JOURNAL OF NUMBER THEORY 6, 99–104 (1974)

Class Numbers of Algebraic Number Fields of Eisenstein Type, II

MAKOTO ISHIDA

Department of Mathematics, Tokyo Metropolitan University, Setagaya, Tokyo, Japan

Communicated by P. Roquette

Received October 12, 1970

Let K be an algebraic number field, of degree n, with a completely ramifying prime p, and let t be a common divisor of n and $(p-1)/2$. Then it is proved that if K does not contain the unique subfield, of degree t, of the p-th cyclotomic number field, then we have $(h_K, n) > 1$, where h_K is the class number of K. As applications, we give several results on h_K of such algebraic number fields K.

In the preceding paper [2], we have investigated class number factors of algebraic number fields of Eisenstein type. Also in this paper, using the fundamental lemma in [2], we shall show several facts on the class numbers of such algebraic number fields. Our main result is as follows: let K be an algebraic number field of degree n and of Eisenstein type with respect to (an odd prime) p and ζ_p a primitive p-th root of unity. Let t be a common divisor of n and $(p-1)/2$. If K does not contain the unique subfield, of degree t, of $\mathbf{Q}(\zeta_p)$, then we have $(h_K, t) > 1$, where h_K is the class number of K. As an application, we see that, for an odd prime number p and a divisor n of $(p-1)/2$, the class numbers h_K of all the algebraic number fields K of degree n and of Eisenstein type with respect to p are larger than 1, except the case where K is the unique subfield, of degree n, of $\mathbf{Q}(\zeta_p)$. Moreover, we give many examples of an Eisenstein polynomial whose root generates an algebraic number field of class number >1.

1. Let K be an algebraic number field of degree n and of Eisenstein type with respect to an odd prime number p. That is, K is obtained by adjoining to $\mathbf{Q}$ a root of an Eisenstein polynomial, of degree n, with respect to p. Also as shown in [2], it is equivalent to saying that p ramifies completely in K. We restate a fundamental lemma in [2].

LEMMA. *Let γ be an integer in K. Then we have $N_{K/\mathbf{Q}}(\gamma) \equiv x^n \pmod{p}$ with some $x \in \mathbf{Z}$.*

Let ζ_p be a primitive p-th root of unity. In the following, we denote, for a divisor t of $p-1$, by k_t the unique subfield, of degree t, of $\mathbf{Q}(\zeta_p)$. Since $\mathbf{Q}(\zeta_p)$ is a cyclic extension of $\mathbf{Q}$, we have $k_{t_1} \subset k_{t_2}$ if and only if $t_1 \mid t_2$.

Now let t be a common divisor of n and $p-1$ and we suppose that we have

$$(*) \qquad (h_K, t) = 1,$$

where h_K is the class number of K. Let $\mathfrak{a}$ be an integral ideal of K with $(\mathfrak{a}, p) = 1$ and let m be the order of the class containing $\mathfrak{a}$ in the ideal class group C_K of K; so m divides h_K. Since $\mathfrak{a}^m = (\alpha)$ with an integer α in K, we have, by Lemma,

$$N\mathfrak{a}^m \equiv | N_{K/Q}(\alpha) | \equiv \pm x^n = \pm (x^{n/t})^t \qquad (\mathrm{mod}\, p),$$

where $x \in \mathbf{Z}$ with $p \nmid x$. On the other hand, we have

$$N\mathfrak{a}^t \equiv N\mathfrak{a}^t \qquad (\mathrm{mod}\, p).$$

As $(m, t) = 1$ by (*), we have consequently

$$N\mathfrak{a} \equiv \pm y^t \qquad (\mathrm{mod}\, p),$$

where $y \in \mathbf{Z}$ with $p \nmid y$. Put $s = (p-1)/t$; so we have $st = p - 1$. We consider the case where s is even, which is equivalent to saying that t is a common divisor of n and $(p-1)/2$. Then we have

$$N\mathfrak{a}^s \equiv 1 \qquad (\mathrm{mod}\, p).$$

Now we apply the class field theory. Let $\tilde{p} = pp_\infty$, where p_∞ is the infinite prime divisor of $\mathbf{Q}$, and let $A_{\tilde{p}}$ and $S_{\tilde{p}}$ be the whole ideal group and the ray ideal group with the defining modulus $\tilde{p}$ in $\mathbf{Q}$. Since $A_{\tilde{p}}/S_{\tilde{p}}$ is a cyclic group of order $p-1$, there is an ideal group $H_{\tilde{p}}$ such that $H_{\tilde{p}}/S_{\tilde{p}}$ is a subgroup, of $A_{\tilde{p}}/S_{\tilde{p}}$, of order $s = (p-1)/t$. Clearly we have $(a) \in H_{\tilde{p}}$ if and only if $(a)^s = (a^s) \in S_{\tilde{p}}$. As shown above, for any integral ideal $\mathfrak{a}$ with $(\mathfrak{a}, p) = 1$, we have

$$N\mathfrak{a}^s \equiv 1 \qquad (\mathrm{mod}\, p) \text{ and so } (\mathrm{mod}\, \tilde{p}),$$

which implies $(N\mathfrak{a}) \in H_{\tilde{p}}$. On the other hand, as $(A_{\tilde{p}} : H_{\tilde{p}}) = t$, the subfield k_t corresponds to the ideal group $H_{\tilde{p}}$ in the sense of the class field theory. Hence, by the 'Verschiebungssatz' of the class field theory

([1], p. 140), the abelian extension k_tK/K corresponds to the whole ideal group with the defining modulus $\tilde{p}$ in K. So we have

$$[k_tK : K] = 1, \qquad \text{i.e.,} \quad k_t \subset K.$$

Here we note that, as $t \mid (p-1)/2$, k_t is contained in the maximal real subfield $\mathbf{Q}(\zeta_p)_0 = \mathbf{Q}(\cos 2\pi/p)$ of $\mathbf{Q}(\zeta_p)$.

Thus we have the following:

THEOREM 1. *Let K be an algebraic number field of degree n and of Eisenstein type with respect to p. Let t be a common divisor of n and $(p-1)/2$. If $K \not\supset k_t$, then we have $(h_K, t) > 1$, where h_K is the class number of K. In other words, if $t \mid (n, (p-1)/2)$ and $t \nmid [K \cap \mathbf{Q}(\zeta_p)_0 : \mathbf{Q}]$, then we have $(h_K, t) > 1$.*

Proof. The second part is trivial, because we have $k_t \subset K$ if and only if $k_t \subset K \cap \mathbf{Q}(\zeta_p)_0$, i.e., $t \mid [K \cap \mathbf{Q}(\zeta_p)_0 : \mathbf{Q}]$.

Remark. Theorem 1 says nothing wehn $(n, (p-1)/2) = 1$ (in particular, when $p = 3$). In fact, K always contains $k_1 = \mathbf{Q}$.

We can give the following two modifications of Theorem 1.

(1) When $s = (p-1)/t$ is odd, we see that t is even and $t/2 \mid (n, (p-1)/2)$. Hence if $K \not\supset k_{t/2}$ then we have $(h_K, t/2) > 1$.

(2) In the case where K is totally imaginary, we have $N_{K/\mathbf{Q}}(\alpha) > 0$ for all $\alpha\,(\neq 0) \in K$. Hence (even when $s = (p-1)/t$ is odd), we have $N\mathfrak{a}^s \equiv 1 \pmod{p}$ $((\mathfrak{a}, p) = 1)$. So, in this case, if $t \mid (n, p-1)$ and $K \not\supset k_t$, then we have $(h_K, t) > 1$.

COROLLARY. *Let $d = (n, (p-1)/2)$; so $[K \cap \mathbf{Q}(\zeta_p)_0 : \mathbf{Q}]$ is a divisor of d. If $[K \cap \mathbf{Q}(\zeta_p)_0 : \mathbf{Q}] < d$, then we have $(h_K, d) > 1$ and so $h_K > 1$.*

Proof. We take $t = d$ in Theorem 1.

For example, if $(p-1)/2 \mid n$ and $K \not\supset \mathbf{Q}(\zeta_p)_0 = \mathbf{Q}(\cos 2\pi/p)$, then we have $(h_K, (p-1)/2) > 1$.

(a) For $p = 7$ and $3 \mid n$, we have $(h_K, 3) > 1$, i.e., $3 \mid h_K$, if $K \not\supset \mathbf{Q}(\cos 2\pi/7)$.

On the other hand, let $p \equiv 1 \pmod 4$. If $2 \mid n$ and $K \not\supset k_2 = \mathbf{Q}(\sqrt{p})$, then we have $(h_K, 2) > 1$, i.e., $2 \mid h_K$.

(b) For $p = 5$ and $2 \mid n$, we have $2 \mid h_K$, if $K \not\supset \mathbf{Q}(\sqrt{5})$.

2. In order to apply Theorem 1, we need to have some (sufficient) conditions for $K \not\supset k_t$, where t is a divisor of $(n, (p-1)/2)$. As for the decomposition of prime numbers q in $k_t \subset \mathbf{Q}(\zeta_p)$, it is known that

(A_0) if $q \neq p$, then q does not ramify in k_t,

(B_0) if $q \neq p$ and $q^{(p-1)/t} \not\equiv 1 \pmod p$, then all the prime divisors of q in k_t are of degree >1, and

(C_0) if $q \neq p$ and $q^{(p-1)/t} \equiv 1 \pmod p$, then all the prime divisors of q in k_t are of degree 1.

Therefore we have the following sufficient conditions (A), (B), and (C) for $K \not\supset k_t$.

(A) Another prime number $q \neq p$ ramifies completely in K, i.e., K is also of Eisenstein type with respect to q.

If (A) is satisfied, then we have $K \not\supset k_t$ for any $t \mid (p-1)/2$ $(t \neq 1)$, i.e., $K \cap \mathbf{Q}(\zeta_p)_0 = \mathbf{Q}$.

THEOREM 2. *Assume $K \cap \mathbf{Q}(\zeta_p)_0 = \mathbf{Q}$ (say the case where K is also of Eisenstein type with respect to $q \neq p$). Then, for any common prime divisor l of n and $(p-1)/2$, we have $l \mid h_K$.*

We state (a corollary to) Theorem 2 in another way: *If (at least) two prime numbers p and q ramify completely in an algebraic number field K of degree n, then we have $l \mid h_K$ for any prime factor l of $(n, (p-1)/2) \times (n, (q-1)/2)$.*

(B) Another prime number $q \neq p$ with $q^{(p-1)/t} \not\equiv 1 \pmod p$ has a prime divisor of degree 1 in K.

If (B) is satisfied, then we have $K \not\supset k_t$ $(t \neq 1)$. In particular, if a prime number q, which is a primitive root modulo p, has a prime divisor of degree 1 in K, then we have $K \not\supset k_t$ for any $t \mid (p-1)/2$ $(t \neq 1)$; this is the case treated in [2]. Here we consider the cases $t = (p-1)/2$ and $t = 2$ (for $p \equiv 1 \pmod 4$). (i) If there is a prime number $q \neq p$ with $q \not\equiv \pm 1 \pmod p$ and having a prime divisor of degree 1 in K, then we have $K \not\supset \mathbf{Q}(\zeta_p)_0$. (ii) On the other hand, if there is a prime number $q \neq p$ with $q^{(p-1)/2} \not\equiv 1 \pmod p$, i.e., $\left(\frac{q}{p}\right) = -1$[1] and having a prime divisor of degree 1 in K, then we have $K \not\supset \mathbf{Q}(\sqrt{p})$.

EXAMPLE 1. Let $f(X) = X^n + aX + b$ be an Eisenstein trinomial, of degree n, with respect to p (>3) and let $K = \mathbf{Q}(\alpha)$ with $f(\alpha) = 0$. Let q be a prime number $\neq p$, and assume $q \nmid a$, $q \mid b$ and $q \nmid (n-1)$. Then,

[1] As $p \equiv 1 \pmod 4$, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

as q does not divide the discriminant $n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n$ of $f(X)$ and we have $f(X) \equiv X(X^{n-1} + a) \pmod q$, the prime number q has a prime divisor of degree 1 in K. (i) Suppose $(p-1)/2 \mid n$. If $q \not\equiv \pm 1 \pmod p$, then we have $K \not\supset \mathbf{Q}(\zeta_p)_0$ and so $(h_K, (p-1)/2) > 1$. (ii) Suppose $p \equiv 1 \pmod 4$ and $2 \mid n$. If $\left(\frac{q}{p}\right) = -1$, then we have $K \not\supset \mathbf{Q}(\sqrt{p})$ and so $2 \mid h_K$.

(c) For $K = \mathbf{Q}(\alpha)$ with $\alpha^n + 7C_1\alpha + 21C_2 = 0$, where $3 \mid n$ and $(C_1, 3) = (C_2, 7) = 1$ $(C_1, C_2 \in \mathbf{Z})$, we have $3 \mid h_K$ $(p = 7, q = 3)$.

(d) For $K = \mathbf{Q}(\alpha)$ with $\alpha^n + 5D_1\alpha + 10D_2 = 0$, where $2 \mid n$ and $(D_1, 2) = (D_2, 5) = 1$ $(D_1, D_2 \in \mathbf{Z})$, we have $2 \mid h_K$ $(p = 5, q = 2)$.

(C) Another prime number $q \neq p$ with $q^{(p-1)/t} \equiv 1 \pmod p$ has a prime divisor of degree $> n/t$ in K.

If (C) is satisfied, then we have also $K \not\supset k_t$ $(t \neq 1)$. We consider the case $t = 2$ (for $p \equiv 1 \pmod 4$). If there is a prime number $q \neq p$ with $q^{(p-1)/2} \equiv 1 \pmod p$, i.e., $\left(\frac{q}{p}\right) = 1$ and having a prime divisor of degree $> n/2$ (i.e., of degree n) in K, then we have $K \not\supset \mathbf{Q}(\sqrt{p})$.

EXAMPLE 2. Let l be an odd prime number and q a prime number, which is a primitive root modulo l. Let $f(X)$ be an Eisenstein polynomial, of degree $n = l - 1$, with respect to p such that $p \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = 1$, and let $K = \mathbf{Q}(\alpha)$ with $f(\alpha) = 0$. Assume that $f(X)$ is congruent to the l-th cyclotomic polynomial $\Phi_l(X) = X^{l-1} + X^{l-2} + \cdots + X + 1$ modulo q. Then clearly q does not divide the discriminant of $\Phi_l(X)$ and so that of $f(X)$. As q is a primitive root modulo l, q remains prime in $\mathbf{Q}(\zeta_l)$, which implies that $\Phi_l(X)$ and so $f(X)$ are irreducible modulo q. Hence we see that q also remains prime in K and so we have $K \not\supset \mathbf{Q}(\sqrt{p})$.

(e) For $K = \mathbf{Q}(\alpha)$ with $\alpha^4 + 17E_1\alpha^3 + 17E_2\alpha^2 + 17E_3\alpha + 17E_4 = 0$, where $(E_1E_2E_3E_4, 2) = 1$ and $(E_4, 17) = 1$ $(E_1, E_2, E_3, E_4 \in \mathbf{Z})$, we have $2 \mid h_K$ $(p = 17, l = 5, q = 2)$.

3. Next we consider the special case $n \mid (p-1)/2$.

THEOREM 3. *If* $n \mid (p-1)/2$ *and* $K \not\subset \mathbf{Q}(\zeta_p)_0$, *i.e.*, $K \neq k_n$ *(say if* $n \mid (p-1)/2$ *and K is not totally real), then we have* $(h_K, n) > 1$.[2]

[2] A special case of Theorem 3 ($n = l$ is an odd prime divisor of $p - 1$) was proved in [2]. There we have also shown that $k_l K$ is an unramified abelian extension, of degree l, of K.

Proof. Then k_n is contained in K if and only if $K = k_n$.

We state Theorem 3 in another way: *Let n be a divisor of $(p-1)/2$. Then the class numbers h_K of all the algebraic number fields K of degree n and of Eisenstein type with respect to p satisfy $(h_K, n) > 1$, except the case where K is the unique subfield k_n, of degree n, of $\mathbf{Q}(\zeta_p)$.*[3]

COROLLARY. *Let $f(X) = X^n + aX^m + b$ ($n > m > 0$ and $a \neq 0$) be an Eisenstein trinomial with respect to an odd prime number $p \equiv 1 \pmod{2n}$. Let $K = \mathbf{Q}(\alpha)$ with $f(\alpha) = 0$. If $n \geqslant 5$, then we have $(h_K, n) > 1$. If $n = 4$ and $m = 1$ or 3, then we have also $(h_K, 4) > 1$, i.e., $2 \mid h_K$.*[4]

Proof. By Theorem 3, it suffices to show that K is not totally real. If $n - m$ is even, $f'(X) = nX^{n-1} + maX^{m-1} = X^{m-1}(nX^{n-m} + ma)$ has at most three real roots and so $f(X)$ has at most four real roots. Hence if $n \geqslant 5$, K is not totally real. If $n - m$ is odd, $f'(X)$ has at most two real roots and so $f(X)$ has at most three real roots. Hence if $n \geqslant 5$ or $n = 4$ with $m = 1, 3$, K is not totally real.

EXAMPLE 3. Similar arguments as in the proof of Corollary to Theorem 3 give many consequences. For example, let $p \equiv 1 \pmod 8$ and let $f(X) = X^4 + aX^2 + bX + c$ be an Eisenstein polynomial with respect to p. Let $K = \mathbf{Q}(\alpha)$ with $f(\alpha) = 0$. (As a remark, every algebraic number field of degree 4 and of Eisenstein type with respect to p is obtained by adjoining a root of such an $f(X)$ to $\mathbf{Q}$.) Assume $8a^3 + 27b^2 > 0$ (say $a > 0$). Then the discriminant of $f'(X) = 4X^3 + 2aX + b$ is negative and so $f'(X)$ has only one real root. Hence $f(X)$ has at most two real roots and so K is not totally real, which implies that we have $(h_K, 4) > 1$, i.e., $2 \mid h_K$.

Note added in proof. After the manuscript was submitted, our results were generalized in the papers of Madan (*Crelles J.* **252** (1972)), Frey and Geyer (*Crelles J.* **254** (1972)) and Ishida (to appear in *Crelles J.*).

REFERENCES

1. H. HASSE, Vorlesungen über Klassenkörpertheorie, Würzburg (1967).
2. M. ISHIDA, Class numbers of algebraic number fields of Eisenstein type, *J. Number Theory* **2** (1970), 404–413.

[3] We can not say anything about the class number of k_n.

[4] We have considered Eisenstein binomials and cubic Eisenstein trinomials in [2].