On Algebraic Number Fields whose Class Numbers are Multiples of 3

Dedicated to Professor S. Tomatsu on his 60th birthday

Kiichiro OHTA

Dept. of Math., Fac. of Gen. Educ., Gifu Univ.

(Received Oct. 5, 1981)

§ 1. Introduction

As usual we denote by $\mathbf{Z}$ and $\mathbf{Q}$ the ring of rational integers and the rational number field respectively.

T. Honda proved in 1967 the following theorem (cf. [1]) by means of dealing with the monic irreducible polynomials of degree 3 in $\mathbf{Z}[X]$ such that each of their splitting fields is unramified over its quadratic subfield respectively. Namely;

THEOREM. *(Honda) Set* $K(m, n)=Q(\sqrt{4m^3-27n^2})$ *for* $m, n \in \mathbf{Z}$. *If* $(m, 3n)=1$ *and if* m *cannot be represented in a form* $(n+h^3)/h$ *with* $h \in \mathbf{Z}$, *the class number of* $K(m, n)$ *is a multiple of 3.*

In this paper, using the solvability of the alternative group A_4 of degree 4, we shall prove in general that algebraic number fields of degree $n!/12$ of certain type, where $n \geqq 4$, have class numbers which are always divisible by 3 (Theorem 1). Moreover, considering the special case where $n=4$, we shall give the quadratic number fields of another type such that their class numbers are also multiples of 3 (Theorem 4).

§ 2. Main theorems

Let K be an algebraic number field. In following we shall say that K is an S_n-extension of $\mathbf{Q}$ if the Galois group $G(K/\mathbf{Q})$ is isomorphic to the symmetric group S_n of degree n.

THEOREM 1. *Let* $f(X)$ *be a monic irreducible polynomial of degree* $n \geqq 4$ *in* $\mathbf{Z}[X]$, *whose roots and discriminant we denote by* $\theta_1, \ldots, \theta_n$ *and* D *respectively. Moreover, let* K *be the splitting field of* $f(X)$ *and suppose that* K *is an* S_n*-extension of* $\mathbf{Q}$. *If there exist no prime ideals in* K *whose ramification indexes with respect to* $\mathbf{Q}$ *are multiples of 3, then the class number of the field* $F=\mathbf{Q}(\sqrt{D}, \theta_1, \ldots, \theta_{n-4})$ *(if* $n=4$, *then* $F=\mathbf{Q}(\sqrt{D})$*) is a multiple of 3.*

PROOF. It is clear from our assumption that the Galois group $G(K/F)$ is isomorphic to the alternative group A_4 of degree 4. Hence, it follows immediately from the solvability of A_4 that there exists an intermediate field L between F and K such that L/F is an abelian exten-

sion of degree 3. Now, from our assumption it follows immediately that L is unramified over F, and this implies that the class number of F is a multiple of 3. q. e. d.

It is known that there exist polynomials of several types in $\mathbf{Z}[X]$ such that each of their splitting fields has no finite prime ideals which ramify over the quadratic subfield (cf. [**2**], [**3**] and [**4**]). If we apply Theorem 1 to these polynomials, then we have immediately the following theorem;

THEOREM 2. *Let notations be as in Theorem* 1 *and suppose K is an S_n-extension of* $\mathbf{Q}$. *If $f(X)$ is any one of the following;*

(1) $f(X)=X^n-aX+b$, *where* $((n-1)a, nb)=1$,

(2) $f(X)=X^n-aX^2+b$, *where* $(2(n-2)a, nb)=1$,

(3) $f(X)=X^n-aX^s\pm 1$, *where* $(n, s(n-s)a)=1$,

(4) $f(X)=(X-a)^r(X-b)^t\pm 1$, *where* $s+t=n$ *and* $(n, bs+at)=1$,

then the class number of the field $F=Q(\sqrt{D}, \theta_1, \ldots, \theta_{n-4})$ *(if* $n=4$, *then* $F=Q(\sqrt{D})$*) is always divible by 3.*

PROOF. Since there exist no finite prime ideals in K which ramify in $K/Q(\sqrt{D})$ in every case in our theorem (cf, [**2**], [**3**] and [**4**]), our assertion follows immediately from Theorem 1. q. e. d.

Now, we shall show that we can extend the polynomials of types (1), (2) and (3) in Theorem 2 to the Eisenstein polynomials respectively. Namely, we have the following;

THEOREM 3. *Let notations be as in Theorem 1. Moreover, let* $p_1, \ldots p_r$ *be prime numbers different from each other and* $\alpha_1, \ldots, \alpha_r$ *be positive integers. Suppose K is an S_n-extension of* $\mathbf{Q}$. *If $f(X)$ is any one of the following;*

(5) $f(X)=X^n-ap_1^{\alpha_1}\ldots p_r^{\alpha_r}X+bp_1\ldots p_r$, *where* $(3nab, p_1\ldots p_r)=1$ *and* $((n-1)a, nb)=1$,

(6) $f(X)=X^n-ap_1^{\alpha_1}\ldots p_r^{\alpha_r}X^2+bp_1\ldots p_r$, *where* $(3nab, p_1\ldots p_r)=1$ *and* $(2(n-2)a, nb)=1$,

(7) $f(X)=X^n-ap_1^{\alpha_1}\ldots p_r^{\alpha_r}X^s\pm p_1\ldots p_r$, *where* $(3na, p_1\ldots p_r)=1$ *and* $(n, s(n-s)a)=1$,

then the class number of the field $F=Q(\sqrt{D}, \theta_1, \ldots, \theta_{n-4})$ *(if* $n=4$, *then* $F=Q(\sqrt{D})$*) is always divible by 3.*

PROOF. We denote by p any one of prime numbers $p_1, \ldots, p_r$ and let $\mathfrak{P}$ and $\mathfrak{p}$ be prime ideals in K and $k=Q(\theta_1)$ respectively such that we have $\mathfrak{p}|(p)$ and $\mathfrak{P}|\mathfrak{p}$. Since $f(X)$ is an Eisenstein polynomial with respect to prime number p, it is well known that we have $(p)=\mathfrak{p}^n$. Hence, if we suppose $\mathfrak{P}^e\|(p)$, then we have $n|e$ clearly. Now, we denote by T and V the inertial field and the first ramification field of $\mathfrak{P}$ in K/Q respectively and we set $p^\nu=[K:V]$, where $\nu\geqq 0$, and $e_0=[V:T]$ respectively. Then, as we have $e=e_0p^\nu$, $(e_0, p)=1$ and moreover $(p, n)=1$ in our case, it follows $n|e_0$ clearly. Since the Galois group $G(V/T)$ is a cyclic group with order e_0, it is easily seen that there exists an element of $G(K/\mathbf{Q})$ whose order is e_0. But, since the Galois group $G(K/\mathbf{Q})$ is isomorphic to the symmetric group S_n of degree n, it follows easily that there exists no element of $G(K/\mathbf{Q})$ whose order is a proper multiple of n. Hence, we must have $e_0=n$. Moreover, if $\mathfrak{P}$ ramifies in K/F, then the ramification index of $\mathfrak{P}$ in K/F must be a power of p because we have $k\subset F$ and $(p)=\mathfrak{p}^n$. Hence, if the ramification index of $\mathfrak{P}$ in K/F is divisible by 3, then we must have $p=3$. But in our case we have $p\neq 3$ from our assumption. Thus, if we denote by L the intermediate field between F and K which is an abelian extension of degree 3 over F, then the factor of (p)

in L is unramified in L/F clearly.

Finally, for any prime number q different from p_i $(i=1, \ldots, r)$ we can easily verify that every prime factor of (q) in K is unramified in K/F, because as in cases (1), (2) and (3) in Theorem 2 every prime factor of (q) in K is unramified in $K/\mathbf{Q}(\sqrt{D})$.

§ 3. The case n=4

Now, we shall deal with the case where $n=4$ in (5). It is easily seen that the discriminant of polynomial $f(X)=X^4-ax+b$ is equal to $D=4^4b^3-3^3a^4$. Using this we can prove the following theorem. Namely;

THEOREM 4. *Let a and b be rational integers and $p_1, \ldots, p_r$ be prime numbers different from each other such that we have $(6ab, p_1 \ldots p_r)=1$ and $(3a, 4b)=1$. Moreover, let $\alpha_1, \ldots, \alpha_r$ be positive integers. If we have either*

$$(8)\quad \begin{cases} ap_1^{\alpha_1} \ldots p_r^{\alpha_r} \equiv \pm 1 & (\mathrm{mod}\ 3) \\ bp_1 \ldots p_r \equiv 1 & (\mathrm{mod}\ 3) \end{cases}$$

or

$$(9)\quad \begin{cases} ap_1^{\alpha_1} \ldots p_r^{\alpha_r} \equiv \pm 2 & (\mathrm{mod}\ 5) \\ bp_1 \ldots p_r \equiv 1 & (\mathrm{mod}\ 5), \end{cases}$$

then the class number of the quadratic number field

$$k=\mathbf{Q}(\sqrt{p_1 \ldots p_r(4^4b^3-3^3a^4p_1^{4\alpha_1-3} \ldots p_r^{4\alpha_r-3})})$$

is divisible by 3.

PROOF. Set $f(X)=X^4+ap_1^{\alpha_1} \ldots p_r^{\alpha_r}X+bp_1 \ldots p_r$, where we suppose $(6ab, p_1 \ldots p_r)=1$ and $(3a, 4b)=1$, then the discriminant of $f(X)$ is $D=(p_1 \ldots p_r)^3(4^4b^3-3^3a^4p_1^{4\alpha_1-3} \ldots p_r^{4\alpha_r-3})$ clearly. If the splitting field K of $f(X)$ is an S_4-extension of $\mathbf{Q}$, then our assertion follows immediately from Theorem 3. Hence, we have only to prove that K is an S_4-extension of $\mathbf{Q}$ in our cases.

(a) Case (8)

we have either

$$f(X) \equiv X^4-X+1 \equiv (X+1)(X^3-X^2+X+1) \quad (\mathrm{mod}\ 3)$$

or

$$f(X) \equiv X^4+X+1 \equiv (X-1)(X^3+X^2+X-1) \quad (\mathrm{mod}\ 3)$$

and both X^3-X^2+X+1 and X^3+X^2+X-1 are irreducible with respect to mod 3. Moreover D is prime to 3 clearly. From these facts we can easily prove that the Galois group $G(K/\mathbf{Q})$ contains an element of order 3. On the other hand, as the ramification index of each factor of (p_i) in K with respect to $\mathbf{Q}$ is equal to 4 clearly, it is easily seen that $G(K/\mathbf{Q})$ contains an element whose order is 4. Now, from these facts it follows immediately that $G(K/\mathbf{Q})$ is isomorphic to S_4.

(b) case (9)

we have either

$$f(X) \equiv X^4-2X+1 \equiv (X-1)(X^3+X^2+X-1) \quad (\mathrm{mod}\ 5)$$

or

$$f(X) \equiv X^4+2X+1 \equiv (X+1)(X^3-X^2+X+1) \quad \mathrm{mod}\ 5)$$

and both X^3+X^2+X-1 and X^3-X^2+X+1 are irreducible with respect to mod 5. Moreo-

ver, it is easily seen that D is not divisible by 5 because we have $D\equiv -1 \pmod 5$. From these facts we can easily prove that $G(K/\mathbf{Q})$ is isomorphic to S_4 as well as in case (8).

p. e. b.

Example 1. If $f(X)=X^4+7X+7$, then we have $\mathbf{Q}(\sqrt{D})=\mathbf{Q}(\sqrt{469})$, whose class number is 3.

Example 2. If $f(X)=X^4-13X+26$, then we have $\mathbf{Q}(\sqrt{D})=\mathbf{Q}(\sqrt{2201})$, whose class number is 6.

§ 4. The case n=5

Finally, we shall deal with the case where $n=5$. in (5) and (6). Namely, we have the following theorem.

THEOREM 5. *Let $f(X)$ be a monic irreducible polynomial of degree 5 in $\mathbf{Z}[X]$, whose root and discriminant we denoteo and D respectively. Moreover, let a and b be integers and $p_1, \ldots,$ p_r be prime numbers different from each other such that we have $(15ab, p_1 \ldots p_r)=1$ and $(6a, 5b)=1$. If we have either*

(10) *$f(X)=X^5-ap_1^{\alpha_r}\ldots p_r^{\alpha_r}X+bp_1\ldots p_r$, where $\alpha_1, \ldots, \alpha_r$ are positive integers and $ap_1^{\alpha_1}\ldots p_r^{\alpha_r}\equiv -2 \pmod{17}$, $bp_1\ldots p_r\equiv 1 \pmod{17}$,*

or

(11) *$f(X)=X^5-ap_1^{\alpha_1}\ldots p_r^{\alpha_r}X^2+bp_1\ldots p_r$, where $\alpha_1, \ldots, \alpha_r$ are positive integers and either $ap_1^{\alpha_1}\ldots p_r^{\alpha_r}\equiv bp_1\ldots p_r\equiv -1 \pmod 3$ or $ap_1^{\alpha_1}\ldots p_r^{\alpha_r}\equiv -1 \pmod{17}$ and $bp_1\ldots p_r\equiv 1 \pmod{17}$, then the class number of the field $F=\mathbf{Q}(\sqrt{D}, \theta)$ is divisible by 3.*

PROOF. We denote by K the spitting field of $f(X)$. From Theorem 3 we have only to prove that K is an S_5-extension of $\mathbf{Q}$. But this is done for both cases in [**4**] and [**2**] respectively. Namely, for case (10) we have

$$f(X)\equiv (X^2+9X+10)(X^3+8X^2+3X+12) \pmod{17}$$

and this implies that the Galois group $G(K/\mathbf{Q})$ contains a transposition and hence $G(K/\mathbf{Q})$ is isomorphic to S_5 clearly. For case (11) we have either

$$f(X)\equiv (X^2-X+1)(X^3+X^2-X+1) \pmod 3$$

or

$$f(X)\equiv (X^2+X+3)(X^3-X^2-2X+6) \pmod{17}$$

and hence it is easily seen that $G(K/\mathbf{Q})$ is isomorphic to S_5 as well as in case (10).

References

[**1**] T. Honda, On real quadratic fields whose class numbers are multiples of 3, J. Reine Angew. Math. 233 (1968), 101-102.

[**2**] K. Ohta, On unramified Galois extensions of quadratic number fields, (in Japanese) Sūgaku 24 (1972), 39-40.

[**3**] K. Uchida, Unramified extensions of quadratic number fields, Tōhoku Math. J. 22 (1970) 138-141 and 220-224.

[**4**] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970), 57-76.