Notations

Z is the ring of rational integers and Q is the field of rational numbers.

Let $a \in Z$ and p a rational prime number. If p is a divisor of a, we write $p \mid a$ ($p \nmid a$ in negative case). Moreover if p^e is the exact power of p dividing a, then we write $p^e \parallel a$.

Let $a, b \in Z$. Then (a, b) denotes the greatest common divisor of a and b.

Let p_∞ be the (unique) infinite prime divisor of Q. For an integral divisor $\tilde{m}$ of Q (i.e. $\tilde{m} = m$ or mp_∞ with some $m \in Z$ $(m > 0)$), $A_{\tilde{m}}$ denotes the group of all (principal) ideals, prime to m, in Q and $S_{\tilde{m}}$ the 'Strahl mod $\tilde{m}$' in Q i.e. the subgroup of $A_{\tilde{m}}$ consisting of all ideals (a) with $a \equiv 1 \pmod{^\times \tilde{m}}$ (multiplicative congruence). A subgroup $H_{\tilde{m}}$ of $A_{\tilde{m}}$, containing $S_{\tilde{m}}$, is called an ideal group with defining modulus $\tilde{m}$.

For a positive rational integer $m \in Z$, ζ_m denotes a primitive m-th root of unity. Then $Q(\zeta_m)$ is the m-th cyclotomic number field and $Q(\zeta_m)_o$ is its maximal real subfield.

Let K be an algebraic number field of finite degree. Then D_K denotes the discriminant of K, O_K the ring of integers in K. The norm mapping defined for elements and ideals of K is denoted by N_K. Moreover C_K is the ideal class group and h_K is the class number of K. (When we consider the ideal class group or the class number in 'narrow' sense, we denote them by C_K^+ or h_K^+ respectively.) For a prime number q, $d^{(q)}C_K$ is the q-rank of C_K. i.e. the number of invariants of C_K which is a power of q.

Let p be a rational prime number and let

$$(p) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

be the prime ideal decomposition of p in K. Then e(p) is the greatest common divisor of $e_1, e_2, \ldots, e_m$ and $d^*(p) = (e(p), p - 1)$. Moreover $k^*(p)$ is the unique subfield, of degree $d^*(p)$, of $Q(\zeta_p)$.

For an algebraic number field K, K* is the genus field of K, $g_K = [K^* : K]$ the genus number of K and k* the maximal absolute abelian subfield of K* (as for the definitions, see Chapters 1 and 4).

Finally, for several algebraic number fields $K_1, K_2, \ldots, K_t$,

$$\prod_{i=1}^{t} K_i = K_1 K_2 \ldots K_t$$

denotes the composite field of them i.e. the smallest number field containing all of them.

References

[1] Z.I.Borevich and I.R.Shafarevich, 'Number theory' (English translation), Academic Press, New York, 1966.

[2] P.Barrucand and H.Cohn, A rational genus, class number divisibility and unit theorem for pure cubic fields, J. Number Theory 2 (1970), 7-21.

[3] H.Cohn, 'A second course in number theory', Wiley, New York, 1962.

[4] I.Connell and D.Sussman, The p-dimension of class groups of number fields, J. London Math. Society (second series) 2 (1970), 525-529.

[5] G.Frey and W.D.Geyer, Über die Fundamentalgruppe von Körpern mit Divisorentheorie, J. Reine Angew. Math. 254 (1972), 110-122.

[6] A.Fröhlich, The genus field and genus group in finite number fields, Mathematika 6 (1959), 40-46.

[7] A.Fröhlich, The genus field and genus group in finite number field, II, Mathematika 6 (1959), 142-146.

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

[9] Y.Furuta, Über das Geschlecht und die Klassenzahl eines relativ-Galoissches Zahlkörpers von Primzahlpotenzgrade, Nagoya Math. J. 37 (1970), 197-200.

[10] H.Hasse, 'Vorlesungen über Klassenkörpertheorie', Physica-Verlag, Würzburg, 1967.

[11] H.Hasse, 'Zahlentheorie', Akademie-Verlag, Berlin, 1969.

[12] H.Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörpern, J. Math. Soc. Japan 3 (1951), 45-51.

[13] H.Hasse, A supplement to Leopoldt's theory of genera in abelian number fields, J. Number Theory 1 (1969), 4-7.

[14] M.Ishida, A note on class numbers of algebraic number fields, J. Number Theory 1 (1969), 65-69.

[15] M.Ishida, Class numbers of algebraic number fields of Eisenstein type, J. Number Theory 2 (1970), 404-413.

[16] M.Ishida, Class numbers of algebraic number fields of Eisenstein type, II, J. Number Theory 6 (1974), 99-104.

[17] M.Ishida, Fundamental units of certain algebraic number fields, Abh. Math. Sem. Univ. Hamburg 39 (1973), 245-250.

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

[19] M.Ishida, On the genus field of an algebraic number field of odd prime degree, J. Math. Soc. Japan 27 (1975), 289-293.

[20] M.Ishida, On the genus field of an algebraic number field of odd prime degree, II (in Japanese), preprint.

[21] M.Ishida, 'Algebraic number theory' (in Japanese), Morikita, Tokyo, 1974.

[22] S.Iyanaga and T.Tamagawa, Sur la théorie du corps de classes sur le corps des nombres rationnels, J. Math. Soc. Japan 3 (1951), 220-227.

[23] H.W.Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr. 9 (1953), 350-362.

[24] M.L.Madan, Class groups of global fields, J. Reine Angew. Math. 252 (1972), 171-177.

[25] P.Roquette and H.Zassenhaus, A class rank estimate for algebraic number fields, J. London Math. Soc. 44 (1969), 31-38.

[26] T.Takagi, 'Algebraic number theory' (in Japanese), Iwanami, Tokyo, 1948.

Appendix. An algorithm for constructing the genus field in the case of odd prime degree

In this appendix, we extend the result of Chapter 6 to the case of arbitrary odd prime degree. Namely, we show that we can determine the genus field of an algebraic number field of odd prime degree explicitly from the coefficients of the minimal polynomial of a primitive element by the method obtained in Chapter 5. As for the details of the proofs, see the forthcoming paper in Jour. Fac. Sci. Univ. of Tokyo (vol. 24-1).

Let K be an algebraic number field of odd prime degree q. We keep the notations in Chapter 5 ; in particular, let

$k^*(p)$ = the unique subfield, of degree q, of $Q(\zeta_p)$, for $p \equiv 1 \pmod{q}$,

$k_1^* = \prod_{i=1}^{t} k^*(p_i)$, where $p_1, p_2, \cdots, p_t$ are all the totally ramifying rational prime numbers (in K) such that $p_i \equiv 1 \pmod{q}$,

k_o = the unique subfield, of degree q, of $Q(\zeta_{q^2})$.

Then, by Theorem 5, the maximal absolute abelian subfield k^* of the genus field $K^* = k^*K$ of K is given by

(A1) $$k^* = k_1^* \, k_2^*,$$

where $k_2^* = Q$ or k_o. The case $k_2^* = k_o$ occurs if and only if the following two conditions are satisfied :

1) q is totally ramified in K. (Accordingly, there is a primitive element π of K such that the minimal polynomial $f(X) = X^q + a_1X^{q-1} + \dots + a_q \in Z[X]$ of π is of Eisenstein type with respect to q. Then)

2) $a_1 + a_q \equiv a_2 \equiv \dots \equiv a_{q-1} \equiv 0 \pmod{q^2}$.

Now we explain our method to determine the subfield k^*. Suppose that there is given the minimal polynomial

$$X^q + d_1X^{q-1} + \dots + d_q \in Z[X]$$

of a primitive element δ of K. Then $\beta = q\delta + d_1$ is also a primitive element of K and the minimal polynomial of β is of the form

(A2) $$g(X) = X^q + b_2X^{q-2} + \dots + b_q \in Z[X].$$

Of course, the coefficients $b_2, \dots , b_q$ of $g(X)$ are easily calculated from $d_1, d_2, \dots , d_q$. Moreover, without loss of generality, we may assume that

(A3) there is no prime p such that $p^i \mid b_i$ $(i=2,\dots,q)$.

In fact, if there is such a rational prime number p, we can replace β by β/p.

Therefore we may start with the minimal polynomial $g(X)$ (of a primitive element of K), which is of the form (A2) and has the property (A3).

In this case, we see that

(A4) $p \neq q$ is totally ramified in K

$$\Longrightarrow \quad b_2 \equiv \dots \equiv b_q \equiv 0 \pmod{p} \text{ and } p^s \,\|\, b_q \text{ with } 1 \leqq s \leqq q-1,$$

(A5) q is totally ramified in K

$$\Longrightarrow \quad b_2 \equiv \dots \equiv b_{q-1} \equiv 0 \pmod{q} \text{ and } q^s \,\|\, b_q \text{ with } 0 \leqq s \leqq q-1.$$

Then we can know all the primes, totally ramifying in K, and can decide whether $k_2{}^* = k_o$ or not in the following way (cf. the latter half of Chapter 5).

First, suppose that a rational prime number p $(\neq q)$ satisfies the conditions (cf. (A4))

(*) $b_2 \equiv \dots \equiv b_q \equiv 0 \pmod{p}$ and $p^s \,\|\, b_q$ with $1 \leqq s \leqq q-1$.

Then there exist $m, n \in Z$ such that $ms = 1 + nq$ $(1 \leqq m \leqq q-1,$ $n \geqq 0)$ and $\gamma = \beta^m/p^n$ is a primitive element of K. Let $h(X) = X^q + c_1 X^{q-1} + \ldots + c_q \in Q[X]$ be the minimal polynomial of γ, where $c_q \in Z$ and $p \parallel c_q$.

Lemma A1. Under the conditions (*), p is totally ramified in K

$$\Longleftrightarrow \quad c_1 \equiv c_2 \equiv \ldots \equiv c_{q-1} \equiv 0 \pmod p.$$

Next, suppose that q satisfies the conditions (cf. (A5))

(**) $\qquad b_2 \equiv \ldots \equiv b_{q-1} \equiv 0 \pmod q$ and $q^s \parallel b_q$ with $0 \leqq s \leqq q-1$.

We consider two cases $s \geqq 1$ and $s = 0$ separately. In case $s \geqq 1$, similarly as above, for $m, n \in Z$ with $ms = 1 + nq$ $(1 \leqq m \leqq q-1,$ $n \geqq 0)$, let $t(X) = X^q + r_1 X^{q-1} + \ldots + r_q \in Q[X]$ be the minimal polynomial of $\rho = \beta^m/q^n$, where $r_q \in Z$ and $q \parallel r_q$.

Lemma A2. Under the conditions (**) with $s \geqq 1$, we have $k_2^* = k_0$ (i.e. $k_0 K$ is unramified over K)

$$\Longleftrightarrow \quad r_1 + r_q \equiv r_2 \equiv \ldots \equiv r_{q-1} \equiv 0 \pmod{q^2}.$$

Since $q \parallel r_q$, the first congruence $r_1 + r_q \equiv 0 \pmod{q^2}$ holds if and only if

$$q \parallel r_1 \quad \text{and} \quad \frac{r_1}{q} + \frac{r_q}{q} \equiv 0 \pmod{q}.$$

In case $s = 0$ i.e. $q \nmid b_q$, we replace β by $\beta' = \beta + b_q$. Then the minimal polynomial of β' is

$$g'(X) = g(X - b_q) = X^q + b_1'X^{q-1} + \dots + b_q' \in Z[X].$$

If q is totally ramified in K, then we have $q^{s'} \parallel b_q'$ with $1 \leqq s' \leqq q - 1$. There are also $m', n' \in Z$ such that $m's' = 1 + n'q$ $(1 \leqq m' \leqq q - 1,\ n' \geqq 0)$. Let $t'(X) = X^q + r_1'X^{q-1} + \dots + r_q' \in Q[X]$ be the minimal polynomial of $\rho' = \beta'^{m'}/q^{n'}$, where $r_q' \in Z$ and $q \parallel r_q'$.

<u>Lemma A3</u>. Under the conditions (**) with $s = 0$, we have $k_2^* = k_o$ (i.e. k_oK is unramified over K)

$$\Longleftrightarrow \quad q^{s'} \parallel b_q' \text{ with } 1 \leqq s' \leqq q - 1 \text{ and}$$
$$r_1' + r_q' \equiv r_2' \equiv \dots \equiv r_{q-1}' \equiv 0 \pmod{q^2}.$$

Note that the coefficients c_i, r_i and r_i' of $h(X)$, $t(X)$ and $t'(X)$ can be calculated from b_j in (A2) in elementary way.

Therefore, by (A1) and by Lemmas A1, A2, A3, we can determine k^* and so $K^* = k^*K$ from the coefficients $b_2, \dots, b_q$ of $g(X)$. Thus we obtain an algorithm for constructing the genus field K^*

of K.

Here we restate our algorithm in more explicit form.

First we introduce a notation. Let q be an odd prime number and let α be an algebraic integer, of degree q, with the minimal polynomial

$$\text{(A6)} \qquad f(X) = X^q + a_1 X^{q-1} + \dots + a_q \in Z[X].$$

Then, for $m \in Z$ $(1 \leqq m \leqq q - 1)$, α^m is also an algebraic integer, of degree q. Let

$$\text{(A7)} \qquad f_m(X) = X^q + a_1^{(m)} X^{q-1} + \dots + a_q^{(m)} \in Z[X]$$

be the minimal polynomial of α^m. By the fundamental theorem on symmetric polynomials, the coefficients $a_1^{(m)}, a_2^{(m)}, \dots, a_q^{(m)}$ of $f_m(X)$ can be calculated from $a_1, a_2, \dots, a_q$ in elementary (but somewhat complicated) way.

The algorithm

Let K be an algebraic number field, of odd prime degree q, and let

$$\text{(A8)} \qquad g(X) = X^q + b_2 X^{q-2} + \dots + b_q \in Z[X]$$

be the minimal polynomial of a primitive element β of K with the property

(A9) there is no prime p such that $p^i \mid b_i$ $(i=2,\ldots,q)$.

Then the maximal absolute abelian subfield k^* of the genus field K^* of K is given by

$$\text{(A10)} \qquad k^* = \prod_{p \equiv 1 \pmod q} k^*(p)^{\delta_p} \; k_o^{\delta_q} \quad \text{(composite)}$$

with δ_p, $\delta_q = 0$ or 1,

where the first product (composite) ranges over all the rational prime numbers $p \equiv 1 \pmod q$. Here, for an algebraic number field k, we denote

$$k^0 = Q \quad \text{and} \quad k^1 = k.$$

The 'exponents' δ_p and δ_q are determined as follows.

(I) $p \neq q$ $(p \equiv 1 \pmod q)$

We have $\delta_p = 1$ if and only if

(1a) $b_2 \equiv \ldots \equiv b_q \equiv 0 \pmod p$, (1b) $p^s \| b_q$ with $1 \leqq s \leqq q-1$,

(1c) for $m, n \in Z$ with $ms = 1 + nq$ $(1 \leqq m \leqq q-1,\ n \geqq 0)$,

$b_1^{(m)} \equiv 0 \pmod{p^{n+1}}, \ \ldots\ , b_{q-1}^{(m)} \equiv 0 \pmod{p^{(q-1)n+1}}$.

(II) $p = q$

We have $\delta_q = 1$ if and only if

(2a) $b_2 \equiv \ldots \equiv b_{q-1} \equiv 0 \pmod{q}$,

(2b) $q^s \| b_q$ with $0 \leqq s \leqq q-1$,

($2c_1$) when $s \geqq 1$, for $m, n \in Z$ with $ms = 1 + nq$ $(1 \leqq m \leqq q-1,\ n \geqq 0)$,

$$\begin{cases} q^{n+1} \| b_1^{(m)}, \quad \dfrac{b_1^{(m)}}{q^{n+1}} + \dfrac{b_q^{(m)}}{q^{qn+1}} \equiv 0 \pmod{q}, \\ b_2^{(m)} \equiv 0 \pmod{q^{2n+2}}, \ \ldots\ , b_{q-1}^{(m)} \equiv 0 \pmod{q^{(q-1)n+2}}. \end{cases}$$

($2c_2$) when $s = 0$, for $g'(X) = g(X - b_q) = X^q + b_1'X^{q-1} + \ldots + b_q' \in Z[X]$,

$q^{s'} \| b_q' = g(-b_q)$ with $1 \leqq s' \leqq q-1$

and, for $m', n' \in Z$ with $m's = 1 + n'q$ $(1 \leqq m' \leqq q-1,\ n' \geqq 0)$,

$$\begin{cases} q^{n'+1} \,\|\, b_1{}'^{(m')}, \quad \dfrac{b_1{}'^{(m')}}{q^{n'+1}} + \dfrac{b_q{}'^{(m')}}{q^{qn'+1}} \equiv 0 \pmod q \\ b_2{}'^{(m')} \equiv 0 \pmod{q^{2n'+2}}, \ \dots, \\ \qquad b_{q-1}{}'^{(m')} \equiv 0 \pmod{q^{(q-1)n'+2}}. \end{cases}$$

In the following, we apply our algorithm to polynomials of special type.

A) Trinomial case

We consider an irreducible trinomial

(A11) $$g(X) = X^q + aX + b \in Z[X]$$

of odd prime degree q, having the property

(A12) there is no prime p such that $p^{q-1} \mid a$ and $p^q \mid b$.

Let β be a root of $g(X)$ and let $K = Q(\beta)$ be an algebraic number field generated by β over Q. Of course, the degree of K is equal to q. Then we can determine the 'exponents' δ_p and δ_q in

$$k^* = \prod_{p \equiv 1 \pmod q} k^*(p)^{\delta_p} \cdot k_o^{\delta_q}.$$

That is, we have

$$\delta_p = 1 \quad (p \equiv 1 \pmod q)$$

$$\Longleftrightarrow \quad p^s \| b,\ p^s | a \quad (s = 1, 2, \dots, q-1),$$

$$\delta_q = 1$$

$$\Longleftrightarrow \begin{cases} q^{q-1} \| b,\ q^{q-1} \| a \text{ and } \dfrac{a}{q^{q-1}} \equiv -1 \pmod q, \\ \text{or} \\ q = 3 \text{ and } a \equiv 6,\ b \equiv \pm 1 \pmod{3^2}. \end{cases}$$

Thus the genus field $K^* = k^*K$ of K (defined by an irreducible trinomial (A11)) is completely and explicitly determined. In particular, the genus field of a cubic number field is determined (cf. Theorem 6).

Here we give several numerical examples in cubic case. Let $K = Q(\beta)$ with $\beta^3 + a\beta + b = 0$ be a cubic number field.

a	b	D_K	h_K	δ_p $(p \neq 3)$	δ_3	k^*	g_K
-5	5	$-5^2 \cdot 7$	1	0	0	Q	1
4	6	$-2^2\ 307$	3	0	0	Q	1
0	7	$-3^3 \cdot 7^2$	3	$\delta_7=1$, $\delta_p=0$ $(p\neq 7)$	0	$k^*(7)$	3
6	8	$-2^3\ 3^4$	3	0	1	k_o	3
-9	9	3^4	1	0	1	k_o	1

In the last example, $K = k_o$ is cyclic over Q. (The values of D_K and h_K are taken from the paper of Reid in Amer. Jour. of Math. 23 (1901).)

B) <u>Quintic case</u>

Let K be an algebraic number field of degree 5 and let β be a primitive element of K, where the minimal polynomial of β is of the form

$$\text{(A13)} \qquad g(X) = X^5 + b_2X^3 + \dots + b_5 \in Z[X]$$

and has the property

(a14) there is no prime p such that $p^i \mid b_i \quad (i=2,\dots,5)$.

Then we can determine the 'exponents' δ_p and δ_5 in

$$k^* = \prod_{p \equiv 1 \pmod 5} k^*(p)^{\delta_p} \cdot k_o^{\delta_5}.$$

That is, we have the following tables (cf. Chapter 5).

$\delta_p = 1 \quad (p \equiv 1 \pmod 5)$

$\Longleftrightarrow$

the highest exponent of p in			
b_5	b_2	b_3	b_4
1	$\geqq 1$	$\geqq 1$	$\geqq 1$
2	$\geqq 1$	$\geqq 2$	$\geqq 2$
3	$\geqq 2$	$\geqq 2$	$\geqq 3$
4	$\geqq 2$	$\geqq 3$	$\geqq 4$

$\delta_5 = 1$

$\Longleftrightarrow$

the highest exponent of 5 in				
b_5	b_2	b_3	b_4	with the relation
2	$\geqq 2$	2	$\geqq 3$	$\frac{b_3}{5^2} \cdot \frac{b_5}{5^2} \equiv 3 \pmod 5$
3	2	$\geqq 3$	$\geqq 4$	$\frac{b_2}{5^2} \cdot \left(\frac{b_5}{5^3}\right)^2 \equiv 3 \pmod 5$
4	$\geqq 3$	$\geqq 4$	4	$\frac{b_4}{5^4} \equiv -1 \pmod 5$
0	the highest exponent of 5 in			

b_5'	b_1'	b_2'	b_3'	b_4'	with the relation
1	1	$\geqq 2$	$\geqq 2$	$\geqq 2$	$\frac{b_1'}{5} \equiv -\frac{b_5'}{5} \pmod 5$

(Here $g'(X) = g(X - b_5) = X^5 + b_1'X^4 + \ldots + b_5' \in Z[X]$.)

As a remark, the conditions of the last row in the table for δ_5 are satisfied if and only if

$b_5 \pmod{5^2}$	$b_2 \pmod{5^2}$	$b_3 \pmod{5^2}$	$b_4 \pmod{5^2}$
± 1	-10	± 5	10
± 7	10	∓ 10	10

Thus the genus field $K^* = k^*K$ of an algebraic number field K, of degree 5, is completely and explicitly determined.

Subject Index