Formes quadratiques

Claude Levesque (U. Laval)

Ecole CIMPA de Oujda (Juin 2015)

1. Préliminaires

Dans cette section, nous allons considérer les formes quadratiques en général.

Définitions 1.1. Une *forme quadratique* (*i.e.*, une *forme quadratique binaire entière*) est un polynôme homogène du second degré de la forme

$$f = f(X,Y) = aX^2 + bXY + cY^2 \quad \text{avec} \quad a,b,c \in \mathbb{Z},$$

qui sera noté

$$f = \langle a,b,c\rangle .$$

La *matrice associée* à f est

$$M_f = \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix},$$

et le *discriminant* de f est

$$\Delta = \Delta_f = b^2 - 4ac = -4\,dét(M_f).$$

Nous avons alors

$$\begin{aligned} f(X,Y) &= aX^2 + bXY + cY^2 = \begin{pmatrix} X & Y \end{pmatrix} M_f \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}. \end{aligned}$$

Souvent on écrit $f = \langle a,b,\star\rangle$ parce que l'entier c est uniquement déterminé par le discriminant: $c = \dfrac{b^2-\Delta}{4a}$. Parfois on écrit aussi $f = \langle \star,b,c\rangle$.

Définitions 1.2. Une forme quadratique $f(X,Y)$ *représente* un entier $k \in \mathbb{Z}$ s'il existe $x,y \in \mathbb{Z}$ tels que

$$ax^2 + bxy + cy^2 = k,$$

et la représentation est dite *primitive* si $\text{PGCD}(x,y) = 1$.

Remarquons que si $f(X,Y) = aX^2 + bXY + cY^2$, alors

$$\begin{cases} 4af(X,Y) &= (2aX+bY)^2 - \Delta Y^2, \\ 4cf(X,Y) &= (2cY+bX)^2 - \Delta X^2. \end{cases}$$

Nous déduisons que si $\Delta > 0$, alors $f(X,Y)$ représente à la fois des entiers positifs et des entiers négatifs, alors que si Δ est négatif, $f(X,Y)$ représente des entiers qui sont tous positifs ou tous négatifs, selon que respectivement $a > 0$ ou $a < 0$.

Définitions 1.3. Une forme quadratique $f = \langle a,b,c\rangle$ est dite *primitive* si $\text{PGCD}(a,b,c) = 1$. Elle est dite *définie positive* si $\Delta < 0$ avec $a > 0$, $c > 0$, et elle est dite *définie négative* si $\Delta < 0$ avec $a < 0$, $c < 0$. Une forme quadratique f est dite *indéfinie* si $\Delta > 0$. Nous dénoterons par $\mathcal{F}_\Delta$ l'ensemble de toutes formes quadratiques primitives de discriminant Δ.

Pour la suite, nous supposerons toujours que les formes quadratiques rencontrées sont non dégénérées (c'est-à-dire $\Delta \neq 0$) et sont aussi primitives.

Comme $\Delta = b^2 - 4ac$, nous déduisons que Δ est pair (resp. impair) si et seulement si b est pair (resp. impair).

De plus, comme $\Delta \equiv b^2 \pmod 4$ et comme un carré est congru à 0 ou 1 $\pmod 4$, nous déduisons la congruence

$$\Delta \equiv 0 \text{ ou } 1 \pmod 4.$$

Définition 1.4. Le discriminant Δ d'une forme quadratique est dit *fondamental* lorsque

- ou bien $\Delta \equiv 1 \pmod 4$ avec Δ sans facteur carré,
- ou bien $\Delta \equiv 0 \pmod 4$ avec $\Delta = 4m$, $m \equiv 2$ ou $3 \pmod 4$, m sans facteur carré.

Définition 1.5. La *forme quadratique principale* f_0 de discriminant Δ est

$$f_0 = \begin{cases} \langle 1,0,-\frac{1}{4}\Delta\rangle & \text{si } \Delta \equiv 0 \pmod 4, \\ \langle 1,1,\frac{1}{4}(1-\Delta)\rangle & \text{si } \Delta \equiv 1 \pmod 4. \end{cases}$$

Définition 1.6. Posons

$$GL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} : \ r,s,t,u \in \mathbb{Z},\ ru - st = \pm 1 \right\},$$

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} : \ r,s,t,u \in \mathbb{Z},\ ru - st = 1 \right\}.$$

Soit $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$. L'*action* de A sur $f = aX^2 + bXY + cY^2$, notée Af, est le résultat de la fonction

$$\begin{aligned} T_A : \quad \mathcal{F}_\Delta &\longrightarrow \mathcal{F}_\Delta \\ f = \langle a,b,c\rangle &\longmapsto T_A(f) = Af = f' = \langle a',b',c'\rangle, \end{aligned}$$

où par définition, nous avons

$$M_{f'} = A^t M_f A$$
$$= \begin{pmatrix} ar^2+brt+ct^2 & ars+cut+\frac{1}{2}(ru+st)b \\ ars+cut+\frac{1}{2}(ru+st)b & as^2+bsu+cu^2 \end{pmatrix}.$$

Ci-dessus, A^t est la transposée de la matrice A. D'où

$$Af = \begin{pmatrix} r & s \\ t & u \end{pmatrix} f = f' = \langle a', b, ' c' \rangle$$

avec

$$\begin{cases} a' = ar^2+brt+ct^2 = f(r,t), \\ b' = (ru+st)b + 2(ars+cut), \\ c' = as^2+bsu+cu^2 = f(s,u). \end{cases}$$

D'une part, nous avons donc

$$\begin{aligned} Af &= \begin{pmatrix} r & s \\ t & u \end{pmatrix} f \\ &= \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix} M_f \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= \begin{pmatrix} X & Y \end{pmatrix} \underbrace{\begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}} \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a' & \frac{1}{2}b' \\ \frac{1}{2}b' & c' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= a'X^2 + b'XY + c'Y^2, \end{aligned}$$

et d'autre part, nous avons aussi

$$Af = \underbrace{\begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix}} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \underbrace{\begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}}$$
$$= \begin{pmatrix} V & W \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} V \\ W \end{pmatrix}$$
$$= a(rX+sY)^2 + b(rX+sY)(tX+uY) + c(tX+uY)^2$$
$$= aV^2 + bVW + cW^2$$

avec

$$\begin{pmatrix} V \\ W \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} rX+sY \\ tX+uY \end{pmatrix}.$$

Remarque 1.7. Il y a des actions importantes sur $f = \langle a, b, c \rangle$ qu'il vaut la peine d'avoir dans son portefeuille:

- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \langle a, b, c \rangle = \langle c, b, a \rangle$;
- $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \langle a, b, c \rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \langle a, b, c \rangle = \langle c, -b, a \rangle$;
- $\begin{pmatrix} r & 1 \\ 1 & 0 \end{pmatrix} \langle a, b, c \rangle = \langle ar^2+br+c,\ b+2ar,\ a \rangle$;
- $\begin{pmatrix} 0 & 1 \\ 1 & u \end{pmatrix} \langle a, b, c \rangle = \langle c,\ b+2cu,\ a+bu+cu^2 \rangle$;

- $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} f = \begin{pmatrix} -1 & -s \\ 0 & -1 \end{pmatrix} \langle a, b, c \rangle = \langle a,\ b+2as,\ as^2+bs+c \rangle$;
- $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} f = \begin{pmatrix} -1 & 0 \\ -t & -1 \end{pmatrix} \langle a, b, c \rangle = \langle a+bt+ct^2,\ b+2ct,\ c \rangle$;
- $\begin{pmatrix} r & -1 \\ 1 & 0 \end{pmatrix} f = \begin{pmatrix} -r & 1 \\ -1 & 0 \end{pmatrix} \langle a, b, c \rangle = \langle ar^2+br+c,\ -b-2ar,\ a \rangle$;
- $\begin{pmatrix} 0 & -1 \\ 1 & u \end{pmatrix} f = \begin{pmatrix} 0 & 1 \\ -1 & -u \end{pmatrix} \langle a, b, c \rangle = \langle c,\ -b+2cu,\ a-bu+cu^2 \rangle$;
- $\begin{pmatrix} -1 & s \\ 0 & 1 \end{pmatrix} f = \begin{pmatrix} 1 & -s \\ 0 & -1 \end{pmatrix} \langle a, b, c \rangle = \langle a,\ -b-2as,\ c+bs+as^7 \rangle$;
- $\begin{pmatrix} 1 & 0 \\ t & -1 \end{pmatrix} f = \begin{pmatrix} -1 & 0 \\ -t & 1 \end{pmatrix} \langle a, b, c \rangle = \langle a+bt+ct^2,\ -b-2ct,\ c \rangle$;
- $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} f = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \langle a, b, c \rangle = \langle a, -b, c \rangle$.

Définitions 1.8. Soit f et g deux formes quadratiques.

• D'une part, la forme f est dite *équivalente au sens large* à g, en symboles $f \approx g$, s'il existe une matrice $A \in GL_2(\mathbb{Z})$ telle que $g = Af$. Il est par contre d'usage fréquent d'omettre l'expression *au sens large* et d'écrire seulement f est *équivalente* à g. Posons

$$C\ell(\Delta) := \mathcal{F}_\Delta / \approx$$

et soit $h = h_\Delta$ la cardinalité de $C\ell(\Delta)$. Un élément de $C\ell(\Delta)$ est appelé une *classe au sens large* et h est dit le *nombre de classes au sens large*.

• D'autre part, f est dite *équivalente au sens strict* à g, en symboles $f \sim g$, s'il existe $A \in SL_2(\mathbb{Z})$ telle que $g = Af$. On dit aussi que f est *équivalente au sens restreint* à g, ou encore que f est *équivalente au sens étroit* à g; parfois on dit aussi que f est *équivalente au sens propre* à g ou encore que f est *proprement équivalente* à g. Posons

$$C\ell^+(\Delta) := \mathcal{F}_\Delta / \sim$$

et soit $h^+ = h^+_\Delta$ la cardinalité de $C\ell^+(\Delta)$. Un élément de $C\ell^+(\Delta)$ est appelé une *classe au sens strict* et h^+ est dit le *nombre de classes au sens strict*.

Remarques 1.9. Voici une façon de retenir ces définitions.

(1) D'une part, l'équivalence au sens *large* fait intervenir un déterminant qui peut être 1 ou -1, c'est-à-dire

l'admissibilité à une classe fait intervenir un critère plus *large*.

(2) D'autre part, l'équivalence au sens *strict*, *restreint*, *étroit* fait intervenir un déterminant égal à 1, c'est-à-dire l'admissibilité à une classe fait intervenir un critère plus *strict*, plus *restreint*, plus *étroit*.

(3) Il est préférable d'éviter les expressions "*au sens fort*" et "*au sens faible*" car leurs définitions varient selon les auteurs. En fait, même les symboles $\approx$ et $\sim$ ne font pas l'unanimité.

(4) De plus, dans le cas de l'équivalence au sens large, si la matrice qui agit sur f pour donner g est de déterminant $+1$, on dit parfois que f est *proprement équivalente* à g, et si la matrice qui agit sur f pour donner g est de déterminant -1, on dit alors que f est *improprement équivalente* à g.

Exercice 1.1. Prouvez que $\approx$ et $\sim$ sont des relations d'équivalence.

Exercice 1.2. Prouvez que deux formes quadratiques équivalentes (au sens strict ou au sens large) ont forcément le même discriminant.

Exercice 1.3. Exhibez deux formes quadratiques vérifiant à la fois la propriété "f est *proprement équivalente à g*" et la propriété "f *est improprement équivalente à g*".

Exercice 1.4. Supposons que

$$f = \langle a, b, c\rangle = aX^2 + bXY + cY^2$$

et qu'il existe des entiers r et t copremiers entre eux pour lesquels nous avons $k = f(r, t)$. Prouvez qu'il existe des entiers b', c' tels que $f \sim \langle k, b', c'\rangle$.
Suggestion. L'identité de Bezout est dans le décor.

2. Formes quadratiques définies positives

Concentrons-nous maintenant sur les formes quadratiques définies positives.

Définition 2.1. Une forme quadratique définie positive $f = \langle a, b, c\rangle$ est dite *réduite* si $|b| \leq a \leq c$ et si de plus $b \geq 0$ lorsque $|b| = a$ ou lorsque $c = a$.

Proposition 2.2. **(1)** *Soit $f = \langle a, b, c\rangle$ une forme quadratique définie positive réduite. Alors les propriétés suivantes sont vérifiées:*

(**i**) $b^2 \equiv \Delta \pmod 4$ *et* $b \equiv \Delta \pmod 2$;
(**ii**) $0 \leq |b| \leq a \leq \sqrt{\frac{1}{3}|\Delta|}$;
(**iii**) $a \left| \dfrac{b^2-\Delta}{4} \right.$ *et* $c \left| \dfrac{b^2-\Delta}{4} \right.$;
(**iv**) $|b| \leq a \leq \dfrac{b^2-\Delta}{4a}$ $(= c)$.

(2) *De plus, il existe une (unique) forme réduite dans chaque classe de formes définies positives.*

Démonstration. **(1)(i)** D'une part,

$$b^2 - \Delta = 4ac \equiv 0 \pmod 4.$$

D'autre part, $b^2 \equiv \Delta \pmod 2$. Comme

$$\Delta \equiv 0 \text{ ou } 1 \pmod 4 \quad \text{et} \quad b^2 \equiv 0 \text{ ou } 1 \pmod 4,$$

nous concluons que $b \equiv \Delta \pmod 2$.

(ii) Nous avons

$$4b^2 \leq 4a^2 \leq 4ac = b^2 - \Delta \leq a^2 - \Delta.$$

D'où

$$3b^2 \leq 3a^2 \leq -\Delta.$$

Donc

$$b^2 \leq a^2 \leq \frac{1}{3}|\Delta|,$$

de sorte que

$$|b| \leq a \leq \sqrt{\frac{1}{3}|\Delta|}.$$

(iii) Les deux divisibilités découlent de l'égalité

$$ac = \frac{b^2-\Delta}{4}.$$

(iv) Si f est réduite, cela signifie que $|b| \leq a \leq c$, de sorte que

$$|b| \leq a \leq c = \frac{b^2-\Delta}{4a}.$$

(2) Soit $f = \langle a, b, c\rangle$ une forme quadratique de discriminant $\Delta < 0$. Montrons maintenant qu'il existe une forme réduite dans la classe de f. Cet objectif est atteint au moyen d'un algorithme standard appelé *algorithme de réduction*. Cet algorithme fait intervenir une combinaison de deux opérations que nous allons immédiatement décrire:

• *S'il s'avère d'une part que f est telle que $a \geq c$, on considère alors*

$$\langle a', b', c' \rangle \;=\; \langle c, -b, a \rangle \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \langle a, b, c \rangle \sim \langle a, b, c \rangle \,,$$

de sorte que nous avons maintenant $a' \leq c'$.

• *Supposons d'autre part que cette forme f est telle que $|b| > a$. Il existe alors un entier δ satisfaisant*

$$\frac{b-c}{2c} \;\leq\; \delta \;\leq\; \frac{b-c}{2c} + 1,$$

c'est-à-dire,

$$|-b + 2c\delta| \;\leq\; c.$$

En faisant agir $\begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$ sur f , nous avons alors

$$\begin{aligned} f \sim \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix} \langle a, b, c \rangle \;&=\; \langle a', b', c' \rangle \\ &=\; \left\langle c, -b + 2c\delta, a - b\delta + c\delta^2 \right\rangle, \end{aligned}$$

de sorte que nous avons maintenant $|b'| \leq a'$.

Si $a' \leq c'$, alors nous avons terminé. Sinon, nous répétons le processus pour obtenir

$$\begin{aligned} \langle a, b, c \rangle \;\sim\; \langle a', b', c' \rangle \;&=\; \langle c, b', c' \rangle \\ &\sim\; \langle a'', b'', c'' \rangle \;=\; \langle c', b'', c'' \rangle \,. \end{aligned}$$

avec $|b''| \leq a'' = c' < a' = c$. Puisque nous continuons l'algorithme de réduction seulement dans le cas où nous

avons $c' < a' = c$, et puisque nous travaillons avec des entiers positifs, alors l'algorithme se termine après un nombre fini d'étapes, et nous avons ainsi trouvé la forme réduite recherchée.

La preuve de l'unicité découle du théorème 2.3 ci-dessous.

Théorème 2.3. *Les formes quadratiques réduites définies positives ne sont jamais strictement équivalentes entre elles.*

Démonstration. Supposons que les formes réduites $f = \langle a, b, c \rangle$ et $f' = \langle a', b', c' \rangle$ sont équivalentes au sens strict, *i.e.*, il existe $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$ tel que

$$\langle a', b', c' \rangle = A \langle a, b, c \rangle = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \langle a, b, c \rangle \,, \tag{2.1}$$

sous l'hypothèse que $|b| \leq a \leq c$ et $|b'| \leq a' \leq c'$. Donc, d'après l'exercice 1.4, il existe des entiers r et t tels que

$$a' = f(r, t) = ar^2 + brt + ct^2.$$

On peut supposer sans perte de généralité que $a \geq a'$. Comme $|b| \leq a \leq c$ (f étant réduite), nous avons

$$\begin{aligned} a \;\geq\; a' \;=\; ar^2 + brt + ct^2 \;&\geq\; a(r^2 + t^2) + brt \\ &\geq\; a(r^2 + t^2) - a|rt| \\ &\geq\; a|rt|, \end{aligned}$$

vu que $r^2 + t^2 \geq 2|rt|$. Donc $(|r| - |t|)^2 \geq 0$ et nous concluons que $|rt| = 0$ ou 1, de sorte que les seuls cas

possibles sont

$$\begin{aligned} (r, t) \;=\; &(1, 0),\, (-1, 0),\, (0, 1),\, (0, -1), \\ &(1, 1),\, (1, -1),\, (-1, 1),\, (-1, -1). \end{aligned}$$

• Soit $(r, t) = (1, 0)$ ou $(-1, 0)$. Alors il existe un entier positif ou négatif s tel que

$$\langle a, b, c \rangle \;\sim\; \langle a, b + 2sa, \star \rangle \,.$$

Cependant, la seule façon d'avoir $|b| \leq a$ et $|b+2sa| \leq a$, c'est lorsque $s = 0$ (auquel cas les formes sont identiques) ou encore lorsque $s = -1$, et dans ce cas, $\langle a, a, c \rangle \sim \langle a, -a, c \rangle$, ou encore lorsque $s = +1$, et dans ce cas, $\langle a, -a, c \rangle \sim \langle a, a, c \rangle$.

• Soit $(r, t) = (0, 1)$ ou $(0, -1)$. Alors il existe un entier positif ou négatif u tel que $\langle a, b, c \rangle$ et $\langle c, -b + 2cu, \star \rangle$ sont des formes réduites équivalentes au sens strict. Comme $|b| \leq c$ et $|-b+2cu| \leq c$, nous concluons une fois de plus que que les coefficients centraux ne peuvent pas être, tous les deux à la fois, suffisamment petits, sauf si $u = 0, +1$ ou -1. Si $u = 0$, alors pour que les formes $\langle a, b, c \rangle$ et $\langle c, -b, a \rangle$ soient toutes les deux réduites, nous devons avoir $c = a$ et par conséquent $\langle a, b, a \rangle \sim \langle a, -b, a \rangle$. Soit $u = +1$; alors $\langle a, b, c \rangle \sim \langle c, -b + 2c, \star \rangle$ de sorte que ou bien $b = -c$ et $\langle a, -c, c \rangle \sim \langle c, -c, a \rangle$, ou bien $b = c$ et $\langle a, c, c \rangle \sim \langle c, c, a \rangle$; ceci force $a = c$ et l'on obtient $\langle a, -a, a \rangle \sim \langle a, -a, a \rangle$ ou $\langle a, a, a \rangle \sim \langle a, a, a \rangle$. Soit $u = -1$; alors $\langle a, b, c \rangle \sim \langle c, -b \pm 2c, \star \rangle$ de sorte que

ou bien $b = c$ et $\langle a, c, c \rangle \sim \langle c, c, a \rangle$, ou bien $b = -c$ et $\langle a, -c, c \rangle \sim \langle c, -c, a \rangle$; ceci force $a = c$ et l'on obtient $\langle a, a, a \rangle \sim \langle a, a, a \rangle$ ou $\langle a, -a, a \rangle \sim \langle a, a, a \rangle$.

• Soit $(r, t) = (1, 1)$ ou $(-1, -1)$. Dans ce cas, nous avons $a \geq a' \geq a|rt| = a$; donc $a = a' = a + b + c$; d'où $c = -b$. Cela signifie que $\langle a', b', c' \rangle \sim \langle a, b, -b \rangle$, mais puisque la forme est réduite, nous avons $a \leq -b$. Comme au préalable, nous avions $|b| \leq a$, nous concluons que $b = -a$, une contradiction. Donc les formes réduites équivalentes sont $\langle a, -a, a \rangle$ et $\langle a, a, a \rangle$.

• Soit $(r, t) = (1, -1)$ ou $(-1, 1)$. Alors $a \geq a' = a - b + c$, c'est-à-dire $c \leq b$. Par hypothèse, $|b| \leq a \leq c$. Donc nous avons $b = c = a$ et $\langle a, b, c \rangle = \langle a, a, a \rangle$. ∎

Dans le cas où $\Delta < 0$, nous avons que $h^+ = h^+_\Delta$ représente la cardinalité de toutes les formes quadratiques définies positives réduites.

Algorithme permettant de calculer, pour un discriminant Δ donné, le nombre de formes quadratiques définies positives réduites

Posons

$$n(a,b) = \begin{cases} 1 \ \textit{si} \ \ b = 0 \ \ \textit{ou si} \ \ b = a \\ \quad \textit{ou si} \ a = \sqrt{\dfrac{b^2-\Delta}{4}}, \\ 2 \ \ \textit{sinon}, \end{cases}$$

$$B = \left\{ b : 0 \le b < \sqrt{|\Delta|/3} \ \ \textit{et} \ \ b \equiv \Delta \ \ (\textit{mod } 2) \right\},$$

et pour $b \in B$, *soit*

$$A_b = \left\{ a : a \,\middle|\, \frac{b^2-\Delta}{4} \quad \textit{et} \ \ b \le a \le \sqrt{\frac{b^2-\Delta}{4}} \right\}.$$

Alors

$$h^+_\Delta = \sum_{b \in B} \sum_{a \in A_b} n(a,b).$$

Exemple. Soit $\Delta = -264 = 4(-2 \cdot 3 \cdot 11)$. Alors

$$\begin{aligned} B &= \left\{ b : 0 \le b < \sqrt{264/3} \ \ \text{et} \ \ b \equiv 0 \pmod 2 \right\} \\ &= \{0, 2, 4, 6, 8\}; \end{aligned}$$

b	$\dfrac{b^2-\Delta}{4}$	(a,c)	A_b
0	66	$(1,66)$ $(2,33)$ $(3,22)$ $(6,11)$	$A_0 = \{1,2,3,6\}$
2	67	$\emptyset$	$A_2 = \emptyset$
4	70	$(5,14)$ $(7,10)$	$A_4 = \{5,7\}$
6	75	$\emptyset$	$A_6 = \emptyset$
8	82	$\emptyset$	$A_8 = \emptyset$

.

Donc

$$\begin{aligned} h^+_{-264} &= n(1,0) + n(2,0) + n(3,0) \\ &\quad + n(6,0) + n(5,4) + n(7,4) \\ &= 1+1+1+1+2+2 \\ &= 8. \end{aligned}$$

D'où les classes propres de formes sont les classes des

formes

$$\begin{cases} \langle 1,0,66\rangle, \ \langle 2,0,33\rangle, \ \langle 3,0,22\rangle, \quad \langle 6,0,11\rangle, \\ \langle 5,4,14\rangle, \ \langle 7,4,10\rangle, \ \langle 5,-4,14\rangle, \ \langle 7,-4,10\rangle. \end{cases}$$

On peut se demander ce que vaut h_{-264}. Notons que

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \langle a,b,c\rangle \ = \ \langle a,-b,c\rangle.$$

Donc,

$$\langle 5,4,14\rangle \overset{\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)}{\longrightarrow} \langle 5,-4,14\rangle$$

et

$$\langle 7,4,10\rangle \overset{\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)}{\longrightarrow} \langle 7,-4,10\rangle.$$

Lorsque $\langle a',b',c'\rangle$ et $\langle a,b,c\rangle$ sont deux formes quadratiques réduites vérifiant $a' < a$, il est impossible d'avoir une matrice

$$B = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$$

vérifiant

$$\langle a',b',c'\rangle = B \langle a,b,c\rangle,$$

c'est-à-dire, il est impossible d'avoir

$$\begin{pmatrix} a' & -\frac{1}{2}b' \\ -\frac{1}{2}b' & c' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix}$$

avec $a' < a$. En effet, si c'était possible, on aurait

$$a' = ax^2 + bxy + cy^2$$

avec $a' < a$, une contradiction avec l'exercice suivant. On conclut alors que $h_{-264} = 6$. ▪

Proposition 2.4. *Soit Δ un discriminant fondamental négatif. Alors $h_\Delta \le \frac{2}{3}|\Delta|$.*

Démonstration. Il faut approximer le nombre de formes quadratiques réduites $\langle a,b,c\rangle$ de discriminant Δ. Il y a au plus $\sqrt{\frac{1}{3}|\Delta|}$ choix pour la valeur de a car $a \le \sqrt{\frac{1}{3}|\Delta|}$. Comme $|b| \le a$, nous avons $|b| \le \sqrt{\frac{1}{3}|\Delta|}$. Or c est uniquement déterminé par a et b. Comme b peut être positif ou négatif, il y a donc au plus

$$\left(2\sqrt{\frac{1}{3}|\Delta|}\right)\left(\sqrt{\frac{1}{3}|\Delta|}\right) = \frac{2}{3}|\Delta|$$

formes quadratiques réduites. ▪

Grâce à des techniques très poussées, on sait que, pour un discriminant fondamental négatif, $h_\Delta \le \sqrt{\Delta}\,\ln|\Delta|$. De plus, Watkins a montré que $h_\Delta > 16$ pour $|\Delta| \ge 31,243$.

Commentaires. Soit m sans facteur carréavec $m < 0$. A. Baker et H. Stark ont indépendemment prouvé qu'il existe 9 valeurs de m, pour lesquelles le nombre de classes h au sens large de formes quadratiques de discriminant fondamental Δ égal à m ou $4m$ est 1, et ce sont pour m égal à

$$-1, \ -2, \ -3, \ -7, \ -11, \ -19, \ -43, \ -67, \ -163.$$

Ils ont aussi prouvé indépendamment que h est égal à 2 pour 18 valeurs de m et ce sont:

-5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427.

Appelons R le nombre d'entiers négatifs $-m$ (ayant la propriété que $-m$ ou $-4m$ est un discriminant négatif) où $h = A$ pour un A donné. Nous avons alors la table suivante qui donne aussi la plus grande valeur de $|-m|$ pour laquelle $h = A$:

h	1	2	3	4	5	6	7	8	9	10
R	9	18	16	54	25	51	31	131	34	87
$\vdash m\vert \leq$	163	427	907	1555	2683	3763	5923	6307	10627	13843

Siegel a démontré que pour les corps quadratiques K de discriminant négatif Δ, (donc pour les formes quadratiques définies), le nombre de classes $h(\Delta)$ tend vers l'infini avec Δ. Ceci veut dire que pour tout entier h_0 donné, il n'y a qu'un nombre fini de corps quadratiques imaginaires dont le nombre de classes vaut h_0.

Exercice 2.1. Vérifiez que $\langle a, b, a\rangle \sim \langle a, -b, a\rangle$ et que $\langle a, a, c\rangle \sim \langle a, -a, c\rangle$.

Exercice 2.2. Trouvez les valeurs des nombres de classes h et h^+ lorsque $\Delta = -15$.

Exercice 2.3 Soit

$$f(X, Y) = aX^2 + bXY + cY^2$$

une forme quadratique définie positive avec $|b| \leq a \leq c$, et soit v un entier de $\{1, 2, \ldots, a\}$. Prouvez que si $v \in \{1, 2, \ldots, a-1\}$, alors $f(X, Y) = v$ n'a pas de solution entière. De plus, prouvez que les solutions possibles (r, t) de $f(X, Y) = a$ sont données par

$$(r, t) \;=\; \begin{cases} (1,0),\ (-1,0), & \\ (0,1),\ (0,-1) & \text{lorsque } c = a, \\ (1,-1),\ (-1,1) & \text{lorsque } c = b = a > 0, \\ (1,1),\ (-1,-1) & \text{lorsque } c = -b = a > 0. \end{cases}$$

Concluez que a est le plus petit entier positif représenté par la forme quadratique $aX^2 + bXY + cY^2$.

3. Formes quadratiques indéfinies

Passons aux formes quadratiques indéfinies.

Définition 3.1. Une forme quadratique $f = \langle a, b, c\rangle$ de discriminant Δ_f est dite *indéfinie* si $\Delta_f > 0$. De plus, f est dite *réduite* si les deux conditions suivantes sont satisfaites:

(i) $0 < b < \sqrt{\Delta}$,

(ii) $\sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$
ou $\sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b$.

Le nombre de formes quadratiques indéfinies réduites est donc fini, car il n'y a qu'un nombre fini de possibilités pour b et a, l'entier c étant déterminé par le discriminant et les valeurs de a et b. De plus, lorsque f est réduite, $ac < 0$.

Proposition 3.2. *Soit $f = \langle a, b, c\rangle$, une forme quadratique de discriminant $\Delta > 0$. Alors*

f est réduite
$\Leftrightarrow 0 < b < \sqrt{\Delta}$ *et* $\sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$
$\Leftrightarrow 0 < b < \sqrt{\Delta}$ *et* $\sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b$
$\Leftrightarrow \langle c, b, a\rangle$ *est réduite.*

Démonstration. Il suffit de prouver la partie "⇒"de la deuxième équivalence. Supposons

$$0 < b < \sqrt{\Delta} \text{ et } \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b.$$

Comme $\Delta = b^2 - 4ac$, nous avons

$$(\sqrt{\Delta} - b)(\sqrt{\Delta} + b) \;=\; -4ac \;=\; (2|a|)(2|c|).$$

Si $2|c| \leq \sqrt{\Delta} - b$, alors nous obtenons la contradiction

$$(2|c|)(2|a|) < (\sqrt{\Delta} - b)(\sqrt{\Delta} + b) \;=\; \Delta - b^2 \;=\; -4ac.$$

Si $2|c| \geq \sqrt{\Delta} + b$, alors nous obtenons la contradiction

$$(2|c|)(2|a|) > (\sqrt{\Delta} - b)(\sqrt{\Delta} + b) \;=\; \Delta - b^2 \;=\; -4ac.$$

D'où $\sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b$. ∎

Remarque. Soit $f = \langle a, b, c\rangle$ une forme quadratique indéfinie réduite de déterminant Δ. Alors

$$ac < 0, \quad |a| < \sqrt{\Delta} \quad \text{et} \quad |c| < \sqrt{\Delta}.$$

.

Exemple. Trouvons toutes les formes quadratiques indéfinies réduites de discriminant $\Delta = 316 = 4 \cdot 79$. Nous cherchons à avoir

$$0 < b < \sqrt{\Delta} \quad \text{avec} \quad 4|(\Delta - b^2) \quad (\text{car } \Delta = b^2 - 4ac).$$

Alors

$$b \in \{2, 4, 6, 8, 10, 12, 14, 16\}.$$

De plus, nous voulons

$$\sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b \quad \text{et} \quad \sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b.$$

Nous obtenons le tableau suivant:

b	$\sqrt{\Delta}-b$	$\sqrt{\Delta}+b$	$(\lvert a\rvert,\lvert c\rvert)$
2	15.77	19.77	$\emptyset$
4	13.77	21.77	$\emptyset$
6	11.77	23.77	$(7,10)$
			$(10,7)$
8	9.77	25.77	$(7,9)$
			$(9,7)$
10	7.77	27.77	$(6,9)$
			$(9,6)$
12	5.77	29.77	$\emptyset$
14	3.77	31.77	$(2,15)$
			$(3,10)$
			$(5,6)$
			$(6,5)$
			$(10,3)$
			$(15,2)$
16	1.77	33.77	$(1,15)$
			$(3,5)$
			$(5,3)$
			$(15,1)$

Les 32 formes quadratiques réduites de discriminant $\Delta = 316$ sont alors

$$\begin{cases} \langle \pm 7, 6, \mp 10\rangle\,, & \langle \pm 10, 6, \mp 7\rangle\,, & \langle \pm 6, 10, \mp 9\rangle\,, \\ \langle \pm 7, 8, \mp 9\rangle\,, & \langle \pm 9, 8, \mp 7\rangle\,, & \langle \pm 9, 10, \mp 6\rangle\,, \\ \langle \pm 2, 14, \mp 15\rangle\,, & \langle \pm 15, 14, \mp 2\rangle & \langle \pm 3, 14, \mp 10\rangle\,, \\ \langle \pm 10, 14, \mp 3\rangle\,, & \langle \pm 5, 14, \mp 6\rangle\,, & \langle \pm 6, 14, \mp 5\rangle\,, \\ \langle \pm 3, 16, \mp 5\rangle\,, & \langle \pm 5, 16, \mp 3\rangle\,, & \langle \pm 1, 16, \mp 15\rangle\,, \\ \langle \pm 15, 16, \mp 1\rangle\,. \end{cases}$$

Définition 3.3. À une forme quadratique $f = \langle a, b, c\rangle$ indéfinie de discriminant Δ, nous *associons* les nombres quadratiques réels

$$\omega = \omega(f) = \frac{b+\sqrt{\Delta}}{2|a|} \quad \text{et} \quad \Omega = \Omega(f) = \frac{b+\sqrt{\Delta}}{2|c|},$$

qui sont respectivement les valeurs absolues de certaines racines judicieuses des polynômes irréductibles ax^2+bx+c et cy^2+by+a.

On rappelle que le *conjugué* (algébrique) α' du nombre quadratique $\alpha = x + y\sqrt{m}$ est égal à $x - y\sqrt{m}$.

Définition 3.4. Un nombre quadratique α est dit *réduit* si $\alpha > 1$ et si ,en plus, le conjugué α' de α vérifie $-1 < \alpha' < 0$.

Acceptons le résultat suivant.

Proposition 3.5. *Une forme quadratique indéfinie f est réduite si et seulement si $\omega(f)$ est réduit si et seulement si $\Omega(f)$ est réduit.*

Proposition 3.6. *Toute forme quadratique indéfinie f de discriminant Δ est strictement équivalente à une forme réduite de même discriminant.*

Démonstration. Nous utiliserons ce qui est classiquement appelé un *algorithme de réduction*. Soit $\langle a, b, c\rangle$ une forme quadratique non réduite. Choisissons l'unique entier δ vérifiant

$$\frac{b+\sqrt{\Delta}}{2|c|} - 1 < \frac{2c}{2|c|}\delta < \frac{b+\sqrt{\Delta}}{2|c|},$$

de sorte que

$$\sqrt{\Delta} - 2|c| < -b + 2c\delta < \sqrt{\Delta}\,.$$

En faisant agir $\begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$ sur $\langle a, b, c\rangle$, nous avons

$$\langle a, b, c\rangle \;\sim\; \left\langle c, -b + 2c\delta, a - b\delta + c\delta^2\right\rangle \;=\; \langle a', b', c'\rangle\,.$$

Si $|c'| = |a - b\delta + c\delta^2| < |c| = |a'|$, alors le processus est répété pour obtenir

$$\langle a, b, c\rangle \;\sim\; \langle a', b', c'\rangle \sim \langle a'', b'', c''\rangle\,.$$

Si $|c''| < |a''| = |c'| < |a'|$, le processus est répété, quoique l'algorithme de réduction doive se terminer après un nombre fini d'étapes. Plus précisément, le processus se termine

lorsque nous obtenons une forme $\langle A, B, C\rangle$ telle que

$$|A| \le |C| \quad \text{et} \quad \sqrt{\Delta} - 2|A| < B < \sqrt{\Delta}.$$

Si ces conditions sont satisfaites, nous avons alors

$$\sqrt{\Delta} - B < 2|A|.$$

De plus, puisque

$$|\sqrt{\Delta} - B| \cdot |\sqrt{\Delta} + B| \;=\; (2|A|)(2|C|),$$

nous devons alors obligatoirement avoir $|\sqrt{\Delta}+B| > 2|C|$. Nous obtenons alors

$$|\sqrt{\Delta} + B| \;>\; 2|C| \;>\; 2|A| > \sqrt{\Delta} - B.$$

Des deux extrémités de cette chaîne d'inégalités, nous voyons que B doit être positif, de sorte que $0 < B < \sqrt{\Delta}$ et $\langle A, B, C\rangle$ est réduite. ▪

Définition 3.7. Les formes quadratiques $\langle a, b, a'\rangle$ et $\langle a', b', c'\rangle$ sont dites *adjacentes* si $b + b' \equiv 0 \pmod{2a'}$. On dit alors:

$\langle a, b, a'\rangle$ est *adjacente à gauche* de $\langle a', b', c'\rangle$,
$\langle a', b', c'\rangle$ est *adjacente à droite* de $\langle a, b, a'\rangle$.

Pour sa part, Gauss dirait plutôt que $\langle a, b, a'\rangle$ est le voisin à gauche de $\langle a', b', c'\rangle$ et que $\langle a', b', c'\rangle$ est le voisin à droite de $\langle a, b, a'\rangle$.

Proposition 3.8. *Soit $f = \langle a, b, c\rangle$ une forme quadratique réduite de discriminant $\Delta > 0$.*

(1) *Alors il existe une unique forme quadratique réduite $\langle c, b', c'\rangle$ adjacente à f à droite qui soit strictement équivalente à f. Il s'agit de prendre b' tel qu'à la fois*

$$b + b' \equiv 0 \pmod{2c} \quad \textit{et} \quad \sqrt{\Delta} - 2|c| < b' < \sqrt{\Delta}\,.$$

(2) *De plus, il existe une unique forme quadratique réduite $\langle a'', b'', a\rangle$ adjacente à f à gauche qui soit strictement équivalente à f. Il s'agit de prendre b'' tel qu'à la fois*

$$b + b'' \equiv 0 \pmod{2a} \quad \textit{et} \quad \sqrt{\Delta} - 2|a| < b'' < \sqrt{\Delta}\,.$$

Démonstration. **(1)** Soit b' tel que

$$b + b' \equiv 0 \pmod{2c} \quad \text{et} \quad \sqrt{\Delta} - 2|c| < b' \leq \sqrt{\Delta}$$

et soit u l'entier $\dfrac{b+b'}{2c}$. On aura alors

$$\frac{\sqrt{\Delta}}{2|c|} - 1 < \frac{b'}{2|c|} < \frac{\sqrt{\Delta}}{2|c|},$$

de sorte que

$$\frac{b+\sqrt{\Delta}}{2|c|} - 1 < \frac{b+b'}{2|c|} < \frac{b+\sqrt{\Delta}}{2|c|}.$$

Alors $|u| = \dfrac{b+b'}{2|c|}$ est un entier qui s'avère être égal à la partie entière de $\Omega(f) = \dfrac{b+\sqrt{\Delta}}{2|c|}$ et la valeur de b' est

uniquement déterminée par l'égalité $b' = -b + 2cu$. Donc la forme $\langle c, b', c'\rangle$ adjacente à f à droite est uniquement déterminée par l'entier u vérifiant

$$\begin{pmatrix} 0 & -1 \\ 1 & u \end{pmatrix} f \;=\; \begin{pmatrix} 0 & -1 \\ 1 & \dfrac{b+b'}{2c} \end{pmatrix} \langle a, b, c\rangle$$
$$= \langle c, -b + 2cu, \star\rangle \;=\; \langle c, b', c'\rangle\,,$$

parce que b' est unique et c' est uniquement déterminé par l'égalité $\Delta = b'^2 - 4cc'$.

Prouvons maintenant que $\langle c, b', c'\rangle$ est réduite. Par hypothèse, $\langle a,\ b,\ c\rangle$ est réduite. On a déjà prouvé que $2|c| < \sqrt{\Delta}$. L'entier b' est tel que

$$b + b' \equiv 0 \pmod{2c} \quad \text{et} \quad \sqrt{\Delta} - 2|c| < b' < \sqrt{\Delta}.$$

Or $\sqrt{\Delta} - 2c > 0$. Donc $b' > 0$. De plus $b' < \sqrt{\Delta}$. Nous voulons montrer que

$$\sqrt{\Delta} - 2|c| < b' < \sqrt{\Delta} + 2|c|.$$

Nous avons déjà la première inégalité, car elle provient de la définition de b'. Il ne reste qu'à prouver l'inégalité $b' < \sqrt{\Delta} + 2|c|$.

Supposons le contraire, *i.e.*, supposons

$$\sqrt{\Delta} + 2|c| \leq b' = -b + 2|a||c|$$

où par définition

$$|a| = \frac{b+b'}{2|c|} = \left[\frac{b+\sqrt{\Delta}}{2|c|}\right].$$

Donc

$$b + \sqrt{\Delta} \leq -2|c| + 2|a||c|,$$

c'est-à-dire

$$\frac{b+\sqrt{\Delta}}{2|c|} \leq |a| - 1,$$

ce qui est une contradiction.

(2) Soit b'' tel que

$$b + b'' \equiv 0 \pmod{2a} \quad \text{et} \quad \sqrt{\Delta} - 2|a| < b'' \leq \sqrt{\Delta}$$

et soit r l'entier $\dfrac{b+b''}{2a}$ où la valeur de b'' est uniquement déterminée par l'égalité $b'' = -b + 2ar$. On aura alors

$$\frac{\sqrt{\Delta}}{2|a|} - 1 < \frac{b''}{2|a|} < \frac{\sqrt{\Delta}}{2|a|},$$

de sorte que

$$\frac{b+\sqrt{\Delta}}{2|a|} - 1 < \frac{b+b''}{2|a|} < \frac{b+\sqrt{\Delta}}{2|a|}.$$

Alors $|r| = \dfrac{b+b''}{2|a|}$ est un entier qui s'avère être égal à la partie entière de $\omega(f) = \dfrac{b+\sqrt{\Delta}}{2|a|}$ et la valeur de b'' est uniquement déterminée par l'égalité $b'' = -b + 2ar$. Donc la forme $\langle a'', b', a\rangle$ adjacente à f à gauche est uniquement déterminée par l'entier r vérifiant

$$\begin{pmatrix} -r & -1 \\ 1 & 0 \end{pmatrix} f \;=\; \begin{pmatrix} -\frac{b+b''}{2a} & -1 \\ 1 & 0 \end{pmatrix} \langle a, b, c\rangle$$
$$= \langle \star, -b + 2ar, a\rangle \;=\; \langle a'', b'', a\rangle\,,$$

parce que b'' est unique et a'' est uniquement déterminé par l'égalité $\Delta = b''^2 - 4a''a$. De plus, la forme $\langle a'', b'', a\rangle$ est réduite (Exercice).

Proposition 3.9. *L'ensemble $\mathcal{F}_\Delta$ des formes quadratiques réduites de discriminant $\Delta > 0$ peut être partitionné en cycles de formes adjacentes. De plus, à l'intérieur de chaque cycle, les formes sont strictement équivalentes entre elles.*

Démonstration. L'ensemble $\mathcal{F}_\Delta$ des formes réduites de discriminant Δ donné est fini. En effet, $\Delta = b^2 - 4ac$ avec b prenant un nombre fini de valeurs, vu que

$$0 \leq b \leq \sqrt{\Delta}.$$

De plus, comme

$$\sqrt{\Delta} - b \leq 2|a| \leq \sqrt{\Delta} + b,$$

nous avons aussi que a prend un nombre fini de valeurs. Enfin, c est uniquement déterminé par $\dfrac{\Delta - b^2}{4a}$.

Choisissons un élément quelconque dans cet ensemble $\mathcal{F}_\Delta$, disons f, puis trouvons l'unique forme g de $\mathcal{F}_\Delta$ qui lui est ajdacente à droite. Infailliblement, nous arriverons à la

forme unique qui est à la gauche de f. On aura alors exhibé un premier cycle. On recommence ensuite avec une autre forme, non équivalente à f, et ainsi de suite, jusqu'à ce que toutes les formes de $\mathcal{F}_\Delta$ aient été "classées". Soulignons que les formes adjacentes sont équivalentes par la matrice de transformation

$$\begin{pmatrix} 0 & -1 \\ 1 & \dfrac{b+b'}{2c} \end{pmatrix}.$$

Puisque l'équivalence au sens strict est transitive, toutes les formes dans un cycle donné sont donc strictement équivalentes entre elles. Cette opération est réalisable en un temps fini puisque $\mathcal{F}_\Delta$ est fini.

Théorème 3.10. *Soit f et f', deux formes quadratiques indéfinies réduites de même discriminant. Alors f et f' sont équivalentes au sens strict si et seulement si f et f' appartiennent au même cycle.*

Démonstration. ($\Leftarrow$) C'est le contenu de la proposition 3.9.

($\Rightarrow$) Cette implication est de loin la plus ardue, et nous en donnerons plus loin l'idée maîtresse. ▪

Comme $h^+ = h^+_\Delta$ représente la cardinalité de $C\ell^+(\Delta)$, nous avons alors que $h^+ = h^+_\Delta$ est le nombre de cycles de formes réduites.

4. Fractions continues et formes quadratiques

Nous allons faire quelques rappels sur les fractions continues et indiquer comment elles nous servent pour exhiber toutes les formes quadratiques indéfinies réduites de discriminant $\Delta > 0$.

Le développement d'un nombre $\alpha = \alpha_0$ en fraction continue s'effectue de la façon suivante. Soit $a_0 = [\alpha_0]$ la partie entière de α_0. Posons

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} \qquad \text{et} \qquad a_1 = [\alpha_1].$$

Donc $\alpha_0 = a_0 + \dfrac{1}{\alpha_1}$. Posons ensuite

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} \qquad \text{et} \qquad a_2 = [\alpha_2],$$

de sorte que $\alpha_1 = a_1 + \dfrac{1}{\alpha_2}$. Dans la même veine, pour $n \geq 1$, posons

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} \qquad \text{et} \qquad a_{n+1} = [\alpha_{n+1}].$$

Nous avons alors

$$\alpha_n \;=\; a_n + \frac{1}{\alpha_{n+1}} = \frac{a_n\alpha_{n+1}+1}{1\alpha_{n+1}+0} \;=:\; \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \alpha_{n+1}.$$

Donc

$$\alpha_0 \;=\; a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots\, a_{n-2} + \cfrac{\ddots\ 1}{a_{n-1} + \cfrac{1}{\alpha_n}}}}}}$$
$$=:\; [a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n].$$

La dernière égalité introduit une convention qui permet de sauver de l'espace.

Définitions. Une *fraction continue* α est une expression de la forme

$$\alpha \;=\; a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}}$$
$$=\; [a_0, a_1, a_2, a_3, a_4, \ldots]$$

où $a_i \in \mathbb{R}$ pour $i \in \mathbb{N}$. Dans la littérature, une fraction continue est aussi appelée *fraction continuée* ou (rarement) *fraction continuelle*. Les a_i sont appelés les *quotients partiels* de la fraction continue α. Si les quotients partiels a_i sont des entiers > 0 pour $i > 0$, on est en présence d'une *fraction continue simple infinie*. S'il existe l et k minimaux, tels que $a_n = a_{n+l}$ pour tout $n \geq k$, alors la

fraction continue est dite périodique et on écrit

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{l+k-1}}],$$

la barre hirizontale indiquant ce qui est continuellement répété. Les suites

$$a_0, a_1, \ldots, a_{k-1} \quad \text{et} \quad a_k, a_{k+1}, \ldots, a_{l+k-1}$$

sont respectivement appelées *prépériode* et *période* de la fraction continue. De plus $[a_0, a_1, \ldots, a_t]$ est dit la *t-ième réduite* ou le *t-ième convergent* de α.

Proposition 4.1. *Soit $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$. Pour $n \geq 1$, posons*

$$\frac{p_n}{q_n} \;:=\; [a_0, a_1, a_2, \ldots, a_{n-1}, a_n]$$

(1) *Alors pour tout $n \geq 1$,*

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2}, \\ q_n = a_n q_{n-1} + q_{n-2}. \end{cases}$$

(2) *De plus, pour tout $n \geq 0$,*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} \quad \textit{et} \quad \text{PGCD}(p_n, q_n) = 1.$$

Démonstration. **(1)** Les formules sont vraies pour $n = 0, 1$. Nous les supposerons vraies pour $0, 1, \ldots, n$:

$$\begin{cases} p_{-2}=0, & q_{-2}=1;\\ p_{-1}=1, & q_{-1}=0;\\ p_0=a_0, & q_0=1;\\ p_1=a_1a_0+1, & q_1=a_1;\\ \quad\vdots & \quad\vdots\\ p_n=a_np_{n-1}+p_{n-2}, & q_n=a_nq_{n-1}+q_{n-2}; \end{cases}$$

$$\begin{cases} [a_0]=\frac{p_0}{q_0}, \quad [a_0,a_1]=a_0+\frac{1}{a_1}=\frac{p_1}{q_1},\dots,\\ [a_0,a_1,\dots,a_n] \;=\; \frac{p_n}{q_n} \;=\; \dfrac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}}. \end{cases}$$

Montrons-les pour $n+1$. Nous avons:

$$\begin{aligned}
\frac{p_{n+1}}{q_{n+1}} &= [a_0,a_1,\dots,a_n,a_{n+1}]\\
&= [a_0,a_1,\dots,a_n,a'_n] \text{ avec } a'_n=a_n+\frac{1}{a_{n+1}}=\frac{a_{n+1}a_n+1}{a_{n+1}}\\
&= \frac{a'_np_{n-1}+p_{n-2}}{a'_nq_{n-1}+q_{n-2}} \qquad \text{(d'après l'hypothèse d'induction)}\\
&= \frac{\left(\dfrac{a_na_{n+1}+1}{a_{n+1}}\right)p_{n-1}+p_{n-2}}{\left(\dfrac{a_na_{n+1}+1}{a_{n+1}}\right)q_{n-1}+q_{n-2}}\\
&= \frac{a_na_{n+1}p_{n-1}+p_{n-1}+a_{n+1}p_{n-2}}{a_na_{n+1}q_{n-1}+q_{n-1}+a_{n+1}q_{n-2}}\\
&= \frac{a_{n+1}(a_np_{n-1}+p_{n-2})+p_{n-1}}{a_{n+1}(a_nq_{n-1}+q_{n-2})+q_{n-1}}\\
&= \frac{a_{n+1}p_n+p_{n-1}}{a_{n+1}q_n+q_{n-1}} \qquad \text{(d'après l'hypothèse d'induction),}
\end{aligned}$$

Donc

$$p_{n+1}=a_{n+1}p_n+p_{n-1} \quad \text{et} \quad q_{n+1}=a_{n+1}q_n+q_{n-1}.$$

(2) Soit

$$H_n=\begin{pmatrix} p_n & p_{n-1}\\ q_n & q_{n-1}\end{pmatrix} \quad \text{et} \quad U_n=\begin{pmatrix} a_n & 1\\ 1 & 0\end{pmatrix}.$$

Alors $H_{n+1}=U_{n+1}H_n$ d'après la partie (1). Nous voulons

prouver que $\det(H_n)=(-1)^{n+1}$. Ceci est vrai pour $n=0$:

$$\det(H_0) \;=\; \det\begin{pmatrix} a_0 & 1\\ 1 & 0\end{pmatrix}=(-1)^1=-1.$$

Supposons la formule vraie pour n et montrons-la pour n+1:

$$\begin{aligned}
\det(H_{n+1}) &= \det(U_{n+1})\det(H_n)\\
&= (-1)(-1)^{n+1}=(-1)^{n+2}.
\end{aligned}$$

De cette formule pour le déterminant, nous concluons que

$$\text{PGCD}(P_n,Q_n)=1.$$

Définition Soit $\alpha=[a_0,a_1,a_2,\dots]$. On dénote par $C_n=\dfrac{p_n}{q_n}$ la *n-ième réduite* (ou le *n-ième quotient partiel*) de α.

Corollaire. **(1)** *Pour tout* $n\geq 1$,

$$C_n-C_{n-1}=\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^{n+1}}{q_nq_{n-1}}.$$

(2) *Pour tout* $n\geq 1$,

$$p_nq_{n-2}-p_{n-2}q_n=(-1)^na_n.$$

Démonstration. **(1)** Cette partie est directe.
(2) La formule est vraie pour $n=1$:

$$p_1q_{-1}-p_{-1}q_1=(a_1a_0+1)-a_1=(-1)a_1.$$

Supposons-la vraie pour n, et montrons-la pour $n+1$:

$$\begin{aligned}
p_{n+1}q_{n-1} \;-\; p_{n-1}q_{n+1} &= \det\begin{pmatrix} p_{n+1} & q_{n+1}\\ p_{n-1} & q_{n-1}\end{pmatrix}\\
&= \det\begin{pmatrix} a_{n+1}p_n+p_{n-1} & a_{n+1}q_n+q_{n-1}\\ p_{n-1} & q_{n-1}\end{pmatrix}\\
&= a_{n+1}\det\begin{pmatrix} p_n & q_n\\ p_{n-1} & q_{n-1}\end{pmatrix}=a_{n+1}(-1)^{n+1}.
\end{aligned}$$

Théorème 4.2. *Soit* $C_s=[a_0,a_1,a_2,\dots,a_s]$ *le s-ième convergent du développement en fraction continue de* α.
(1) *Alors* $C_1>C_3>C_5>\ldots>C_{2s-1}>C_{2s}>C_{2s-2}>\ldots>C_4>C_2>C_0$.
(2) *Pour tout* $k\geq 1$, $q_k\geq k$.
(3) $\alpha=\lim_{k\to\infty}C_k$.

Démonstration. **(1)** D'après le corollaire précédent,

$$C_k-C_{k-2} \;=\; \frac{p_k}{q_k}-\frac{p_{k-2}}{q_{k-2}} \;=\; \frac{(-1)^kp_k}{q_kq_{k-2}}.$$

Si k est pair, alors $C_k>C_{k-2}$ et si k est impair, alors $C_{k-2}>C_k$. De plus, d'après le corollaire, pour tout k,

$$C_{2k+1}-C_{2k}=\frac{(-1)^{2k+1}}{q_kq_{k-1}}=\frac{1}{q_kq_{k-1}}>0,$$

c'est-à-dire

$$C_{2k+1}>C_{2k}.$$

Donc, quel que soit $k\geq 0$, nous avons pour tout $i\geq 0$,

$$C_{2i+1}\geq C_{2i+1+2k}>C_{2i+2k}\geq C_{2k},$$

c'est-à-dire que pour tout $k, i \geq 0$, nous avons

$$C_{2i+1} > C_{2k}.$$

(2) Nous avons $q_1 = a_1 \geq 1$. Soit $q_k \geq k$. Alors

$$q_{k+1} = a_{k+1}q_k + q_{k-1} \geq 1k + (k-1) \geq k+1.$$

(3) Une preuve rigoureuse pourrait être donnée. Contentons-nous d'observer que

$$C_{2s+1} - C_{2s} = \frac{1}{q_{(2s+1)}q_{2s}} \leq \frac{1}{(2s+1)(2s)}$$

et que si

$$\lim_{k\to\infty} C_{2k+1} = \alpha_1, \lim_{k\to\infty} C_{2k} = \alpha_2,$$

alors $\alpha_1 = \alpha_2 = \alpha_1$. ▪

Acceptons le résultat fondamental suivant.

Proposition 4.3. *Soit α un nombre réel . Alors le développement de α en fraction continue est infini (resp. fini) si et seulement si α est irrationnel (resp. rationnel). De plus, le développement de α est périodique si et seulement si α en fraction continue est une irrrationnalité quadratique.*

Définition 4.4. Le signe d'un entier c sera noté $\sigma(c)$. Par exemple, $\sigma(6) = +1$ et $\sigma(-6) = -1$.

Algorithme calculant les quotients partiels d'irrationnalités quadratiques

Soit

$$\begin{aligned} K = \mathbb{Q}(\sqrt{m}) &= \mathbb{Q}(\sqrt{\Delta}) \\ &= \{s + t\sqrt{m} \ : \ s,t \in \mathbb{Q}\} \end{aligned}$$

avec m libre de carrés, et

$$\Delta = \begin{cases} m \ \ si \ \ m \equiv 1 \pmod 4, \\ 4m \ \ si \ \ m \equiv 2 \ ou \ 3 \pmod 4. \end{cases}$$

Soit

$$\alpha = \alpha_0 = \frac{P_0 + \sqrt{\Delta}}{2Q_0},$$

où $4Q_0 \,|\, (\Delta - P_0^2)$ *avec* $P_0, Q_0 \in \mathbb{Z}$.

Pour $i \geq 0$ posons

$$\begin{cases} \alpha_i = \dfrac{P_i + \sqrt{\Delta}}{2Q_i} \quad et \quad a_i = [\alpha_i], \\ P_{i+1} = 2a_iQ_i - P_i, \\ Q_{i+1} = \dfrac{\Delta - P_{i+1}^2}{4Q_i}. \end{cases}$$

Alors $\alpha = \alpha_0 = [a_0, a_1, a_2, \ldots]$ et nous avons le tableau suivant:

P_0	P_1	P_2	P_3	$\ldots$
Q_0	Q_1	Q_2	Q_3	$\ldots$
a_0	a_1	a_2	a_3	$\ldots$

Remarque. L'algorithme précédent peut être légèrement modifié de la façon suivante: Soit m sans facteur carré et soit

$$\alpha_0 = \frac{p_0 + \sqrt{m}}{q_0} \quad \text{avec} \quad q_0 | (m - p_0^2).$$

Pour $i \geq 0$, posons

$$\begin{cases} \alpha_i = \dfrac{p_i + \sqrt{m}}{q_i} \quad \text{et} \quad a_i = [\alpha_i], \\ p_{i+1} = a_iq_i - p_i, \\ q_{i+1} = \dfrac{m - p_{i+1}^2}{q_i}, \end{cases}$$

de sorte que nous avons $\alpha = \alpha_0 = [a_0, a_1, a_2, a_3, \ldots]$ via le tableau

p_0	p_1	p_2	p_3	$\ldots$
q_0	q_1	q_2	q_3	$\ldots$
a_0	a_1	a_2	a_3	$\ldots$

Algorithme calculant le cycle des formes réduites équivalentes au sens strict à une forme quadratique réduite

(1) Soit $f_0 = \langle a_0, b_0, c_0 \rangle$, une forme quadratique réduite de discriminant $\Delta > 0$. Alors

$$\alpha_0 = \frac{b_0 + \sqrt{\Delta}}{2|c_0|} = [\overline{u_0, u_1, \ldots, u_{l-1}}]$$

où l est la longueur de la période de la fraction continue.

Ceci mène au tableau suivant:

$P_0 = b_0$	P_1	P_2	...	P_{l-1}	$P_l = P_0$	P_1	P_2	...	P_{l-1}	...
$Q_0 = \lvert c_0 \rvert$	Q_1	Q_2	...	Q_{l-1}	$Q_l = Q_0$	Q_1	Q_2	...	Q_{l-1}	...
u_0	u_1	u_2	...	u_{l-1}	$u_l = u_0$	u_1	u_2	...	u_{l-1}	...

(2) Le cycle des formes réduites strictement équivalentes à f_0 est formé des formes réduites $f_0, f_1, \ldots, f_{r-1}$ où

$$r = \begin{cases} l & \text{si } l \text{ est pair} \\ 2l & \text{si } l \text{ est impair,} \end{cases}$$

et où pour $0 \leq i \leq r-2$,

$$\begin{aligned} f_{i+1} &= \langle a_{i+1}, b_{i+1}, c_{i+1} \rangle \\ &= \begin{pmatrix} 0 & -1 \\ 1 & \sigma(c_i)u_i \end{pmatrix} f_i \ = \ \begin{pmatrix} 0 & -1 \\ 1 & -\sigma(a_i)u_i \end{pmatrix} f_i \\ &= \left\langle (-1)^i \sigma(c_0) Q_i, \ P_{i+1}, \ (-1)^{i+1} \sigma(c_0) Q_{i+1} \right\rangle. \end{aligned}$$

Il est important de réaliser le fait suivant:

- Si ℓ est impair, alors le cycle de la forme $\langle a, b, c\rangle$ inclut la forme $\langle -a, b, -c\rangle$.
- Si ℓ est pair, alors le cycle de la forme $\langle a, b, c\rangle$ est différent du cycle de la forme $\langle -a, b, -c\rangle$.

Remarque. L'étape (2) de l'algorithme peut aussi s'exprimer de façon équivalente comme suit:

(2′) Le cycle des formes réduites proprement équivalentes à f_0 est formé des formes réduites $f_0, f_1, \ldots, f_{l-1}$ où, pour $0 \le i \le l-2$,

$$\begin{aligned} f_{i+1} &= \langle a_{i+1}, b_{i+1}, c_{i+1}\rangle \\ &= \begin{pmatrix} 0 & 1 \\ -1 & \sigma(c_i)u_i \end{pmatrix} f_i \\ &= \left\langle (-1)^i\sigma(c_0)Q_i,\ P_{i+1},\ (-1)^{i+1}\sigma(c_0)Q_{i+1}\right\rangle. \end{aligned}$$

Auxquelles s'ajoutent, lorsque l est impair, les formes réduites

$$f_l = \langle -a_0, b_0, -c_0\rangle, f_{l+1}, \ldots, f_{2l+1},$$

où pour $0 \le i \le (l-2)$,

$$\begin{aligned} f_{i+l+1} &= \begin{pmatrix} 0 & 1 \\ -1 & -\sigma(c_i)u_i \end{pmatrix} f_{i+l} \\ &= \left\langle (-1)^{i+1}\sigma(c_0)Q_i,\ P_{i+1},\ (-1)^i\sigma(c_0)Q_{i+1}\right\rangle. \end{aligned}$$

Donnons trois exemples.

Exemple 1. Soit $m = 10$, $\Delta = 40$. Les 8 formes réduites de discriminant $\Delta = 40$ sont:

$$\begin{cases} \langle 2,4,-3\rangle, \ \langle -1,6,1\rangle, \ \langle 3,2,-3\rangle, \ \langle -3,4,2\rangle, \\ \langle -2,4,3\rangle, \ \langle -3,2,3\rangle, \ \langle 3,4,-2\rangle, \ \langle 1,6,-1\rangle. \end{cases}$$

Considérons l'irrationnalité quadratique

$$\Omega = \frac{4+\sqrt{40}}{6} = [\,\overline{1,1,2}\,]$$

associée à la forme $\langle 2,4,-3\rangle$. Le développement en fraction continue est obtenu via le tableau

4	2	4	4	2	4	...
3	3	2	3	3	2	...
1	**1**	**2**	**1**	**1**	**2**	...

La longueur étant impaire, associons à **1**, **1**, **2**, **1**, **1**, **2** la suite signée $-1, 1, -2, 1, -1, 2$. Nous obtenons alors un cycle de longueur 6:

$$\begin{array}{ccccc} & \overset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)}{\longrightarrow} & & \overset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)}{\longrightarrow} & \\ \langle 2,4,-3\rangle & & \langle -3,2,3\rangle & & \langle 3,4,-2\rangle \\ \left(\begin{smallmatrix} 0 & -1 \\ 1 & 2 \end{smallmatrix}\right)\uparrow & & & & \downarrow\left(\begin{smallmatrix} 0 & -1 \\ 1 & -2 \end{smallmatrix}\right) \\ \langle -3,4,2\rangle & & \langle 3,2,-3\rangle & & \langle -2,4,3\rangle \\ & \underset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)}{\longleftarrow} & & \underset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)}{\longleftarrow} & \end{array}$$

Considérons cette fois-ci l'irrationnalité quadratique

$$\Omega = \frac{6+\sqrt{40}}{2} = [\,\overline{6}\,]$$

associée à la forme $\langle 1,6,-1\rangle$. Le développement en fraction continue est obtenu via le tableau

6	6	...
1	1	...
6	**6**	...

Associons à **6**, **6** la suite signée $-6,\ 6$. Nous obtenons alors un cycle de longueur 2:

$$\langle 1,6,-1\rangle \quad \underset{\longleftarrow}{\overset{\longrightarrow}{\left(\begin{smallmatrix} 0 & -1 \\ 1 & -6 \end{smallmatrix}\right)}} \quad \left(\begin{smallmatrix} 0 & -1 \\ 1 & 6 \end{smallmatrix}\right) \quad \langle -1,6,1\rangle$$

Nous concluons qu'il y a au total 2 cycles et que $h_{10}^+ = 2$.

▪

Remarquons en passant que nous aurions pu commencer avec la forme $\langle -3,2,3\rangle$ à laquelle est associée l'irrationnalité quadratique

$$\Omega = \frac{2+\sqrt{40}}{6} = [\,\overline{1,2,1}\,].$$

ou encore avec la forme $\langle 3,4,-2\rangle$ à laquelle est associée l'irrationnalité

$$\Omega = \frac{4+\sqrt{40}}{4} = [\,\overline{2,1,1}\,].$$

Exemple 2. Soit $m = 15$, $\Delta = 60 = 4 \cdot 15$. Les 8 formes quadratiques réduites sont:

$$\begin{cases} \langle -1,6,6\rangle, \ \langle 1,6,-6\rangle, \ \langle -2,6,3\rangle, \ \langle 2,6,-3\rangle, \\ \langle -3,6,2\rangle, \ \langle 3,6,-2\rangle, \ \langle -6,6,1\rangle, \ \langle 6,6,-1\rangle. \end{cases}$$

Considérons l'irrationnalité quadratique

$$\Omega = \frac{6+\sqrt{60}}{6} = [\,\overline{2,3}\,]$$

associée à la forme $\langle 2,6,-3\rangle$. Le développement en fraction continue est obtenu via le tableau

6	6	...
3	2	...
2	**3**	...

La longueur étant paire, associons à **2**, **3** la suite signée $-2, 3$. Nous obtenons alors un cycle de longueur 2:

$$\langle 2,6,-3\rangle \quad \underset{\longleftarrow}{\overset{\longrightarrow}{\left(\begin{smallmatrix} 0 & -1 \\ 1 & -2 \end{smallmatrix}\right)}} \quad \left(\begin{smallmatrix} 0 & -1 \\ 1 & 3 \end{smallmatrix}\right) \quad \langle -3,6,2\rangle$$

Considérons maintenant l'irrationnalité quadratique

$$\Omega = \frac{6+\sqrt{60}}{6} = [\,\overline{2,3}\,]$$

associée à la forme $\langle -2,6,3\rangle$, et dont le développement en fraction continue apparaît dans le tableau ci-dessus. Associons cette fois-ci à **2**, **3** la suite signée $2,-3$. Nous obtenons alors un cycle de longueur 2:

$$\langle -2,6,3\rangle \quad \begin{matrix}\begin{pmatrix}0&-1\\1&-2\end{pmatrix}\\ \longrightarrow\\ \longleftarrow\\ \begin{pmatrix}0&-1\\1&3\end{pmatrix}\end{matrix} \quad \langle 3,6,-2\rangle$$

Considérons de plus l'irrationnalité quadratique

$$\frac{6+\sqrt{60}}{2} = [\,\overline{6,1}\,]$$

associée à la forme $\langle 6,6,-1\rangle$. Le développement en fraction continue est obtenu via le tableau

6	6	…
1	6	…
6	**1**	…

Associons à **6**, **1** la suite signée $-6,\ 1$. Nous obtenons alors le cycle de longueur 2:

$$\langle 6,6,-1\rangle \quad \begin{matrix}\begin{pmatrix}0&-1\\1&-6\end{pmatrix}\\ \longrightarrow\\ \longleftarrow\\ \begin{pmatrix}0&-1\\1&1\end{pmatrix}\end{matrix} \quad \langle -1,6,6\rangle$$

Considérons maintenant l'irrationnalité quadratique

$$\frac{6+\sqrt{60}}{2} = [\,\overline{6,1}\,]$$

associée à la forme $\langle -6,6,1\rangle$, et dont le développement en fraction continue apparaît dans le tableau ci-dessus. Associons à **6**, **1** la suite signée $6,-1$. Nous obtenons alors le cycle de longueur 2:

$$\langle -6,6,1\rangle \quad \begin{matrix}\begin{pmatrix}0&-1\\1&6\end{pmatrix}\\ \longrightarrow\\ \longleftarrow\\ \begin{pmatrix}0&-1\\1&-1\end{pmatrix}\end{matrix} \quad \langle 1,6,-6\rangle$$

Ceci qui nous amène à un total de 4 cycles, de sorte que $h^+_{60} = 4$.

Exemple 3. Soit $\Delta = m = 145$, où $m \equiv 1 \pmod 4$. Les 28 formes réduites sont:

$$\begin{cases}
\langle -6,5,5\rangle, & \langle 6,5,-5\rangle, & \langle -4,7,6\rangle, & \langle 4,7,-6\rangle,\\
\langle -3,7,8\rangle, & \langle 3,7,-8\rangle, & \langle -8,7,3\rangle, & \langle 8,7,-3\rangle,\\
\langle -6,7,4\rangle, & \langle 6,7,-4\rangle, & \langle -6,1,6\rangle, & \langle 6,1,-6\rangle,\\
\langle -5,5,6\rangle, & \langle 5,5,-6\rangle, & \langle -2,9,8\rangle, & \langle 2,9,-8\rangle,\\
\langle -4,9,4\rangle, & \langle 4,9,-4\rangle, & \langle -8,9,2\rangle, & \langle 8,9,-2\rangle,\\
\langle 1,11,-6\rangle, & \langle -1,11,6\rangle, & \langle -2,11,3\rangle, & \langle 2,11,-3\rangle,\\
\langle -3,11,2\rangle, & \langle 3,11,-2\rangle, & \langle -6,11,1\rangle, & \langle 6,11,-1\rangle.
\end{cases}$$

Considérons la forme $f = \langle 5,5,-6\rangle$, à laquelle on associe le nombre quadratique

$$\Omega = \frac{5+\sqrt{145}}{12} = [\,\overline{1,2,2,1,1}\,].$$

Le développement en fraction continue est obtenu via le tableau

5	7	9	7	5	5	7	9	7	5	…
6	4	4	6	5	6	4	4	6	5	…
1	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	…

Associons à **1**, **2**, **2**, **1**, **1**, **1**, **2**, **2**, **1**, **1** la suite signée $-1,\ 2,\ -2,\ 1,\ -1,\ 1,\ -2,\ 2,\ -1, 1$. Pour simplifier l'écriture,

posons

$$A(u) = \begin{pmatrix}0&-1\\1&u\end{pmatrix}.$$

Nous obtenons alors un cycle de longueur 10:

$$\begin{array}{ccccccc}
\langle 5,5,-6\rangle & \xrightarrow{A(-1)} & \langle -6,7,4\rangle & \xrightarrow{A(2)} & \langle 4,9,-4\rangle & \xrightarrow{A(-2)} & \langle -4,7,6\rangle\\
{\scriptstyle A(1)}\uparrow & & & & & & \downarrow{\scriptstyle A(1)}\\
\langle -6,5,5\rangle & & & & & & \langle 6,5,-5\rangle\\
{\scriptstyle A(-1)}\uparrow & & & & & & \downarrow{\scriptstyle A(-1)}\\
\langle 4,7,-6\rangle & \xleftarrow{A(2)} & \langle -4,9,4\rangle & \xleftarrow{A(-2)} & \langle 6,7,-4\rangle & \xleftarrow{A(1)} & \langle -5,5,6\rangle
\end{array}$$

Considérons maintenant la forme $g = \langle 8,7,-3\rangle$ à laquelle est associée l'irrationnalité quadratiqu

$$\Omega = \frac{7+\sqrt{145}}{6} = [\,\overline{3,5,1}\,.].$$

Le développement en fraction continue est obtenu via le tableau

7	11	9	7	11	9	…
3	2	8	3	2	8	…
3	**5**	**1**	**3**	**5**	**1**	…

Associons à $\mathbf{3}, \mathbf{5}, \mathbf{1}, \mathbf{3}, \mathbf{5}, \mathbf{1}$ la suite signée $-3,\ 5,\ -1,\ 3,\ -5,\ 1$. Nous obtenons alors un cycle de longueur 6:

$$\begin{array}{ccccc} \langle 8,7,-3\rangle & \xrightarrow{A(-3)} & \langle -3,11,2\rangle & \xrightarrow{A(5)} & \langle 2,9,-8\rangle \\ {\scriptstyle \mathrm{A(1)}}\uparrow & & & & \downarrow{\scriptstyle \mathrm{A(-1)}} \\ \langle -2,9,8\rangle & \xleftarrow{A(5)} & \langle 3,11,-2\rangle & \xleftarrow{A(3)} & \langle -8,7,3\rangle \end{array}$$

Considérons aussi la forme $h = \langle 6,1,-6\rangle$, à laquelle est associé le nombre quadratique

$$\Omega = \frac{1+\sqrt{145}}{12} = [\,\overline{1,11,1}\,].$$

Le développement en fraction continue est obtenu via le tableau

1	11	11	1	11	11	...
6	1	6	6	1	6	...
1	**11**	**1**	**1**	**11**	**1**	...

Associons à $\mathbf{1}, \mathbf{11}, \mathbf{1}, \mathbf{1}, \mathbf{11}, \mathbf{1}$ la suite signée $-1,\ 11,\ -1,\ 1,\ -11,\ 1$. Nous obtenons alors un cycle de longueur 6:

$$\begin{array}{ccccc} \langle 6,1,-6\rangle & \xrightarrow{A(-1)} & \langle -6,11,1\rangle & \xrightarrow{A(11)} & \langle 1,11,-6\rangle \\ {\scriptstyle \mathrm{A(1)}}\uparrow & & & & \downarrow{\scriptstyle \mathrm{A(-1)}} \\ \langle -1,11,6\rangle & \xleftarrow{A(-11)} & \langle 6,11,-1\rangle & \xleftarrow{A(1)} & \langle -6,1,6\rangle \end{array}$$

Considérons enfin la forme $q = \langle 3,7,-8\rangle$, à laquelle est associé $\Omega = \frac{7+\sqrt{145}}{16} = [\,\overline{1,5,3}\,]$. Le développement en fraction continue est obtenu via le tableau

7	9	11	7	9	11	...
8	2	3	8	2	3	...
1	**5**	**3**	**1**	**5**	**3**	...

Associons à $\mathbf{1}, \mathbf{5}, \mathbf{3}, \mathbf{1}, \mathbf{5}, \mathbf{3}$ la suite signée $-1, 5, -3, 1, -5, 3$. Nous obtenons alors un cycle de longueur 6:

$$\begin{array}{ccccc} \langle 3,7,-8\rangle & \xrightarrow{A(-1)} & \langle -8,9,2\rangle & \xrightarrow{A(5)} & \langle 2,11,-3\rangle \\ {\scriptstyle \mathrm{A(3)}}\uparrow & & & & \downarrow{\scriptstyle \mathrm{A(-3)}} \\ \langle -2,11,3\rangle & \xleftarrow{A(-5)} & \langle 8,9,-2\rangle & \xleftarrow{A(1)} & \langle -3,7,8\rangle \end{array}$$

En conclusion, nous avons 4 cycles et $h^+_{145} = 4$.

Revenons un instant sur une proposition dont nous avions omis une partie de la démonstration.

Théorème 4.5. *Deux formes quadratiques réduites de discriminant $\Delta > 0$ sont strictement équivalentes si et seulement si elles appartiennent au même cycle.*

Démonstration. ($\Leftarrow$) C'est le contenu du théorème 3.10.

($\Rightarrow$) Nous ne donnerons que les idées maîtresses. Soit $f = \langle a,b,c\rangle$ une forme quadratique réduite et soit g une forme quadratique réduite équivalente au sens strict à f. Alors

$$f \sim g = \langle a',b',c'\rangle = Af = \begin{pmatrix} r & s \\ t & u \end{pmatrix} f$$

avec

$$A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Considérons

$$\Omega(f) = \frac{b+\sqrt{\Delta}}{2|c|}.$$

Il s'avère que

$$\Omega(g) = \Omega(Af) = \frac{r\Omega(f)+s}{t\Omega(f)+u} = \cdots = \frac{P_j+\sqrt{\Delta}}{2Q_{j-1}}.$$

Ce dernier nombre est un nombre quadratique réduit associé à la forme $\langle Q_{j-1}, P_j, -Q_j\rangle$ ou à la forme $\langle -Q_{j-1}, P_j, Q_j\rangle$ appartenant au cycle de f.

Les points de suspension ci-dessus cachent une longue preuve que nous ne reproduisons pas ici. Ce sont de belles propriétés des fractions continues qui interviennent. Par exemple, si g est réduite, alors $\Omega = \Omega(g)$ est un nombre réduit et pour toute matrice unimodulaire

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z}),$$

le nombre algébrique défini par

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \Omega = \frac{r\Omega+s}{t\Omega+u}$$

est aussi un nombre quadratique réduit, qui d'une part se retrouve dans le développement en fraction continue de Ω, et qui d'autre part s'avère relié à une forme quadratique réduite que l'on peut écrire explicitement. ▪

Exercice 4.1. Ecrivez toutes les formes quadratiques de discriminant $\Delta = 120$.

5. Groupe de classes de formes quadratiques

Tout au long de cette section, le discriminant Δ d'une forme quadratique est positif ou négatif. Nous avons l'identité suivante:

$$(a_1X_1^2+bX_1Y_1+ca_2Y_1^2)(a_2X_2^2+bX_2Y_2+ca_1Y_2^2) \\ = a_1a_2X^2+bXY+cY^2$$

où

$$\begin{cases} X &= X_1X_2-cY_1Y_2, \\ Y &= a_1X_1Y_2+a_2Y_1X_2+bY_1Y_2. \end{cases}$$

Ceci veut dire que si

$$f_1=\langle a,b,ca'\rangle\,,\quad f_2=\langle a',b,ca\rangle\,,\quad F=\langle aa',b,c\rangle\,,$$

alors

$$f_1(X_1,Y_1)f_2(X_2,Y_2)=F(X,Y).$$

Définition. Deux formes quadratiques $f_1=\langle a_1,b_1,c_1\rangle$ et $f_2=\langle a_2,b_2,c_2\rangle$ de discriminant Δ sont dites *concordantes* si

$$a_1a_2\neq 0,\quad b_1=b_2,\quad a_1|c_2\quad\text{et}\quad a_2|c_1.$$

En d'autres mots, les formes quadratiques $f_1=\langle a_1,b,a_2c\rangle$ et $f_2=\langle a_2,b,a_1c\rangle$ de discriminant Δ avec $a_1a_2\neq 0$ sont dites *concordantes*.

Expliquons pourquoi la deuxième définition est équivalente à la première. Soit $f_1=\langle a_1,b,c_1\rangle$ et $f_2=\langle a_2,b,c_2\rangle$

deux formes quadratiques *concordantes* de discriminant Δ. Comme $a_1|c_2$ et $a_2|c_1$, il existe deux entiers c et r tels que $c_2=a_1c$ et $c_1=a_2r$. Or

$$\Delta=b^2-4a_1c_1=b^2-4a_2c_2,$$

i.e., $a_1c_1=a_2c_2$. Donc $a_1(a_2r)=a_2(a_1c)$, *i.e.*, $r=c$. D'où $c_2=a_1c$ et $c_1=a_2c$.

On constate donc que deux formes concordantes ont même discriminant Δ .

Définition. L'opération $*$ sur deux formes concordantes f_1 et f_2 est définie par

$$f_1*f_2=\langle a_1,b,a_2c\rangle*\langle a_2,b,a_1c\rangle=\langle a_1a_2,b,c\rangle=F$$

et se lit la "*composition des formes f_1 et f_2 est la forme F*" décrite ci-dessus.

On peut en pratique omettre les troisièmes entrées des deux formes concordantes et écrire

$$\langle a_1,b,\star\rangle*\langle a_2,b,\star\rangle=\langle a_1a_2,b,\star\rangle\,.$$

On peut aussi remarquer que

$$\begin{aligned}\langle a_1,b,\star\rangle*\langle a_2,b,\star\rangle &= \langle a_1a_2,b,\star\rangle \\ &= \langle a_2a_1,b,\star\rangle \\ &= \langle a_2,b,\star\rangle*\langle a_1,b,\star\rangle\,.\end{aligned}$$

Définition. Supposons que $[f]$ veut dire la classe d'équivalence au sens strict de f. Alors nous définissons

une loi de composition $*$ sur les classes de f_1 et f_2 par

$$[f_1]*[f_2]=[F],$$

qui se lit de la façon suivante: "*la composition de la classe de la forme f_1 et de la classe de la forme f_2 est la classe de la forme F*" décrite ci-dessus.

Nous nous proposons de montrer que cela induit une loi de composition sur les classes d'équivalence au sens strict de formes quadratiques de discriminant Δ.

Théorème 5.1. *L'ensemble des classes d'équivalence au sens strict de formes quadratiques primitives de discriminant $\Delta\neq 0$ forme un groupe abélien. La loi de groupe $*$ est telle que si les formes de $\mathcal{C}_1$ et $\mathcal{C}_2$ représentent respectivement m_1 et m_2, alors les formes de $\mathcal{C}_1*\mathcal{C}_2$ représentent m_1m_2.*

Quelques lemmes préparatoires sont nécessaires.

Proposition 5.2. *Si les formes concordantes f_1 et f_2 représentent respectivement m_1 et m_2, alors f_1*f_2 représente m_1m_2.*

Démonstration. C'est évident d'après la formule du début de la section. ∎

Lemme 5.3. *Soit $f=\langle a,b,c\rangle$, une forme quadratique primitive et soit M, un entier différent de zéro. Alors il existe un entier $\neq 0$ relativement premier à M tel que f le représente.*

Démonstration. Rappelons que par convention, un produit vide est égal à 1. Ecrivons M comme

$$M=\pm\left(\prod_i p_i\right)\left(\prod_j q_j\right)\left(\prod_k \ell_k\right),$$

où p_i,q_j,ℓ_k sont des nombres premiers divisant M et tels que p_i divise a et ne divise pas c, q_j divise à la fois a et c, et ℓ_k ne divise pas a. Soit

$$r=\prod_i p_i\quad et\quad t=\prod_k \ell_k.$$

En utilisant le fait que q_j ne divise pas b (car f est primitive), il s'ensuit que

$$\text{PGCD}(f(r,t),M)=\text{PGCD}(ar^2+brt+ct^2,M)=1.\ \blacksquare$$

Lemme 5.4. *Soit $\mathcal{C}_1$, $\mathcal{C}_2$ et $\mathcal{C}_3$ trois classes d'équivalences au sens strict de formes primitives de discriminant $\Delta\neq 0$. Soit $M\neq 0\in\mathbb{Z}$.*

(1) *Alors il existe une paire de formes concordantes $f_1=\langle a_1,B,\star\rangle\in\mathcal{C}_1$ et $f_2=\langle a_2,B,\star\rangle\in\mathcal{C}_2$ telles que* $\text{PGCD}(a_1,a_2)=1$ *et* $\text{PGCD}(a_1a_2,M)=1$.

(2) *Il existe aussi un ensemble de trois formes quadratiques données par*

$$f_i=\langle a_i,B,\star\rangle\in\mathcal{C}_i\quad(i=1,2,3)$$

vérifiant

$$\text{PGCD}(a_1,a_2)=1,\ \text{PGCD}(a_1,a_3)=1,\ \text{PGCD}(a_2,a_3)=1,$$

et telles que n'importe quelle paire d'entre elles sont concordantes.

DÉMONSTRATION. **(1)** Pour commencer, expliquons pourquoi on peut choisir une forme $F_1 = \langle a_1, b_1, \star\rangle \in \mathcal{C}_1$ telle que $a_1 \neq 0$ et $\text{PGCD}(a_1, M) = 1$. Pour ce faire, prenons d'abord une forme f quelconque dans la classe $\mathcal{C}_1$. Soit r, t, une paire d'entiers relativement premiers tels que

$$a_1 = f(r,t) \neq 0 \quad \text{et} \quad \text{PGCD}(a_1, M) = 1.$$

La paire r, t peut être choisie, par exemple, comme dans la preuve du lemme précédent. Soit $s, u \in \mathbb{Z}$ tels que selon le lemme de Bezout $ur - st = 1$, de sorte que

$$A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Alors la forme $F_1 = Af = \langle a_1, b_1, \star\rangle$ est telle que nous le désirons.

De façon similaire, choisissons la forme quadratique $F_2 = \langle a_2, b_2, \star\rangle \in \mathcal{C}_2$ de façon à ce que

$$a_2 \neq 0 \quad \text{et} \quad \text{PGCD}(a_2, a_1 M) = 1.$$

Ensuite, prenons des entiers n_1, n_2 tels que

$$b_1 + 2a_1 n_1 = b_2 + 2a_2 n_2.$$

Cette équation peut être écrite comme

$$a_1 n_1 - a_2 n_2 = \frac{b_2 - b_1}{2}.$$

Des solutions n_1 et n_2 existent parce que d'une part

$$b_1 \equiv \Delta \equiv b_2 \pmod 2,$$

et parce que d'autre part $\text{PGCD}(a_1, a_2) = 1$. Il est alors clair que les formes

$$f_1 = \begin{pmatrix} 1 & n_1 \\ 0 & 1 \end{pmatrix} F_1 = \langle a_1, b, \star\rangle$$

et

$$f_2 = \begin{pmatrix} 1 & n_2 \\ 0 & 1 \end{pmatrix} F_2 = \langle a_2, b, \star\rangle$$

avec $b = b_1 + 2a_1 n_1 = b_2 + 2a_2 n_2$ sont concordantes, tel que demandé dans l'énoncé du lemme, parce que

$$b^2 - 4a_1 c_1 = b^2 - 4a_2 c_2$$

entraîne $a_1 c_1 = a_2 c_2$, de sorte que $a_1 | c_2$ et $a_2 | c_1$ vu que $\text{PGCD}(a_1, a_2) = 1$.

(2) En procédant comme dans la démonstration de la partie (1), nous savons qu'il existe une forme $g_1 \in \mathcal{C}_1$ avec $a_1 \neq 0$, une forme $g_2 \in \mathcal{C}_2$ telle que $a_2 \neq 0$ et $\text{PGCD}(a_2, a_1) = 1$, et une forme $g_3 \in \mathcal{C}_3$ telle que $a_3 \neq 0$ et $\text{PGCD}(a_3, a_1 a_2) = 1$. Nous avons donc que les entiers a_1, a_2, a_3 sont copremiers deux à deux, de sorte qu'il existe des entiers m_1, m_2, m_3 pour lesquels nous avons l'égalité de Bezout

$$m_1 a_1 + m_2 a_2 + m_3 a_3 = 1. \tag{5.2}$$

Nous pouvons supposer que m_1 est pair. En effet, supposons que m_1 est impair. Vu que $\text{PGCD}(a_2, a_3) = 1$, il

existe $r_2, r_3 \in \mathbb{Z}$ tels que $r_2 a_2 + r_3 a_3 = 1$, de sorte que

$$a_1 r_2 a_2 + a_1 r_3 a_3 = a_1.$$

Donc l'équation (5.1) s'écrit

$$(m_1 - 1)a_1 + (m_2 + a_1 r_2)a_2 + (m_3 + a_1 r_3)a_3 = 1. \tag{5.3}$$

avec $m_1 - 1$ pair.

Montrons qu'il existe des entiers n_1, n_2, n_3 tels que

$$b_1 + 2a_1 n_1 \;=\; b_1 + 2a_1 n_1 \;=\; b_1 + 2a_1 n_1 \;=\; B, \tag{5.4}$$

disons. Nous voulons donc exhiber des entiers n_1, n_2, n_3 qui vérifient

$$\begin{cases} n_1 a_1 - n_2 a_2 \;=\; \frac{1}{2}(b_2 - b_1), \\ n_1 a_1 - n_3 a_3 \;=\; \frac{1}{2}(b_3 - b_1), \end{cases}$$

où $\frac{1}{2}(b_2 - b_1)$ et $\frac{1}{2}(b_3 - b_1)$ sont des entiers vu que pour $i = 1, 2, 3$, $b_i \equiv \Delta \pmod 2$. Additionnant ces deux équations, nous obtenons

$$2n_1 a_1 - n_2 a_2 - n_3 a_3 \;=\; u \tag{5.5}$$

avec $u = \frac{1}{2}(b_2 + b_3) - b_1$, où u est un entier.

Multiplions chaque membre de l'équation (5.1) par u pour obtenir

$$m_1 u_1 a_1 + m_2 u_1 a_2 + m_3 u_1 a_3 = u. \tag{5.6}$$

Nous concluons alors qu'avec

$$n_1 = \frac{1}{2} u m_1, \quad n_2 = -u m_2 \quad n_3 = -u m_3,$$

les égalités (5.3) et (5.4) sont vérifiées.

Considérons maintenant les formes

$$f_i \;=\; \begin{pmatrix} 1 & n_i \\ 0 & 1 \end{pmatrix} g_i \;=\; \langle a_i, B, \star\rangle \qquad (i = 1, 2, 3).$$

Elles vérifient la propriété (5.3) et chaque paire de formes parmi ces trois formes est un ensemble de formes concordantes.

Proposition 5.5. *Soit $\mathcal{C}_1$ et $\mathcal{C}_2$, deux classes d'équivalence au sens strict de formes primitives de discriminant $\Delta \neq 0$. Soit $f_1 \in \mathcal{C}_1$ et $f_2 \in \mathcal{C}_2$, une paire de formes concordantes. Soit $g_1 \in \mathcal{C}_1$ et $g_2 \in \mathcal{C}_2$, une autre paire de formes concordantes. Alors $f_1 * f_2$ est strictement équivalente à $g_1 * g_2$.*

DÉMONSTRATION. Commençons par écrire les formes considérées:

$$\begin{cases} f_1 = \langle a_1, b, a_2 c\rangle\,, \quad f_2 = \langle a_2, b, a_1 c\rangle\,, \\ g_1 = \langle a_1', b', a_2' c'\rangle\,, \quad g_2 = \langle a_2', b', a_1' c'\rangle\,. \end{cases}$$

La preuve s'effectuera en quatre étapes.

(1) Soit $f_1 = g_1$ et $\text{PGCD}(a_1, a_2') = 1$. Donc $a_1 = a_1'$, $b = b'$. Alors f_1 est concordante avec f_2 et g_2, et nous devons prouver que $f_1 * f_2 \sim f_1 * g_2$. Soit

$$B = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$$

telle que $Bf_2 = g_2$. Nous avons alors les égalités suivantes (où $b = b'$):

$$\begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} a_2 & \frac{1}{2}b \\ \frac{1}{2}b & a_1c \end{pmatrix} = \begin{pmatrix} a_2' & \frac{1}{2}b \\ \frac{1}{2}b & a_1'c' \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1}$$
$$= \begin{pmatrix} a_2' & \frac{1}{2}b \\ \frac{1}{2}b & a_1'c' \end{pmatrix}\begin{pmatrix} u & -s \\ -t & r \end{pmatrix}.$$

En comparant les éléments $(1,2)$ de ces produits de matrices, nous obtenons $ta_1c = -a_2's$. Comme $\text{PGCD}(a_1, a_2') = 1$, nous en déduisons $a_1|s$. Donc

$$B' = \begin{pmatrix} r & s/a_1 \\ ta_1 & u \end{pmatrix} \in SL_2(\mathbb{Z}).$$

La première étape est donc complétée si nous pouvons montrer que $B'(f_1 * f_2) = f_1 * g_2$.

Soit

$$F = f_1 * f_2 = \langle a_1a_2, b, c\rangle$$

et posons

$$H = \begin{pmatrix} r & s/a_1 \\ ta_1 & u \end{pmatrix} F = \langle h_1, h_2, h_3\rangle.$$

Nous voulons prouver que $H = f_1 * g_2$. Calculons h_1 et h_3. D'une part,

$$\begin{aligned} h_1 &= F(r, ta_1) = a_1a_2r^2 + brta_1 + ct^2a_1^2 \\ &= a_1\left(a_2r^2 + brt + ca_1t^2\right) = a_1f_2(r,t) \end{aligned}$$

$$\begin{aligned} &= a_1a' \quad (\text{car } Bf_2 = g_2) \\ &= a_1'a_2' \quad (\text{car } f_1 = f_1'). \end{aligned}$$

D'autre part,

$$\begin{aligned} h_3 &= F(s/a_1, u) = a_1a_2\frac{s^2}{a_1^2} + b\frac{s}{a_1}u + cu^2 \\ &= \frac{1}{a_1}\left(a_2s^2 + bsu + a_1cu^2\right) = \frac{1}{a_1}f_2(s,u) \\ &= \frac{1}{a_1}(a_1'c') \quad (\text{car } Bf_2 = g_2) \\ &= \frac{1}{a_1'}(a_1'c') \quad (\text{car } a_1 = a_1') \\ &= c'. \end{aligned}$$

Donc

$$H = \langle h_1, h_2, h_3\rangle = \langle a_1'a_2', \star, c'\rangle = g_1 * g_2 = f_1 * g_2.$$

(2) Soit $b = b'$ et $\text{PGCD}(a_1, a_2') = 1$. Par hypothèse, f_1 et f_2 sont concordantes. Montrons que f_1 et g_2 sont aussi concordantes; en effet,

$$\Delta = b^2 - 4a_1a_2c = b^2 - 4a_2'a_1'c',$$

i.e., $a_1a_2c = a_1'a_2'c'$; comme $\text{PGCD}(a_1, a_2') = 1$, nous concluons que $a_1|a_1'c'$ et $a_2'|a_2c$. D'après la partie (1), nous avons alors d'une part $f_1 * f_2 \sim f_1 * g_2$. Or nous avons aussi que g_2 et g_1 sont deux formes concordantes et que g_2 et f_1 sont aussi concordantes. Donc toujours d'après la

partie (1), nous avons $g_2 * g_1 \sim g_2 * f_1$. La transitivité de la relation d'équivalence stricte et la communtativité de $*$ nous donne alors que $f_1 * f_2 \sim g_1 * g_2$.

(3) Soit $\text{PGCD}(a_1a_2, a_1'a_2') = 1$. Soit $L, n, n' \in \mathbb{Z}$ tels que

$$b + 2a_1a_2n = b' + 2a_1'a_2'n' = L,$$

disons. Posons

$$\begin{cases} F_1 = \begin{pmatrix} 1 & a_2n \\ 0 & 1 \end{pmatrix} f_1 = \langle a_1, L, c_1\rangle \in \mathcal{C}_1, \\ F_2 = \begin{pmatrix} 1 & a_1n \\ 0 & 1 \end{pmatrix} f_2 = \langle a_2, L, c_2\rangle \in \mathcal{C}_2, \\ H_1 = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} (f_1 * f_2) = \langle a_1a_2, L, d\rangle, \end{cases}$$

sans qu'il soit nécessaire d'écrire explicitement les valeurs de c_1, c_2 et d. La valeur du discriminant Δ de F_1, F_2 et H_1 nous donne les égalités

$$a_1a_2d = a_1; \qquad c_1 = a_2c_2.$$

Ceci nous permet de dire que $a_1|a_2c_2$ et $a_2|a_1c_1$, et de conclure que F_1 et F_2 sont concordantes. Similairement, les formes

$$G_1 = \langle a_1', L, \star\rangle \in \mathcal{C}_1 \quad \text{et} \quad G_2 = \langle a_2', L, \star\rangle \in \mathcal{C}_2$$

sont concordantes et

$$H_2 = \langle a_1'a_2', L, \star\rangle \sim g_1 * g_2.$$

Dès lors, nous pouvons appliquer la deuxième étape aux quatre formes F_1, F_2, G_1, G_2, pour lesquelles nous avons en particulier $\text{PGCD}(a_1, a_2') = 1$, et conclure que nous avons $F_1 * F_2 \sim G_1 * G_2$. Nous déduisons donc que

$$f_1 * f_2 \sim H_1 = F_1 * F_2 \sim G_1 * G_2 = H_2 \sim g_1 * g_2.$$

(4) Cas général. Il existe des formes concordantes

$$F_1 = \langle A_1, B, \star\rangle \in \mathcal{C}_1 \quad \text{et} \quad F_2 = \langle A_2', B, \star\rangle \in \mathcal{C}_2$$

telles que $\text{PGCD}(A_1A_2, a_1a_2a_1'a_2') = 1$. Comme en particulier, nous avons $\text{PGCD}(A_1A_2, a_1a_2) = 1$, nous déduisons de l'étape précédente que $F_1 * F_2 \sim f_1 * f_2$. Comme on a aussi $\text{PGCD}(A_1A_2, a_1'a_2') = 1$, nous déduisons encore de l'étape précédente que $F_1 * F_2 \sim g_1 * g_2$. D'où, par transitivité, $f_1 * f_2 \sim g_1 * g_2$. Ceci termine la émonstration.

Théorème 5.6. *Soit Δ un discriminant différent de zéro. L'ensemble des classes d'équivalence au sens strict des formes quadratiques binaires primitives de discriminant Δ est un groupe abélien fini par rapport à la loi "composition des classes". L'élément neutre du groupe est la classe de la forme principale I. L'inverse dans le groupe de la classe d'une forme primitive f est la classe de toute forme improprement équivalente à f.*

DÉMONSTRATION. Grâce à la proposition 5.5, nous savons que la loi de composition $*$ est une fonction bien définie. Il y a 4 propriétés à démontrer.

(1) *Commutativité.* Cette partie est claire d'après la définition de la composition de deux formes concordantes.

(2) *Élément neutre.* Soit $\mathcal{C}$ une classe d'équivalence au sens strict et soit $\langle a, b, \star\rangle$ une forme appartenant à $\mathcal{C}$, où $a \neq 0$. Soit $\mathcal{C}_0$ la classe d'équivalence au sens strict de la forme principale f_0 (aussi notée I) définie par

$$f_0 = \begin{cases} \left\langle 1, 0, -\frac{1}{4}\Delta\right\rangle & \text{si } \Delta \equiv 0 \pmod 4, \\ \left\langle 1, 1, \frac{1}{4}(1-\Delta)\right\rangle & \text{si } \Delta \equiv 1 \pmod 4. \end{cases}$$

Or $\langle 1, b, \star\rangle$ et f_0 sont dans la même classe d'équivalence au sens strict puisque $b \equiv \Delta \pmod 2$ et

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} f_0 \;=\; \langle 1, b, \star\rangle \;\text{ pour } s = \begin{cases} b/2 & \text{si } 2|\Delta, \\ (b-1)/2 & \text{si } 2 \nmid \Delta. \end{cases}$$

Donc $f_0 \sim \langle 1, b, \star\rangle$. Par conséquent, $\mathcal{C}_0\mathcal{C}$ est la classe de $\langle 1, b, \star\rangle * \langle a, b, \star\rangle = \langle a, b, \star\rangle \in \mathcal{C}$, de sorte que $\mathcal{C}_0\mathcal{C} = \mathcal{C}$. Donc $\mathcal{C}_0$ est l'élément neutre de la composition des classes.

(3) *Inverses.* Soit $\mathcal{C}$ une classe de formes. En vertu du lemme 5.3, il existe une forme $\langle a, b, c\rangle \in \mathcal{C}$ telle que $a \neq 0$. On peut supposer que $c \neq 0$, car on n'aurait qu'à considérer

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \langle a, b, c\rangle$$

pour un n convenable. Toute forme improprement équivalente à une forme de $\mathcal{C}$ est proprement équivalente à

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \langle a, b, c\rangle \;=\; \langle c, b, a\rangle\,,$$

cette dernière forme étant concordante à gauche avec $\langle a, b, c\rangle$. Nous évaluons ensuite la composition pour constater que le résultat est dans la classe principale de f_0:

$$\langle a, b, c\rangle \;*\; \langle c, b, a\rangle \;=\; \langle ac, b, 1\rangle \;=\; \begin{pmatrix} r & -1 \\ 1 & 0 \end{pmatrix} f_0$$

avec

$$r = \begin{cases} -b/2 & \text{si } 2|\Delta, \\ -(b-1)/2 & \text{si } 2 \nmid \Delta. \end{cases}$$

Donc

$$[\langle a, b, c\rangle] * [\langle c, b, a\rangle] = [f_0],$$

de sorte que la classe de $\langle c, b, a\rangle$ est la classe inverse de la classe $\mathcal{C}$.

(4) *Associativité.* Soit $\mathcal{C}_1, \mathcal{C}_2$ et $\mathcal{C}_3$, trois classes quelconques. Nous voulons prouver

$$\mathcal{C}_1 * (\mathcal{C}_2 * \mathcal{C}_3) \;=\; (\mathcal{C}_1 * \mathcal{C}_2) * \mathcal{C}_3.$$

D'après la partie (2) du lemme 5.4, il existe des formes

$$\begin{cases} f_1 \;=\; \langle a_1, B, \star\rangle \in \mathcal{C}_1, \\ f_2 \;=\; \langle a_2, B, \star\rangle \in \mathcal{C}_2, \\ f_3 \;=\; \langle a_3, B, \star\rangle \in \mathcal{C}_3 \end{cases}$$

telles que n'importe quelle paire d'entre elles sont concordantes. Alors nous pouvons calculer

$$\begin{aligned} (f_1 * f_2) * f_3 \;&=\; \langle a_1a_2, B, \star\rangle * \langle a_3, B, \star\rangle \\ &=\; \langle a_1a_2a_3, B, \star\rangle \\ &=\; f_1 * (f_2 * f_3). \end{aligned}$$

Donc la composition des classes est associative. ∎

Il existe une autre loi de composition des classes qui génère une structure de groupe et qui a été définie par Dirichlet. Elle a l'avantage d'être facile à programmer. Dirichlet a introduit la notion de *formes unies*. Cela a permis à D. Shanks d'exhiber une méthode pour trouver $f_1 * f_2$ lorsque f_1 et f_2 sont unies.

Proposition 5.9 (Dirichlet)**.** *Soit $f = \langle a, b, c\rangle$ et $f' = \langle a', b', c'\rangle$ deux formes primitives de discriminant $\Delta \neq 0$. Soit*

$$d = \text{PGCD}\left(a, a', \frac{b+b'}{2}\right) \;=\; au + a'v + \frac{b+b'}{2}w$$

pour des entiers $u, v, w \in \mathbb{Z}$ (non nécessairement uniques). Alors

$$f * f' \;=\; \langle A, B, C\rangle$$

où

$$A = \frac{aa'}{d^2},\; B = \frac{1}{d}\left(aub' + a'vb + \frac{bb'+\Delta}{2}w\right),\; C = \frac{B^2-\Delta}{4A}.$$

Démonstration. Pour les grandes lignes, se référer au volume de Buell. ∎

Exemple. Soit $\Delta = -264 = -4 \cdot 66$, où $-66 \equiv 2 \pmod 4$, de sorte que Δ est un discriminant fondamental. Nous avons

$$\begin{cases} I = \langle 1, 0, 66\rangle\,, & Q_1 = \langle 2, 0, 33\rangle\,, \\ Q_2 = \langle 3, 0, 22\rangle\,, & Q_3 = \langle 6, 0, 11\rangle\,, \\ Q_4 = \langle 5, 4, 14\rangle\,, & Q_5 = \langle 5, -4, 14\rangle\,, \\ Q_6 = \langle 7, 4, 10\rangle\,, & Q_7 = \langle 7, -4, 10\rangle\,. \end{cases}$$

Soit $\mathcal{I}$ la classe d'équivalence au sens strict de la forme principale I, et soit $\mathcal{C}_i$ la classe d'équivalence de Q_i (où $1 \leq i \leq 7$). Nous voulons démontrer que nous avons alors le tableau suivant, où $\mathcal{I}$ est l'élément neutre du groupe des classes, et où la loi de composition $*$ est commutative:

$*$	$\mathcal{I}$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$
$\mathcal{I}$	$\mathcal{I}$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$
$\mathcal{C}_1$	$\mathcal{C}_1$	$\mathcal{I}$	$\mathcal{C}_3$	$\mathcal{C}_2$	$\mathcal{C}_7$	$\mathcal{C}_6$	$\mathcal{C}_5$	$\mathcal{C}_4$
$\mathcal{C}_2$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{I}$	$\mathcal{C}_1$	$\mathcal{C}_5$	$\mathcal{C}_4$	$\mathcal{C}_7$	$\mathcal{C}_6$
$\mathcal{C}_3$	$\mathcal{C}_3$	$\mathcal{C}_2$	$\mathcal{C}_1$	$\mathcal{I}$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_4$	$\mathcal{C}_5$
$\mathcal{C}_4$	$\mathcal{C}_4$	$\mathcal{C}_7$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_2$	$\mathcal{I}$	$\mathcal{C}_1$	$\mathcal{C}_3$
$\mathcal{C}_5$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_4$	$\mathcal{C}_7$	$\mathcal{I}$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_1$
$\mathcal{C}_6$	$\mathcal{C}_6$	$\mathcal{C}_5$	$\mathcal{C}_7$	$\mathcal{C}_4$	$\mathcal{C}_1$	$\mathcal{C}_3$	$\mathcal{C}_2$	$\mathcal{I}$
$\mathcal{C}_7$	$\mathcal{C}_7$	$\mathcal{C}_4$	$\mathcal{C}_6$	$\mathcal{C}_5$	$\mathcal{C}_3$	$\mathcal{C}_1$	$\mathcal{I}$	$\mathcal{C}_2$

Calculons $\mathcal{C}_1 * \mathcal{C}_1$. Nous cherchons donc $\langle 2, 0, 33\rangle * \langle 2, 0, 33\rangle$. Ici

$$\delta = \text{PGCD}(2, 2, 0) = 2 = 1 \cdot 2 + 0 \cdot 2 + 0 \cdot 0.$$

Prenons alors $u = 1, v = 0, w = 0$. D'où

$$A = 1, B = 0, C = 66.$$

Donc

$$\langle 2, 0, 33\rangle * \langle 2, 0, 33\rangle = \langle 1, 0, 66\rangle = I,$$

c'est-à-dire $\mathcal{C}_1 * \mathcal{C}_1 = \mathcal{I}$.

Calculons $\mathcal{C}_4 * \mathcal{C}_4$. Nous cherchons donc la valeur de $\langle 5, 4, 14\rangle * \langle 5, 4, 14\rangle$. Ici

$$\delta = \text{PGCD}(5, 5, 4) = 1 = 1 \cdot 5 + 0 \cdot 5 - 1 \cdot 4.$$

Prenons alors $u = 1, v = 0, w = -1$. D'où

$$A = 25, B = 144, C = 210.$$

Or

$$\begin{aligned}
&\langle 25, 144, 210\rangle \\
&\sim \langle 210, -144, 25\rangle \quad \text{où} \quad 144 + b' \equiv 0 \pmod{420} \\
&\sim \langle 25, -6, 3\rangle \qquad \text{où} \quad -144 + b' \equiv 0 \pmod{50} \\
&\sim \langle 3, 0, 22\rangle = Q_2 \quad \text{où} \quad -6 + b' \equiv 0 \pmod{6}.
\end{aligned}$$

Donc $\mathcal{C}_4 * \mathcal{C}_4 = \mathcal{C}_2$.

Calculons $\mathcal{C}_2 * \mathcal{C}_5$. Nous cherchons donc la valeur de $\langle 3, 0, 22\rangle * \langle 5, -4, 14\rangle$. Or

$$\delta = \text{PGCD}(3, 5, -2) = 1 = 2 \cdot 3 - 1 \cdot 5 + 0 \cdot 2.$$

Prenons alors $u = 2, v = -1, w = 0$. D'où

$$A = 15, B = -24, C = 14.$$

Or

$$\langle 15, -24, 14\rangle \sim \langle 14, -4, 5\rangle \sim \langle 5, 4, 14\rangle.$$

Donc $\mathcal{C}_2 * \mathcal{C}_5 = \mathcal{C}_4$.

Les autres calculs se font de façon semblable.

Concentrons-nous maintenant sur la structure de ce groupe d'ordre 8, en nous rappelant qu'il y a exactement 5 groupes d'ordre 8.

– Est-ce $\mathbb{Z}/8\mathbb{Z}$? Non, car il n'y a aucun élément d'ordre 8.

– Est-ce $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? Non, car $\mathcal{C}_4$ est d'ordre 4.

– Est-ce le groupe diédral D_8? Non, car D_8 n'est pas abélien.

– Est-ce le groupe des quaternions Q_8? Non, car Q_8 n'est pas abélien.

– Est-ce $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$? Oui, et c'est le seul choix qu'il nous restait, vu qu'à isomorphisme près il n'y a que 5 groupes possibles d'ordre 8. Remarquons que concrètement

$$\langle \mathcal{C}_1\rangle \times \langle \mathcal{C}_4\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Exercice 5.1 Dans le dernier exemple, vérifiez d'autres valeurs de la table de composition.

6. Conclusion.

Il y a d'autres propriétés à étudier comme la représentation d'un entier par une forme quadratique, le genre des formes quadratiques, les formes ambigues, la factorisation d'un entier via les formes quadratiques, les cryptosystèmes via un groupe de classes.

Nous voulons terminer en mentionnant que l'arithmétique des formes quadratiques en propriétés pour les idéaux de l'anneau des entiers algébriques d'un corps de nombres algébriques. Cette transformation se fait en associant à la forme quadratique de discriminant $\Delta = b^2 - 4ac$ l'idéal J de $\mathbb{Q}(\sqrt{\Delta})$ engendré par a et $\frac{b+\sqrt{\Delta}}{2}$:

$$\langle a, b, c\rangle \longmapsto \left[a, \frac{b + \sqrt{\Delta}}{2}\right].$$

Addendum: Solutions

Exercice 1.1. Prouvez que $\approx$ et $\sim$ sont des relations d'équivalence.

Solution. En effet, ces relations sont réflexives, symétriques et transitives.

Exercice 1.2. Prouvez que deux formes quadratiques équivalentes (au sens strict ou au sens large) ont forcément le même discriminant.

Solution. Soit $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$ et soit

$$f = \langle a, b, c\rangle \quad \text{et} \quad g = \langle a', b', c'\rangle$$

deux formes quadratiques telles que $g = Af$. En utilisant les formules (1.1), nous trouvons que

$$\Delta_g = (rs - tu)^2(b^2 - 4ac) = 1 \cdot \Delta_f = \Delta_f.$$

Exercice 1.3. Exhibez deux formes quadratiques vérifiant à la fois la propriété "f est *proprement équivalente à* g"et la propriété "f *est improprement équivalente à* g".

Solution. Considérons $f = \langle a, 0, c\rangle$ et $g = \langle c, 0, a\rangle$. Nous avons

$$g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} f \qquad \text{et} \qquad g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} f.$$

Exercice 1.4. Supposons que

$$f = \langle a, b, c\rangle = aX^2 + bXY + cY^2$$

et qu'il existe des entiers r et t copremiers entre eux pour lesquels nous avons $k = f(r,t)$. Prouvez qu'il existe des entiers b', c' tels que $f \sim \langle k, b', c' \rangle$.

SOLUTION. Supposons que s et u sont des entiers pour lesquels $ru - st = 1$. Alors il existe des entiers b', c' pour lesquels

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} f \;=\; \langle k, b', c' \rangle\,, \quad \text{c'est-à-dire,} \quad f \sim \langle k, b', c' \rangle\,.$$

Exercice 2.1. Vérifierz que $\langle a, b, a \rangle \sim \langle a, -b, a \rangle$ et que $\langle a, a, c \rangle \sim \langle a, -a, c \rangle$.

SOLUTION. D'une part,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \langle a, b, a \rangle \;=\; \langle a, -b, a \rangle.$$

D'autre part,

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \langle a, a, c \rangle \;=\; \langle a, -a, c \rangle.$$

Exercice 2.2. Trouvez les valeurs des nombres de classes h et h^+ lorsque $\Delta = -15$.

SOLUTION. Appliquez l'algorithme.

Exercice 2.3. Soit $f(X,Y) = aX^2 + bXY + cY^2$ une forme quadratique définie positive avec $|b| \leq a \leq c$, et soit v un entier de $\{1, 2, \ldots, a\}$. Prouvez que si $v \in \{1, 2, \ldots, a-1\}$, alors $f(X,Y) = v$ n'a pas de solution

entière. De plus, prouvez que les solutions possibles (r,t) de $f(X,Y) = a$ sont données par

$$(r,t) \;=\; \begin{cases} (1,0),\ (-1,0), & \\ (0,1),\ (0,-1) & \text{lorsque } c = a, \\ (1,-1),\ (-1,1) & \text{lorsque } c = b = a > 0, \\ (1,1),\ (-1,-1) & \text{lorsque } c = -b = a > 0. \end{cases}$$

Concluez que a est le plus petit entier positif représenté par la forme quadratique $aX^2 + bXY + cY^2$.

SOLUTION. Nous avons l'égalité

$$f(X,Y) = a\left(X + \frac{b}{2a}Y\right)^2 + \frac{|\Delta|}{4a}Y^2.$$

Soit (r,t) une solution vérifiant $f(r,t) \leq a$. Alors nous avons l'inégalité $\dfrac{|\Delta|}{4a}t^2 \leq a$, de sorte que $t^2 \leq \dfrac{4}{|\Delta|}a^2$. De plus, d'après la proposition 2.2(ii), $a \leq \sqrt{|\Delta|/3}$. D'où

$$t^2 \leq \frac{4}{|\Delta|}\frac{|\Delta|}{3} = \frac{4}{3}.$$

Donc $t \in \{0, 1, -1\}$. Si $t = 0$, alors nous avons $r = \pm 1$ et $F(\pm 1, 0) = a$.

Soit $t = \pm 1$. Alors nous déduisons que $ar^2 \pm br + c \leq a$. Comme $|b| \leq a$, nous avons $ar^2 \pm br \geq 0$. L'hypothèse $a \leq c$ force donc $a = c$. Il faut alors résoudre

$$ar^2 \pm br = (ar \pm b)r = 0.$$

Si $r = 0$, alors $(r,t) = (0,1)$ ou $(0,-1)$. Si $ar + b = 0$, alors $r = -b/a$. Or $|b| \leq a$. Donc $|b| = a$. Si $b = a$, alors $(r,t) = (-1,1)$. Si $b = -a$, alors $(r,t) = (1,-1)$. Ceci termine la solution de l'exercice et on a vu au passage que $f(X,Y) < a$ n'a pas de solution.

Exercice 4.1. Ecrivez toutes les formes quadratiques de discriminant $\Delta = 120$. Donnez la valeur du nombre de classes au sens restreint. Donnez la valeur du nombre de classes au sens restreint.

Solution. On trouve un premier cycle de formes quadratiques réduites formé par

$$\langle 7, 8, -2 \rangle, \langle -2, 8, 7 \rangle, \langle 7, 6, -3 \rangle, \langle -3, 6, 7 \rangle,$$

puis un autre donné par

$$\langle -7, 8, 2 \rangle, \langle 2, 8, -7 \rangle, \langle -7, 6, 3 \rangle, \langle 3, 6, -7 \rangle.$$

On a aussi le cycle formé par

$$\langle 1, 10, -5 \rangle, \langle -5, 10, 1 \rangle,$$

puis un autre donné par

$$\langle -1, 10, 5 \rangle, \langle 5, 10, -1 \rangle.$$

Donc le nombre de classes h_{120} vaut 4.

Exercice 5.1 Dans le dernier exemple, vérifiez d'autres valeurs de la table de composition.

Bibliographie

D.A. Buell, *Binary quadratic forms, Classical theory and modern computations*, Springer-Verlag, 1984, x+247 pages.

A. Faisant, *L'équation diophantienne du second degré*, Hermann, 1991, vi+238 pages.

D. Flath, *Introduction to number theory*, J.Wiley, 1989, xii+212 pages.

G.L. Watson, *Integral quadratic forms*, Cambridge Tracts in Math. Phys. **57**, Cambridge U. Press, 1960, 6543 pages.

R. Mollin, *Quadratics*, CRC, 1996, xx+387 pages.