J. Math. Soc. Japan
Vol. 27, No. 2, 1975

On the genus field of an algebraic number field of odd prime degree

By Makoto ISHIDA

(Received June 12, 1974)

Let K be an algebraic number field of finite degree. Then the genus field $\tilde{K}$ of K is defined as the maximal abelian extension of K, which is a composite of an abelian extension $\tilde{k}_0$ of $\boldsymbol{Q}$ with K and is unramified at all the finite prime ideals of K (cf. Fröhlich [1]). The extension degree of $\tilde{K}$ over K is also called the genus number of K.

In the preceding paper [3], we have shown how we can construct explicitly the genus field $\tilde{K}$ of K, under the assumption that the degree and the discriminant of K are coprime.

The purpose of this paper is to determine the genus field and the genus number of an (arbitrary) algebraic number field K of odd prime degree l.

1. Let l be an odd prime number and let K be an algebraic number field of degree l.

Consider the p^n-th cyclotomic number field $k=\boldsymbol{Q}(\zeta_{p^n})$, where p is a prime number and ζ_{p^n} is a primitive p^n-th root of unity. Suppose that the decomposition of p in K as follows:

$$p=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_m^{e_m}, \qquad N\mathfrak{p}_i=p^{f_i}, \tag{1}$$

where we have

$$\sum_{i=1}^{m} e_i f_i=[K:\boldsymbol{Q}]=l. \tag{2}$$

For a subfield k_0, of degree $d>1$, of $k=\boldsymbol{Q}(\zeta_{p^n})$, if the composite field k_0K is unramified (at all the finite prime ideals of K, i.e. at $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m$), then, in (1), d divides $e_1, e_2, \cdots, e_m$ and so, by (2), d divides l i.e. we have $d=l$. So $m=1$, $e_1=l$, $f_1=1$, i.e. p is totally ramified in K. On the other hand, as d divides $\varphi(p^n)=p^{n-1}(p-1)=[k:\boldsymbol{Q}]$, there are two cases:

(i) $p\neq l$. Then $d=l$ divides $p-1$ and so we have $k_0\subset\boldsymbol{Q}(\zeta_p)$, i.e. k_0 is the unique subfield, of degree l, of $\boldsymbol{Q}(\zeta_p)$. In this case, as is shown in [3], the converse assertion holds. That is, if $p\equiv 1 \pmod{l}$ is totally ramified in K then k_0K is unramified over K.

(ii) $p=l$. Then we have $k_0\subset\boldsymbol{Q}(\zeta_{l^2})$, i.e. k_0 is the unique subfield, of degree l, of $\boldsymbol{Q}(\zeta_{l^2})$. So the problem to be considered is to decide when k_0K is unramified over K.

2. Let $k=\boldsymbol{Q}(\zeta_{l^2})$ and let k_0 the unique subfield, of degree l, of k. Of course, k_0 is contained in the maximal real subfield k' of k. On the other hand, let K be an algebraic number field of degree l, in which l is totally ramified.

As in [3], we use the terminologies of class field theory. Let $A_l(\boldsymbol{Q})$ be the group of all the ideals, prime to l, in $\boldsymbol{Q}$ and let $S_{l^2}(\boldsymbol{Q})$ be the 'Strahl' mod l^2 in $\boldsymbol{Q}$ i.e. the subgroup of $A_l(\boldsymbol{Q})$ consisting of all (principal) ideals (a) with $a\equiv 1 \pmod{^\times l^2}$ (multiplicative congruence). Then the subfield k_0 of k' corresponds to the ideal group

$$H_{l^2}(\boldsymbol{Q})=\{(a)\in A_l(\boldsymbol{Q}) \mid a^{l-1}\equiv 1 \ (\mathrm{mod}^\times l^2)\}\,,$$

in $\boldsymbol{Q}$, with defining modulus l^2. So the 'Verschiebungssatz' implies that k_0K is the abelian extension of K corresponding to the ideal group

$$H_{l^2}(K)=\{\mathfrak{a} \mid (\mathfrak{a}, l)=1,\ N\mathfrak{a}^{l-1}\equiv 1 \ (\mathrm{mod}^\times l^2)\}\,,$$

in K, with defining modulus l^2. Hence we see that k_0K is unramified over K if and only if $H_{l^2}(K)$ contains all the principal ideals, prime to l, in K.

Now as l is totally ramified in K, we can find a primitive element π of K, whose minimal polynomial is of Eisenstein type with respect to l:

$$f(X)=X^l+a_1X^{l-1}+\cdots+a_l\in \boldsymbol{Z}[X] \tag{3}$$

with $l\mid a_i$ $(i=1, 2, \cdots, l)$ and $l^2 \nmid a_l$ (cf. [2]).

(A) Suppose that k_0K is unramified over K. Then, for the integer $\gamma=1-y\pi$ in K $(y\in \boldsymbol{Z})$, we must have

$$N_K\gamma^{l-1}=N(\gamma)^{l-1}\equiv 1 \pmod{l^2}.$$

On the other hand, as $l\mid a_i$, we have

$$\begin{aligned} N_K\gamma^{l-1}&=(1+a_1y+\cdots+a_ly^l)^{l-1}\\ &\equiv 1-(a_1y+\cdots+a_ly^l) \pmod{l^2}. \end{aligned}$$

So it holds that

$$a_1y+a_2y^2+\cdots+a_ly^l\equiv 0 \pmod{l^2}$$

for any y in $\boldsymbol{Z}$. Writing $a_i=lb_i$ $(b_i\in \boldsymbol{Z})$, we see that

$$b_1+b_2y+\cdots+b_ly^{l-1}\equiv 0 \pmod{l}$$

for $y=1, 2, \cdots, l-1$. Then, as $l\nmid b_l$, we must have

$$b_1+b_2Y+\cdots+b_lY^{l-1}\equiv b_l(Y^{l-1}-1) \pmod{l}$$

as a polynomial of Y over $\boldsymbol{Z}$. Hence we have

$$l \mid b_2, \cdots, b_{l-1} \ ; \ b_1 \equiv -b_l \pmod{l},$$

i.e. the coefficients a_i of $f(X)$ satisfy the following condition:

$$(\#) \qquad l^2 \mid a_2, \cdots, l^2 \mid a_{l-1} \ ; \ a_1 + a_l \equiv 0 \pmod{l^2}.$$

(B) Conversely suppose that the coefficients a_i of the minimal polynomial $f(X)$ of π satisfy the condition (#). We need the following

LEMMA. *Let $X_1, X_2, \cdots, X_l$ be l independent variables and consider a monomial $M = X_1^{k_1} X_2^{k_2} \cdots X_l^{k_l}$ with $k_1 \geqq 2$. Let $F(X_1, X_2, \cdots, X_l)$ be the 'smallest' symmetric polynomial containing M as its term. Using the fundamental symmetric polynomials $Y_1 = X_1 + X_2 + \cdots + X_l$, $Y_2 = X_1X_2 + \cdots + X_iX_j + \cdots + X_{l-1}X_l$, $\cdots$, $Y_l = X_1X_2 \cdots X_l$, we can write*

$$F(X_1, X_2, \cdots, X_l) = c + aY_1 + bY_l + \cdots \in \boldsymbol{Z}[Y_1, Y_2, \cdots, Y_l].$$

Then we have $c = a = 0$ and $b \equiv 0 \pmod{l}$.

PROOF.

$$c = F(0, 0, \cdots, 0) = 0.$$

$$a = \frac{\partial F}{\partial X_1}(0, 0, \cdots, 0) = 0.$$

$$b \equiv \frac{\partial^l F}{\partial X_1 \partial X_2 \cdots \partial X_l}(0, 0, \cdots, 0) = 0 \qquad (\mathrm{mod}\ l).$$

In fact, consider the coefficient s_N of $X_1X_2 \cdots X_l$ in a monomial $N = Y_1^{h_1} Y_2^{h_2} \cdots Y_l^{h_l}$ as a polynomial of $X_1, X_2, \cdots, X_l$. Of course, we may restrict our consideration to such an N with $h_1 + 2h_2 + \cdots + lh_l = l$. Then

(a) $h_l \neq 0 \Rightarrow N = Y_l \Rightarrow s_N = 1$,

(b) $h_l = 0 \Rightarrow$ for an index $j (< l)$, $h_j \neq 0 \Rightarrow s_N$ is a multiple of ${}_lC_j \Rightarrow s_N \equiv 0 \pmod{l}$.

COROLLARY. *In our case (i.e. under the assumption (#)), let $\pi = \pi^{(1)}, \pi^{(2)}, \cdots, \pi^{(l)}$ be all the conjugates of π over $\boldsymbol{Q}$. Then we have*

$$F(\pi^{(1)}, \pi^{(2)}, \cdots, \pi^{(l)}) \equiv 0 \qquad (\mathrm{mod}\ l^2).$$

PROOF.

$$F(\pi^{(1)}, \pi^{(2)}, \cdots, \pi^{(l)}) \equiv b\pi^{(1)}\pi^{(2)} \cdots \pi^{(l)} = -ba_l \equiv 0 \qquad (\mathrm{mod}\ l^2).$$

Let $l = \mathfrak{l}^l$ in K, where $\mathfrak{l}$ is a prime ideal of K. Then we have $\mathfrak{l} \| \pi$. Let $\boldsymbol{Q}_l$ be the l-adic completion of $\boldsymbol{Q}$ and $K_\mathfrak{l}$ the $\mathfrak{l}$-adic completion of K. As is well-known, π is a prime element of $K_\mathfrak{l}$ and $1, \pi, \cdots, \pi^{l-1}$ constitute the integral basis of $K_\mathfrak{l}$ over $\boldsymbol{Q}_l$ ($K_\mathfrak{l}$ is totally ramified over $\boldsymbol{Q}_l$). So any $\mathfrak{l}$-adic integer Γ in $K_\mathfrak{l}$ can be written as

$$\Gamma = x_0 + x_1\pi + \cdots + x_{l-1}\pi^{l-1}$$

with l-adic integers x_i in $\boldsymbol{Q}_l$. Then, by Corollary of Lemma, we have

$$
\begin{aligned}
(4) \qquad N_{K\mathfrak{l}/\boldsymbol{Q}_l}\Gamma &= N_{K\mathfrak{l}/\boldsymbol{Q}_l}(x_0+x_1\pi+\cdots x_{l-1}\pi^{l-1}) \\
&\equiv N_{K\mathfrak{l}/\boldsymbol{Q}_l}(x_0+x_1\pi) = x_0{}^l - a_1x_0{}^{l-1}x_1 + \cdots - a_lx_1{}^l \\
&\equiv x_0{}^l - a_1x_0{}^{l-1}x_1 - a_lx_1{}^l \\
&= x_0{}^l - lx_1(b_1x_0{}^{l-1}+b_lx_1{}^{l-1}) \qquad (\mathrm{mod}\ l^2)\,.
\end{aligned}
$$

Then Γ is prime to $\mathfrak{l}$ if and only if x_0 is prime to l. Moreover, if $l \nmid x_0$ and $l \nmid x_1$, then $b_1x_0{}^{l-1}+b_lx_1{}^{l-1} \equiv b_1+b_l \equiv 0 \pmod{l}$. Hence, for an $\mathfrak{l}$-adic integer Γ, prime to $\mathfrak{l}$, we have, by (4),

$$N_{K\mathfrak{l}/\boldsymbol{Q}_l}\Gamma^{l-1} \equiv x_0{}^{l(l-1)} \equiv 1 \qquad (\mathrm{mod}\ l^2)\,.$$

So, for any integer γ, prime to $\mathfrak{l}$, of K, we have

$$N(\gamma)^{l-1} = N_K\gamma^{l-1} = N_{K\mathfrak{l}/\boldsymbol{Q}_l}\gamma^{l-1} \equiv 1 \qquad (\mathrm{mod}\ l^2)\,,$$

which implies that k_0K is unramified over K as stated above.

As a remark, in the case where K is cyclic over $\boldsymbol{Q}$ and l is totally ramified in K, we know that k_0K is unramified over K. In fact, it is known that if l is totally ramified in an abelian extension L (of degree l^2) over $\boldsymbol{Q}$, then L is cyclic over $\boldsymbol{Q}$.

3. Combining the results obtained in [3] and **2**, we have the following

THEOREM. *Let l be an odd prime number and let K be an algebraic number field of degree l. For all the prime numbers $p_1, p_2, \cdots, p_t$ such that p_i is totally ramified in K and $p_i \equiv 1 \pmod{l}$, put*

k_1 = the composite field of all the (unique) subfields, of degree l, of $\boldsymbol{Q}(\zeta_{p_i})$ $(i=1, 2, \cdots, t)$.

Moreover, when l is totally ramified in K, take a primitive element π of K whose minimal polynomial $f(X)=X^l+a_1X^{l-1}+\cdots+a_l \in \boldsymbol{Z}[X]$ is of Eisenstein type with respect to l. Consider the condition

$$(\sharp) \qquad l^2 \mid a_2, \cdots, l^2 \mid a_{l-1}\ ;\ \ a_1+a_l \equiv 0 \pmod{l^2}$$

and put

$$k_0 = \begin{cases} \text{the unique subfield, of degree } l, \text{ of } \boldsymbol{Q}(\zeta_{l^2}), & \text{if } (\sharp) \text{ is satisfied,} \\ \boldsymbol{Q}, & \text{otherwise.} \end{cases}$$

Then, for the abelian extension $\tilde{k}_0=k_1k_0$ of $\boldsymbol{Q}$, $\tilde{K}=\tilde{k}_0K$ is the genus field of K. So the genus number g_K of K is given as follows:

(i) *K is not cyclic over $\boldsymbol{Q}$.*

$$(5) \qquad g_K = \begin{cases} l^{t+1}, & \text{if } l \text{ is totally ramified in } K \text{ and } (\sharp) \text{ is satisfied,} \\ l^t, & \text{otherwise.} \end{cases}$$

(ii) *K is cyclic over $\boldsymbol{Q}$.*

$$g_K = \begin{cases} l^t, & \text{if } l \text{ is totally ramified in } K, \\ l^{t-1}, & \text{otherwise.} \end{cases} \tag{6}$$

In our case, the genus number g_K of K is, of course, a divisor of the class number h_K of K. Moreover, as the Galois group of $\tilde{k}_0$ is of type $(l, l, \cdots, l)$, the l-rank of the ideal class group C_K of K is not less than $\log g_K/\log l$ $(=t+1, t, t, t-1$ respectively).

References

[1] A. Fröhlich, The genus field and genus group in finite number fields I, II, Mathematatika, **6** (1959), 40-46, 142-146.
[2] M. Ishida, Class numbers of algebraic number fields of Eisenstein type, J. Number Theory, **2** (1970), 404-413.
[3] M. Ishida, Some unramified abelian extensions of algebraic number fields, J. Reine Angew. Math., **268/269** (1974), 165-173.

Makoto ISHIDA
Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Fukazawa, Setagaya-ku
Tokyo, Japan