Contents

Units

$d \equiv 2, 3 \mod 4$

$$N(\alpha) = a^2 - db^2 = 1$$

Note $d < 0$ so either $a^2 = 1$ or $-db^2 = 1$.

$$a = \pm 1$$

When $d = -1$, then $b = \pm 1$ so we also have $\pm i$.

$d \equiv 1 \mod 4$

$$N(\alpha) = 1 \Leftrightarrow (2a+b)^2 - db^2 = 4$$
$$d = -3, -7, -11, ...$$

We cannot have $-db^2 \leq 4$ for $d < -3$, so $b = 0$.

$$(2a + 0) = 4 \Rightarrow a = \pm 1$$

Now consider $d = -3$. $|b| \geq 2 \Rightarrow -db^2 \geq 12$. So $b = -1, 0, 1$. Then by solving we find all units for $d = -3$ are the 6th roots of unity.

Summary

Note $\bar{\omega} = \omega^{n-1}$ so $N(\omega) = \omega\bar{\omega} = \omega^n$.

Motivation

When we take $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, then α/β has a nearest integer κ, which can also be written $\alpha = \kappa\beta + \rho \Rightarrow \rho = \beta\left(\frac{\alpha}{\beta} - \kappa\right)$.

Since $\alpha = \kappa\beta + \rho$ with $N(\rho) < N(\beta)$, then we see $N\left(\frac{\alpha}{\beta} - \kappa\right) < 1$.

Euclidean Imaginary Quadratic Fields

See `ch6-euclid.py`. With $d = -19$, the top vertex becomes $1.14i$.

$$N\left(\frac{\alpha}{\beta} - \kappa\right) > 1 \Rightarrow N(\rho) = N(\alpha - \kappa\beta) > N(\beta)$$

which means it is non-euclidean.

Let $\alpha = 28\sqrt{d}, \beta = 108$, then $\alpha/\beta = 1.13i$. Then we can confirm the above is true.

$x = qu + r$ for u a non unit, and $r = 0$ or r a unit

I is the maximal ideal containing all non units of R. Let $u \in I$ such that $\phi(u)$ is minimal in I. Then

$$x = qu + r \text{ with } \phi(r) < \phi(u) \text{ or } r = 0$$

If $r = 0$, then $x = qu$. So assume $r \neq 0$.

$r \notin I$ because $\phi(u)$ is minimal, so r is a unit.

$\mathbb{Z}_K$ is not Euclidean

By previous result, $u|\alpha$ or $u|2 \pm 1$.

u cannot divide 1 since it is not a unit, so $u|2$ or 3.

$$N\left(a + b\left(\frac{1+\sqrt{d}}{2}\right)\right) = a^2 + ab + b^2\left(\frac{1-d}{4}\right)$$

$d < -11 \Rightarrow k = \frac{1-d}{4} \geq 4$.

$$a^2 + ab + kb^2 = 2, 3$$

Complete the square and see there's no solution. So both $2, 3$ are irreducible. $u = 2, -2, 3, -3$.

Now let $\alpha = \frac{1+\sqrt{d}}{2}$, but $u \nmid \alpha$ and $u \nmid \alpha \pm 1$. So u does not exist.

Quadratic Forms

Positive definite forms $f(x, y) \geq 0$ and $f(x, y) = 0 \Rightarrow (x, y) = (0, 0)$.

Therefore $a, c > 0$ since $f(x, 0), f(0, y) > 0$. Complete the square to see $b^2 - 4ac < 0$.

$$ax^2 + bxy + cy^2 = a\left(x + \frac{b}{2a}y\right)^2 + \left(c - \frac{b^2}{4a}\right)y^2$$

A form is normal if $-a < b \leq a$.

A form is reduced if it is normal and $a < c$ or $a = c$ and $b \geq 0$.

Generators for $\mathrm{SL}_2(\mathbb{Z})$

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Which correspond to

$$(a, b + 2a, c + b + a) \qquad \text{and} \qquad (c, -b, a)$$

Minimum Values

(x, y) are coprime.

$$|x| \geq 2 \Rightarrow f(x, y) > c$$
$$|y| \geq 2 \Rightarrow f(x, y) > c$$

x	y	$f(x,y)$
-1	-1	$> c$
-1	0	a
-1	1	$\geq c$
0	-1	c
0	1	c
1	-1	$\geq c$
1	0	a
1	1	$> c$

When $a = c$, there are 4 pairs $f(x, y) = a$, which becomes 6 when $a = b = c$.

$|y| = 1, |x| \geq 2$

Complete the square

$$\begin{aligned} 4af(x, y) &= 4a(ax^2 + bxy + cy^2) \\ &= (2ax + by)^2 - (b^2 - 4ac)y^2 \\ &= (2ax + by)^2 - (b^2 - 4ac) \end{aligned}$$

But note that

$$|2ax + by| \geq |2ax| - |by| \geq 4a - |b| \geq 3a$$

since $|y| = 1$ and $b \leq a$.

$$\Rightarrow 4af(x, y) \geq 9a^2 - (b^2 - 4ac) = 4ac + 8a^2 + (a^2 - b^2)$$

but $|b| \leq a$ so $4af(x, y) \geq 4ac$ or

$$f(x, y) \geq c$$

$|y| \geq 2$

$$4af(x,y) = (2ax+by)^2 - (b^2-4ac)y^2 \geq -(b^2-4ac)y^2$$
$$y^2 \geq 4$$
$$\Rightarrow 4af(x,y) \geq -4(b^2-4ac) = 16ac - 4b^2$$

Note $b^2 - 4ac < 0$ and we can factor that out.

$$4af(x,y) \geq 12ac + 4(ac - b^2) \geq 12ac \geq 4ac$$

$$f(x,y) > c$$

Remaining Cases

$(x,y) = 1$ and if $y = 0$, then $x = \pm 1$ so

$$f(\pm 1, 0) = a$$

$$f(0, \pm 1) = c$$
$$f(\pm 1, \pm 1) = a + b + c > c$$
$$f(\pm 1, \mp 1) = a - b + c \geq c$$

Decompose $M \in \mathbf{SL}_2(\mathbb{Z})$

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Use S to make a, c positive.

Then use T^{-1} to reduce a so $a < 0$ and $-a < c$. Then flip them with S. This reduces c. Repeat this process. The final matrix is $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ which is some power of T. We now have a decomposition for M by inverting the chain of operations.

Every positive definite form is properly equivalent to a reduced form (theorem 6.14)

We already saw above that the smallest possible value for a reduced form is $f(x,y) = a$.

Algorithm

```
if a > c or (a = c and b < 0):
    (a, b, c) → (c, -b, a)                    #1
# Remaining two cases
elif a < c:
    if b <= -a:
        (a, b, c) → (a, b + 2a, c + b + a)   #2
    else:
        assert b > a
        (a, b, c) → (a, b - 2a, c - b + a)   #3
elif a = c and b >= 0:
    assert b > a
    (a, b, c) → (a, b - 2a, c - b + a)       #4
```

First observe that in all the steps, a does not increase. Eventually it must become constant.

In the remaining two cases, the absolute value of $|b|$ gets smaller. We will show that for each case.

Branch 2: $b \leq -a$

First assume $b = -a \Rightarrow |b| = a$, then we see that $(a', b', c') = (a, a, c)$ and $b' = |b|$. Now $a = b < c$ so the form is reduced.

Now assume $b < -a \Rightarrow a + b < 0 \Rightarrow 2a + b < a$. But since $a > 0 \Rightarrow -a < 0$, we see $b < -a < 0$.

If $2a + b > 0$ then $|2a + b| = |b'| < a$. But $b < -a \Rightarrow a < |b| \Rightarrow |b'| < |b|$.

Else $b' = 2a + b < 0$, then $a > 0, b < 0 \Rightarrow 2a + b > b$ so $|b'|$ also is smaller.

Branch 3: $b > a$

$b > a$ and $a > 0 \Rightarrow 0 < a < b$.

$$b - 2a < b$$

If $b - 2a \geq 0$ then $|b - 2a| < |b|$ and we are done.

So now $b - 2a < 0$. Also $b > a \Rightarrow b - a > 0$. We want to disprove $|b - 2a| \geq |b|$.

First assume $|b - 2a| = |b|$, then $b > 0 \Rightarrow b - 2a = -b \Rightarrow a = 0$ which is impossible so $|b - 2a| > |b| = b$.

$$\Rightarrow b - 2a < -b$$

$$2b - 2a < 0$$

$$b < a$$

which is a contradiction.

Branch 4

The proof is essentially the same as branch 3, since $b > a$ and the transform is the same.

Determinant is Fixed

We can easily show algebraically the determinant is unchanged when applying any transform. So $b'^2 - 4a'c' = b^2 - 4ac$.

When $a = b$, then c is also fixed.

Description of Stages

1. Ordered bases of ideals:
    1. Show every ideal in $\mathbb{Z}_K$ is written $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$. Do this by taking $\alpha = a \in \mathfrak{a}$ to be minimal, and $b + c\omega \in \mathfrak{a}$ with c minimal. Then reducing an element $m + n\omega \in \mathfrak{a}$, we see $(m + n\omega) - s(b + c\omega) - ta = 0$.
    2. $c|a$ follows from $a \in \mathfrak{a} \Rightarrow a\omega \in \mathfrak{a}$ and $a\omega - t(b + c\omega)$ with $r = a - tc$ where $r < c$ or $r = 0$. But c is minimal so $r = 0 \Rightarrow c|a$.
    3. $c|b$ follows similarly from $(b + c\omega)\omega \in \mathfrak{a}$.
    4. Dimensionality of cosets is therefore ac.
    5. $ac|c^2d - b^2$ for $d \equiv 2, 3 \bmod 4$ else $ac|c^2\left(\frac{d-1}{4}\right) - b^2 - bc$. when $d \equiv 1 \bmod 4$. We can see this by taking $\alpha = ax + (b + c\omega)y \in \mathfrak{a}$ and expanding $\alpha\omega$. We also know $\alpha\omega = as + (b + c\omega)t$ for some s, t, and comparing across the basis $\{1, \omega\}$, we get 2 linear equations. Then we solve for s substituting t and we get the desired result.
    6. We can plainly see $N_{K/\mathbb{Q}}(ax + (b + c\omega)y) = N_{K/\mathbb{Q}}(\mathfrak{a})f_{\alpha,\beta}(x, y)$.
    7. $f_{\alpha,\beta}$ is positive definite since $N_{K/\mathbb{Q}}(\alpha x + \beta y)$ and $N_{K/\mathbb{Q}}(\mathfrak{a})$ are always positive. We can see the first relation from $N_{K/\mathbb{Q}}(\alpha x + \beta y) = N_{K/\mathbb{Q}}(ax + by + c\sqrt{d}y) = (ax + by)^2 - dc^2y^2$ which is positive since $-d > 0$. For the $d \equiv 1 \bmod 4$ case, we have $N_{K/\mathbb{Q}}(\alpha x + \beta y) = (ax + by)^2 + c^2\left(\frac{1-d}{4}\right)$.
2. Effect of changing ordered generators:
    1. Ordered generator means β/α lies in the upper-half of the complex plane.
    2. We see that $M \in \mathrm{SL}_2(\mathbb{Z})$ acting on (α, β) preserves ordering.
    3. We can use any ordered basis and they will map to the same class.
3. From ideal classes to proper equivalence classes of quadratic forms:
    1. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if $\mathfrak{a} - \mathfrak{b} = \langle\theta\rangle$ for some principal ideal. Let $\theta = A/B$, then $B\mathfrak{b} = A\mathfrak{a}$.
    2. We show $\Phi(A\mathfrak{a}) = \Phi(\mathfrak{a})$ which by the same argument implies $\Phi(B\mathfrak{b}) = \Phi(\mathfrak{b})$.

        3. Which means $\Phi(\mathfrak{a}) = \Phi(\mathfrak{b})$.
    4. And back again
        1. We show $\Psi(f)$ is an ideal.
        2. We also show applying the transforms to f keeps it within the same equivalence classes.
        3. Lastly $[\Phi(\Psi(f))] = [f]$, and $[\Psi(\Phi(\mathfrak{a}))] = [\mathfrak{a}]$.

$\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$ with $c|a$ and $c|b$

$\mathfrak{a} = \langle a, b + c\omega \rangle$

Let $m + n\omega \in \mathfrak{a}$

There is an s such that

$$n = sc + r \text{ with } r < c \text{ or } r = 0$$

but c is minimal so $r = 0$ and

$$(m + n\omega) - s(b + c\omega) = m - sb$$

b is chosen to be non-negative.

Now we have

$$(m - sb) = ta + r_a$$

but a is minimal so $r_a = 0$

$$(m - sb) = (m + n\omega) - s(b + c\omega)$$

$$\Rightarrow m + n\omega = s(b + c\omega) + ta$$

$$m + n\omega \in a\mathbb{Z} + (b + c\omega)\mathbb{Z}$$

$c|a$

Since c is minimal, we can use the same remainder trick to prove $c|a$ and $c|b$

$$a \in \mathfrak{a} \Rightarrow a\omega \in \mathfrak{a}$$

$a = tc + r \Rightarrow a\omega - t(b + c\omega) = -tb + r\omega$ with $r < c$, but c is minimal so $r = 0$ and $a = tc$.

$c|b$

Likewise

$$b + c\omega \in \mathfrak{a} \Rightarrow b\omega + cd \in \mathfrak{a}$$

again $b = tc + r$ so $(cd + b\omega) = t(b + c\omega) + ((-tb + cd) + r\omega) \Rightarrow r = 0$.

$N_{K/\mathbb{Q}}(\mathfrak{a}) = ac$

$$M = [a, b + c\omega], \qquad S = \{r + s\omega : 0 \leq r < a, 0 \leq s < c\}$$

We prove $x + y\omega \in \mathbb{Z}_K$ is congruent mod M to an element of S.

Let $y = cq + s$ where $q \in \mathbb{Z}$ and $0 \leq s < c$ then

$$(x + y\omega) - q(b + c\omega) = x' + s\omega$$

$$\Rightarrow x + y\omega \equiv x' + s\omega \mod M$$

Now write $x' = aq' + r$ where $q' \in \mathbb{Z}$ and $0 \leq r < a$ then

$$x' + s\omega \equiv r + s\omega \mod M$$

$$N_{K/\mathbb{Q}}(\mathfrak{a}) = \#S = ac$$

$ac|c^2d - b^2$

Let $\alpha \in \mathfrak{a}$ then $\alpha\omega \in \mathfrak{a}$

$$\begin{aligned} \alpha &= ax + (b + c\omega)y \\ \alpha\omega &= cdy + (ax + by)\omega \\ &= as + (b + c\omega)t \quad \text{for some } s, t \in \mathbb{Z} \end{aligned}$$

Comparing coefficients

$$\begin{aligned} as + bt &= cdy \\ ct &= ax + by \end{aligned} \tag{1}$$

$$t = \frac{ax + by}{c} \in \mathbb{Z} \Leftrightarrow c|a \text{ and } c|b$$

to see this choose $x, y = 0, 1$ or $1, 0$.

Combining (1) with t, and setting $x = 0$, we get that $ac|c^2d - b^2$.

Φ

$$\Phi = \frac{N_{K/\mathbb{Q}}(ax + (b + c\omega)y)}{N_{K/\mathbb{Q}}(\mathfrak{a})}$$

$$N_{K/\mathbb{Q}}(ax + by + c\omega y) = (ax + by)^2 - dc^2y^2$$

This is positive and so is $N_{K/\mathbb{Q}}(\mathfrak{a})$, so $\Phi(\mathfrak{a})$ is positive definite.

Let $\alpha = a, \beta = b + c\omega$

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha x + \beta y) &= (\alpha x + \beta y)(\bar{\alpha} x + \bar{\beta} y) \\ &= N_{K/\mathbb{Q}}(\alpha)x^2 + T_{K/\mathbb{Q}}(\alpha\bar{\beta})xy + N_{K/\mathbb{Q}}(\beta)y^2 \end{aligned}$$

Equivalence of Forms within Same Class

$$F_{\alpha,\beta} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad F_{\gamma,\delta} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix},$$

$$F_{\alpha,\beta} = MF_{\gamma,\delta}$$

$$\Rightarrow \mathbf{v}^T F_{\alpha,\beta} = \mathbf{v}^T MF_{\gamma,\delta}$$

and also that

$$\mathbf{v}^T F_{\bar{\alpha},\bar{\beta}} = \mathbf{v}^T MF_{\bar{\gamma},\bar{\delta}}$$

Also note that

$$\mathbf{v}^T F = F^T \mathbf{v} \tag{1}$$

$$\begin{aligned} N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot f_{\alpha,\beta}(\mathbf{v}) &= N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot f_{\alpha,\beta}(x, y) = N_{K/\mathbb{Q}}(\alpha x + \beta y) \\ &= (\alpha x + \beta y)(\bar{\alpha} x + \bar{\beta} y) \\ &= \mathbf{v}^T F_{\alpha,\beta} \mathbf{v}^T F_{\bar{\alpha},\bar{\beta}} \\ &= \mathbf{v}^T F_{\alpha,\beta} F_{\bar{\alpha},\bar{\beta}}^T \mathbf{v} \qquad \text{by 1} \\ &= \mathbf{v}^T MF_{\gamma,\delta} (MF_{\bar{\gamma},\bar{\delta}})^T \mathbf{v} \\ &= \mathbf{v}^T MF\bar{F}^T M^T \mathbf{v} \\ &= (\mathbf{v}^T M)F(\mathbf{v}^T M)\bar{F} \\ &= N_{K/\mathbb{Q}}(\gamma(px + qy) + \delta(rx + sy)) \\ &= N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot f_{\gamma,\delta}(px + qy, rx + sy) \end{aligned}$$

```
sage: var("p r q s x y a b g d")
(p, r, q, s, x, y, a, b, g, d)
sage: v = matrix([[x], [y]])
sage: M = matrix([[p, r], [q, s]])
sage: vTM = v.transpose() * M
sage: vTM
[p*x + q*y r*x + s*y]
sage: F = matrix([[g], [d]])
sage: var("gb db")
(gb, db)
sage: Fb = matrix([[gb], [db]])
sage: vTM*F*vTM*Fb
[((r*x + s*y)*d + (p*x + q*y)*g)*(r*x + s*y)*db + ((r*x + s*y)*d + (p*x + q*y)*g)*(p*x + q*y)*gb]
sage: vTM*F*vTM*Fb == (g*(p*x + q*y) + d*(r*x + s*y))*(gb*(p*x + q*y) + db*(r*x + s*y))
True
```

$\mathfrak{a}$ and $\mathfrak{b}$ in the Same Ideal Class $\Rightarrow \Phi(\mathfrak{a}) = \Phi(\mathfrak{b})$ (Proposition 6.27)

$\mathfrak{a} \sim \mathfrak{b} \Rightarrow \frac{\mathfrak{a}}{\mathfrak{b}} = \langle\theta\rangle$ *since the class group is defined modulo principal ideals.*

There exists $\theta \in K$ such that $\mathfrak{b} = \langle\theta\rangle\mathfrak{a}$. Write $\theta = A/B$ for $A, B \in \mathbb{Z}_K$.

When $d < 0$ then $N_{K/\mathbb{Q}}(\gamma) = |N_{K/\mathbb{Q}}(\gamma)|$. We will prove $\Phi(\mu\mathfrak{a}) = \Phi(\mathfrak{a})$. Note $\mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta$.

$$
\begin{aligned}
f_{\alpha,\beta} &= \frac{N_{K/\mathbb{Q}}(\alpha x + \beta y)}{N_{K/\mathbb{Q}}(\mathfrak{a})} \\
f_{\mu\alpha,\mu\beta} &= \frac{N_{K/\mathbb{Q}}(\mu\alpha x + \mu\beta y)}{N_{K/\mathbb{Q}}(\mu\mathfrak{a})} \\
&= \frac{N_{K/\mathbb{Q}}(\mu)N_{K/\mathbb{Q}}(\alpha x + \beta y)}{N_{K/\mathbb{Q}}(\langle\mu\rangle)N_{K/\mathbb{Q}}(\mathfrak{a})} \\
&= \frac{N_{K/\mathbb{Q}}(\mu)N_{K/\mathbb{Q}}(\alpha x + \beta y)}{|N_{K/\mathbb{Q}}(\mu)|N_{K/\mathbb{Q}}(\mathfrak{a})} \\
&= \frac{N_{K/\mathbb{Q}}(\alpha x + \beta y)}{N_{K/\mathbb{Q}}(\mathfrak{a})} \\
&= f_{\alpha,\beta}
\end{aligned}
$$

Since $\mathfrak{b} = \frac{A}{B}\mathfrak{a} \Rightarrow B\mathfrak{b} = A\mathfrak{a}$, then $\Phi(\mathfrak{a}) = \Phi(A\mathfrak{a}) = \Phi(B\mathfrak{b}) = \Phi(\mathfrak{b})$.

$d \equiv 1 \pmod 4$

Only the first and last stages are changed.

Stage 1

$\mathfrak{a} = a\mathbb{Z} + (b + c\rho)\mathbb{Z}$ with $c|a$ and $c|b$

Same proof as before. Take a and $b + c\rho$ where a, c are minimal and positive. Then subtract $m + n\rho$ to show there is an integer remainder.

Then $c|a$ because $a \in \mathfrak{a} \Rightarrow a\rho \in \mathfrak{a}$, meaning $a\rho - t(b + c\rho) \Rightarrow r = a - tc$ with either $r < c$ or $r = 0$. But c is minimal so $r = 0$ proving the statement.

Now we prove $c|b$. Note $\bar{\rho} = \frac{\sqrt{d}-1}{2} = \rho - 1$, and $\rho\bar{\rho} = \frac{d-1}{4}$. Then since $b + c\rho \in \mathfrak{a}$,

$$
b\bar{\rho} + c\left(\frac{d-1}{4}\right) = b\rho - b + c\left(\frac{d-1}{4}\right) \in \mathfrak{a}
$$

Subtracting a multiple of $b + c\rho$, we see the coefficient for ρ is $r = b - tc$ with $r = 0$ or $r < c$ but c is minimal so $c|b$.

$ac|c^2\left(\frac{d-1}{4}\right)-b^2-bc$

$$\begin{aligned}\alpha\bar{\rho} &= ax\bar{\rho}+by\bar{\rho}+cy\left(\frac{d-1}{4}\right) \\ &= (ax+by)\rho+(-ax-by+cy\left(\frac{d-1}{4}\right)) \qquad \text{since } \bar{\rho}=\rho-1 \\ &= as+(b+c\rho)t\end{aligned}$$

Comparing coefficients for ρ we see

$$\begin{aligned}ct &= ax+by \\ as+bt &= -ax-by+cy\left(\frac{d-1}{4}\right) \\ \Rightarrow as &= -ax-by+cy\left(\frac{d-1}{4}\right)-bt \\ &= -ax-by+cy\left(\frac{d-1}{4}\right)-bt \\ &= -ax-by+cy\left(\frac{d-1}{4}\right)-b\frac{ax+by}{c} \\ acs &= -acx-bcy+c^2y\left(\frac{d-1}{4}\right)-b(ax+by)\end{aligned}$$

and since $c|b \Rightarrow ac|ab$

$$ac|(-bc+c^2\left(\frac{d-1}{4}\right)-b^2)$$

$\Phi(\mathfrak{a})$

The conjugate of $\rho^*=\frac{1-\sqrt{d}}{2}$.

$$\begin{aligned}N_{K/\mathbb{Q}}(ax+by+c\rho y) &= (ax+by+cy\cdot\mathrm{re}(\rho))^2-(cy\cdot\mathrm{im}(\rho))^2 \\ &= \left(ax+by+cy\cdot\frac{1}{2}\right)^2-\left(cy\cdot\frac{\sqrt{d}}{2}\right)^2\end{aligned}$$

```
sage: R.<x, y> = SR[]
sage: var("a b c d")
(a, b, c, d)
sage: f = (a*x + b*y + c*(1/2)*y)^2 - c^2*(d/4)*y^2
sage: f
a^2*x^2 + (a*(2*b + c))*x*y + (-1/4*c^2*d + 1/4*(2*b + c)^2)*y^2
sage: f.coefficients()
[a^2, a*(2*b + c), -1/4*c^2*d + 1/4*(2*b + c)^2]
```

Then extracting the common factor $N_{K/\mathbb{Q}}(\mathfrak{a})=ac$ gives a form with integer coefficients by the results above.

Discriminant is also the same. `f` $= N_{K/\mathbb{Q}}(\alpha x+\beta y)$ and `f2` $= \Phi(\mathfrak{a})=N_{K/Q}(\alpha x+\beta y)/N_{K/\mathbb{Q}}(\mathfrak{a})$.

```
sage: f
a^2*x^2 + (a*(2*b + c))*x*y + (-1/4*c^2*d + 1/4*(2*b + c)^2)*y^2
sage: f2 = f/(a*c)
sage: A, B, C = f2.coefficients()
# Discriminant is unchanged
sage: (B^2 - 4*A*C).expand()
d
```

Stage 4

$\Phi(\Psi((a,b,c)))=(a,b,c)$

$$\Psi((a,b,c))=\mathbb{Z}a+\mathbb{Z}\left(\frac{b+\sqrt{d}}{2}\right)$$

$$A = a, \qquad B = \frac{b-1}{2}, \qquad C = 1$$

$$\Rightarrow N_{K/\mathbb{Q}}(\mathfrak{a}) = AC = a$$

$$\alpha = a, \qquad \beta = \frac{b-1}{2} + \rho = \frac{b+\sqrt{d}}{2}$$

$$\frac{N_{K/\mathbb{Q}}(\alpha x + \beta y)}{N_{K/\mathbb{Q}}(\mathfrak{a})} = \frac{1}{a}\left((ax + \frac{b}{2}y)^2 - \frac{d}{4}y^2\right)$$

```
sage: N = (a*x + (b/2)*y)^2 - (d/4)*y^2
sage: N
a^2*x^2 + a*b*x*y + (1/4*b^2 - 1/4*d)*y^2
sage: N/a
a*x^2 + b*x*y + (1/4*(b^2 - d)/a)*y^2
```

But note $d = b^2 - 4ac$ so

```
sage: a*x^2 + b*x*y + (1/4*(b^2 - (b^2 - 4*a*c))/a)*y^2
a*x^2 + b*x*y + c*y^2
```

$[\Psi(\Phi(\mathfrak{a}))] = [\mathfrak{a}]$

$$\begin{aligned}\Phi(\mathfrak{a}) &= \frac{N_{K/\mathbb{Q}}(ax + (b + c\rho))}{N_{K/\mathbb{Q}}(\mathfrak{a})} \\ &= \frac{1}{ac}\left((ax + by + c \cdot \mathrm{re}(\rho)y)^2 - (c \cdot \mathrm{im}(\rho)y)^2\right) \\ &= \frac{1}{ac}\left((ax + by + c \cdot \frac{1}{2}y)^2 - (c \cdot \frac{d}{2}y)^2\right)\end{aligned}$$

```
sage: f = (a*x + b*y + c*(1/2)*y)^2 - (c*(d/2)*y)^2
sage: f /= (a*c)
sage: f
a/c*x^2 + ((2*b + c)/c)*x*y + (-1/4*(c^2*d^2 - (2*b + c)^2)/(a*c))*y^2
```

(see also bottom of page 142 for the formula for $\Phi(\mathfrak{a})$)

$$\begin{aligned}\Psi(\Phi(\mathfrak{a})) &= \Psi\left(\frac{a}{c}x^2 + \left(\frac{2b}{c} + 1\right)xy + \left(\frac{b^2 + bc + c^2\frac{1-d}{4}}{ac}\right)y^2\right) \\ &= \mathbb{Z}\frac{a}{c} + \mathbb{Z}\left(\frac{(\frac{2b}{c} + 1) - 1}{2} + \rho\right) \\ &= \mathbb{Z}\frac{a}{c} + \mathbb{Z}\left(\frac{b}{c} + \rho\right) \\ &= \frac{1}{c}(\mathbb{Z}a + \mathbb{Z}(b + c\rho))\end{aligned}$$

$$\Rightarrow [\Psi(\Phi(\mathfrak{a}))] = [\mathfrak{a}]$$