On a family of quadratic fields whose class numbers are divisible by five

By Masahiko SASE

Deparment of Mathematics, Faculty of Science, Gakushuin University, 1-5-1
Mejiro, Toshima-ku, Tokyo 171-8588

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 14, 1998)

Abstract: In this paper, we construct a family of quadratic fields whose class numbers are divisible by five. We obtain this result by extending the method of Kishi and Miyake [1] and using a family of quintics introduced by Kondo [2].

Notation. Throughout this paper, we shall use the following notation. $\boldsymbol{Z}$, $\boldsymbol{Q}$ will be used in the usual sense. For a rational prime p and $a \in \boldsymbol{Z}$, $a \neq 0$, $\nu_p(a)$ will mean the greatest exponent m such that $P^m \mid a$. We shall consider various number fields, i.e. finite extensions of $\boldsymbol{Q}$, k, K, L, F, ... If $\mathfrak{p}$ is a prime ideal and $\mathfrak{a}$ an integral ideal $\neq 0$ in a number field, $\nu_{\mathfrak{p}}(\mathfrak{a})$ will mean the greatest exponent m such that $\mathfrak{p}^m \mid \mathfrak{a}$. If $\mathfrak{p}$ is a prime ideal dividing p, $e_{\mathfrak{p}/p}$ will mean the ramification index of $\mathfrak{p}$. For $f(x) \in \boldsymbol{Z}[x]$, $f^{(j)}(x)$ will mean the jth derivative of $f(x)$. C_n will mean the cyclic group with order n; D_n the dihedral group with order $2n$. h_k will mean the class number of a number field k. If K is a Galois extension of k, $G(K/k)$ will mean the Galois group for K/k.

1. Ramification of primes. Let q be an odd prime and $f(x)$ be an irreducible polynomial of degree q in $\boldsymbol{Q}[x]$. Let θ be a root of $f(x)$ and $F = \boldsymbol{Q}(\theta)$. We denote by L the minimal splitting field of $f(x)$ over $\boldsymbol{Q}$. We shall first prove:

Proposition 1. *Suppose* $[L:\boldsymbol{Q}] \leq 2q$ *and that no prime number is totally ramified in* F. *Then* $G(L/\boldsymbol{Q})$ *is isomorphic to* D_q *and* L *is an unramified cyclic extension of degree* q *over the quadratic field* k *contained in* L *which is unique.*

Proof. Since $[L:\boldsymbol{Q}] \leq 2q$ and $q \mid [L:\boldsymbol{Q}]$, $G(L/\boldsymbol{Q})$ should be C_q or D_q. But C_q is excluded because of our assumption on the ramification in $F/\boldsymbol{Q}$. Thus $G(L/\boldsymbol{Q}) \cong D_q$ and there is a unique k such that $L \supset k \supset \boldsymbol{Q}$, $[k:\boldsymbol{Q}] = 2$ and $[L:k] = q$. Next, we have to prove that L/k is unramified. Suppose a prime ideal $\mathfrak{P}$ of L is ramified in L/k. Its ramification index is q since L/k is a cyclic extension with degree q. Since $[L:F] = 2$, the prime $\mathfrak{p} = \mathfrak{P} \cap F$ is totaly ramified in $F/\boldsymbol{Q}$. This contradicts to the assumption. Since q is odd, the infinite primes of k are also unramified. □

We next study the ramification of a prime in F. We write the polynomial $f(x)$ of the form

$$f(x) = x^q + \sum_{j=0}^{q-1} a_j x^j,\ a_j \in \boldsymbol{Z}, \quad (*)$$

and consider the following condition for the coefficients of $f(x)$ and a prime p:

$C(f, p)$: There is a number $j \in \{0, 1, \ldots, q-1\}$ such that $\nu_p(a_j) < q - j$.

The following lemma is an obvious consequence of [5, Proposition 6.2.1].

Lemma 1. *Let* p *be a prime that is totally ramified in* F. *Then the factorization of* $f(x)$ *modulo* p *is given by*

$$f(x) \equiv (x + a)^q \bmod p,$$

with some $a \in \boldsymbol{Z}$.

For a proof of next lemma, we refer to Bauer [4] or Llorente and Nart [3].

Lemma 2. *Let* p *be a prime. Assume that* $f(0) \equiv 0 \bmod p$, *and the condition* $C(f, p)$ *is satisfied. Then* p *is totally ramified in* F *if and only if the Newton polygon of* $f(x)$ *with respect to* p *has only one side.*

We are now ready to mention a criterion for a prime to be totally ramified in F.

Proposition 2. *Let* p *be a prime and* $f(x)$ *be an irreducible polynomial of degree* q *of the form* $(*)$ *satisfing* $C(f, p)$, *and furthermore, assume that* $a_{q-1} = 0$. *Then* p *is totally ramified in* F *if and only if the following conditions are satisfied.*

(a) *If* $p \neq q$,

$$0 < \frac{\nu_p(a_0)}{q} \leq \frac{\nu_p(a_j)}{q-j} \text{ for any } j \in \{1, 2, \cdots, q-2\}.$$