29. A Characterization of Certain Real Quadratic Fields

By Ryuji SASAKI
Department of Mathematics, College of Science
and Technology, Nihon University

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1986)

§1. Introduction. Let d be a positive square-free integer. We denote by $\omega(d)$ the algebraic integer $\sqrt{d}$ (resp. $(1/2)(1+\sqrt{d})$) in the real quadratic field $\boldsymbol{Q}(\sqrt{d})$ if $d\equiv 2$ or $3 \pmod 4$ (resp. $d\equiv 1 \pmod 4$), and by $\Delta(d)$ and $h(d)$ the discriminant and the class number of $\boldsymbol{Q}(\sqrt{d})$, respectively. The positive real quadratic irrational $\omega(d)$ can be expanded into the periodic infinite continued fraction:

$$\begin{aligned}\omega(d)&=[a_0, \dot{a}_1, \cdots, \dot{a}_k]=[a_0, a_1, \cdots, a_k, a_1, \cdots, a_k, \cdots]\\&=a_0+\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}+\cdots,\end{aligned}$$

where $a_0, a_1, \cdots$ are positive integers. We call k the *period* of $\omega(d)$ or of $\boldsymbol{Q}(\sqrt{d})$ and denote it by $k(d)$.

The purpose of this note is to give a characterization of real quadratic fields $\boldsymbol{Q}(\sqrt{d})$ with $h(d)=k(d)=1$, in analogy to Rabinovitch's theorem ([5], [6]) characterizing imaginary quadratic fields whose class number is 1.

§2. Preliminaries. We recall some facts about integral indefinite binary quadratic forms (cf. [2], Ch. VI). Let $Q(\Delta(d))$ denote the set of integral quadratic forms $aX^2+bXY+cY^2$ with the discriminant $\Delta(d)=b^2-4ac$. Two forms $aX^2+bXY+cY^2$ and $a'X^2+b'XY+c'Y^2$ in $Q(\Delta(d))$ are said to be (*properly*) *equivalent* if $a'(X')^2+b'X'Y'+c'(Y')^2=aX^2+bXY+cY^2$, $(X', Y')=(X, Y)M$, for some $M\in SL_2(\boldsymbol{Z})$. We denote by $Q_+(\Delta(d))$ the quotient of $Q(\Delta(d))$ by this equivalence relation. There is a natural bijection between $Q_+(\Delta(d))$ and the ideal class group of $\boldsymbol{Q}(\sqrt{d})$ in the narrow sense. We shall denote its order by $h_+(d)$.

A quadratic form $aX^2+bXY+cY^2$ in $Q(\Delta(d))$ is said to be *reduced* if $0<\sqrt{\Delta(d)}-b<2|a|<\sqrt{\Delta(d)}+b$. Using the continued fraction $\omega(d)=[a_0, \dot{a}_1, \cdots, \dot{a}_{k(d)}]$, we define reduced forms, in $Q(\Delta(d))$, $\Phi_i=(-1)^i A_i X^2+B_i XY+(-1)^{i+1}A_{i+1}Y^2$, $i=0, 1, \cdots$, where A_i and B_i are inductively defined by $A_0=1$, $B_0=\mathrm{Tr}\,(a_0-\omega(d))$, $A_1=-\mathrm{Nm}\,(a_0-\omega(d))$, $B_{i+1}+B_i=2a_{i+1}A_{i+1}$ and $(B_i+\sqrt{\Delta(d)})/(2A_{i+1})=[a_{i+1}, a_{i+2}, a_{i+3}, \cdots]$. By the periodicity of $\omega(d)$, we get $\Phi_{k(d)}=\Phi_0$ or $\Phi_{2k(d)}=\Phi_0$ according as $k(d)$ is even or odd. Moreover any reduced form which is equivalent to Φ_0 coincides with Φ_i for some i.

§3. Finiteness of the number of real quadratic fields with given class number and period. Let $\omega(d)=[a_0, \dot{a}_1, \cdots, \dot{a}_{k(d)}]$ be as above; then we have the following:

Lemma 1. (1) $a_i=a_{k(d)-i}$ *for* $0<i<k(d)$ *and* $a_{k(d)}=\mathrm{Tr}\,(a_0-\omega(d))$.

(2) $a_i \leqslant a_0$ *for* $0<i<k(d)$.

Proof. (1) is well-known (cf. [1]). Since a similar proof works in case $d\equiv 1 \pmod 4$, we shall prove (2) only in case $d\equiv 2$ or $3 \pmod 4$. Since Φ_i is reduced, we have $0<\sqrt{\Delta(d)}-B_i<2A_i$. Similarly we get $0<\sqrt{\Delta(d)}-B_0<2A_0=2$. Since $B_0=2a_0$, it follows that all B_i are even. Assume $A_i=1$ $(i>0)$. Then we have $B_i=B_0$; hence $A_{i+1}=A_1$. Thus we get $(B_i+\sqrt{\Delta(d)})/(2A_{i+1})=(B_0+\sqrt{\Delta(d)})/(2A_1)$; this means $i\equiv 0 \pmod{k(d)}$. Since $(B_{i-1}+\sqrt{\Delta(d)})/(2A_i)=[a_i, a_{i+1}, \cdots]$, we get $a_i<(B_{i-1}+\sqrt{\Delta(d)})/(2A_i)$; hence $2A_ia_i<B_{i-1}+2\omega(d)$. Since B_{i-1} is even, we have $B_i+B_{i-1}=2a_iA_i\leqslant 2a_0+B_{i-1}$. Thus we have $B_i\leqslant 2a_0$. Similarly we have $A_{i+1}a_{i+1}\leqslant a_0+B_i/2$; hence $A_{i+1}a_{i+1}\leqslant 2a_0$. If $0\leqslant i<k(d)-1$, then $A_{i+1}\geqslant 2$; hence $a_{i+1}\leqslant a_0$. Q.E.D.

Let $\eta(d)$ be the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{d})$, which is given by $\eta(d)=p_{k(d)-1}+\omega' q_{k(d)-1}$, where $\omega'=\omega(d)$ (resp. $\omega(d)-1$) if $d\equiv 2, 3 \pmod 4$ (resp. $d\equiv 1 \pmod 4$). Then $p_{k(d)-1}/q_{k(d)-1}$ is the $(k(d)-1)$-th convergent to $\omega(d)=[a_0, \dot{a}_1, \cdots, \dot{a}_{k(d)}]$ (cf. [2], [3]). Moreover we have $\mathrm{Nm}(\eta(d))=(-1)^{k(d)}$; hence we have $h(d)=h_+(d)$ if $k(d)$ is odd.

Lemma 2. $(3/2)^{k(d)-2}\sqrt{\Delta(d)}<\eta(d)<\sqrt{\Delta(d)}^{k(d)}$.

Proof. Assume $d\equiv 2$ or $3 \pmod 4$. Let p_n/q_n be the n-th convergent to the infinite continued fraction $\omega(d)=[a_0, \dot{a}_1, \cdots, \dot{a}_{k(d)}]$, i.e., p_n and q_n are given by

$$p_0=a_0,\quad p_1=a_1a_0+1,\quad p_n=a_np_{n-1}+p_{n-2}\quad (n\geqslant 2)$$
$$q_0=1,\quad q_1=a_1,\quad q_n=a_nq_{n-1}+q_{n-2}\quad (n\geqslant 2).$$

We shall prove $p_n+\sqrt{d}\,q_n<(2\sqrt{d})^{n+1}$. By the above equations and Lem. 1 (2), we have $p_0+\sqrt{d}\,q_0=a_0+\sqrt{d}<2\sqrt{d}$ and $p_1+\sqrt{d}\,q_1=a_0a_1+1+\sqrt{d}\,a_1\leqslant(a_0)^2+1+\sqrt{d}\,a_0<(2\sqrt{d})^2$. Inductively we get $p_n+\sqrt{d}\,q_n=a_n(p_{n-1}+\sqrt{d}\,q_{n-1})+p_{n-2}+\sqrt{d}\,q_{n-2}<a_0(2\sqrt{d})^n+(2\sqrt{d})^{n-1}<(2\sqrt{d})^{n+1}$. Next we shall show the first inequality. Let u_n denote the Fibonacci sequence which is defined by $u_1=1$, $u_2=1$ and $u_n=u_{n-1}+u_{n-2}$ for $n\geqslant 3$. Then we have $p_n+\sqrt{d}\,q_n>u_{n+2}\sqrt{d}$. For $p_0+\sqrt{d}\,q_0=a_0+\sqrt{d}>\sqrt{d}=u_2\sqrt{d}$ and $p_1+\sqrt{d}\,q_1=a_1a_0+1+\sqrt{d}\geqslant a_0+1+\sqrt{d}>2\sqrt{d}=u_3\sqrt{d}$. Inductively we have $p_n+\sqrt{d}\,q_n=a_n(p_{n-1}+\sqrt{d}\,q_{n-1})+(p_{n-2}+\sqrt{d}\,q_{n-2})>(u_{n+1}+u_n)\sqrt{d}=u_{n+2}\sqrt{d}$. Since $u_{n+2}/u_{n+1}\geqslant 3/2$ $(n\geqslant 0)$, it follows that $p_n+\sqrt{d}\,q_n>u_{n+2}\sqrt{d}=(u_{n+2}/u_{n+1})(u_{n+1}/u_n)\cdots(u_4/u_3)2\sqrt{d}=2(3/2)^{n-1}\sqrt{d}=(3/2)^{n-1}\sqrt{\Delta(d)}$. A similar proof works in case $d\equiv 1 \pmod 4$. Q.E.D.

Theorem 1. *For given positive integers h and k, there exist a finite number of real quadratic fields $\boldsymbol{Q}(\sqrt{d})$ with $k=k(d)$ and $h=h(d)$.*

Proof. Suppose there exists an infinite sequence $\{d_n\}$ of square-free positive integers such that $d_1<d_2<\cdots$ and $k(d_i)=k$. By Siegel's theorem (cf. [3] Ch. 12), we have

$$\text{(E)}\qquad \lim_{i\to\infty}\frac{\log(h(d_i)\log\eta(d_i))}{\log\sqrt{d_i}}$$
$$=\lim_{i\to\infty}\frac{\log(h(d_i)k)}{\log\sqrt{d_i}}+\lim_{i\to\infty}\frac{\log((1/k)\log\eta(d_i))}{\log\sqrt{d_i}}=1.$$

By Lem. 2, we have $0<\log \eta(d_i)<k \log \sqrt{\Delta(d_i)}$. It follows that the second term in the middle of (E) is 0; hence the first term is 1, which guarantees our assertion. Q.E.D.

§3. **Main Theorems.** We shall begin with the following:

Lemma 3. *Let α be a positive real number and a_0, a_1, a_2 positive integers; then we have*

(1) $\alpha=[a_0, \dot{a}_1] \Longleftrightarrow \alpha=(1/2)(2a_0-a_1+\sqrt{a_1^2+4})$

(2) $\alpha=[a_0, \dot{a}_1, \dot{a}_2] \Longleftrightarrow \alpha=(1/2)(2a_0-a_2)+(1/(2a_1))\sqrt{a_1a_2(a_1a_2+4)}$.

Proof. Straightforward. Q.E.D.

For a square-free positive integer d, let $P(X)$ denote the polynomial $X^2+\mathrm{Tr}(\omega(d))X+\mathrm{Nm}(\omega(d))$. We denote by $[\alpha]$ the greatest integer not exceeding a real number α.

Lemma 4. *Assume $d\equiv 1 \pmod 4$. If*

$$P([(1/2)\sqrt{d}])=-1 \ (resp.\ P([(1/2)\sqrt{d}])=1),$$

then $k(d)=1$ (resp. $k(d)=2$ or $d=5$).

Proof. Set $\omega(d)=[a_0, \dot{a}_1, \cdots, \dot{a}_{k(d)}]$, then $a_0<\omega(d)=(1/2)(1+\sqrt{d})<a_0+1$; hence $[(1/2)\sqrt{d}]=a_0$ or a_0-1. If $[(1/2)\sqrt{d}]=a_0$ and $P(a_0)=a_0^2+a_0+(1/4)(1-d)=-1$, then $\omega(d)=(1/2)\{2(a_0+1)-(2a_0+1)+\sqrt{(2a_0+1)^2+4}\}=[a_0+1, 2\dot{a}_0-1]$ by Lem. 3; this means $k(d)=1$. If $[(1/2)\sqrt{d}]=a_0$ and $P(a_0)=1$, then $d=(2a_0+1)^2-4=(2a_0-1)(2a_0-1+4)$ and $\omega(d)=(1/2)\{2a_0-(2a_0-1)+\sqrt{(2a_0-1)(2a_0-1+4)}\}$; hence $\omega(d)=[a_0, \dot{1}, 2\dot{a}_0-1]$. If $a_0=1$, $\omega(d)=[1, \dot{1}]$; this means $d=5$. We shall omit a similar proof which works in case $[(1/2)\sqrt{d}]=a_0-1$. Q.E.D.

Theorem 2. *Assume $d\equiv 2 \pmod 4$; then $h(d)=k(d)=1$ if and only if $d=2$.*

Proof. If $d=2$, then $h(2)=1$ and $\omega(2)=\sqrt{2}=[1, \dot{2}]$; hence $k(2)=1$. Conversely assume $h(d)=k(d)=1$. Then we have $\sqrt{d}=[a_0, \dot{a}_1]$ for some positive integers a_0, a_1; hence, by Lem. 3, $\sqrt{d}=(1/2)(2a_0-a_1+\sqrt{a_1^2+4})$. It follows that $2a_0=a_1$ and $d=a_0^2+1$. Since $d\equiv 2 \pmod 4$, a_0 is odd. Suppose $a_0\geqslant 3$. Since $0<\sqrt{\Delta(d)}-2(a_0-1)<4<\sqrt{\Delta(d)}+2(a_0-1)$, the quadratic form $2X^2+2(a_0-1)XY-a_0Y^2$ is a reduced one with the discriminant $\Delta(d)=4d$. Since $h(d)=k(d)=1$, by the fact stated in the last part in §2, any reduced form must be $\Phi_0=X^2+2a_0XY-Y^2$ or $\Phi_1=-X^2+2a_0XY+Y^2$; this is a contradiction. Thus we have $a_0=1$ and $d=2$. Q.E.D.

Remark. If $d\equiv 3 \pmod 4$, then $k(d)$ is even.

Theorem 3. *Assume $d\equiv 1 \pmod 4$; then the following (1)–(4) are equivalent:*

(1) $h(d)=k(d)=1$.

(2) *$d=p^2+4$ is a prime, where p is an odd prime or 1. Let $n=\mathrm{Nm}(x+\omega(d)y)$, $x, y\in \boldsymbol{Z}$, such that $(x, y)=(p, n)=1$ and $|n|<(2p-3)^2$; then $|n|$ is a prime or 1.*

(3) *$d=p^2+4$ is a prime, where p is an odd prime or 1. If $x\in \boldsymbol{Z}$ satisfies $0\leqslant x<2p-3$ and $x\neq(1/2)(3p+1)$, $(3/2)(p-1)$, then $|P(x)|$ is a prime or 1.*

(4) $d=5$, *or* $|P(0)|, \cdots, |P([(1/2)\sqrt{d}]-1)|$ *are primes and* $P([(1/2)\sqrt{d}]) = -1$.

Proof. (1)⇨(2): Since $k(d)=1$, $\omega(d)=(1/2)(1+\sqrt{d})=[a_0, \dot{a}_1]=(1/2)(2a_0-a_1+\sqrt{a_1^2+4})$ for some positive integers a_0, a_1; hence $\sqrt{d}=2a_0-a_1-1+\sqrt{a_1^2+4}$ and $d=(2a_0-1)^2+4$. Let $p=2a_0-1$; then p is a prime or 1. For, suppose p is neither a prime nor 1, we have $p=p_1p_2$ with $3\leqslant p_1\leqslant p_2$. Since p_1 is odd, we can set $p_1=2b-1$ for some $2\leqslant b\in \boldsymbol{Z}$. Then $4\,\mathrm{Nm}\,(b+\omega(d))=(2b+1)^2-d=(2b-1)(2b+3)-p^2$; hence p_1 divides $\mathrm{Nm}\,(b+\omega(d))$. Since $\sqrt{\Delta(d)}-\mathrm{Tr}\,(b+\omega(d))=\sqrt{d}-(2b+1)>0$, we have a non-negative integer n such that $0<\sqrt{\Delta(d)}-\mathrm{Tr}\,(b+np_1+\omega(d))<2p_1$. Then the quadratic form $Q=p_1X^2+\mathrm{Tr}\,(b+np_1+\omega(d))XY+(1/p_1)\,\mathrm{Nm}\,(b+np_1+\omega(d))Y^2$ is an integral reduced form with the discriminant $\Delta(d)=d$. Since $h(d)=k(d)=1$, Q must be equal to $\Phi_0=X^2+\mathrm{Tr}\,(a_0-\omega(d))XY-Y^2$ or $\Phi_1=-X^2+\mathrm{Tr}\,(a_0-\omega(d))XY+Y^2$; this is impossible. Next we shall show that p^2+4 is a prime number. Suppose $p^2+4=q_1q_2$ such that $q_1=2b+1$ is a prime number and $3\leqslant q_1<q_2$. By the same argument as above, using q_1 and b, we get the conclusion. The last part of (2) is proved by F. G. Frobenius ([4] § 5).

(2)⇨(3): Since $P(x)=(1/4)\{(2x+1)^2-(p^2+4)\}=(1/4)\{(2x-1)(2x+3)-p^2\}=\mathrm{Nm}\,(x+\omega(d))$, (2) implies (3).

(3)⇨(4): If $p=1$, then $d=5$. If $p\geqslant 3$, then $[(1/2)\sqrt{d}]=[(1/2)\sqrt{p^2+4}]=(1/2)(p-1)$ and $P([(1/2)\sqrt{d}])=-1$.

(4)⇨(1): Since $h(5)=k(5)=1$, we assume $d\neq 5$. By Lem. 4, we have $k(d)=1$. Suppose $h(d)\geqslant 2$, and there exists a non-principal integral prime ideal $\mathfrak{a}$ such that $1<\mathrm{Nm}\,\mathfrak{a}<(1/2)\sqrt{\Delta(d)}$. Since $\mathfrak{a}$ is not a principal ideal, $\mathrm{Nm}\,\mathfrak{a}=q$ is a prime. There exists an integer b such that $\mathfrak{a}=[q, b+\omega(d)]=\boldsymbol{Z}q\oplus\boldsymbol{Z}(b+\omega(d))$ and $0\leqslant b<q<(1/2)\sqrt{\Delta(d)}=(1/2)\sqrt{d}$. Then q divides $\mathrm{Nm}\,(b+\omega(d))=P(b)$; this contradicts to the assumption (4). Q.E.D.

Remark. There are six fields $\boldsymbol{Q}(\sqrt{d})$ with $h(d)=k(d)=1$;

$$d=5 \quad 13 \quad 29 \quad 53 \quad 173 \quad 293$$
$$p=1 \quad 3 \quad 5 \quad 7 \quad 13 \quad 17.$$

I do not know whether there are other such fields (cf. [4]).

By the same method we obtain similar results for real quadratic fields $\boldsymbol{Q}(\sqrt{d})$ with $h(d)k(d)\leqslant 2$.

References

[1] H. Davenport: The Higher Arithmetic. London, Hutchinson (1952).
[2] L. E. Dickson: Introduction to the Theory of Numbers. Dover Publ. Inc., New York (1957).
[3] L. K. Hua: Introduction to Number Theory. Springer-Verlag (1952).
[4] F. G. Frobenius: Über quadratische Formen, die viele Primzahlen darstellen: Sitzungsberichite, 966–980 (1912); Gesam. Abhand., Springer-Verlag, Bd. III, 573–587 (1968).
[5] G. Rabinovitchi: Eindeutigkeit der Zerlegung in Primzahlfactoren in quadratischen Zahlkörpern. J. reine angew. Math., **142**, 153–164 (1913).
[6] R. Sasaki: On a lower bound for the class number of an imaginary quadratic field. Proc. Japan Acad., **62A**, 37–39 (1986).