1}=2\cdot 2^s=2n .$$

Then we have $\alpha^2 \equiv \eta (\operatorname{mod} \mathfrak{L}^{2n})$, which implies that the congruence equation

$$X^2 \equiv \eta (\operatorname{mod} \mathfrak{L}^{2n})$$

has an integral solution α in F. (Note that $\mathfrak{L}^n \| 1+(-1)$, where -1 is a primitive second root of unity.) So, as is well known (cf. Hecke [1]), $\mathfrak{L}$ is unramified in $E=F(\sqrt{\eta})$.

Since $\mathfrak{L}$ is an arbitrary prime divisor of 2 in F, we see that E is unramified over F. Therefore we have

$$k_2^*=\boldsymbol{Q}(\zeta_{2^{s+1}})$$

and our assertion in case A is also verified.

§4. Final results.

Now we return to the general situation: $K=\boldsymbol{Q}(\sqrt[n]{a})$ ($n>1$ is arbitrary and a has the property ($*$)). Then, combining the results in [3] and in §1, we have the following final results. (We denote by ζ_m a primitive mth root of unity.)

THEOREM. *Let $K=\boldsymbol{Q}(\sqrt[n]{a})$ with $a\in\boldsymbol{Z}$ ($a\neq\pm1$) be a pure number field, where a has the property*

$$(*)\qquad p^v\,\|\,a \Longrightarrow (v, n)=1$$

for any prime divisor p of a. Let

$$2^s\,\|\,n \quad and \quad 2^v\,\|\,a\ .$$

Then the maximal abelian subfield k^* of the genus field K^* of K is given as follows ($K^*=k^*K$):

$$k^*=k_1^*\cdot k_2^* \qquad (composite)\ ,$$

where

$$k_1^*=\prod_{p\mid a\ (p:\ prime)}\{\text{the subfield, of degree } (n, p-1), \text{ of the cyclotomic number field } \boldsymbol{Q}(\zeta_p)\} \qquad (composite)$$

and

$$k_2^*=\begin{cases}\boldsymbol{Q} \text{ if } n \text{ is odd (i.e., } s=0)\ ,\\ \boldsymbol{Q} \text{ if } n \text{ is even and } a\equiv1 \pmod 4\ ,\\ \boldsymbol{Q}(\sqrt{2}) \text{ if } n \text{ is even, } a \text{ is even (i.e., } v>0) \\ \qquad\qquad \text{and } a/2^v\equiv1 \pmod 4\ ,\\ \boldsymbol{Q}(\sqrt{-2}) \text{ if } n \text{ is even, } a \text{ is even (i.e., } v>0) \\ \qquad\qquad \text{and } a/2^v\equiv3 \pmod 4\ ,\\ \boldsymbol{Q}(\zeta_{2^d}) \text{ with } d=\operatorname{Min}(N, s+1) \text{ if } n \text{ is even} \\ \qquad\qquad \text{(i.e., } s>0),\ a\equiv3 \pmod 4 \text{ and } 2^N\,\|\,a+1\ .\end{cases}$$

§5. Genus number.

In order to give the genus number g_K of the pure number field $K=\boldsymbol{Q}(\sqrt[n]{a})$, it suffices to decide the maximal abelian subfield k_0 of K:

$$\begin{aligned} g_K&=[K^*: K]=[k^*: \boldsymbol{Q}]/[k_0: \boldsymbol{Q}]\\ &=[k_1^*: \boldsymbol{Q}][k_2^*: \boldsymbol{Q}]/[k_0: \boldsymbol{Q}]\ ,\end{aligned}$$

(cf. [2]). Under the assumption $(*)$ on a, we can show that $k_0=\boldsymbol{Q}$ if n is odd and $k_0=\boldsymbol{Q}(\sqrt{a})$ if n is even.

We sketch the proof of this fact.* First, if $\boldsymbol{Q}(\zeta_n)\cap K=\boldsymbol{Q}$, then we see easily, by investigating the structure of the Galois group of $\boldsymbol{Q}(\zeta_n, \sqrt[n]{a})$ over $\boldsymbol{Q}$, that $\boldsymbol{Q}((\sqrt[n]{a})^{n/f})$ is the unique subfield, of $K=\boldsymbol{Q}(\sqrt[n]{a})$, of degree f $(f\,|\,n)$. Now suppose that, for an odd prime q, $q^t\,\|\,[k_0\colon \boldsymbol{Q}]$ with $t>0$. Let $q^{s'}\,\|\,n$ and $K_1=\boldsymbol{Q}((\sqrt[n]{a})^{n/q^{s'}})\subset K$. Then k_0 contains a subfield F of degree q^t and, as $[K\colon K_1]$ is prime to q, K_1 must contain F.

(i) If $\pm a$ is not a power of q, then there is a prime divisor $p\neq q$ of a and p is totally ramified in K_1 (cf. the property $(*)$). Accordingly we have $\boldsymbol{Q}(\zeta_{q^{s'}})\cap K_1=\boldsymbol{Q}$ and, as is remarked above, F coincides with $\boldsymbol{Q}(\sqrt[q^t]{a})$. So F contains $\zeta_{q^t}(t>0)$, which is a contradiction.

(ii) If $\pm a$ is a power of q, then F is a subfield of $\boldsymbol{Q}(\zeta_{q^M})$ for some $M\in\boldsymbol{Z}$. On the other hand, by the definition, F is contained in the maximal abelian subfield of the genus field of K_1. So we have $F=\boldsymbol{Q}$ (cf. Theorem and §2 of [3]), which is also a contradiction.

Hence $[k_0\colon \boldsymbol{Q}]$ is a power of 2 and k_0 is contained in $K_0=\boldsymbol{Q}((\sqrt[n]{a})^{n/2^s})$, where $2^s\,\|\,n$.

(iii) If $\pm a$ is not a power of 2, then, in a similar way as in (i), we have $k_0=\boldsymbol{Q}((\sqrt[n]{a})^{n/2})=\boldsymbol{Q}(\sqrt{a})$.

(iv) If $\pm a$ is a power of 2, then, also in a similar way as in (ii), we have $k_0=\boldsymbol{Q}(\sqrt{\pm 2})=\boldsymbol{Q}(\sqrt{a})$ (cf. Theorem and §3 of [3]).

COROLLARY. *As for the maximal abelian subfield k_0 of $K=\boldsymbol{Q}(\sqrt[n]{a})$, we have*

$$k_0=\begin{cases}\boldsymbol{Q} & \text{if } n \text{ is odd,}\\ \boldsymbol{Q}(\sqrt{a}) & \text{if } n \text{ is even}\,.\end{cases}$$

So the genus number $g_k=[K^*\colon K]$ of K is given as follows:

$$g_K=\prod_{p\,|\,a}(n, p-1)\times\begin{cases}1 \text{ if } n \text{ is odd,}\\ 1/2 \text{ if } n \text{ is even, } a\equiv 1(\mathrm{mod}\, 4),\\ 1 \text{ if } n \text{ is even, } a\equiv 0(\mathrm{mod}\, 2),\\ 2^{d-2} \text{ with } d=\mathrm{Min}\,(N, s+1) \text{ if } n \text{ is even}\\ \qquad (2^s\,\|\,n),\ a\equiv 3(\mathrm{mod}\, 4) \text{ and } 2^N\,\|\,a+1\,.\end{cases}$$

§6. Remarks.

We prove our Theorem and Corollary under the assumption that a

* Of course, as for subfields of pure field extensions, more general results are obtained by algebraic considerations (without the property $(*)$) (a private communication of Prof. Endo).

has the property $(*)$. However, without this assumption, we can obtain some information on the genus fields of pure number fields.

For example, we treat the case

$$K=\boldsymbol{Q}(\sqrt[n]{a}) \quad \text{where} \quad (a, n)=1 \quad \text{and} \quad [K:\boldsymbol{Q}]=n$$

(without the property $(*)$ of a). Let

$$n=q_0^{s_0}q_1^{s_1}\cdots q_t^{s_t} \qquad (s_0\geqq 0;\ s_1, \cdots, s_t>0)\ ,$$

where $q_0=2$ and q_i are odd primes, and put

$$K_i=\boldsymbol{Q}((\sqrt[n]{a})^{n/q_i^{s_i}}) \qquad (i=0, 1, \cdots, t)\ .$$

As $[K:\boldsymbol{Q}]=n$, we have $[K_i:\boldsymbol{Q}]=q_i^{s_i}$. We denote by k^* and $k^{(i)*}$ the maximal abelian subfields of the genus fields of K and K_i respectively. Then we have

$$k^*=k^{(0)*}\cdot k^{(1)*}\cdot\cdots\cdot k^{(t)*}$$

(cf. [2]).

Now, for the simplicity, put, for a fixed $i(0\leqq i\leqq t)$,

$$L=K_i\ , \qquad q=q_i\ , \qquad s=s_i \quad \text{and} \quad k'^*=k^{(i)*}\ .$$

First, let $k_2'^*$ be the maximal subfield of k'^* such that $k_2'^*\subset\boldsymbol{Q}(\zeta_{q^M})$ for some M. Here note that $q\nmid a$. If $q\neq 2$, then the results of cases (2) and (3) in §2 of [3] also hold and so we have $k_2'^*=\boldsymbol{Q}$. If $q=q_0=2$, then the results of case (1) in §3 of [3] and of §1 also hold and so we have $k_2'^*=\boldsymbol{Q}$ for $a\equiv 1 (\mathrm{mod}\ 4)$ and $k_2'^*=\boldsymbol{Q}(\zeta_{2^d})$ with $d=\mathrm{Min}\,(N, s+1)$ for $a\equiv 3 (\mathrm{mod}\ 4)$ $(2^N \| a+1,\ s=s_0)$. Next, we determine, for a prime divisor p of a, the greatest common divisor $e(p)$ of the ramification indices of all the prime divisors of p in L: $e(p)=(e_1, \cdots, e_g)$ where $(p)=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$ in L. Let $a=p^v b$ $(p\nmid b)$ and $v=q^c w$ $(q\nmid w)$. Clearly $a^{1/q^s}=p^{q^c w/q^s}\cdot b^{1/q^s}$. So, if $s\leqq c$, we have $L=\boldsymbol{Q})\sqrt[q^s]{b})$ and, as $p\nmid b$ $(p\neq q)$, p is unramified in L; and so we have $e(p)=1$. If $s>c$, we see easily that p is unramified in $L_1=\boldsymbol{Q}((\sqrt[q^s]{a})^{q^{s-c}})=\boldsymbol{Q}(\sqrt[q^c]{b})$ $((p)=\mathfrak{p}_1\cdots\mathfrak{p}_g$ in $L_1)$ and L is of Eisenstein type with respect to each $\mathfrak{p}_i(i=1, \cdots, g)$. So $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ are totally ramified in L and we have $e(p)=[L:L_1]=q^{s-c}$. Hence k'^* is obtained as

$$k'^*=\prod_{p|a}\{\text{the subfield, of degree } (q^{s-\mathrm{Min}\,(s,c)}, p-1), \text{ of } \boldsymbol{Q}(\zeta_p)(p^v\|a,\ q^c\|v)\} \\ \times k_2'^* \qquad \text{(composite)}$$

(cf. Chapter 4 in [2]).

Therefore we have the following assertion: Let K, n, a and k^* be as above. For a prime divisor p of a, let

$$p^v \| a \quad \text{and} \quad v = q_0^{c_0} q_1^{c_1} \cdots q_t^{c_t} u \qquad ((u, n) = 1,\ c_i \geqq 0)$$

and put

$$k^*(p) = \text{the subfield, of degree } \left(\prod_{i=0}^{t} q_i^{s_i - \mathrm{Min}\,(s_i, c_i)},\ p-1 \right), \text{ of } \boldsymbol{Q}(\zeta_p)\ .$$

Then we have

$$k^* = k_1^* \cdot k_2^*\ ,$$

where

$$k_1^* = \prod_{p \mid a} k^*(p) \qquad \text{(composite)}$$

and

$$k_2^* = \begin{cases} \boldsymbol{Q}(\zeta_{2^d}) & \text{if } n \text{ is even, } a \equiv 3 (\mathrm{mod}\ 4)\ (d = \mathrm{Min}\,(N, s_0 + 1), \\ & \qquad 2^N \| a + 1)\ , \\ \boldsymbol{Q} & \text{otherwise}\ . \end{cases}$$

References

[1] E. HECKE, Vorlesungen über die Theorie der Algebraischen Zahlen, Chelsea, New York, 1948 (Satz 119).

[2] M. ISHIDA, The genus fields of algebraic number fields, Lecture Notes in Math., **555**, Springer, Berlin-Heidelberg-New York, 1976.

[3] M. ISHIDA, On the genus fields of pure number fields, Tokyo J. Math., **3** (1980), 177-185.

Present Address:
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCES
TOKYO METROPOLITAN UNIVERSITY
FUKAZAWA, SETAGAYA-KU, TOKYO 158