Hacettepe Journal of Mathematics and Statistics
Volume 36 (1) (2007), 27 – 36

SOME REMARKS ON INDEFINITE BINARY QUADRATIC FORMS AND QUADRATIC IDEALS

Ahmet Tekcan*

Received 07 : 11 : 2006 : Accepted 25 : 01 : 2007

Abstract

Let δ denote a real quadratic irrational with trace $t = \delta + \overline{\delta}$ and norm $n = \delta\overline{\delta}$. Given a real quadratic irrational $\gamma \in \mathbb{Q}(\delta)$, there are rational integers P and Q such that $\gamma = \frac{P+\delta}{Q}$ with $Q|(\delta + P)(\overline{\delta} + P)$. Hence for each $\gamma = \frac{P+\delta}{Q}$, there is a corresponding ideal $I_\gamma = [Q, P + \delta]$, and an indefinite binary quadratic form $F_\gamma(x, y) = Q(x + \delta y)(x + \overline{\delta} y)$ of discriminant $\Delta = t^2 - 4n$.

In the first section, we give some preliminaries from binary quadratic forms and ideals. In the second section, we obtain some properties of I_γ and F_γ for $\delta = \sqrt{D}$, where $D \neq 1$ is the Extended-Richaud-Degert type (ERD-type), that is, $D = w^2 + v$ for positive integers w and v such that $v|4w$. In the third section, we obtain some properties of a special family of ideals I_γ and indefinite quadratic forms F_γ for $\gamma = \frac{w+1+\sqrt{D}}{2w-v+1}$.

Keywords: ERD-type, Ideal, Indefinite quadratic form, Quadratic irrational, Cycle of an ideal, Cycle of a form, Ambiguous form.

2000 AMS Classification: 11E20, 11E25, 11E76, 11J70.

1. Introduction.

A real binary quadratic form (or just a form) F is a polynomial in two variables x, y of the type

(1.1) $$F = F(x, y) = ax^2 + bxy + cy^2$$

with real coefficients a, b, c. We denote F briefly by $F = (a, b, c)$. The discriminant of F is defined by the formula $b^2 - 4ac$ and is denoted by Δ. If $\gcd(a, b, c) = 1$, then F is called *primitive*. A quadratic form F of discriminant Δ is called *indefinite* if $\Delta > 0$, and

*Uludag University, Faculty of Science, Department of Mathematics, Görükle, 16059 Bursa, Turkey. E-mail: tekcan@uludag.edu.tr

is called reduced if $\left|\sqrt{\Delta}-2|a|\right|<b<\sqrt{\Delta}$ (for further details on binary quadratic forms see [1,2,3]).

There is a strong connection between binary quadratic forms and the extended modular group $\overline{\Gamma}$. Gauss (1777-1855) defined the group action of $\overline{\Gamma}$ on the set of forms as follows:

$$\begin{aligned} gF(x,y) = \left(ar^2+brs+cs^2\right)x^2 + (2art+bru+bts+2csu)\,xy \\ + \left(at^2+btu+cu^2\right)y^2 \end{aligned} \tag{1.2}$$

for $g=\begin{pmatrix} r & s \\ t & u \end{pmatrix}\in\overline{\Gamma}$ and $F=(a,b,c)$. Two forms F and G are called *equivalent* iff there exists a $g\in\overline{\Gamma}$ such that $gF=G$. If $\det g=1$, then F and G are called *properly equivalent*. If $\det g=-1$, then F and G are called *improperly equivalent*. A quadratic form F is said to be *ambiguous* if it is improperly equivalent to itself (see [7] for the connection between the extended modular group and binary quadratic forms).

Let $F=(a,b,c)$ be an indefinite reduced quadratic form of discriminant Δ. Then the cycle of F is given by the following theorem.

1.1. Theorem. [1, Sec: 6.10, p.106] *Let $F=(a,b,c)$ be an indefinite reduced quadratic form of discriminant Δ. Then the cycle of F of length l is $F_0\sim F_1\sim F_2\sim\cdots\sim F_{l-1}$, where $F_0=F=(a_0,b_0,c_0)$,*

$$s_i=|s(F_i)|=\left[\frac{b_i+\sqrt{\Delta}}{2|c_i|}\right] \tag{1.3}$$

and

$$\begin{aligned} F_{i+1} &= (a_{i+1},b_{i+1},c_{i+1}) \\ &= \left(|c_i|,\,-b_i+2s_i|c_i|,\,-(a_i+b_is_i+c_is_i^2)\right) \end{aligned} \tag{1.4}$$

for $0\le i\le l-2$.

Mollin [4, p.4] considers the arithmetic of ideals in his book. Let $D\neq1$ be a square free integer and let $\Delta=\frac{4D}{r^2}$, where $r=2$ if $D\equiv1 \pmod 4$, and $r=1$, otherwise. If we set $\mathbb{K}=\mathbb{Q}(\sqrt{D})$, then $\mathbb{K}$ is called a *quadratic number field of discriminant* Δ and O_Δ is the ring of integers of the quadratic field $\mathbb{K}$ of discriminant Δ. Let $I=[\alpha,\beta]$ denote the $\mathbb{Z}$-module $\alpha\mathbb{Z}\oplus\beta\mathbb{Z}$, i.e., the additive abelian group, with basis elements α and β consisting of $\{\alpha x+\beta y: x,y\in\mathbb{Z}\}$. Note that $O_\Delta=\left[1,\ \frac{1+\sqrt{D}}{r}\right]$. In this case $w_\Delta=\frac{r-1+\sqrt{D}}{r}$ is called the *principal surd*. Every principal surd $w_\Delta\in O_\Delta$ can be uniquely expressed as $w_\Delta=x\alpha+y\beta$, where $x,y\in\mathbb{Z}$ and $\alpha,\beta\in O_\Delta$. We call α,β an *integral basis for* $\mathbb{K}$.

If $\frac{\alpha\overline{\beta}-\beta\overline{\alpha}}{\sqrt{\Delta}}>0$, then α and β are called *ordered basis elements*. Recall that two bases of an ideal are ordered if and only if they are equivalent under an element of $\overline{\Gamma}$. If I has ordered basis elements, then we say that I is *simply ordered*. If I is ordered, then

$$F(x,y)=\frac{N(\alpha x+\beta y)}{N(I)}$$

is a quadratic form of discriminant Δ. In this case we say that F *belongs to* I, and write $I\to F$. Conversely, let us assume that

$$G(x,y)=Ax^2+Bxy+Cy^2=d(ax^2+bxy+cy^2)$$

is a quadratic form, where $d = \pm\gcd(A, B, C)$ and $b^2 - 4ac = \Delta$. If $B^2 - 4AC > 0$, then we get $d > 0$ and if $B^2 - 4AC < 0$, then we choose d such that $a > 0$. If

$$I = [\alpha, \beta] = \begin{cases} \left[a, \frac{b-\sqrt{\Delta}}{2}\right] & \text{for } a > 0 \\ \left[a, \frac{b-\sqrt{\Delta}}{2}\right]\sqrt{\Delta} & \text{for } a < 0 \text{ and } \Delta > 0, \end{cases}$$

then I is an ordered O_Δ-ideal. Note that if $a > 0$, then I is primitive and if $a < 0$, then $\frac{I}{\sqrt{\Delta}}$ is primitive. Thus to every form G, there corresponds an ideal I to which G belongs and we write $G \to I$. Hence we have a correspondence between ideals and quadratic forms (for further details see [4, p. 350]).

1.2. Theorem. [4, Sec:1.2, p.9] *If $I = [a, b + cw_\Delta]$, then I is a non-zero ideal of O_Δ if and only if*

$$c|b,\ c|a \text{ and } ac|N(b + cw_\Delta).$$

Let δ denote a real quadratic irrational integer with trace $t = \delta + \overline{\delta}$ and norm $n = \delta\overline{\delta}$. Given a real quadratic irrational $\gamma \in \mathbb{Q}(\delta)$, there are rational integers P and Q such that $\gamma = \frac{P+\delta}{Q}$ with $Q \mid (\delta + P)(\overline{\delta} + P)$. Hence for each $\gamma = \frac{P+\delta}{Q}$ there is a corresponding $\mathbb{Z}$-module

$$(1.5) \qquad I_\gamma = [Q,\ P + \delta],$$

(in fact, this module is an ideal by Theorem 1.2), and an indefinite quadratic form

$$(1.6) \qquad F_\gamma(x, y) = Q(x + \delta y)(x + \overline{\delta} y)$$

of discriminant $\Delta = t^2 - 4n$.

The ideal I_γ in (1.5) is said to be *reduced* if and only if

$$(1.7) \qquad P + \delta > Q \text{ and } -Q < P + \overline{\delta} < 0,$$

and is said to be *ambiguous* if and only if it contains both $\frac{P+\delta}{Q}$ and $\frac{P+\overline{\delta}}{Q}$, hence if and only if $\frac{2P}{Q} \in \mathbb{Z}$.

Let $\langle m_0, \overline{m_1 m_2 \ldots m_{l-1}}\rangle$ denote the continued fraction expansion of $\gamma = \frac{P+\delta}{Q}$ with period length $l = l(I)$. Then the cycle of I_γ is $I_\gamma = I_\gamma^0 \sim I_\gamma^1 \sim \ldots \sim I_\gamma^{l-1}$, where

$$(1.8) \qquad m_i = \left[\frac{P_i + \delta}{Q_i}\right],\ P_{i+1} = m_i Q_i - P_i \text{ and } Q_{i+1} = \frac{\delta^2 - P_{i+1}^2}{Q_i}$$

for $0 \le i \le l - 1$ (see also [5,6]).

2. Indefinite quadratic forms and ideals

Let $\gamma = \frac{P+\delta}{Q}$ be a quadratic irrational. If we take $\delta = \sqrt{D}$, then we have $I_\gamma = [Q, P + \sqrt{D}]$ and $F_\gamma = \left(Q, 2P, \frac{P^2-D}{Q}\right)$ of discriminant $\Delta = 4D$ by (1.5) and (1.6), respectively. In [8], we consider the cycle of ideals I_γ and cycles of indefinite quadratic forms F_γ for some specific values of D. In the present paper we obtain some properties of the ideals I_γ and indefinite quadratic forms F_γ for quadratic irrationals $\gamma = \frac{P+\sqrt{D}}{Q}$, where $D \neq 1$ is the Extended-Richaud-Degert type (ERD-type), that is, $D = w^2 + v$ for positive integers w and v such that $v|4w$.

Let $w = kv$ for a positive integer $k \ge 1$. Then $D = k^2v^2 + v$ is the ERD-type since $\frac{4w}{v} = \frac{4kv}{v} = 4k$. Let $Q = v$ and $P = w = kv$. Then

$$(2.1) \qquad \gamma = \frac{kv + \sqrt{k^2v^2 + v}}{v}$$

is a quadratic irrational. Therefore

(2.2) $\quad I_\gamma = [v, kv + \sqrt{k^2v^2 + v}]$

is an ideal and

(2.3) $\quad F_\gamma = (v, 2kv, -1)$

is an indefinite quadratic form of discriminant $\Delta = 4(k^2v^2 + v)$.

2.1. Theorem. *The ideal I_γ in (2.2) is ambiguous and reduced.*

Proof. It is easily seen that $\frac{2P}{Q} = \frac{2kv}{v} = 2k \in \mathbb{Z}$. Therefore I_γ is ambiguous.

Note that $k^2v^2 < k^2v^2 + v$. Therefore

$$k^2v^2 < k^2v^2 + v \iff P^2 < D \iff P < \sqrt{D} \iff P - \sqrt{D} < 0.$$

Since $v + 2kv > 1$, we have

$$\begin{aligned} & 0 < v + 2kv - 1 \\ \iff & 0 < v^2 + 2kv^2 - v \\ \iff & v < v^2 + 2kv^2 \\ \iff & k^2v^2 + v < v^2 + 2kv^2 + k^2v^2 \\ \iff & k^2v^2 + v < (kv + v)^2 \\ \iff & D < (P + Q)^2 \\ \iff & \sqrt{D} < P + Q \\ \iff & -Q < P - \sqrt{D}. \end{aligned}$$

Hence we get $-Q < P - \sqrt{D} < 0$. Similarly it can be shown that $P + \sqrt{D} > Q$. Therefore I_γ is reduced by (1.7). □

2.2. Theorem. *The continued fraction expansion of γ is $\langle 2k, 2kv \rangle$, and the cycle of I_γ is the cycle*

$$I_\gamma^0 = [v, kv + \sqrt{k^2v^2 + v}] \sim I_\gamma^1 = [1, kv + \sqrt{k^2v^2 + v}]$$

of length 2.

Proof. Let $I = I_0 = [v, kv + \sqrt{k^2v^2 + v}]$. Then by (1.8), we have

$$m_0 = \left[\frac{P_0 + \sqrt{D}}{Q_0} \right] = \left[\frac{kv + \sqrt{k^2v^2 + v}}{v} \right] = 2k$$

and hence

$$\begin{aligned} P_1 &= m_0Q_0 - P_0 = 2k.v - kv = kv, \\ Q_1 &= \frac{D - P_1^2}{Q_0} = \frac{k^2v^2 + v - k^2r^2}{v} = 1. \end{aligned}$$

For $i = 1$ we have

$$m_1 = \left[\frac{P_1 + \sqrt{D}}{Q_1} \right] = \left[\frac{kv + \sqrt{k^2v^2 + v}}{1} \right] = 2kv$$

and hence

$$\begin{aligned} P_2 &= m_1Q_1 - P_1 = 2kv.1 - kv = kv = P_0 \\ Q_2 &= \frac{D - P_2^2}{Q_1} = \frac{k^2v^2 + v - k^2v^2}{1} = v = Q_0. \end{aligned}$$

Therefore, the continued fraction expansion of γ is $\langle 2k, 2kv\rangle$, and the cycle of I_γ is $I_\gamma^0 = [v, kv + \sqrt{k^2v^2+v}] \sim I_\gamma^1 = [1, kv + \sqrt{k^2v^2+v}]$. □

2.3. Example. Let $v = 5$ and $k = 7$. Then the continued fraction expansion of $\gamma = \dfrac{35+\sqrt{1230}}{5}$ is $\langle 14, 70\rangle$, and the cycle of $I_\gamma = [5, 35+\sqrt{1230}]$ is $I_\gamma^0 = [5, 35+\sqrt{1230}] \sim I_\gamma^1 = [1, 35+\sqrt{1230}]$.

2.4. Theorem. *The indefinite quadratic form F_γ in (2.3) is ambiguous and reduced.*

Proof. Let $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \overline{\Gamma}$ and $F_\gamma = (v, 2kv, -1)$. Then by (1.2), the system of equations

$$\begin{aligned} vr^2 + 2kvrs - s^2 &= v \\ 2vrt + 2kvru + 2kvts - 2su &= 2kv \\ vt^2 + 2kvtu - u^2 &= -1 \end{aligned}$$

has a solution for $r = 1$, $s = 2kv$, $t = 0$ and $u = -1$, i.e. $gF_\gamma = F_\gamma$. Hence F_γ is improperly equivalent to itself since $\det g = -1$. So F_γ is ambiguous by definition.

Note that $v, kv > 0$. Therefore,

$$\begin{aligned} k^2v^2 < k^2v^2 + v &\iff 4k^2v^2 < 4(k^2v^2+v) \\ &\iff \sqrt{4k^2v^2} < \sqrt{4(k^2v^2+v)} \\ &\iff 2kv < \sqrt{\Delta} \\ &\iff b < \sqrt{\Delta}. \end{aligned}$$

Since $k^2v^2 + v < k^2v^2 + 2kv^2 + v^2$, we have

$$\begin{aligned} k^2v^2 + v < (kv+v)^2 &\iff \sqrt{k^2v^2+v} < \sqrt{(kv+v)^2} \\ &\iff \sqrt{k^2v^2+v} < kv + v \\ &\iff 2\sqrt{k^2v^2+v} < 2kv + 2v \\ &\iff \sqrt{4(k^2v^2+v)} < 2kv + 2v \\ &\iff \sqrt{4(k^2v^2+v)} - 2v < 2kv \\ &\iff \sqrt{\Delta} - 2|a| < b. \end{aligned}$$

Hence $|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$. Therefore, F_γ is reduced. □

2.5. Theorem. *The cycle of $F_\gamma = (v, 2kv, -1)$ is the cycle*

$$F_\gamma^0 = (v, 2kv, -1) \sim F_\gamma^1 = (1, 2kv, -v)$$

of length 2.

Proof. Let $F_\gamma^0 = F_\gamma = (a_0, b_0, c_0) = (v, 2kv, -1)$. Then by (1.3), we get

$$s_0 = \left[\frac{b_0 + \sqrt{\Delta}}{2|c_0|}\right] = \left[\frac{2kv + \sqrt{4(k^2v^2+v)}}{2|-1|}\right] = \left[kv + \sqrt{k^2v^2+v}\right] = 2kv,$$

and hence

$$\begin{aligned} F_\gamma^1 = (a_1, b_1, c_1) &= \left(|c_0|,\ -b_0 + 2s_0|c_0|,\ -a_0 - b_0s_0 - c_0s_0^2\right) \\ &= \left(1, -2kv + 4kv,\ -v - 2kv.2kv + (2kv)^2\right) \\ &= (1,\ 2kv,\ -v) \end{aligned}$$

by (1.4). For $i = 1$ we have

$$s_1 = \left[\frac{b_1 + \sqrt{\Delta}}{2|c_1|}\right] = \left[\frac{2kv + \sqrt{4(k^2v^2 + v)}}{2|-v|}\right] = \left[\frac{kv + \sqrt{k^2v^2 + v}}{v}\right] = 2k,$$

and hence

$$\begin{aligned} F_\gamma^2 &= (a_2, b_2, c_2) = \big(|c_1|,\ -b_1 + 2s_1|c_1|,\ -a_1 - b_1 s_1 - c_1 s_1^2\big) \\ &= \big(v, -2kv + 2.2k.v, -1 - 2kv.2k + v.4k^2\big) \\ &= (v, 2kv,\ -1) \\ &= F_0. \end{aligned}$$

Therefore the cycle of F is $F_\gamma^0 = (v, 2kv, -1) \sim F_\gamma^1 = (1, 2kv, -v)$. □

3. A special family of ideals and quadratic forms

Let $D = w^2 + v$ be of ERD-type, and let $w = kv$ for an integer $k \geq 1$. Let $Q = 2kv - v + 1$ and $P = kv + 1$. Then

(3.1) $$\gamma = \frac{kv + 1 + \sqrt{k^2v^2 + v}}{2kv - v + 1}$$

is a quadratic irrational. Therefore

(3.2) $$I_\gamma = [2kv - v + 1, kv + 1 + \sqrt{k^2v^2 + v}]$$

is an ideal and

(3.3) $$F_\gamma = (2kv - v + 1, 2kv + 2, 1)$$

is an indefinite quadratic form of discriminant $\Delta = 4(k^2v^2 + v)$.

3.1. Theorem. *I_γ is not reduced.*

Proof. Note that $2kv + 1 > v$. Hence

$$\begin{aligned} 2kv + 1 > v &\iff k^2v^2 + 2kv + 1 > k^2v^2 + v \\ &\iff P^2 > D \\ &\iff P > \sqrt{D} \\ &\iff P - \sqrt{D} > 0, \end{aligned}$$

which is a contradiction to (1.7). Therefore I_γ is not reduced. □

3.2. Theorem. *I_γ is ambiguous if and only if $k = 1$, that is $w = v$.*

Proof. Let I_γ be ambiguous. Then

$$\frac{2P}{Q} = \frac{2kv + 2}{2kv - v + 1} = 1 + \frac{v + 1}{2kv - v + 1}$$

must be an integer. It is easily seen that it is an integer for $k = 1$. Indeed, for $k = 1$ we have

$$\frac{2P}{Q} = \frac{2kv + 2}{2kv - v + 1} = 1 + \frac{v + 1}{2kv - v + 1} = 1 + \frac{v + 1}{v + 1} = 2 \in \mathbb{Z}.$$

Conversely let us assume that $k = 1$. Then

$$\frac{2P}{Q} = \frac{2kv + 2}{2kv - v + 1} = \frac{2v + 2}{v + 1} = 2 \in \mathbb{Z}.$$

Therefore I_γ is ambiguous. □

3.3. Theorem. *The continued fraction expansion of* γ *is* $\langle 1, 2k-1, \overline{2kv, 2k}\rangle$*, and the cycle of* I_γ *is*

$$\begin{aligned} I_\gamma^0 &= [2kv - v + 1, kv + 1 + \sqrt{k^2v^2+v}] \\ \sim I_\gamma^1 &= [v, kv - v + \sqrt{k^2v^2+v}] \\ \sim I_\gamma^2 &= [1, kv + \sqrt{k^2v^2+v}] \\ \sim I_\gamma^3 &= [v, kv + \sqrt{k^2v^2+v}]. \end{aligned}$$

Proof. Let $I_\gamma = I_\gamma^0 = [2kv - v + 1, kv + 1 + \sqrt{k^2v^2+v}]$. Then by (1.8), we get

$$m_0 = \left[\frac{P_0 + \sqrt{D}}{Q_0}\right] = \left[\frac{kv + 1 + \sqrt{k^2v^2+v}}{2kv - v + 1}\right] = 1,$$

and hence

$$\begin{aligned} P_1 &= m_0Q_0 - P_0 = 1.(2kv - v + 1) - (kv + 1) = kv - v \\ Q_1 &= \frac{D - P_1^2}{Q_0} = \frac{k^2v^2 + v - (kv - v)^2}{2kv - v + 1} = \frac{v(2kv - v + 1)}{2kv - v + 1} = v. \end{aligned}$$

For $i = 1$ we have

$$m_1 = \left[\frac{P_1 + \sqrt{D}}{Q_1}\right] = \left[\frac{kv - v + \sqrt{k^2v^2+v}}{v}\right] = 2k - 1,$$

and hence

$$\begin{aligned} P_2 &= m_1Q_1 - P_1 = (2k - 1)v - (kv - v) = kv \\ Q_2 &= \frac{D - P_2^2}{Q_1} = \frac{k^2v^2 + v - k^2v^2}{v} = 1. \end{aligned}$$

For $i = 2$ we have

$$m_2 = \left[\frac{P_2 + \sqrt{D}}{Q_2}\right] = \left[\frac{kv + \sqrt{k^2v^2+v}}{1}\right] = 2kv,$$

and hence

$$\begin{aligned} P_3 &= m_2Q_2 - P_2 = 2kv.1 - kv = kv \\ Q_3 &= \frac{D - P_3^2}{Q_2} = \frac{k^2v^2 + v - k^2v^2}{1} = v. \end{aligned}$$

For $i = 3$ we have

$$m_3 = \left[\frac{P_3 + \sqrt{D}}{Q_3}\right] = \left[\frac{kv + \sqrt{k^2v^2+v}}{v}\right] = 2k,$$

and hence

$$\begin{aligned} P_4 &= m_3Q_3 - P_3 = 2kv - kv = kv \\ Q_4 &= \frac{D - P_4^2}{Q_3} = \frac{k^2v^2 + v - k^2v^2}{v} = 1. \end{aligned}$$

For $i = 4$ we have

$$m_4 = \left[\frac{P_4 + \sqrt{D}}{Q_4}\right] = \left[\frac{kv + \sqrt{k^2v^2+v}}{1}\right] = 2kv = m_2.$$

Therefore, the continued fractional expansion of γ is $\langle 1, 2k-1, \overline{2kv, 2k}\rangle$, and hence the cycle of I_γ is $I_\gamma^0 = [2kv - v + 1, kv + 1 + \sqrt{k^2v^2+v}] \sim I_\gamma^1 = [v, kv - v + \sqrt{k^2v^2+v}] \sim I_\gamma^2 = [1, kv + \sqrt{k^2v^2+v}] \sim I_\gamma^3 = [v, kv + \sqrt{k^2v^2+v}]$. □

3.4. Example. Let $v = 3$ and $k = 3$. Then the continued fraction expansion of $\gamma = \dfrac{10+\sqrt{84}}{16}$ is $\langle 1, 5, \overline{18, 6}\rangle$, and the cycle of $I_\gamma = [16, 10 + \sqrt{84}]$ is

$$I_\gamma^0 = [16, 10+\sqrt{84}] \sim I_\gamma^1 = [3, 6+\sqrt{84}] \sim I_\gamma^2 = [1, 9+\sqrt{84}] \sim I_\gamma^3 = [3, 9+\sqrt{84}].$$

3.5. Theorem. *F_γ is not reduced.*

Proof. Note that $2kv + 1 > v$. Then

$$\begin{aligned} 2kv+1 > v &\iff 8kv+4 > 4v \\ &\iff 4k^2v^2 + 8kv + 4 > 4k^2v^2 + 4v \\ &\iff (2kv+2)^2 > 4(k^2v^2+1) \\ &\iff (2kv+2)^2 > 4D \\ &\iff (2kv+2)^2 > \Delta \\ &\iff 2kv+2 > \sqrt{\Delta} \\ &\iff b > \sqrt{\Delta}. \end{aligned}$$

Therefore, F_γ is not reduced. □

If a quadratic form $F = (a, b, c)$ of discriminant Δ is not reduced, then we can get it reduced by using the following reduction algorithm: Let $F = F_0 = (a_0, b_0, c_0)$ be a non-reduced form of discriminant Δ, let

$$(3.4) \qquad s_i = \begin{cases} \operatorname{sign}(c_i)\left[\frac{b_i}{2|c_i|}\right] & \text{if } |c_i| \geq \sqrt{\Delta}, \\ \\ \operatorname{sign}(c_i)\left[\frac{b_i+\sqrt{\Delta}}{2|c_i|}\right] & \text{if } |c_i| < \sqrt{\Delta}, \end{cases}$$

and let

$$(3.5) \qquad R^{i+1}(F) = (c_i, -b_i + 2s_ic_i, c_is_i^2 - b_is_i + a_i)$$

for $i \geq 0$. The number s_i is called the *reducing number*, and the form $R^{i+1}(F)$ is called the *reduction* of F. If $R^1(F)$ is not reduced, then we apply the reduction algorithm again and hence we get $R^2(F)$. If $R^2(F)$ is not reduced, then we apply the reduction algorithm again and hence we get $R^3(F)$. After a finite number of steps $j \geq i$, the form $R^j(F)$ is reduced. The form $R^j(F)$ is called the *reducing type* of F (for further details see [1, p.90]).

We proved in Theorem 3.5 that the form $F_\gamma = (2kv - v + 1, 2kv + 2, 1)$ is not reduced. But we can get a reducing type of F_γ as we mentioned above. For $i = 0$, we have

$$\begin{aligned} s_0 &= \operatorname{sign}(c_0)\left[\frac{b_0+\sqrt{\Delta}}{2|c_0|}\right] \\ &= \left[\frac{2kv+2+\sqrt{4(k^2v^2+v)}}{2}\right] \\ &= \left[kv+1+\sqrt{k^2v^2+v}\right] \\ &= 2kv+1 \end{aligned}$$

by (3.4), and hence

$$\begin{aligned} R^1\big(F_\gamma\big) &= (c_0, -b_0 + 2s_0c_0, c_0s_0^2 - b_0s_0 + a_0) \\ &= \big(1,\ -(2kv+2) + 2(2kv+1), \\ &\qquad\qquad (2kv+1)^2 - (2kv+2)(2kv+1) + 2kv - v + 1\big) \\ &= (1, 2kv, -v) \end{aligned}$$

by (3.5). Note that the form $R^1\big(F_\gamma\big)$ is reduced. Therefore we have proved:

3.6. Theorem. *The reducing type of* F_γ *is* $R^1(F_\gamma) = (1, 2kv, -v)$.

3.7. Theorem. *The cycle of* $R^1\big(F_\gamma\big) = (1, 2kv, -v)$ *is the cycle*

$$R^1\big(F_\gamma^0\big) = (1, 2kv, -v) \sim R^1\big(F_\gamma^1\big) = (v, 2kv, -1)$$

of length 2.

Proof. Let $R^1\big(F_\gamma\big) = R^1\big(F_\gamma^0\big) = (1, 2kv, -v)$. For $i = 0$, we have

$$s_0 = \left[\frac{b_0 + \sqrt{\Delta}}{2|c_0|}\right] = \left[\frac{2kv + \sqrt{4(k^2v^2+v)}}{2|-v|}\right] = \left[\frac{kv + \sqrt{k^2v^2+v}}{v}\right] = 2k,$$

and hence

$$\begin{aligned} R^1\big(F_\gamma^1\big) &= (a_1, b_1, c_1) \\ &= (|c_0|, -b_0 + 2s_0|c_0|, -a_0 - b_0s_0 - c_0s_0^2) \\ &= (|-v|, -2kv + 2(2k)|-v|, -1 - 2kv(2k) - (-v)(2k)^2) \\ &= (v, 2kv, -1). \end{aligned}$$

For $i = 1$, we have

$$s_1 = \left[\frac{b_1 + \sqrt{\Delta}}{2|c_1|}\right] = \left[\frac{2kv + \sqrt{4(k^2v^2+v)}}{2|-1|}\right] = \left[kv + \sqrt{k^2v^2+v}\right] = 2kv,$$

and hence

$$\begin{aligned} R^1\big(F_\gamma^2\big) &= (a_2, b_2, c_2) \\ &= (|c_1|,\ -b_1 + 2s_1|c_1|,\ -a_1 - b_1s_1 - c_1s_1^2) \\ &= (|-1|,\ -2kv + 2(2kv)|-1|,\ -v - 2kv(2kv) - (-1)(2kv)^2) \\ &= (1, 2kv, -v) \\ &= R^1\big(F_\gamma^0\big). \end{aligned}$$

Therefore, the cycle of $R^1(F_\gamma)$ is completed and is

$$R^1(F_\gamma^0) = (1, 2kv, -v) \sim R^1\big(F_\gamma^1\big) = (v, 2kv, -1).$$

□

References

[1] Buchmann, J. *Algorithms for Binary Quadratic Forms*, (In preparation, accepted by Springer-Verlag).

[2] Buell, D. A. *Binary Quadratic Forms, Clasical Theory and Modern Computations* (Springer-Verlag, New York, 1989).

[3] Flath, D. E. *Introduction to Number Theory* (Wiley, 1989).

[4] Mollin, R. A. *Quadratics* (CRS Press, Boca Raton, New York, London, Tokyo, 1996).

[5] Mollin, R. A. and Poorten, A. J. *A note on symmetry and ambiguity*, Bull. Austral. Math. Soc. **51**, 215–233, 1995.

[6] Mollin, R. A. and Cheng, K. *Palindromy and ambiguous ideals revisited*, Journal of Number Theory **74**, 98–110, 1999.

[7] Tekcan, A. and Bizim, O. *The connection between quadratic forms and the extended modular group*, Mathematica Bohemica **128** (3), 225–236, 2003.

[8] Tekcan, A. *On the cycles of indefinite quadratic forms and cycles of ideals*, Hacettepe Journal of Mathematics and Statistics **35** (1), 63–70, 2006.