TOKYO J. MATH.
VOL. 3, NO. 1, 1980

On the Genus Fields of Pure Number Fields

Makoto ISHIDA

Tokyo Metropolitan University

In this paper, we shall investigate the genus fields of pure number fields $K=\boldsymbol{Q}(\sqrt[n]{a})$ with $a\in\boldsymbol{Z}$. In the case of odd n, the genus fields of such number fields K are explicitly determined in Fröhlich [1] and Ishida [3]. On the other hand, in the case of even n, the situations are somewhat complicated, as is expected from the genus theory of quadratic number fields. Here we shall show some partial results for the even degree cases and also give a new elementary proof for the odd degree cases. As for the definitions and some fundamental properties of genus fields, see Ishida [3].

§ 1. Preliminaries.

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. Then, of course, the degree of K over $\boldsymbol{Q}$ is n. Let

$$n=q_0^{s_0}q_1^{s_1}q_2^{s_2}\cdots q_t^{s_t}\quad(s_0\geqq0;\ s_1,\ s_2,\ \cdots,\ s_t>0)\ ,$$

where $q_0=2$ and q_i $(i=1,\,2,\,\cdots,\,t)$ are odd primes, and put

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

Then we have

$$K=K_0\cdot K_1\cdot K_2\cdot\ \cdots\ \cdot K_t\quad\text{(composite)}\ .$$

Now let K^* be the genus field of K and k^* the maximal abelian subfield of K^*: $K^*=k^*K$. Also let $k^{(i)*}$ $(i=0,\,1,\,\cdots,\,t)$ be the maximal abelian subfield of the genus field of K_i. Since the degrees of K_i over $\boldsymbol{Q}$ are coprime to each other, we have

Received September 4, 1979

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

(cf. Proposition 2 in [3]). We denote by ζ_m a primitive m-th root of unity. Then $k^{(t)*}$ is obtained as the composite of two abelian subfields $k_1^{(t)*}$ and $k_2^{(t)*}$:

$$k^{(t)*}=k_1^{(t)*}\cdot k_2^{(t)*}\quad (k_1^{(t)*}\cap k_2^{(t)*}=\boldsymbol{Q})$$

(cf. Chapter 4 in [3]). Here

$$k_1^{(t)*}=\prod_{p\mid a,\,p\neq q_i}\{\text{the subfield, of degree } (q_i^{e_i}, p-1), \text{ of the cyclotomic number field } \boldsymbol{Q}(\zeta_p)\}\ \text{(composite)}$$

and, of course, the restrictions $p\neq q_i$ can be removed. On the other hand, as the degree $q_i^{e_i}$ of K_i is a power of prime q_i,

$$k_2^{(t)*}=\text{a subfield of the cyclotomic number field } \boldsymbol{Q}(\zeta_{q_i^r}) \text{ for some } r\in\boldsymbol{Z}\,.$$

Considering the ramification indices of q_i in $k_2^{(t)*}$ and K_i, we see easily that the degree $[k_2^{(t)*}:\boldsymbol{Q}]$ is a power of q_i. Therefore our problem is to decide k_2^* in special cases $n=q^e$ (q is an odd prime) and $n=2^e$ respectively.

§ 2. The case $n=q^e$.

Let q be an odd prime and let $K=\boldsymbol{Q}(\alpha)$, where $\alpha=\sqrt[q^e]{a}$ and $a\in\boldsymbol{Z}$ has the property (*) for $n=q^e$ (cf. Fröhlich [1] and Ishida [3]).

Then k_2^* is a subfield of $\boldsymbol{Q}(\zeta_{q^r})$ for some r and the degree $[k_2^*:\boldsymbol{Q}]$ is a power of q. So, for the unique subfield k_0, of degree q, of the cyclotomic number field $\boldsymbol{Q}(\zeta_{q^2})$, we see that

$$\begin{aligned}k_2^*=\boldsymbol{Q} &\Longleftrightarrow k_2^*\not\supset k_0\\ &\Longleftrightarrow k_0K \text{ is not unramified over } K\,.\end{aligned}$$

On the other hand, in the sense of class field theory, the absolute abelian field k_0 corresponds to the ideal group

$$H_q=\{(a)\,|\,(a,q)=1,\ a^{q-1}\equiv 1(\mathrm{mod}^{\times} q^2)\}$$

in $\boldsymbol{Q}$, with defining modulus q^2. Accordingly, by the 'Verschiebungssatz', we see

$$k_0K \text{ is unramified over } K\Longleftrightarrow \text{for any number } \gamma \text{ in } K, \text{ prime to } q,\ (N_{K/\boldsymbol{Q}}\gamma)^{q-1}\equiv 1(\mathrm{mod}^{\times} q^2)\,.$$

Now we consider the three cases separately. Here we denote by N the norm mapping $N_{K/Q}$. (For the cases (1) and (2), the same proofs are already given in [3].)

(1) $q|a$. By (*), we have $q^v \| a$ with $(v, q)=1$ and so there are $x, y \in \boldsymbol{Z}$ $(1 \leqq x \leqq q^s-1, y \geqq 0)$ such that $vx=1+q^s y$. Then $\beta=\alpha^x/q^y$ is an integer of K and $\beta^{q^s}=b \in \boldsymbol{Z}$ with $q \| b$. Put

$$\gamma=1+\beta \in K .$$

Then we have $N\gamma=1+b$ and so

$$(N\gamma)^{q-1} \equiv 1+(q-1)b \equiv 1-b \not\equiv 1 \pmod{q^2} .$$

(2) $q \| a^{q-1}-1$. Put

$$\gamma=\alpha \in K .$$

Then we have $N\gamma=a$ and so

$$(N\gamma)^{q-1}=a^{q-1} \not\equiv 1 \pmod{q^2} .$$

(3) $q^2 | a^{q-1}-1$. Note that, for $c \in \boldsymbol{Z}$ with $(c, q)=1$, $c^{q-1} \equiv 1 \pmod{q^2}$ is equivalent to $c \equiv d^q \pmod{q^2}$ for some $d \in \boldsymbol{Z}$.

LEMMA 1. *There is an integer u such that*

$$1+u^q \not\equiv y^q \pmod{q^2}$$

for any $y \in \boldsymbol{Z}$. (Of course, then u is prime to q.)

PROOF. Suppose that, for any $x \in \boldsymbol{Z}$, $1+x^q \equiv y^q \pmod{q^2}$ with some $y \in \boldsymbol{Z}$. Then, putting $S=\{x^q \pmod{q^2} \mid x \in \boldsymbol{Z}\}$, we can define an injective mapping

$$f: x^q \pmod{q^2} \longmapsto 1+x^q \pmod{q^2}$$

of the finite set S to itself. Then f is bijective and so is $f^q=f \circ f \circ \cdots \circ f$. Accordingly we have $0^q \pmod{q^2}=q+x^q \pmod{q^2}$ for some $x \in \boldsymbol{Z}$, which implies $q|x$ and so $q^2|q$. This is a contradiction.

In (3), we have $a \equiv t^q \pmod{q^2}$ for some $t \in \boldsymbol{Z}$. Let u be the integer in Lemma 1 and $v \in \boldsymbol{Z}$ a solution of $vt \equiv u \pmod{q^2}$. Put

$$\gamma=1+v\alpha \in K .$$

Then we have $N\gamma=1+v^{q^s}a$ and so

$$N\gamma \equiv 1+v^q a \equiv 1+v^q t^q \equiv 1+u^q \not\equiv y^q \pmod{q^2}$$

for any $y \in Z$. So we have

$$(N\gamma)^{q-1} \not\equiv 1 \pmod{q^2} .$$

Hence, for any case, there exists an integer γ of K such that

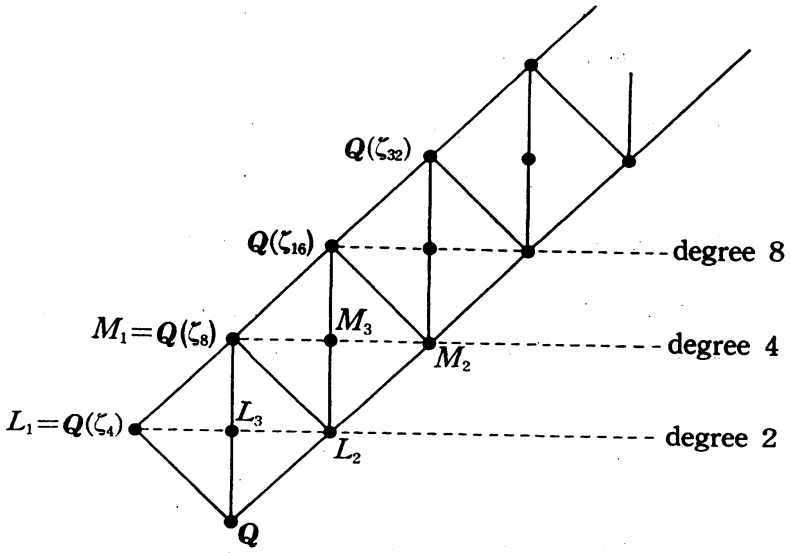
$$\gamma \text{ is prime to } q \text{ and } (N_{K/Q}\gamma)^{q-1} \not\equiv 1 \pmod{q^2} .$$

This implies that k_0K is not unramified over K and so we have

$$k_2^* = Q .$$

§ 3. The case $n=2^s$.

Let $K=Q(\alpha)$, where $\alpha=\sqrt[2^s]{a}$ and $a \in Z$ has the property (*) for $n=2^s$. Then k_2^* is a subfield of the cyclotomic number field $Q(\zeta_{2^r})$ for some r and the degree $[k_2^*: Q]$ is a power of 2. So we consider all the subfields, of $Q(\zeta_{2^r})(r=0, 1, 2, \cdots)$, of degree $2^0=1, 2, 2^2, \cdots$. They are easily listed up and illustrated by dots explicitly in the following diagram.



$L_1=Q(\sqrt{-1})$,
$L_2=Q(\sqrt{2})$=the maximal real subfield of $Q(\zeta_8)$,
$L_3=Q(\sqrt{-2})$,
$M_2=Q(\zeta_{16}+\zeta_{16}^{-1})$=the maximal real subfield of $Q(\zeta_{16})$,
$M_3=Q(\zeta_{16}-\zeta_{16}^{-1})$.

That is, there are three such fields of degree 2 and also three such fields

of degree 4. Moreover, in the sense of class field theory, they correspond to the ideal groups respectively, in Q, with defining modulus $16p_\infty$ (p_∞= the infinite prime of Q), as is shown in the following table.

field	ideal gruop $\{(a)\}$ with $a\equiv$
$Q(\zeta_{16})$	1
$M_1=Q(\zeta_8)$	1, 9
M_2	1, 15
M_3	1, 7
$L_1=Q(\zeta_4)$	1, 5, 9, 13
$L_2=Q(\sqrt{2})$	1, 7, 9, 15
$L_3=Q(\sqrt{-2})$	1, 3, 9, 11
Q	1, 3, 5, 7, 9, 11, 13, 15

Then, by the 'Verschiebungssatz', we see that, for example,

$M_2\subset k_2^* \Longleftrightarrow M_2K$ is unramified over K (in narrow sense) $\Longleftrightarrow$ for any totally positive number γ in K, prime to 2, $N_{K/Q}\gamma\equiv 1$ or $15(\mathrm{mod}^\times 16p_\infty)$.

Of course, if $k_2^*\neq Q$ i.e., $[k_2^*: Q]>1$ then k_2^* contains at least one of L_i ($i=1, 2, 3$). Also, if $[k_2^*: Q]>2$ then k_2^* contains at least one of M_i ($i=1, 2, 3$). On the other hand, for even a, by (*), we have $2^v\| a$ with odd v and so there are $x, y\in Z$ ($1\leqq x\leqq 2^s-1$, $y\geqq 0$) such that $vx=1+2^sy$. Then $\beta=\alpha^x/2^v$ is an integer of K and $\beta^{2^s}=b\in Z$ with $2\| b$. Writing $a=2^vc$, we have $b=2c^x$ and so

$$c\equiv 1(\mathrm{mod}\ 4)\Longleftrightarrow b\equiv 2(\mathrm{mod}\ 8),$$
$$c\equiv 3(\mathrm{mod}\ 4)\Longleftrightarrow b\equiv 6(\mathrm{mod}\ 8).$$

For odd a, we put $\beta=\alpha$ ($x=1$) and $b=a$. Then the classical genus theory and the fact $Q(\sqrt{b})\subset Q(\alpha)=K$ show that

$$b(=a)\equiv 3(\mathrm{mod}\ 4)\Longrightarrow k_2^*\supset L_1,$$
$$b\equiv 2(\mathrm{mod}\ 8)\Longrightarrow k_2^*\supset L_2,$$
$$b\equiv -2(\mathrm{mod}\ 8)\Longrightarrow k_2^*\supset L_3.$$

Now put

$$\gamma_1=A+\beta\quad (A\in Z)\quad\text{and}\quad \gamma_2=1+\beta^2+\beta\in K,$$

where A is so large that γ_1 is totally positive. Note that γ_2 is totally positive. Then we have $N_{K/Q}\gamma_1=A^{2^s}-b$.

LEMMA 2. *We have* $N_{K/Q}\gamma_2=1+b+b^2$.

PROOF. Let $K'=Q(\alpha^2)$. Then, as $\beta=\alpha^x/2^y$ with odd x, we have $N_{K/K'}\gamma_2=(1+\beta^2+\beta)(1+\beta^2-\beta)=1+\beta^4+\beta^2$. Accordingly lemma is proved by the induction on s.

We consider the five cases separately. Here we denote by N the norm mapping $N_{K/Q}$.

(1) $a=b\equiv 1(\mathrm{mod}\ 4)$. Choose as A a large integer divisible by 16 and so we have $N\gamma_1\equiv -a(\mathrm{mod}\ 16)$. If $a\equiv 1(\mathrm{mod}\ 16)$ then $N\gamma_1\equiv 15(\mathrm{mod}\ 16p_\infty)$ and $N\gamma_2\equiv 3(\mathrm{mod}\ 16p_\infty)$. Consequently the above table implies that k_2^* contains none of L_i $(i=1, 2, 3)$ and so we have $k_2^*=Q$. In similar ways,

$$a\equiv 5(\mathrm{mod}\ 16)\Longrightarrow N\gamma_1\equiv 11,\ N\gamma_2\equiv 15(\mathrm{mod}\ 16p_\infty)\Longrightarrow k_2^*=Q\ ,$$
$$a\equiv 9(\mathrm{mod}\ 16)\Longrightarrow N\gamma_1\equiv 7,\ N\gamma_2\equiv 11(\mathrm{mod}\ 16p_\infty)\Longrightarrow k_2^*=Q\ ,$$
$$a\equiv 13(\mathrm{mod}\ 16)\Longrightarrow N\gamma_1\equiv 3,\ N\gamma_2\equiv 7(\mathrm{mod}\ 16p_\infty)\Longrightarrow k_2^*=Q\ .$$

Hence we have

$$k_2^*=Q \quad \text{if} \quad a\equiv 1(\mathrm{mod}\ 4)\ .$$

(2) $2|a$ and $b\equiv 2(\mathrm{mod}\ 8)$. Choose as A a large integer such that $A^{2^s}\equiv 1(\mathrm{mod}\ 16)$ and so we have $N\gamma_1\equiv 1-b(\mathrm{mod}\ 16)$. If $b\equiv 2(\mathrm{mod}\ 16)$ then $N\gamma_1\equiv 15(\mathrm{mod}\ 16p_\infty)$ and $N\gamma_2\equiv 7(\mathrm{mod}\ 16_\infty)$. Consequently the above table implies that k_2^* contains none of M_i $(i=1, 2, 3)$. On the other hand, as is remarked above, k_2^* contains $L_2=Q(\sqrt{2})$. So we have $k_2^*=L_2$. In a similar way,

$$b\equiv 10(\mathrm{mod}\ 16)\Longrightarrow N\gamma_1\equiv 7,\ N\gamma_2\equiv 15(\mathrm{mod}\ 16p_\infty)\Longrightarrow k_2^*=L_2\ .$$

Hence we have

$$k_2^*=L_2=Q(\sqrt{2}) \quad \text{if} \quad b\equiv 2(\mathrm{mod}\ 8)\ .$$

(3) $2|a$ and $b\equiv -2(\mathrm{mod}\ 8)$. Choose as A a large integer such that $A^{2^s}\equiv 1(\mathrm{mod}\ 16)$. Then also in similar ways as in (2),

$$b\equiv 6(\mathrm{mod}\ 16)\Longrightarrow N\gamma_1\equiv 11(\mathrm{mod}\ 16p_\infty)\Longrightarrow k_2^*=L_3\ ,$$
$$b\equiv 14(\mathrm{mod}\ 16)\Longrightarrow N\gamma_1\equiv 3(\mathrm{mod}\ 16p_\infty)\Longrightarrow k_2^*=L_3\ .$$

Hence we have

$$k_2^*=L_3=Q(\sqrt{-2}) \quad \text{if} \quad b\equiv -2(\mathrm{mod}\ 8)\ .$$

(4) $a=b\equiv 3 \pmod 8$. Choose as A a large integer divisible by 16 and so we have $N\gamma_1\equiv -a \pmod{16}$. Then also in similar ways as in (2),

$$a\equiv 3 \pmod{16} \Longrightarrow N\gamma_1\equiv 13 \pmod{16p_\infty} \Longrightarrow k_2^*=L_1 ,$$
$$a\equiv 11 \pmod{16} \Longrightarrow N\gamma_1\equiv 5 \pmod{16p_\infty} \Longrightarrow k_2^*=L_1 .$$

Hence we have

$$k_2^*=L_1=Q(\zeta_4)=Q(\sqrt{-1}) \quad \text{if} \quad a\equiv 3 \pmod 8 .$$

(5) Then the remaining case is $a\equiv 7 \pmod 8$. In this case, $\alpha+1=\sqrt[2^s]{a}+1$ is a root of the Eisenstein polynomial $(X-1)^{2^s}-a$ with respect to 2. So 2 is totally ramified in $K=Q(\alpha)$. Now we have the following

LEMMA 3. *If $s=2$ and $K=Q(\sqrt[4]{a})$ $(a\equiv 7 \pmod 8)$, then we have*

$$k_2^*=Q(\zeta_8)(=M_1) .$$

PROOF. By considering the degrees of K and $M_1=Q(\zeta_8)$, it suffices to prove that M_1K is unramified over K. Since we have $M_1K=(M_1(\sqrt{a}))(\sqrt[4]{a})$ and

$$\sqrt{a}-\frac{(\sqrt{a}+1)^2}{(\zeta_8+\zeta_8^{-1})^2}=\frac{2\sqrt{a}-(a+2\sqrt{a}+1)}{2}=\frac{-(a+1)}{2}\equiv 0 \pmod 4 ,$$

any prime ideal, dividing 2, in $M_1(\sqrt{a})$ is unramified in M_1K (cf. Hilbert [2]). Then it is easily seen that M_1K is unramified over K.

Hence, for general case $s\geqq 2$ with $a\equiv 7 \pmod 8$, it is shown that $Q(\zeta_8)K$ is unramified over K (in narrow sense) and so we have

$$k_2^*\supset Q(\zeta_8) .$$

We note that $Q(\zeta_{16})$ is the only extension of $Q(\zeta_8)$, of degree 8 over Q, in the above diagram. On the other hand, choosing as A a large integer divisible by 16, we have $N\gamma_1\equiv -a \pmod{16}$. Consequently if $a\equiv 7 \pmod{16}$ and $s\geqq 2$ then we have $k_2^*\not\supset Q(\zeta_{16})$ and so

$$k_2^*=M_1=Q(\zeta_8) .$$

Of course, if $a\equiv 7 \pmod{16}$ and $s=1$ then we have $k_2^*=L_1=Q(\sqrt{-1})$. The cases $a\equiv 15 \pmod{16}$ and $s\geqq 3$ is still open.

§ 4. Conclusion.

Combining the results of § 1, § 2 and § 3, we can determine the genus

field K^* of a pure number field $K=\boldsymbol{Q}(\sqrt[n]{a})$, except the case $2^3|n$ and $a\equiv 15 \pmod{16}$. (In Theorem 7 of [3], the restrictions $p\neq q_i$ are unnecessary and must be removed (cf. §1).)

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

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

for any prime divisor p of a. Then the maximal abelian subfield k^* of the genus field K^* of K is given as follows $(K^*=k^*K)$:

$$k^*=k_1^*\cdot k_2^* \quad (\textit{composite}),$$

where

$$k_1^*=\prod_{p|a} \{\textit{the subfield, of degree } (n, p-1), \textit{ of the cyclotomic number field } \boldsymbol{Q}(\zeta_p)\} \quad (\textit{composite})$$

and

k_2^*	n	a
$\boldsymbol{Q}$	odd	
	even	$a\equiv 1 \pmod 4$
$\boldsymbol{Q}(\sqrt{2})$	even	$2^v \| a$ $(v>0)$ and $a/2^v\equiv 1 \pmod 4$
$\boldsymbol{Q}(\sqrt{-2})$	even	$2^v \| a$ $(v>0)$ and $a/2^v\equiv 3 \pmod 4$
$\boldsymbol{Q}(\sqrt{-1})$	even	$a\equiv 3 \pmod 8$
	$2\|\|n$	$a\equiv 7 \pmod 8$
$\boldsymbol{Q}(\zeta_8)$	$2^2\|n$	$a\equiv 7 \pmod{16}$
	$2^2\|\|n$	$a\equiv 15 \pmod{16}$
$?(\supset \boldsymbol{Q}(\zeta_8))$	$2^3\|n$	$a\equiv 15 \pmod{16}$

References

[1] A. FRÖHLICH, The genus field and genus group in finite number fields II, Mathematika, **6** (1959), 142-146.

[2] D. HILBERT, Über die Theorie des relativquadratischen Zahlkörpers, Math. Ann., **51** (1898), 1-127 (Satz 5).

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

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