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 $P^m | a$. 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 $\mathfrak{p}^m | \mathfrak{a}$. 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 $q | [L:\boldsymbol{Q}]$, $G(L/\boldsymbol{Q})$ 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 $p \neq q$,*

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

(b) *If $p = q$, one of the following conditions* (i), (ii) *holds*:

(i) $0 < \frac{\nu_q(a_0)}{q} \leq \frac{\nu_q(a_j)}{q-j}$ *for any* $j \in \{1, 2, \cdots, q-2\}$,

(ii) $\nu_q(a_0) = 0$, $\nu_q(a_j) > 0$ *for any* $j \in \{1, 2, \cdots, q-2\}$,

$$\frac{\nu_q(f(-a_0))}{q} \leq \frac{\nu_q(f^{(j)}(-a_0))}{q-j} \text{ for any } j \in \{1, 2, \cdots, q-1\},$$

and $\nu_q(f^{(j)}(-a_0)) < q-j$ *for some* $j \in \{0, 1, \ldots, q-1\}$.

Proof. *Case I.* $\nu_p(a_0) > 0$. In this case, we can easily show by Lemma 2 that p is totally ramified if and only if p satisfies that $0 < \nu_p(a_0)/q \leq \nu_p(a_j)/(q-j)$ for all j.

Case II. $\nu_p(a_0) = 0$ and $p \neq q$. Then we have $f(x) \not\equiv (x+a)^q \bmod p$, for any $a \in \boldsymbol{Z}$, since $a_{q-1} = 0$. So by Lemma 1, p is not totally ramified in F.

Case III. $\nu_p(a_0) = 0$ and $p = q$. If $\nu_q(a_j) = 0$ for some $j > 0$, then it is shown in the same manner as in the Case II that q is not totally ramified in F. Now consider the case $\nu_q(a_j) > 0$ for all $j > 0$. Then $f(x) \equiv (x+a_0)^q \bmod q$. We use $f_1(x) = f(x-a_0)$ instead of $f(x)$;

$$f_1(x) = x^q + \sum_{j=0}^{q-1} \frac{f^{(j)}(-a_0)}{j!} x^j \in \boldsymbol{Z}[x].$$

We have $f_1(0) \equiv f(-a_0) \equiv 0 \bmod q$ and see that the condition $C(f_1, q)$ means $\nu_q(f^{(j)}(-a_0)) < q - j$ for some j, $0 \leq j \leq q-1$. So by Lemma 2, under the condition $C(f_1, q)$, q is totally ramified or not in F, according as the inequality $\nu_q(f(-a_0))/q \leq \nu_q(f^{(j)}(-a_0))/(q-j)$ for all j holds or does not hold. Finally, assume that $\nu_q(f^{(j)}(-a_0)) \geq q-j$ for all j. Then putting $f_2(x) = f_1(qx)/q^q \in \boldsymbol{Z}[x]$, we see that the coefficient of $f_2(x)$ of degree $q-1$ is $-a_0$, so $f_2(x) \not\equiv (x+a)^q \bmod q$, for any $a \in \boldsymbol{Z}$. Hence q is not totally ramified in F.

The proof is easily completed by the above argument. □

2. A family of certain quintics. In this section, we consider a family of quintics introduced by Kondo [2]. Let A, B be indeterminates and put

$$f(x; A, B) = x^5 + (A-3)x^4 + (B-A+3)x^3 + (A^2-A-1-2B)x^2 + Bx + A. \quad (**)$$

The discriminant of $f(x; A, B)$ is

$$d(f) = A^2 \Delta(A, B)^2$$

where

$$\Delta(A, B) = -4B^3 + (A^2-30A+1)B^2 + (24A^3-34A^2-14A)B - 4A^5 + 4A^4 + 40A^3 - 91A^2 + 4A.$$

Kondo [2] showed the following result about this family:

Proposition 3 (Kondo [2]). *Let A, B be indeterminates which are algebraically independent over $\boldsymbol{Q}$ and L be the minimal splitting field of $f(x; A, B)$ over $\boldsymbol{Q}(A, B)$. Then, $G(L/\boldsymbol{Q}(A, B))$ is isomorphic to D_5 and the quadratic field over $\boldsymbol{Q}(A, B)$ contained in L is given by $\boldsymbol{Q}(A, B, \sqrt{\Delta(A, B)})$.*

From this, $G(L/\boldsymbol{Q}(A, B))$ is solvable (cf. Dummit [5]) and the discriminant of $f(x; a, b)$ is a square in $\boldsymbol{Q}$ for any $a, b \in \boldsymbol{Q}$. So we obtain the following:

Proposition 4. *For $a, b \in \boldsymbol{Q}$, let L be the minimal splitting field of $f(x; a, b)$ over $\boldsymbol{Q}$. If $f(x; a, b)$ is irreducible over $\boldsymbol{Q}$, then $G(L/\boldsymbol{Q})$ is isomorphic to C_5 or D_5.*

3. Main theorem. Now we give a family of quadratic fields whose class numbers are divisible by five.

Theorem. *Let $b, c \in \boldsymbol{Z}$ and put $g(y; b, c) = y^5 + Sy^3 + Ty^2 + Uy + V$, where*

$$S = -10c^2 - 5c + b,$$
$$T = 20c^3 + 40c^2 + 25c - 3bc - 2b + 5,$$
$$U = -(3c+1)(5c^3 + 20c^2 - bc + 10c - b),$$
$$V = 4c^5 + 30c^4 - bc^3 + 25c^3 - 2bc^2 + 5c^2 - bc + 5c + 3.$$

If $g(y; b, c)$ is irreducible in $\boldsymbol{Q}$ and $(S, T, U) = 1$, then the class number of the quadratic field $k = \boldsymbol{Q}(\sqrt{m})$ is divisible by five, where

$$m = -4b^3 + 5(5c^2 - 24c - 16)b^2 + 50(60c^3 + 90c^2 + 43c + 6)b - 125(100c^5 + 280c^4 + 272c^3 + 119c^2 + 26c + 3).$$

Proof. Putting $A = 5c+3$, $B = b$ in the polynomial (**), we obtain

$$f(x; 5c+3, b) = x^5 + 5cx^4 + (b-5c)x^3 + (25c^2 + 25c + 5 - 2b)x^2 + bx + 5c + 3.$$

Note that $g(y; b, c) = f(y-c; 5c+3, b)$ and that $\Delta(5c+3, b)$ is equal to m. Let θ be a root of $g(y; b, c)$ and $F = \boldsymbol{Q}(\theta)$. By Proposition 2 no prime number is totally ramified in F, for $g(y; b, c)$ is irreducible and $(S, T, U) = 1$. By Propositions 1 and 4, the Galois group of $g(y; b, c)$ is isomorphic to D_5, and the quadratic field $k = \boldsymbol{Q}(\sqrt{m})$ has unramified cyclic extension of degree five. □

Example 1 (THE CASE $c = 0$). Let $b \in \boldsymbol{Z}$, $(b, 5) = 1$, and $m = -4b^3 - 80b^2 + 300b -$

375. Then the class number of $\boldsymbol{Q}(\sqrt{m})$ is divisible by five. Indeed, since $g(y\,;\,b,\,0)=y^5+by^3-(2b-5)y^2+by+3$ is irreducible in $\boldsymbol{Z}/2\boldsymbol{Z}$, g is irreducible in $\boldsymbol{Q}$.

Example 2 (THE CASE $c=-1$). Let $b\in\boldsymbol{Z}$, $(b,5)=1$, and $m=-4b^3+65b^2-300b-500$. If $g(y\,;\,b,\,1)=y^5+(b-5)y^3+by^2+10y+4$ is irreducible in $\boldsymbol{Q}$, then the class number of $\boldsymbol{Q}(\sqrt{m})$ is divisible by five.

Remark. These examples give explicitly a parametric family of quadratic fields k whose class numbers are divisible by five. We need no discussions about the units of k to establish this fact.

Table for Example 1

$c=0$, $m=-4b^3-80b^2+300b-375$, $k=\boldsymbol{Q}(\sqrt{m})$			
b	$m=s^2\cdot m'$	m'	h_k
9	−7071	−1·3·2357	70
8	−5143	−1·37·139	40
7	−3567	−1·3·29·41	20
6	−2319	−1·3·773	30
4	$3^2\cdot(-79)$	−1·79	5
3	−303	−1·3·101	10
2	−127	−1·127	5
1	−159	−1·3·53	10
−1	−751	−1·751	15
−2	−1263	−1·3·421	20
−3	−1887	−1·3·17·3	20
−4	−2599	−1·23·113	30
−6	−4191	−1·3·11·127	60
−7	−5023	−1·5023	25
−8	−5847	−1·3·1949	50
−9	−6639	−1·3·2213	90
−11	−8031	−1·3·2677	60
−12	−8583	−1·3·2861	50
−13	−9007	−1·9007	35
−14	$3^2\cdot(-1031)$	−1·1031	35
−16	−9271	−1·73·127	60
−17	−8943	−1·3·11·271	60
−18	−8367	−1·3·2789	30
−19	−7519	−1·73·103	50
−21	−4911	−1·3·1637	50
−22	−3103	−1·29·107	20
−23	$3^2\cdot(-103)$	−1·103	5
−24	1641	3·547	5
−26	8049	3·2683	5
−27	11937	3·23·173	10
−28	16313	11·1483	5
−29	21201	3·37·191	10

Table for Example 2

$c=0$, $m=-4b^3+65b^2-300b-500$, $k=\boldsymbol{Q}(\sqrt{m})$			
b	$m=s^2\cdot m'$	m'	h_k
19	−10171	−1·7·1453	20
18	$2^2\cdot(-2042)$	−1·2·1021	50
17	−6467	−1·29·223	20
16	$2^2\cdot(-1261)$	−1·13·97	20
14	$2^2\cdot(-734)$	−1·2·367	40
13	−2203	−1·2203	5
12	$2^2\cdot(-413)$	−1·7·59	20
11	−1259	−1·1259	15
9	−851	−1·23·37	10
8	$2^2\cdot(-197)$	−1·197	10
7	−787	−1·787	5
6	$2^2\cdot(-206)$	−1·2·103	20
4	$2^2\cdot(-229)$	−1·229	10
3	−923	−1·13·71	10
2	$2^2\cdot(-218)$	−1·2·109	10
1	−739	−1·739	5
−1	−131	−1·131	5
−3	1093	1093	5
−4	$2^2\cdot 499$	499	5
−6	$2^2\cdot 1126$	2·563	5
−7	6157	47·131	5
−8	$2^2\cdot 2027$	2027	5
−9	10381	7·1483	5
−11	15989	59·271	5
−12	$2^2\cdot 4843$	29·167	10
−13	23173	23173	5
−14	$2^2\cdot 6854$	2·23·149	10
−16	$2^2\cdot 9331$	7·31·43	20
−17	43037	43037	5
−18	$2^2\cdot 12322$	2·61·101	20
−19	56101	56101	5
−21	71509	43·1663	5
−22	$2^2\cdot 20038$	2·43·233	10
−23	89453	7·13·983	10
−24	$2^2\cdot 24859$	24859	25

Acknowledgements. The author wishes to thank Prof. Shokichi Iyanaga, M. J. A., and Prof. Shin Nakano for their warm encouragement.

References

[1] Y. Kishi and K. Miyake: Characterization of the quadratic fields whose class numbers are divisible by three (preprint).
[2] T. Kondo: On a family of sexic polynomials found by Brumer. Proc. of the 2-nd Symp. on Number

Theory, Tsuda Coll., pp. 27–36 (1997).
[3] P. Llorente and E. Nart: Effective determination of the decomposition of the rational primes in a cubic field. Proc. Amer. Math. Soc., **87**, 579–585 (1983).
[4] M. Bauer: Zur allgemeinen Theorie der algebraischen Grössen. J. Reine Angew. Math., **132**, 21–32 (1907).
[5] D. S. Dummit: Solving solvable quintics. Math. Comp., **57**, 387–401 (1991).
[6] H. Cohen: A Course in Computational Algebraic Number Theory. Springer-Verlag GTM 138 (1993).