K. TAKASE
KODAI MATH. J.
5 (1982), 482—494

SOME REMARKS ON THE RELATIVE GENUS FIELDS

BY KOICHI TAKASE

§ 1. Introduction.

Let k be a finite algebraic number field and K its finite extension. We denote by K^* the maximal abelian extension of k such that the composite field K^*K is unramified over K at all the finite or infinite primes, and the field K^*K is called the genus field of K with respect of k. (If K^* were defined as the maximal abelian extension of k such that K^*K was unramified over K at all the finite primes, the field K^*K was called the narrow genus field of K. We do not treat the narrow genus field in this paper.)

The field K^* is explicitly determined when k is the rational number field (see M. Ishida [5], [6] or M. Bhaskaran [1]). In § 3 of this paper we discuss the fundamental structure of K^* for general k. In § 4 we treat, as an example, the case of k=quadratic field of class number one in which 2 remains prime and $(K:k)=2$.

In § 5 we prove the following theorem; let k be a finite algebraic number field of class number one, G any finite abelian group, and m a positive integer such that $ex(G)|m$ and $m\|G|^{\infty}$. Then there exist infinitely many cyclic extensions F of k of degree m such that

$$C_F/C_F^{1-\sigma}\cong G(F^*/F)\cong G\,.$$

This paper contains the author's master thesis at Tokyo Institute of Technology (1981, March).

§ 2. Definitions.

Let k be a finite algebraic number field and K its finite extension. We denote by K^* the maximal abelian extension of k such that K^*K is unramified over K at all the finite or infinite primes. By the class field theory, K^* is the maximal abelian extension of k in the Hilbert class field of K, and $K^*\cap K$ is the maximal abelian extension of k in K. Throughout this paper the following notations are used;

O_k: the integer ring of k
U_k: the unit group of k

Received November 5, 1981

$\phi(\mathfrak{a})$: the Euler function of k
$U_k(\mathfrak{a})=\{\varepsilon\in U_k \mid \varepsilon\equiv 1 \pmod{\mathfrak{a}}\}$, for an integral ideal $\mathfrak{a}$ of k
$k_\mathfrak{p}$: the completion of k at a finite or infinite prime $\mathfrak{p}$ of k
$k_A^\times$: the idele group of k into which we embed $k^\times$ and $k_\mathfrak{p}^\times$ in usual way
$k^{(1)}$ the Hilbert class field of k
$G(K/k)$: the Galois group of Galois extension K/k
$\mathfrak{f}(K/k)$: the conductor of abelian extension K/k.

§ 3. Structure of genus field.

Let k be a finite algebraic number field, K its finite extension, and fix them. For a finite prime $\mathfrak{p}$ of k, we put

$$\mathfrak{p}=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}\ (\mathfrak{P}_1, \cdots, \mathfrak{P}_r\text{: distinct primes of } K,\ e_j>0)$$

$$e_K(\mathfrak{p})=\text{g. c. d. } \{e_1, \cdots, e_r\}\ , \quad g_k(\mathfrak{p})=\phi(\mathfrak{p})/(U_k : U_k(\mathfrak{p}))\ ,$$

$$d_K(\mathfrak{p})=\text{g. c. d. } \{e_K(\mathfrak{p}), g_k(\mathfrak{p})\}\ .$$

Let $S(\mathfrak{p})$ be the ray class field modulo $\mathfrak{p}$ of k. Then $S(\mathfrak{p})/k^{(1)}$ is a cyclic extension of degree $g_k(\mathfrak{p})$, and we put

$k(\mathfrak{p})$: unique intermediate field of $S(\mathfrak{p})/k^{(1)}$ such that $(k(\mathfrak{p}) : k^{(1)})=d_K(\mathfrak{p})$.

Then we have

LEMMA 1. *$k(\mathfrak{p})\subset K^*$ for any finite prime $\mathfrak{p}$ of k.*

Proof. This lemma is proved in [4]. Another proof using Abhyanker's lemma is given in [3].

We define two subfield K_1^* and K_2^* of K^* by

$$K_1^*=\prod_{\mathfrak{p}} k(\mathfrak{p})\text{: composite field, } K_2^*=\bigcap_{\mathfrak{p}} T(\mathfrak{p}),$$

where $\mathfrak{p}$ runs over all finite primes of k such that $e_K(\mathfrak{p})\mid g_k(\mathfrak{p})$, and $T(\mathfrak{p})$ is the inertia field of $\mathfrak{p}$ in K^*/k. Notice that, for distinct finite primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ of k, the fields $k(\mathfrak{p}_1), \cdots, k(\mathfrak{p}_r)$ are linearly disjoint over $k^{(1)}$. Then we have

THEOREM 2.
$$K_1^*\cap K_2^*=k^{(1)}\ , \quad K^*=K_1^*K_2^*\ .$$

Proof. Because the primes of k which are ramified in K_1^* are unramified in K_2^*, the field $K_1^*\cap K_2^*$ is an unramified abelian extension of k. Hence we have $K_1^*\cap K_2^*=k^{(1)}$, since $K_1^*\cap K_2^*$ contains $k^{(1)}$.

Because K^*K/K is unramified, we have $e_{K^*}(\mathfrak{p})\mid e_K(\mathfrak{p})$ for any finite prime $\mathfrak{p}$ of k. Then we have the following inequalities from which the equality

$K^*=K_1^*K_2^*$ follows;

$$(K_1^*:k^{(1)})=(K_1^*K_2^*:K_2^*)\leqq(K^*:K_2^*)\leqq\prod_{\mathfrak{p}}(K^*:T(\mathfrak{p}))$$
$$\leqq\prod_{\mathfrak{p}}(k(\mathfrak{p}):k^{(1)})=(K_1^*:k^{(1)})$$

On the conductor of abelian extension K^*/k, we have the following theorem:

THEOREM 3. *Suppose that K is a normal extension of k. Then $\mathfrak{f}(K^*/k)=\mathfrak{f}(K^*\cap K/k)$. (Notice that the field $K^*\cap K$ is the maximal abelian extension of k in K.)*

Proof. Put $U=\prod_{\mathfrak{P}}U_{\mathfrak{P}}$ the unit idele group of K, where $\mathfrak{P}$ runs over all finite or infinite primes of K and $U_{\mathfrak{P}}$ is the unit group of $K_{\mathfrak{P}}$. Then, by the class field theory, we have

$K^*=$the class field of k corresponding to $k^\times N_{K/k}U$,
$K^*\cap K=$the class field of k corresponding to $k^\times N_{K/k}K_A^\times$.

Since K is normal over k, we have

$$N_{K/k}U=\prod_{\mathfrak{p}}N_{\mathfrak{P}/\mathfrak{p}}U_{\mathfrak{P}}\,,\quad N_{K/k}K_A^\times=k_A^\times\cap\prod_{\mathfrak{p}}N_{\mathfrak{P}/\mathfrak{p}}K_{\mathfrak{P}}^\times$$

where $\mathfrak{p}$ runs over all the finite or infinite primes of k, $\mathfrak{P}$ is any one of the primes of K lying over $\mathfrak{p}$, and $N_{\mathfrak{P}/\mathfrak{p}}$ is the norm from $K_{\mathfrak{P}}$ to $k_{\mathfrak{p}}$. Because the inverse image of $U_{\mathfrak{p}}$ by $N_{\mathfrak{P}/\mathfrak{p}}$ is contained in $U_{\mathfrak{P}}$, we have $\mathfrak{f}(K^*/k)=\mathfrak{f}(K^*\cap K/k)$.

COROLLARY 4. *Suppose that K is a normal extension of k. Then $K_*=K_1^*$ if and only if $K^*\cap K/k$ is unramified at the infinite primes and $e_K(\mathfrak{p})\,|\,g_k(\mathfrak{p})$ for any finite prime $\mathfrak{p}$ of k ramified in $K^*\cap K$.*

Proof. Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be the finite primes of k such that $e_K(\mathfrak{p}_j)\,|\,g_k(\mathfrak{p}_j)$ and $e_K(\mathfrak{p}_j)>1$. Then we have $\mathfrak{f}(K_1^*/k)=\mathfrak{p}_1\cdots\mathfrak{p}_r$. Because $\mathfrak{f}(K_1^*/k)$ and $\mathfrak{f}(K_2^*/k)$ are relatively prime and K^* is the composite field of K_1^* and K_2^*, we have $\mathfrak{f}(K^*k)=\mathfrak{f}(K_1^*/k)\mathfrak{f}(K_2^*/k)$. Because $K_1^*\cap K_2^*$ is equal to $k^{(1)}$ and K_2^* contains $k^{(1)}$, $K^*=K_1^*$ if and only if $\mathfrak{f}(K_2^*/k)=1$, that is, if and onlf if $\mathfrak{f}(K^*/k)\,|\,\mathfrak{f}(K_1^*/k)$. Hence, because of Theorem 3, $K^*=K_1^*$ if and only if $\mathfrak{f}(K^*\cap K/k)\,|\,\mathfrak{f}(K_1^*/k)$, and only-if-part of the assertion is proved.

If $K^*\cap K/k$ is unramified at the infinite primes and $e_K(\mathfrak{p})\,|\,g_k(\mathfrak{p})$ for any finite prime $\mathfrak{p}$ of k which is ramified in $K^*\cap K/k$, $K^*\cap K$ is tamely ramified over k at the finite primes and hence $\mathfrak{f}(K^*\cap K/k)$ is square-free. Because the set $\{\mathfrak{p}_1,\cdots,\mathfrak{p}_r\}$ includes the prime factors of $\mathfrak{f}(K^*\cap K/k)$ by hypothesis, we have $\mathfrak{f}(K^*\cap K/k)\,|\,\mathfrak{f}(K_1^*/k)$.

PROPOSITION 5. *Suppose that K is an abelian extension of k which is unramified over k at the infinite primes and that there exists ouly one finite prime*

$\mathfrak{p}$ of k such that $e_K(\mathfrak{p}) \nmid g_k(\mathfrak{p})$. Then we have

$$K^* = K_1^* K, \quad K_1^* \cap K = \text{the inertia field of } \mathfrak{p} \text{ in } K/k.$$

Proof. Since $\mathfrak{p}$ is unique prime of k which may be ramified in K_2^*, $\mathfrak{p}$ is totally ramified in $K_2^*/k^{(1)}$. Because K^*K is unramified over K, we have $(K_2^*: k^{(1)}) | e_K(\mathfrak{p})$. As $\mathfrak{p}$ is unramified in $K_1^* \cap K$, we have

$$K_1^* \cap K \subset T = \text{the inertia field of } \mathfrak{p} \text{ in } K/k.$$

Therefore we have the following inequalities from which our assertion follows;

$$\begin{aligned}(K_1^*: k) &= (K_1^* K: K)(K_1^* \cap K: k) \\ &\leqq (K^*: K)(T: k) \\ &= (K_1^*: k^{(1)})(K_2^*: k^{(1)})(k^{(1)}: k)/(K.T) \leqq (K_1^*: k).\end{aligned}$$

In Proposition 5 the uniqueness of prime $\mathfrak{p}$ of k such that $e_K(\mathfrak{p}) \nmid g_k(\mathfrak{p})$ is indispensable as the following example shows:

EXAMPLE. Put $k = Q(\sqrt{-11})$. The polynomial $f(X) = X^3 - 3X - 1$ is irreducible over k. Let α be a root of $f(X) = 0$ and put $K = k(\alpha)$. Then K is a cyclic extension of k of degree 3 and the relative discriminant of K over k is $D(K/k) = 3^4$. The prime factors $D(K/k)$ in k are $1+\omega$ and ω where $\omega = (1+\sqrt{-11})/2$. Since $g_k(1+\omega) = g_k(\omega) = 1$, $e_K(1+\omega) = e_K(\omega) = 3$, we have

$$K_1^* = k.$$

On the other hand, by the genus number formula proved in [2], we have

$$(K^*: k) = 9.$$

For the latter use, we prove the following lemma:

LEMMA 6. *Let L and M be finite extension of k such that $(L: k)$ and $(M: k)$ are relatively prime. Then we have $(LM)^* = L^* M^*$.*

Proof. Put $K = LM$. The inclusion $L^* M^* \subset K^*$ is obvious. We have to prove that any finite abelian extension F of k such that FK is unramified over K is contained in $L^* M^*$. We can suppose that $(F: k)$ is a power of a rational prime l and the F is ramified over k. Then, as FK is unramified over K, we have $l | (K: k)$ and hence $l | (L: k)$ or $l | (M: k)$. Suppose $l | (L: k)$. Since $(FL: L) = (F: F \cap L)$ is a power of l, the ramification index in FL/L of the finite primes of L are power of l. Because FK is unramified over K and $l \nmid (M: k) = (K: L)$, FL is unramified over L and so $F \subset L^* \subset L^* M^*$.

§ 4. Examples.

Let k be a finite algebraic number field of class number one in which 2 remains prime. Let $(k:Q)=n$ and $\{\omega_j^2\ (j=1, 2, \cdots, 2^n-1)\}$ be a system of complete representatives of the squares of the multiplicative group of $O_k/(4)$ (its order is easily shown to be 2^n-1). Let m be a square-free integer of k and put $K=k(\sqrt{m})$. We define an integer θ of K by

$$\theta=\begin{cases}(\omega_j+\sqrt{m})/2: & m\equiv\omega_j^2 \pmod 4 \text{ for some } j\\ \sqrt{m} & : \text{otherwise}.\end{cases}$$

Then we have

LEMMA 7. *O_K is a free O_k-module with base $\{1, \theta\}$, and the relative discriminant of K over k is given by*

$$D(K/k)=\begin{cases} m: & m\equiv\omega_j^2 \pmod 4 \text{ for some } j\\ 4m: & \text{otherwise}.\end{cases}$$

Proof. We use the following fact; for integers a, b and c of k, the equation

$$a^2-b^2c\equiv 0 \pmod 4$$

is equivalent to $a\equiv b\omega_j \pmod 2$ if $c\equiv\omega_j^2 \pmod 4$ for some j, and to $a\equiv b\equiv 0 \pmod 2$ if $c\not\equiv\omega_j^2 \pmod 4$ for any j. Because m is a square-free integer of k, we have

$$\begin{aligned} O_K&=\{a+b\sqrt{m}\mid a, b\in k \text{ such that } 2a\in O_k,\ a^2-b^2m\in O_k\}\\ &=\{(a+b\sqrt{m})/2\mid a, b\in O_k \text{ such that } a^2-b^2m\equiv 0 \pmod 4\}.\end{aligned}$$

If $m\equiv\omega_j^2 \pmod 4$ for some j, we have by above remark

$$\begin{aligned} O_K&=\{(a-b\omega_j)/2+b(\omega_j+\sqrt{m})/2\mid a, b\in O_k \text{ such that } a\equiv b\omega_j \pmod 2\}\\ &=\{a+b\theta\mid a, b\in O_k\}.\end{aligned}$$

If $m\not\equiv\omega_j^2 \pmod 4$ for any j, we have

$$O_K=\{a+b\sqrt{m}\mid a, b\in O_k\}.$$

We have

$$K_1^*=\prod_{\mathfrak{p}} k(\mathfrak{p}), \qquad K_2^*=\bigcap_{\mathfrak{p}} T(\mathfrak{p})$$

where $\mathfrak{p}$ runs over the prime factors of $D(K/k)$ in k such that $2\mid g_k(\mathfrak{p})$, and $T(\mathfrak{p})$ is the inertia field of $\mathfrak{p}$ in K^*/k. For a prime factor $\mathfrak{p}$ of $D(K/k)$ in k such that $2\mid g_k(\mathfrak{p})$, $k(\mathfrak{p})$ is a quadratic extension of k, and by Lemma 7, $k(\mathfrak{p})=k(\sqrt{\pi})$ where π is a generator of $\mathfrak{p}$ such that $\pi\equiv\omega_j^2 \pmod 4$ for some j and satisfies conditions on its signature (if necessary).

We treat more explicitly the case of k=quadratic field below.

1) Let k be a imaginary quadratic field of class number one in which 2 remains prime, that is, $k=Q(\sqrt{D})$ where $D=-3, -11, -19, -43, -67, -163$, and put $\omega=(-1+\sqrt{D})/2$. Then $\{a+b\omega \mid a, b=0, 1, 2, 3\}$ is a system of complete representatives of O_k modulo 4. There are only three representatives which are prime to 2 and are congruent modulo 4 to squares, and they are named as in the following table:

D \ name	ω_1	ω_2	ω_3
$-3, -19$ $-67, -163$	1	$\omega\equiv(1+\omega)^2$	$3+3\omega\equiv\omega^2$
$-11, -43$	1	$2+\omega\equiv(1+\omega)^2$	$1+3\omega\equiv\omega^2$

Let m be a square-free integer of k and put $K=k(\sqrt{m})$. Let θ be an integer of K defined by

$$\theta=\begin{cases} (1+\sqrt{m})/2 & : \ m\equiv\omega_1 \pmod 4 \\ (1+\omega+\sqrt{m})/2 & : \ m\equiv\omega_2 \pmod 4 \\ (\omega+\sqrt{m})/2 & : \ m\equiv\omega_3 \pmod 4 \\ \sqrt{m} & : \ \text{otherwise}. \end{cases}$$

Then, by Lemma 7, O_k is a free O_k-module with base $\{1, \theta\}$ and the relative discriminant of K over k is given by

$$D(K/k)=\begin{cases} m: & m\equiv\omega_1, \omega_2, \omega_3 \pmod 4 \\ 4m: & \text{otherwise}. \end{cases}$$

For a finite prime $\mathfrak{p}$ of k, we have

$$k(\mathfrak{p})=\begin{cases} k(\sqrt{\pi}): & \text{if } \mathfrak{p}=(\pi) \text{ where } \pi\equiv\omega_1, \omega_2, \omega_3 \pmod 4 \\ k: & \text{otherwise}. \end{cases}$$

EXAMPLE 1. Put $k=Q(\sqrt{-11})$, $K=k(\sqrt{5})$. Because 5 is a square-free integer of k and $5\equiv\omega_1 \pmod 4$, we have $D(K/k)=5$. The prime factors of $D(K/k)$ in k are $1-\omega$ and $2+\omega$. Since $g_k(1-\omega)=g_k(2+\omega)=2$ and $1-\omega\equiv\omega_3 \pmod 4$, $2+\omega\equiv\omega_2 \pmod 4$, we have by Corollary 4

$$K^*=K_1^*=k(\sqrt{1-\omega}, \sqrt{2+\omega}).$$

EXAMPLE 2. Put $k=Q(\sqrt{-3})$, $K=k(\sqrt{26})$. Because 26 is a square-free integer of k and $26\not\equiv\omega_1, \omega_2, \omega_3 \pmod 4$, we have $D(K/k)=2^3 13$. The prime factors of $D(K/k)$ in k are $2, 3-\omega$ and $4+\omega$. Since $g_k(2)=1$, $g_k(3-\omega)=g_k(4+\omega)=2$ and $3-\omega\equiv\omega_3 \pmod 4$, $4+\omega\equiv\omega_2 \pmod 4$, we have by Proposition 5

$$K^*=K_1^*K=k(\sqrt{26}, \sqrt{3-\omega}, \sqrt{4+\omega}).$$

2) There are ten real quadratic field of discriminant less than 100 of class number one in which 2 remains prime, that is, $Q(\sqrt{D})$ where $D=5$, 13, 21, 29, 37, 53, 61, 69, 77, 93. Let k be one of the ten real quadratic fields and put $\omega=(-1+\sqrt{D})/2$. Then $\{a+b\omega \mid a, b=0, 1, 2, 3\}$ is a system of complete representatives of O_k modulo 4. There are only three representatives of O_k modulo 4 which are prime to 2 and are congruent modulo 4 to squares, and they are named as in the following table

D \ name	ω_1	ω_2	ω_3
5, 21, 37 53, 69	1	$2+\omega\equiv(1+\omega)^2$	$1+3\omega\equiv\omega^2$
13, 29, 61 77, 93	1	$\omega\equiv(1+\omega)^2$	$3+3\omega\equiv\omega^2$

Let m be a square-free integer of k and put $K=k(\sqrt{m})$. Let θ be an integer of K defined by

$$\theta=\begin{cases} (1+\sqrt{m})/2 & : \ m\equiv\omega_1 \pmod 4 \\ (1+\omega+\sqrt{m})/2 & : \ m\equiv\omega_2 \pmod 4 \\ (\omega+\sqrt{m})/2 & : \ m\equiv\omega_3 \pmod 4 \\ \sqrt{m} & : \ \text{otherwise}. \end{cases}$$

Then, by Lemma 7, O_K is a free O_k-module with base $\{1, \theta\}$ and the relative discriminant of K over k is given by

$$D(K/k)=\begin{cases} m: & m\equiv\omega_1, \omega_2, \omega_3 \pmod 4 \\ 4m: & \text{otherwise}. \end{cases}$$

For a finite prime $\mathfrak{p}$ of k, we have

$$k(\mathfrak{p})=\begin{cases} k(\sqrt{\pi}): & \text{if } \mathfrak{p}=(\pi) \text{ where } \pi\equiv\omega_1, \omega_2, \omega_3 \pmod 4 \text{ and } \pi\geqq 0 \\ k \quad : & \text{otherwise} \end{cases}$$

where $\pi\geqq 0$ means that π is totally positive.

EXAMPLE 3. Put $k=Q(\sqrt{13})$, $K=k(\sqrt{53})$. Because 53 is a square-free integer of k and $53\equiv\omega_1 \pmod 4$, we have $D(K/k)=53$. The prime factors of $D(K/k)$ in k are $7-\omega$ and $8+\omega$. Since $g_k(7-\omega)=g_k(8+\omega)=2$ (see the tables at the end of this §), and $7-\omega\equiv\omega_3 \pmod 4$, $8+\omega\equiv\omega_2 \pmod 4$, $7-\omega\geqq 0$, $8+\omega\geqq 0$, we have by Corollary 4

$$K^*=K_1^*=k(\sqrt{7-\omega},\ \sqrt{8+\omega}).$$

EXAMPLE 4. Put $k=Q(\sqrt{29})$, $K=k(\sqrt{10})$. Because 10 is a sequare-free integer of k and $10\not\equiv\omega_1, \omega_2, \omega_3 \pmod 4$, we have $D(K/k)=2^3 5$. The prime factors of $D(K/k)$ in k are $2, 4+\omega$, and $3-\omega$. Since $g_k(2)=1$, $g_k(4+\omega)=g_k(3-\omega)=2$, and $4+\omega\equiv\omega_2 \pmod 4$, $3-\omega\equiv\omega_3 \pmod 4$, $4+\omega\geqq 0$, $3-\omega\geqq 0$, we have by Proposition 5

$$K^*=K_1^*K=k(\sqrt{10},\ \sqrt{4+\omega},\ \sqrt{3-\omega}).$$

EXAMPLE 5. Put $k=Q(\sqrt{53})$, $K=k(\sqrt{221})$. Because 221 is a square-free integer of k and $221\equiv\omega_1 \pmod 4$, we have $D(K/k)=13\cdot 17$. The prime factors of $D(K/k)$ in k are $13+3\omega$, $17+4\omega$, $5-\omega$, and $6+\omega$. Since $g_k(13+3\omega)=g_k(17+4\omega)=g_k(5-\omega)=g_k(6+\omega)=2$, and $13+3\omega\equiv\omega_3 \pmod 4$, $17+4\omega\equiv\omega_1 \pmod 4$, $5-\omega\equiv\omega_3 \pmod 4$, $6+\omega\equiv\omega_2 \pmod 4$, $13+3\omega\geqq 0$, $17+4\omega\geqq 0$, $5-\omega\geqq 0$, $6+\omega\geqq 0$, we have

$$K^*=K_1^*=k(\sqrt{13+3\omega},\ \sqrt{17+4\omega},\ \sqrt{5-\omega},\ \sqrt{6+\omega}).$$

Let L be the genus field of K with respect to the rational number field, that is, the maximal abelian extension of Q such that KL/K is unramified. Then we have by the genus number formula

$$(L:Q)\leqq 2^3 \quad \text{i.e.} \quad (L:k)\leqq 2^2$$

On the other hand, we have $(K^*:k)=2^4$ and hence $L\subsetneqq K^*$.

Tables.

Table of $g_k(\mathfrak{p})$ and prime elements of k above each rational primes. (Blanks mean that the rational prime remains prime in k.)

a) $k=Q(\sqrt{5})$, $\omega=(-1+\sqrt{5})/2$, fundamental unit$=(1+\sqrt{5})/2=1+\omega$

	2	3	5	7	11		13	17	19		23	29	
			$2-\omega$		$3-\omega$	$4+\omega$			$4-\omega$	$5+\omega$		$5-\omega$	$6+\omega$
$g_k(\mathfrak{p})$	1	1	1	3	1	1	$2\cdot 3$	2^3	1	1	11	2	2

31		37	41		43	47	53	59	
$7+2\omega$	$5-2\omega$		$6-\omega$	$7+\omega$				$9+2\omega$	$7-2\omega$
1	1	$2\cdot 3^2$	1	1	$3\cdot 7$	$3\cdot 23$	$2\cdot 13$	1	1

b) $k=Q(\sqrt{13})$, $\omega=(-1+\sqrt{13})/2$, fundamental unit$=(3+\sqrt{13})/2=2+\omega$

	2	3		5	7	11	13	17		19	23	
		ω	$1+\omega$				$1+2\omega$	$4-\omega$	$5+\omega$		$1-3\omega$	$4+3\omega$
$g_k(\mathfrak{p})$	1	1	1	2	3	$3\cdot 5$	3	1	1	3^2	1	1

29		31	37	41	43		47	53		59	61	
$2+3\omega$	$1+3\omega$				$1-4\omega$	$5+4\omega$		$7-\omega$	$8+\omega$		$8-3\omega$	$11+3\omega$
1	1	$3\cdot 5$	$2\cdot 3^2$	$2^2\cdot 3\cdot 5$	1	1	23	2	2	$5\cdot 29$	2	2

c) $k=Q(\sqrt{29})$, $\omega=(-1+\sqrt{29})/2$, fundamental unit$=(5+\sqrt{29})/2=3+\omega$

	2	3	5		7		11	13		17	19	23	
			$1-\omega$	$2+\omega$	ω	$1+\omega$		$4-\omega$	$5+\omega$			$5-\omega$	$6+\omega$
$g_k(\mathfrak{p})$	1	1	2	2	1	1	5	1	1	2^3	3^2	1	1

29	31	37	41	43	47	53		59		61
$1+2\omega$						$5+3\omega$	$2-\omega$	$1-3\omega$	$4+3\omega$	
7	$3\cdot 5$	$2\cdot 3^2$	$2^2\cdot 3\cdot 5$	$3\cdot 7$	23	1	1	1	1	$2\cdot 3\cdot 5$

d) $k=Q(\sqrt{37})$, $\omega=(-1+\sqrt{37})/2$, fundamental unit$=6+\sqrt{37}=7+2\omega$

	2	3		5	7		11		13	17	19	23	29
		$2-\omega$	$3+\omega$		$1-\omega$	$2+\omega$	$4-\omega$	$5+\omega$					
$g_k(\mathfrak{p})$	3	1	1	2	1	1	1	1	$2\cdot 3$	2^3	3^2	11	$2\cdot 5\cdot 7$

31	37	41		43	47		53		59	61
	$1+2\omega$	$8+3\omega$	$5-3\omega$		$7-\omega$	$8+\omega$	$4-3\omega$	$7+3\omega$		
$3\cdot 5$	3^2	1	1	$3\cdot 7$	1	1	1	1	29	$2\cdot 3\cdot 5$

e) $k=Q(\sqrt{53})$, $\omega=(-1+\sqrt{53})/2$, fundamental unit$=(7+\sqrt{53})/2=4+\omega$

	2	3	5	7		11		13		17		19	23
				$2-\omega$	$3+\omega$	$1-\omega$	$2+\omega$	ω	$1+\omega$	$5-\omega$	$6+\omega$		
$g_k(\mathfrak{p})$	1	1	2	3	3	1	1	2	2	2	2	3^2	$3\cdot 11$

29		31	37		41	43		47		53
$6-\omega$	$7+\omega$		$5+2\omega$	$3-2\omega$		$7-\omega$	$8+\omega$	$7-3\omega$	$10+3\omega$	$1+2\omega$
1	1	$3\cdot 5$	1	1	$2^2\cdot 5$	3	3	1	1	13

f) $k=Q(\sqrt{61})$, $\omega=(-1+\sqrt{61})/2$, fundamental unit$=(39+5\sqrt{61})/2=22+5\omega$

	2	3		5		7	11	13		17	19		23
		$4+\omega$	$3-\omega$	$4-\omega$	$5+\omega$			$1-\omega$	$2+\omega$		$11-3\omega$	$14+3\omega$	
$g_k(\mathfrak{p})$	1	1	1	1	1	3	5	$2\cdot 3$	$2\cdot 3$	2^3	1	1	$3\cdot 11$

29	31	37	41		43	47		53	59	61	67
			$7-\omega$	$8+\omega$		$11+3\omega$	$8-3\omega$			$1+2\omega$	
$2^2\cdot 7$	$3\cdot 15$	$2\cdot 3^2$	2^2	2^2	$3\cdot 7$	1	1	$2\cdot 3\cdot 13$	$5\cdot 29$	$3\cdot 5$	?

g) $k=Q(\sqrt{21})$, $\omega=(-1+\sqrt{21})/2$, fundamental unit$=(5+\sqrt{21})/2=3+\omega$

	2	3	5		7	11	13	17		19	23	29	31
		$1-\omega$	$1+\omega$	ω	$3-\omega$			$3+2\omega$	$1-2\omega$				
$g_k(\mathfrak{p})$	1	1	1	1	3	$2\cdot 5$	$2^2\cdot 3$	1	1	$2^2\cdot 3^2$	$2\cdot 3\cdot 11$	$2^2\cdot 3\cdot 7$	$2^2\cdot 3\cdot 5$

37		41		43		47		53	59		61
$6-\omega$	$7+\omega$	$1-3\omega$	$4+3\omega$	$9+2\omega$	$7-2\omega$	$2+3\omega$	$1+3\omega$		$7+4\omega$	$3-4\omega$	
2	2	1	1	1	1	1	1	$2^2\cdot 13$	1	1	$2^2\cdot 3\cdot 5$

h) $k=Q(\sqrt{69})$, $\omega=(-1+\sqrt{69})/2$, fundamental unit$=(25+3\sqrt{69})/2=4+3\omega$

	2	3	5		7	11		13		17		19	23
		$4-\omega$	$3-\omega$	$4+\omega$		$2-\omega$	$3+\omega$	$5-\omega$	$6+\omega$	ω	$1+\omega$		$10-3\omega$
$g_k(\mathfrak{p})$	1	1	1	1	$2\cdot 3$	1	1	2	2	1	1	$2\cdot 3^2$	11

29	31		37	41	43	47	53		59	61	67
	$11+2\omega$	$9-2\omega$					$5+2\omega$	$3-2\omega$			
$2^2\cdot 7$	1	1	$2^2\cdot 3^2$	$2^3\cdot 5$	$2\cdot 3\cdot 7$	$2^2\cdot 23$	1	1	$2^2\cdot 3\cdot 29$	$2^2\cdot 3\cdot 5$	$2\cdot 3\cdot 11$

i) $k=Q(\sqrt{77})$, $\omega=(-1+\sqrt{77})/2$, fundamental unit$=(9+\sqrt{77})/2=5+\omega$

	2	3	5	7	11	13		17		19		23	
				$3-\omega$	$5-\omega$	$2-\omega$	$3+\omega$	$1-\omega$	$2+\omega$	ω	$1+\omega$	$6-\omega$	$7+\omega$
$g_k(\mathfrak{p})$	1	2	2^2	3	5	1	1	1	1	1	1	1	1

29	31	37		41		43	47	53		59
		$7-\omega$	$8+\omega$	$7+2\omega$	$5-2\omega$			$8-\omega$	$9+\omega$	
$2^2\cdot 7$	$2\cdot 3\cdot 5$	2	2	1	1	$2^2\cdot 3\cdot 7$	$2^2\cdot 23$	2	2	$2\cdot 29$

j) $k=Q(\sqrt{93})$, $\omega=(-1+\sqrt{93})/2$, fundamental unit$=(29+3\sqrt{93})/2=16+3\omega$

	2	3	5	7		11		13	17		19	
		$4-\omega$		$5-\omega$	$6+\omega$	$3-\omega$	$4+\omega$		$2-\omega$	$3+\omega$	$6-\omega$	$7+\omega$
$g_k(\mathfrak{p})$	1	1	2^2	1	1	1	1	$2^2\cdot 3$	1	1	1	1

23		29		31	37	41	43	47	53		59	61
ω	$1+\omega$	$9+2\omega$	$7-2\omega$	$14-3\omega$					$14+3\omega$	$11-3\omega$		
1	1	7	7	$3\cdot5$	$2^2\cdot3^2$	$2^3\cdot5$	$2^2\cdot3\cdot7$	$2\cdot3\cdot23$	1	1	$2\cdot29$	$2^2\cdot3\cdot5$

§ 5. Construction of genus field.

For a finite abelian group G, we denote by $|G|$ the order of G, $ex(G)$ the exponent of G, that is, the smallest positive integer which annihilates G. For integer m and n, $n|m^\infty$ means that $n|m^t$ for sufficiently large t.

THEOREM 8. *Let k be a finite algebraic number field of class number one, G any finite abelian group, and m a positive integer such that $ex(G)|m$ and $m\|G|^\infty$. Then there exist infinitely many cyclic extensions F of k of degree m such that*

$$C_F/C_F^{1-\sigma}\cong G(F^*/F)\cong G$$

where C_F is the ideal class group of F on which $G(F/k)$ acts in usual way and σ is one of the generators of cyclic group $G(F/k)$.

To prove this theorem, we use the following lemma proved in [7]. For a rational prime number l and a positive integer n, we put

$$k(l,\ n)=k(\zeta,\ \varepsilon_1^{1/l^{-n}},\ \cdots,\ \varepsilon_r^{1/l^{-n}})$$

where l^δ is the number of l-power roots of unity in k, ζ is a primitive $l^{\delta+n}$-th root of unity, and $\{\varepsilon_1, \cdots, \varepsilon_r\}$ is the fundamental units of k. Then we have

LEMMA 9. *Let k be a finite algebraic number field. For a rational prime number l such that $l\nmid h_k$, a positive integer n, and a finite prime $\mathfrak{p}$ of k, the following three conditions are equivalent;*

1) *Let S be the ray class field modulo $\mathfrak{p}$ of k. Then there exists an intermediate field L of S/k such that $(L:k)=l^n$.*
2) *l^n divides $\phi(\mathfrak{p})/(U_k:U_k(\mathfrak{p}))$.*
3) *$\mathfrak{p}\nmid l$ and $\mathfrak{p}$ splits completely in $k(l, n)$.*

When these three equivalent conditions are fulfilled, L is a cyclic extension of k and $\mathfrak{p}$ is totally ramified in L. Therefore the intermediate field of 1) *is unique.*

Proof of Theorem 8. Suppose first that G is l-primary for a rational prime number l. Then we have

$$G=G_1\times\cdots\times G_t,\qquad m=l^{e_{t+1}}$$

where G_j is cyclic group of order l^{e_j} and $1<e_1\leqq,\cdots,\leqq e_t\leqq e_{t+1}$. By Lemma 9,

there exist distinct finite primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_{t+1}$ of k such that l^{e_j} divides $\phi(\mathfrak{p}_j)/(U_k : U_k(\mathfrak{p}_j))$. Let S_j be the ray class field modulo $\mathfrak{p}_j$ of k, L_j the intermediate field of S_j/k such that $(L_j : k)=l^{e_j}$, and σ_j a generator of cyclic group $G(L_j/k)$. Put $K=\prod_{j=1}^{t+1} L_j$ composite field, then we have

$$G(K/k)=G(L_1/k)\times \cdots \times G(L_{t+1}/k)\,.$$

Let H be the subgroup of $G(K/k)$ generated by $\{\sigma_j\sigma_{t+1}^{l^{n-e_j}} : (1\leqq j\leqq t)\}$, and F the fixed field of H (the construction of F is due to [7]). Then $G(F/k)=G(K/k)/H$ is a cyclic group of order m whose generator is $\sigma_{t+1}H$, and σ_j generates the inertia group of $\mathfrak{p}_j$ in K/k, for $1\leqq j\leqq t+1$. Therefore K is unramified over F, and hence $K\subset F^*$. Since $h_k=1$, we have $(K: k)\geqq(F^* : k)$ by the genus number formula, and hence $K=F^*$. Then we have

$$G(F^*/F)=H\cong G_1\times \cdots \times G_t=G\,.$$

For general G, we have

$$G=G_1\times \cdots \times G_s\,, \qquad m=q_1 \cdots q_s$$

where G_j is the l_j-primary part of G for a rational prime number l_j, and q_j is a power of l_j. Then there exists a cyclic extension F_j of k of degree q_j such that

$$G(F_j^*/F_j)\cong G_j\,.$$

Let $F=\prod_{j=1}^{s} F_j$ composite field. Then, by Lemma 6, we have $F^*=\prod_{j=1}^{s} F_j^*$ composite field. By the genus number formula, $\{(F_j^* : k) : (1\leqq j\leqq s)\}$ are mutually prime, therefore we have

$$G(F^*/F)\cong G(F_1^*/F_1)\times \cdots \times G(F_s^*/F_s)\cong G_1\times \cdots \times G_s=G\,.$$

The infinity of F is follows from the way of construction of F and from Lemma 9. The fact that the Artin mapping gives the isomorphism $C_F/C_F^{1-\sigma} \cong G(F^*/F)$ is proved in [8].

References

[1] M. Bhaskaran, Construction of genus field and some applications. J. Number Theory 11 (1979), 488-497.

[2] Y. Furuta, The genus field and genus number in algebraic number field. Nagoya Math. J. **29** (1967), 281-285.

[3] R. Gold and L. Madan, Some applications of Abhyanker's lemma. Math. Nachr. **82** (1978), 115-119.

[4] M. Ishida, Some unramified abelian extensions of algebraic number field. J. Reine Angew. Math. **268/269** (1974), 165-173.

[5] M. Ishida, The genus fields of algebraic number fields. Springer Lecture Note **555** (1976).

[6] M. ISHIDA, On the genus fields of pure nuumber fields. Tokyo J. Math. Vol. **3** No. 1 (1980), 163-171.
[7] O. YAHAGI, Construction of number fields with prescribed l-class group. Tokyo J. Math. Vol. **1** No. **2** (1978), 275-283.
[8] H. YOKOI, On the class number of relatively cyclic number field. Nagoya Math. J. **29** (1967), 31-44.

DEPARTMENT OF MATHEMATICS
TOKYO INSTITUTE OF TECHNOLOGY