R. Sasaki
Nagoya Math. J.
Vol. 109 (1988), 117-124

GENERALIZED ONO INVARIANT AND RABINOVITCH'S THEOREM FOR REAL QUADRATIC FIELDS

RYUJI SASAKI

§ 1. Introduction

Let d be a square-free integer. Let

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,\ 3 \pmod 4 \\ \frac{1}{2}(1+\sqrt{d}) & \text{if } d \equiv 1 \pmod 4, \end{cases}$$

and $\{1, \omega\}$ forms a Z-basis for the ring of integers of the quadratic field $\boldsymbol{Q}(\sqrt{d})$. We denote by Δ and h_d the discriminant and the class number of $\boldsymbol{Q}(\sqrt{d})$, respectively. We define the polynomial $P(X)$ by

$$P(X) = X^2 + \mathrm{Tr}(\omega)X + \mathrm{Nm}(\omega)$$

where Tr and Nm are the trace and the norm. When d is negative, i.e., $\boldsymbol{Q}(\sqrt{d})$ is an imaginary quadratic field, T. Ono define the natural number p_d by

$$p_d = \max_{0 \leqq a \leqq \frac{1}{4}|\Delta|-1} \deg P(a) \qquad d \neq -1,\ -3,$$
$$p_{-1} = p_{-3} = 1.$$

Here, for a positive integer N, $\deg N$ means the number of prime divisors of N (counting multiplicity). Concerning the Ono invariant p_d, we have the following ([8], [9]):

THEOREM. *Assume $d < 0$, then we have*

(1) $$p_d \leqq h_d,$$

(2) $$p_d = 1 \Longleftrightarrow h_d = 1,$$

(3) $$p_d = 2 \Longleftrightarrow h_d = 2.$$

(2) is so-called Rabinovitch's theorem. In this paper we define p_d

Received July 14, 1986.
Revised March 12, 1987.

for a positive square-free integer d, which we call the generalized Ono invariant (cf. § 3), and we shall prove the following (cf. § 4):

MAIN THEOREM. *Assume $d > 0$, then we have*

$$p_d \leqq h_d , \tag{1}$$

$$p_d = 1 \Longleftrightarrow h_d = 1 . \tag{2}$$

When $d = 4m^2 + 1$ or $d = m^2 + 4$ with odd m, M. Koike proved (1) and H. Yokoi proved (2) ([4], [12]). By a different method from theirs, we gave another characterization of real quadratic fields $\boldsymbol{Q}(\sqrt{d})$, $d = m^2 + 4$, with $h_d = 1$ ([10]).

Using our theorem, we can get some necessary conditions for $h_d = 1$. We shall give some of them in the last Section 5, which contain results proved in [1], [6], [7] and [11].

§ 2. Preliminaries

We fix a positive square-free integer d. Let ω and Δ be as in the introduction. The positive quadratic irrational can be expanded into the periodic infinite continued fraction:

$$\omega = [a_0, \dot{a}_1, \cdots, \dot{a}_k] = [a_0, a_1, \cdots, a_k, a_1, \cdots, a_k, \cdots]$$
$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}},$$

where $a_0, a_1, \cdots$ are positive integers. We call $k = k_d$ the period of ω.

We shall inductively define integers A_i (>0) and B_i, $i = 0, 1, \cdots$, by

$$A_0 = 1 , \qquad B_0 = \mathrm{Tr}(a_0 - \omega) , \qquad A_1 = -\mathrm{Nm}(a_0 - \omega) ,$$
$$B_{i+1} = -B_i + 2a_{i+1}A_{i+1} \quad \text{and} \quad A_{i+1} = (B_i + \sqrt{\Delta})/2\omega_{i+1}$$

where $\omega_{i+1} = [a_{i+1}, a_{i+2}, \cdots]$ is the $(i + 2)$-th complete quotient of (cf. [3] Ch. 10 Th. 8.1). By the periodicity of ω, we have $A_{k+i} = A_i$ and $B_{k+i} = B_i$. As is well known, the integral quadratic forms with the discriminant $\Delta = B_i^2 + 4A_iA_{i+1}$:

$$F_i = (1)^i A_i X^2 + B_i XY + (-1)^{i+1} A_{i+1} Y^2$$

are reduced in the classical sense and equivalent to each other (cf. [2] Ch. VII).

For α, β in $\boldsymbol{Q}(\sqrt{d})$, we denote by $[\alpha, \beta]$ the $\boldsymbol{Z}$-submodule of $\boldsymbol{Q}(\sqrt{d})$ generated by α, β.

LEMMA A. *The modules*

$$\mathfrak{a}_i = \left[A_i, \frac{1}{2}(B_i + \mathrm{Tr}(\omega)) - \omega\right]$$

are principal ideals.

Proof. By a simple calculation, we have

$$\mathrm{Nm}\left(\frac{1}{2}(B_i + \mathrm{Tr}(\omega)) - \omega\right) = -A_iA_{i+1}.$$

It follows that $\mathfrak{a}_i$ becomes an ideal. Now we shall show that it is principal. Assume i is even and put $\frac{1}{2}(B_i + \mathrm{Tr}(\omega)) = b_i$. Consider the correspondence between the ideals in $\boldsymbol{Q}(\sqrt{d})$ and integral binary quadratic forms with the discriminant Δ. Then the ideal $\mathfrak{a}_i$ and the unit ideal $[1, a_0 - \omega]$ correspond to F_i and F_0, respectively. We notice here that the order of bases is carefully chosen. Since F_i and F_0 are equivalent, $\mathfrak{a}_i$ and $[1, \omega] = [1, a_0 - \omega]$ are also equivalent in the narrow sense; hence $\mathfrak{a}_i$ is a principal ideal. When i is odd, the product of ideals

$$[A_i, b_i - \omega][A_{i+1}, b_i - \omega]$$

is equal to the principal ideal $[A_iA_{i+1}, b_i - \omega] = (b_i - \omega)$. Therefore it suffices to show that $[A_{i+1}, b_i - \omega]$ is a principal ideal. This ideal corresponds to the form

$$A_{i+1}X^2 + B_iXY - A_iY^2,$$

which is improperly equivalent to F_i. This means that $[A_{i+1}, b_i - \omega]$ is equivalent to the unit ideal (in the wider sense); hence $\mathfrak{a}_i$ is a principal ideal. Q.E.D.

The following is fundamental in the theory of quadratic indeterminate equations (e.g. cf. [3] Ch. 10 Th. 8.2):

LEMMA B. *The equation* $X^2 - \mathrm{Tr}(\omega)XY + \mathrm{Nm}(\omega)Y^2 = (-1)^iA_i$ *is always soluble. If* $\ell \neq (-1)^iA_i$ *and* $|\ell| < \frac{1}{2}\sqrt{\Delta}$, *then the equation* $X^2 - \mathrm{Tr}(\omega)XY + \mathrm{Nm}(\omega)Y^2 = \ell$ *has no solution.*

§ 3. Generalized Ono invariant

Let the notation be as before. We denote by $\mathfrak{a}(d)$ the set of positive integers:

$$\mathfrak{a}(d) = \{A_0 = 1, A_1, \cdots, A_{k-1}\}$$

where k is the period of ω. Using $\mathfrak{a}(d)$, we shall extend the notion of the degree.

For a natural number N, we define the degree of N with respect to the set $\mathfrak{a}(d)$ by

$$\deg_{\mathfrak{a}(d)} N = \operatorname{Max}\left\{ \ell \,\middle|\, \begin{array}{l}\text{there exists a sequence } (N_1, N_2, \cdots, N_\ell) \\ \text{of divisors of } N \text{ satisfying (1) and (2).}\end{array} \right\}$$

(1) $\quad 1 < N_1, \quad N_i \text{ divides } N_{i+1} \qquad \text{for } 1 \leqq i < \ell.$

(2) $\quad \operatorname{Min}\{N_j/N_i, NN_i/N_j\} \notin \mathfrak{a}(d) \qquad \text{for } 1 \leqq i < j \leqq \ell.$

EXAMPLES 1. If $\mathfrak{a}(d) = \{1\}$, then $\deg_{\mathfrak{a}(d)} N = \deg N$.

2. If $d = m^2 + 1$ or $m^2 + 4$ (m: odd), then $k_d = 1$ and $\mathfrak{a}(d) = \{1\}$; hence we have

$$\deg_{\mathfrak{a}(d)} N = \deg N \qquad \text{for all } N.$$

3. If $d = 4m^2 + 1 > 5$, then $k_d = 3$ and $\mathfrak{a}(d) = \{1, m\}$; hence we have

$$\deg_{\mathfrak{a}(d)} N = \deg N \qquad \text{for } N < m^2.$$

In fact, let $N = p_1 p_2 \cdots p_t$ ($\mathrm{t} = \deg N$) be the decomposition into prime divisors. Set $N_i = p_1 \cdots p_i$ for $1 \leqq i \leqq t$. If $N < m^2$, then we have $(N_j/N_i)(NN_i/N_j) = N < m$. It follows that

$$1 < M_{ij} = \operatorname{Min}\{N_j/N_i, NN_i/N_j\} < m.$$

Therefore $M_{ij} \notin \mathfrak{a}(d) = \{1, m\}$ for $1 \leqq i < j \leqq t$, i.e., the sequence $(N_1, N_2, \cdots, N_t)$ satisfies the conditions (1) and (2). Thus we have the assertion.

Now we define the *generalized Ono invariant* p_d by

$$p_d = \operatorname*{Max}_{0 \leqq a \leqq [\frac{1}{2}(\sqrt{d} - \mathrm{Tr}(\omega))]} (\deg_{\mathfrak{a}(d)}(-P(a))),$$

where $P(X) = \mathrm{Nm}(X + \omega)$ is the polynomial introduced in Section 1 and $[r]$ is the greatest integer not exceeding a real number r. Notice here that $P(a)$ is a negative integer for a in the above interval.

§ 4. Proof of Main Theorem

When once we get the generalized Ono invariant for real quadratic fields, our main theorem will be proved by the same way as in the case of imaginary quadratic fields (cf. [9]).

LEMMA. *Let* a, b $(a > 0,\ b \geqq 0)$ *be integers such that* a *divides* $\mathrm{Nm}(b+\omega)$ *and* $2a < \sqrt{\Delta}$. *If the ideal* $[a, b+\omega]$ *is a principal ideal, then* $a \in \mathfrak{a}(d)$.

Proof. If $[a, b+\omega]$ is a principal ideal generated by $x - y\omega$ $(x, y \in Z)$, its norm is equal to $a = |\mathrm{Nm}(x - y\omega)| = |x^2 - \mathrm{Tr}(\omega)xy + \mathrm{Nm}(\omega)y^2|$. Since $2a < \sqrt{\Delta}$, a coincides with some A_i by Lemma B. Q.E.D.

Proof of Main Theorem. (1) Assume $p_d = \deg_{\mathfrak{a}(d)}(-P(b))$ with $0 \leqq b \leqq [\frac{1}{2}(\sqrt{\Delta} - \mathrm{Tr}(\omega))]$. Let $(N_1, \cdots, N_\ell)$, $\ell = p_d$, be a sequence of divisors of $N = -P(b)$ satisfying the conditions (1) and (2) in Section 3. Then the ideal classes of $\mathfrak{p}_i = [N_i, b+\omega]$, $i = 1, 2, \cdots, \ell$, are mutually distinct. In fact if $\mathfrak{p}_i$ is equivalent to $\mathfrak{p}_j$, then both of $[N_j/N_i, b+\omega]$ and $[NN_i/N_j, b+\omega]$ are principal ideals. Moreover we have $(NN_i/N_j)(N_j/N_i) = N = -P(b) \leqq -P(0) = \mathrm{Nm}(\omega) \leqq \frac{1}{4}\Delta$, where the last equality holds if and only if $d \equiv 2, 3 \pmod 4$. If $(NN_i/N_j)(N_j/N_i) = \frac{1}{4}\Delta = d$ and $NN_i/N_j = N_j/N_i$, it follows that d is a square number; this is impossible. Thus we have $\mathrm{Min}\{NN_i/N_j, N_j/N_i\} < \frac{1}{2}\sqrt{\Delta}$. By the Lemma above, it is contained in $\mathfrak{a}(d)$: this contradicts to the condition (3). Therefore we have $p_d \leqq h_d$.

(2) It is sufficient to show that $p_d = 1$ implies $h_d = 1$. Suppose $h_d \geqq 2$. Let $\mathfrak{p}$ be a non-principal prime ideal having the smallest norm. Then $\mathrm{Nm}\,\mathfrak{p} = p$ is a rational prime number and $1 < \mathrm{Nm}\,\mathfrak{p} < \frac{1}{2}\sqrt{d} \leqq \frac{1}{2}\sqrt{\Delta}$ (cf. Minkowski's lemma). Set $\mathfrak{p} = [p, b+\omega]$ $(0 \leqq b < p < \frac{1}{2}\sqrt{\Delta})$ and $\mathfrak{q} = [N/p, b+\omega]$, where $N = -N(b+\omega)$, then $\mathfrak{p}\mathfrak{q} = [N(b+\omega), b+\omega]$ is a principal ideal; hence $\mathfrak{q}$ is not a principal ideal and $\mathrm{Nm}\,\mathfrak{q} = N/p \geqq p$. The sequence $(N/p, N)$ satisfies the condition (1) in Section 3 and $\mathrm{Min}\{N/(N/p), N(N/p)/N\} = p$. We shall show $p \notin \mathfrak{a}(d)$. Suppose $p = A_i \in \mathfrak{a}(d)$. By Lemma A, we know that $\mathfrak{a}_i = [A_i, b_i - \omega]$, $b_i = \frac{1}{2}(B_i + \mathrm{Tr}(\omega))$, is a principal ideal. Since $p = A_i$ divides both of $\mathrm{Nm}(b+\omega)$ and $\mathrm{Nm}(b_i - \omega)$, p divides $\mathrm{Nm}(b+\omega) - \mathrm{Nm}(b_i - \omega) = (b + b_i)(b - b_i + \mathrm{Tr}(\omega))$. If $b + b_i = np$ for some $n \in Z$, then $[p, b+\omega] = [p, np - b_i + \omega] = [p, b_i - \omega] = \mathfrak{a}_i$ is a principal ideal. If $b - b_i + \mathrm{Tr}(\omega) = np$ for some $n \in Z$, then $[p, b+\omega] = [p, b_i - \mathrm{Tr}(\omega) + np + \omega] = [p, b_i - \omega'] = [p, b_i - \omega]' = \mathfrak{a}_i'$ is a principal

ideal, where $\mathfrak{a}_i'$ is the conjugate of $\mathfrak{a}_i$. Thus we get $p \notin \mathfrak{a}(d)$; hence the sequence $(N/p, N)$ satisfies the conditions (1) and (2) is Section 3. This means $p_d \geqq \deg_{\mathfrak{a}(d)}(-P(b)) \geqq 2$. Q.E.D.

§ 5. Applications

In this section we shall give necessary conditions for h_d to be one in several cases where the period k_d of ω is relatively small. For this problem, we refer to [1, 6, 7, 11].

We begin with the following which is proved in [10]:

PROPOSITION 1. (1) *Assume* $d \equiv 2, 3 \pmod 4$; *then* $h_d = k_d = 1$ *if and only if* $d = 2$.

(2) *Assume* $d \equiv 1 \pmod 4$; *then* $h_d = k_d = 1$ *if and only if* $d = 5$, *or* $p_d = 1$ *and* $P([\sqrt{d}]) = -1$. *In this case* $d = m^2 + 4$, *where* m *is an odd prime or* 1.

In the following we prove only Proposition 5 and Proposition 6. By similar ways, the others will be proved.

PROPOSITION 2. *Let* $d = m^2n^2 + 4m \equiv 1 \pmod 4$ (m, n:*odd*; $n > 0$, $m > 1$); *then* $k_d = 2$ *and* $\mathfrak{a}(d) = \{1, m\}$. *If* $h_d = 1$, *then* m *and* $mn^2 + 4$ *are primes.*

PROPOSITION 3. *Let* $d = m^2 + r \equiv 2, 3 \pmod 4$ *such that* $r \mid 2m$ *and* $m \geqq r > 1$; *then* $k_d = 2$ *and* $\mathfrak{a}(d) = \{1, r\}$. *If* $h_d = 1$, *then* $r = 2$ *and* $\left(\frac{2}{p}\right) = -1$ *for any odd prime divisor* p *of* m, *where* $\left(\frac{-}{}\right)$ *denotes the Legendre symbol. In this case* $m^2 + 2$ *or* $\frac{1}{2}(m^2 + 2)$ *is a prime according as* m *is odd or even.*

PROPOSITION 4. *Let* $d = 4m^2 + 1$ ($m > 1$); *then* $k_d = 3$ *and* $\mathfrak{a}(d) = \{1, m\}$. *If* $h_d = 1$, *then* m *and* $4m^2 + 1$ *are primes.*

PROPOSITION 5. *Let* $d = m^2 - r \equiv 1 \pmod 4$ *such that* m *is even and* $0 < r \mid m$; *then* $k_d = 4$ *and* $\mathfrak{a}(d) = \{1, \frac{1}{4}(2m - r - 1), r\}$. *If* $h_d = 1$, *then* r *and* d/r *are primes.*

Proof. Since m is even, $r \equiv 3 \pmod 4$. By a simple calculation, we have $k_d = 4$ and $\mathfrak{a}(d) = \{1, \frac{1}{4}(2m - r - 1), r\}$. Suppose $r = r'r''$ $(1 < r' \leqq r'')$; then $r' = 2x' + 1$ for some $0 < x' < [\frac{1}{2}(\sqrt{d} - 1)]$. Set $N = -P(x')$, and r' divides $N = -(x')^2 - x' + \frac{1}{4}(m^2 - r - 1) = \frac{1}{4}(m^2 - r - (2x' + 1)^2)$.

Consider the sequence (r', N) of divisors of N. Then $\mathrm{Min}\{N/r', Nr'/N\} = \mathrm{Min}\{\frac{1}{4}(m^2 - r - (r')^2/r', r'\} = r' \notin \mathfrak{a}(d)$; hence $h_d \geqq p_d \geqq \deg_{\mathfrak{a}(d)} N \geqq 2$. Therefore we see that r must be a prime. On the other hand, by the theory of genera, we see that d/r is a prime. Q.E.D.

PROPOSITION 6. *Let* $d = m^2 - r = 2, 3 \pmod 4$ *such that* $r \mid 2m$ *and* $1 < r \leqq m$; *then* $k_d = 4$ *and* $\mathfrak{a}(d) = \{1, 2m - r - 1, r\}$. *If* $h_d = 1$, *then* $r = 2$ *and* $\left(\frac{-2}{p}\right) = -1$ *for any odd prime divisor* $p \neq 2m - 3$ *of* m. *In this case* $m^2 - 2$ *or* $\frac{1}{2}(m^2 - 2)$ *is a prime according as* m *is odd or even.*

Proof. By a simple calculation, we get $k_d = 4$ and $\mathfrak{a}(d) = \{1, 2m - r - 1, r\}$. Suppose r is even and $r > 2$, then $r' = r/2$ is odd. Set $N = -P(r')$. Then r' divides $N = -P(r') = m^2 - r - (r')^2 = r'(m^2/r' - 2 - r')$. Consider the sequence (r', N) of divisors of N, then $\mathrm{Min}\{N/r', Nr'/N\} = \mathrm{Min}\{m^2/r' - 2 - r', r'\} = r' \notin \mathfrak{a}(d)$; hence $p_d \geqq \deg_{\mathfrak{a}(d)} N \geqq 2$. This contradicts to $h_d = 1$. If $r = 2r' + 1$ is odd, then r' divides $-P(r') = m^2 - r - (r')^2 = (m - r' - 1)(m + r' + 1)$. If we consider the sequence $(m - r' - 1, N)$, $N = -P(r')$, we have $p_d \geqq \deg_{\mathfrak{a}(d)} N \geqq 2$. Thus we have $r = 2$ provided $h_d = 1$. Suppose that $r = 2$ and there exists an odd prime divisor $p \neq 2m - 3$ of m with $\left(\frac{-2}{p}\right) = 1$. Then we have a solution s $(0 < s < p)$ for the equation $X^2 \equiv -2 \pmod p$. Then p divides $-P(s) = m^2 - (2 + s^2) = p(m^2/p - (2 + s^2)/p)$. Set $N_1 = p$ and $N_2 = N = -P(s)$, then $\mathrm{Min}\{N_2/N_1, NN_1/N_2\} = p \notin \mathfrak{a}(d)$; hence $p_d \geqq \deg_{\mathfrak{a}(d)} N \geqq 2$. This contradicts to $h_d = 1$. The last assertion comes from the theory of genera. Q.E.D.

REFERENCES

[1] N. C. Ankeny, S. Chowla and H. Hasse, On the class number of the real subfield of a cyclotomic field, J. reine angew. Math., **217** (1965), 217–220.

[2] L. K. Dickson, Introduction to the Theory of Numbers, Dover Publ. Inc., New York (1957).

[3] L. K. Hua, Introduction to Number Theory, Springer-Verlag, Berlin Heiderberg New York (1982).

[4] M. Koike, Ono invariant for real quadratic field, preprint.

[5] M. Kutsuna, On a criterion for the class number of a quadratic number field to be one, Nagoya Math. J., **79** (1980), 123–129.

[6] R. A. Mollin, Lower bounds for class numbers of real quadratic fields, Proc. Amer. Math. Soc., **96** (1986), 545–550.

[7] ——, On the insolubility of a class of Diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type,

Nagoya Math. J., **105** (1987), 39–47.
[8] G. Rabinovitch, Eindeutig keit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkorpern, J. reine angew. Math., **142** (1913), 153–164.
[9] R. Sasaki, On a lower bound for the class number of an imaginary quadratic field, Proc. Japan Acad., **62A** (1986), 37–39.
[10] ——, A characterization of certain real quadratic fields, ibid, 97–100.
[11] H. Yokoi, On the Diophantine equation $x^2-py^2=\pm 4q$ and the class number of real subfields of a cyclotomic field, Nagoya Math. J., **91** (1983), 151–161.
[12] ——, Class number one problem for certain kind of real quadratic fields, preprint.

Department of Mathematics,
College of Science and Technology,
Nihon University
Kanda, Tokyo 101
Japan