Formes quadratiques (Leçon 1)

Jorge Jiménez Urroz
(Universitat Politècnica de Catalunya)

Cimpa École, Bamako, Novembre 2010

Préliminaires

Définition

Une forme quadratique *est une fonction polynomiale homogène du second degré à coefficients dans* $\mathbb{Z}$*,*

$$f(x, y) = ax^2 + bxy + cy^2, \qquad a, b, c \in \mathbb{Z},$$

qui sera notée $f = \langle a, b, c \rangle$.

Préliminaires

Définition

Une forme quadratique *est une fonction polynomiale homogène du second degré à coefficients dans* $\mathbb{Z}$,

$$f(x, y) = ax^2 + bxy + cy^2, \qquad a, b, c \in \mathbb{Z},$$

qui sera notée $f = \langle a, b, c \rangle$.

Question: Quels sont les entiers que f représente?

- $f(x, y) = 2x^2 - 6xy + 2y^2 = \langle 2, -6, 2 \rangle$.

- $f(x, y) = 2x^2 - 6xy + 2y^2 = \langle 2, -6, 2 \rangle$.

Définition

La forme $\langle a, b, c \rangle$ *est dite* primitive *si* $pgcd(a, b, c) = 1$

- $f(x, y) = 2x^2 - 6xy + 2y^2 = \langle 2, -6, 2\rangle$.

Définition

La forme $\langle a, b, c\rangle$ *est dite* primitive *si* $pgcd(a, b, c) = 1$

- $f(x, y) = x^2 + y^2 = \langle 1, 0, 1\rangle)$ ne représente eaucun entier négatif.

- $f(x,y) = 2x^2 - 6xy + 2y^2 = \langle 2, -6, 2 \rangle$.

Définition

La forme $\langle a, b, c \rangle$ *est dite* primitive *si* $pgcd(a, b, c) = 1$

- $f(x,y) = x^2 + y^2 = \langle 1, 0, 1 \rangle)$ ne représente eaucun entier négatif.

Définition

La forme $\langle a, b, c \rangle$ *est dite* définie *si* $\Delta = b^2 - 4ac < 0$ *avec* $a > 0$ *(et* $c > 0$*). Elle est dite* indéfinie *si* $\Delta > 0$.

$$4af(x,y) = 4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - \Delta y^2.$$

- $f_1(x, y) = x^2 + 3y^2$ ne représente pas l'entier 2.

- $f_1(x, y) = x^2 + 3y^2$ ne représente pas l'entier 2.
- $f_2(x, y) = 4x^2 + 14xy + 13y^2$, non plus.

- $f_1(x, y) = x^2 + 3y^2$ ne représente pas l'entier 2.

- $f_2(x, y) = 4x^2 + 14xy + 13y^2$, non plus.

Si on fait le changement de variables $x = 2x' - y'$, $y = -x' + y'$, nous avons $f_2(x, y) = f_1(x', y')$, et f et f' représentent le même ensemble d'entiers.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ et } \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

- $f_1(x,y) = x^2 + 3y^2$ ne représente pas l'entier 2.

- $f_2(x,y) = 4x^2 + 14xy + 13y^2$, non plus.

Si on fait le changement de variables $x = 2x' - y'$, $y = -x' + y'$, nous avons $f_2(x,y) = f_1(x',y')$, et f et f' représentent le même ensemble d'entiers.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ et } \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Nous voulons faire un changement de variables pour trouver la forme la plus facile possible pour les calculs. Ce changement de variables doit impliquer une matrice inversible. Posons

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} : \alpha\delta - \beta\gamma = \pm 1 \right\},$$

et

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} : \alpha\delta - \beta\gamma = 1 \right\}.$$

Définition

A chaque forme $f = \langle a, b, c \rangle$, *on associe la matrice*

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Définition

A chaque forme $f = \langle a, b, c\rangle$, on associe la matrice

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Alors on a

$$f(x, y) = (x, y) M_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

Observation: $\Delta = -4\det(M_f)$.

Définition

A chaque forme $f = \langle a, b, c \rangle$*, on associe la matrice*

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Alors on a

$$f(x,y) = (x,y) M_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

Observation: $\Delta = -4\det(M_f)$.

Chaque $A \in \mathrm{GL}_2(\mathbb{Z})$ agit sur f et donne une autre forme f' dont la matrice associée est

$$M_{f'} = A M_f A^t.$$

Définition

A chaque forme $f = \langle a, b, c\rangle$*, on associe la matrice*

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Alors on a

$$f(x, y) = (x, y)M_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

Observation: $\Delta = -4\det(M_f)$.

Chaque $A \in \mathrm{GL}_2(\mathbb{Z})$ agit sur f et donne une autre forme f' dont la matrice associée est

$$M_{f'} = AM_fA^t.$$

En particulier, $\Delta_f = \Delta_{f'}$.

Définition

Etant donné un discriminant Δ, nous appelons $\mathcal{F}_\Delta$ l'ensemble des formes quadratiques de discriminant Δ.

Observation Tout entier $\Delta \equiv 0, 1 \pmod 4$ est discriminant d'une forme quadratique.

Définition

Etant donné un discriminant Δ, nous appelons $\mathcal{F}_\Delta$ l'ensemble des formes quadratiques de discriminant Δ.

Observation Tout entier $\Delta \equiv 0, 1 \pmod 4$ est discriminant d'une forme quadratique.

Définition

Etant donné un discriminant Δ, la forme quadratique principale I de discriminant Δ est

$$I = \begin{cases} \langle 1, 0, -\Delta/4 \rangle & \textit{si } \Delta \equiv 0 \pmod 4, \\ \langle 1, 1, (1-\Delta)/4 \rangle & \textit{si } \Delta \equiv 1 \pmod 4. \end{cases}$$

Définition

Un entier Δ est un $\text{discriminant fondamental}$ *s'il est discriminant d'une forme quadratique primitive et seulement de formes quadratiques primitives.*

Il y a deux possibilités:

- $\Delta \equiv 1 \pmod 4$ avec Δ sans facteur carré,
- $\Delta/4 \equiv 2, 3 \pmod 4$ avec $\Delta/4$ sans facteur carré.

Définition

Un entier Δ est un discriminant fondamental *s'il est discriminant d'une forme quadratique primitive et seulement de formes quadratiques primitives.*

Il y a deux possibilités:

- $\Delta \equiv 1 \pmod 4$ avec Δ sans facteur carré,
- $\Delta/4 \equiv 2, 3 \pmod 4$ avec $\Delta/4$ sans facteur carré.

Etant donnés une matrice $A \in \mathrm{GL}_2(\mathbb{Z})$ et un discriminant Δ, nous avons

$$\begin{aligned} T_A : \quad & F_\Delta \to F_\Delta \\ & f \to T_A(f) = f'. \end{aligned}$$

Définition

Deux formes $f, g \in F_\Delta$ *sont* équivalentes, *en symboles* $f \sim g$, *s'il existe* $A \in \mathrm{GL}_2(\mathbb{Z})$ *tel que* $T_A(f) = g$.
Si $A \in \mathrm{SL}_2(\mathbb{Z})$, *on dit que la forme* f *est* proprement équivalente *à la forme* g, *en symboles* $f \approx g$.

Observation: $\sim$ et $\approx$ sont des relations d'équivalence. On note respectivement $\mathrm{Cl}(\Delta)$ l'ensemble des classes d'équivalence par rapport à $\sim$, et $\mathrm{Cl}^+(\Delta)$ l'ensemble des classes d'équivalence par rapport à $\approx$.

Si $T_A(f) = \langle a', b', c' \rangle$ et $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$, alors

$$\left\{ \begin{array}{lcl} a' & = & f(\alpha, \gamma), \\ b' & = & 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' & = & f(\beta, \delta). \end{array} \right.$$

Si $T_A(f) = \langle a', b', c' \rangle$ et $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$, alors

$$\left\{ \begin{array}{rcl} a' & = & f(\alpha, \gamma), \\ b' & = & 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' & = & f(\beta, \delta). \end{array} \right.$$

Etant donnée une forme $f \in \mathcal{F}_\Delta$, nous voulons trouver la forme équivalente (ou proprement équivalente) à f la plus utile.

Formes définies positives

Nous voulons les coefficients de $\langle a, b, c\rangle$ les plus petits possibles. Si la forme est définie positive, il existe m ayant la propriété

$$m = \min\{f(x,y) \,:\, x,y \in \mathbb{Z}\}.$$

Il est clair que si $m = f(\alpha,\gamma)$, alors $\mathrm{pgcd}(\alpha,\gamma) = 1$ et on peut trouver β,δ telle que $\alpha\delta - \beta\gamma = 1$. Posons $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ et appelons $T_A(f) = \langle a', b', c'\rangle$. Nous avons $a \leq c$, et voulons rendre $|b|$ le plus petit possible.

Formes définies positives

Nous voulons les coefficients de $\langle a, b, c\rangle$ les plus petits possibles. Si la forme est définie positive, il existe m ayant la propriété

$$m = \min\{f(x, y) : x, y \in \mathbb{Z}\}.$$

Il est clair que si $m = f(\alpha, \gamma)$, alors $\operatorname{pgcd}(\alpha, \gamma) = 1$ et on peut trouver β, δ telle que $\alpha\delta - \beta\gamma = 1$. Posons $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ et appelons $T_A(f) = \langle a', b', c'\rangle$. Nous avons $a \leq c$, et voulons rendre $|b|$ le plus petit possible.

Définition

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

Proposition

Il existe une forme quadratique réduite dans chaque classe de formes quadratiques définies positives proprement équivalentes.

Proposition

Il existe une forme quadratique réduite dans chaque classe de formes quadratiques définies positives proprement équivalentes.

Démonstration: Choisissons $\langle a', b', c' \rangle = T_A(f)$ avec $a' = \min\{f(x,y) : x, y \in \mathbb{Z}\}$. Si $|b'| \leq a$, c'est fini. Sinon, nous considérons l'unique entier δ tel que $|-b' + 2a'\delta| \leq a'$, et la matrice $B = M_\delta A'$ ou $M_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$ et $A' = \begin{pmatrix} -\beta & -\delta \\ \alpha & \gamma \end{pmatrix}$. La forme $T_B(f)$ est réduite.

Vous remarquerez que $g = T_{A'}(f) = \langle c', -b', a' \rangle$ et $T_{M_\delta}(g) = \langle a', -b + 2a'\delta, c' + b'\delta + a'\delta^2 \rangle$.

Proposition

Il existe une forme quadratique réduite dans chaque classe de formes quadratiques définies positives proprement équivalentes.

Démonstration: Choisissons $\langle a', b', c' \rangle = T_A(f)$ avec a' =min$\{f(x,y) : x, y \in \mathbb{Z}\}$. Si $|b'| \leq a$, c'est fini. Sinon, nous considérons l'unique entier δ tel que $|-b' + 2a'\delta| \leq a'$, et la matrice $B = M_\delta A'$ ou $M_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$ et $A' = \begin{pmatrix} -\beta & -\delta \\ \alpha & \gamma \end{pmatrix}$. La forme $T_B(f)$ est réduite.

Vous remarquerez que $g = T_{A'}(f) = \langle c', -b', a' \rangle$ et $T_{M_\delta}(g) = \langle a', -b + 2a'\delta, c' + b'\delta + a'\delta^2 \rangle$.

Exercice: Finissez la démonstration.

Théorème

Les seules formes de l'ensemble des formes réduites qui sont équivalentes entre elles sont $\langle a, -b, a\rangle \approx \langle a, b, a\rangle$ *et* $\langle a, -a, c\rangle \approx \langle a, a, c\rangle$.

Théorème

Les seules formes de l'ensemble des formes réduites qui sont équivalentes entre elles sont $\langle a, -b, a\rangle \approx \langle a, b, a\rangle$ *et* $\langle a, -a, c\rangle \approx \langle a, a, c\rangle$.

Démonstration: Soit $\langle a, b, c\rangle$ et $\langle a', b', c'\rangle$ deux formes réduites équivalentes avec $a \geq a'$. Alors, $a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$, et $a \geq a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a(\alpha^2 + \gamma^2) - |b||\alpha\gamma| \geq a|\alpha\gamma|$, de sorte que $\alpha^2 + \gamma^2 \geq 2|\alpha\gamma|$.

Cette inégalité est possible seulement si $\{\alpha, \gamma\} \subset \{0, 1, -1\}$. Si $\alpha = 0$, alors $b' = -b \pm 2c\delta$, $a' = c$, et nous arrivons a f_1. Si $\gamma = 0$, alors $b' = b \pm 2a\delta$, $a' = a$, et nous arrivons à f_2. Finalement, si $|\alpha\gamma| = 1$, alors $a = a' = a \pm b + c$, et nous avons $\langle a, \pm a, a\rangle$.

Comment pouvons-nous trouver la valeur minimale de $f(x, y)$? Dans ce qui suit, on va donner un algorithme standard pour trouver cette valeur:

- Si $f = \langle a, b, c \rangle$ n'est pas réduite, alors il existe un entier unique δ telle que $|-b + 2c\delta| \leq c$.
- Considérons $A = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$ et
  $T_A(f) = \langle c, -b + 2c\delta, a + b\delta + c\delta^2 \rangle = f'$.
- Si $c \leq a + b\delta + c\delta^2$, c'est terminé. Sinon, nous répétons avec f'.

Observation Vous constaterez que si f' n'est pas réduite, alors $0 < c' < c$, de sorte que le processus se terminera après un nombre fini d'étapes.

Proposition

Soit $\langle a, b, c \rangle$ *une forme définie positive réduite. Alors,*

- $|b| \leq \sqrt{\Delta/3}$ *et* $b \equiv \Delta \pmod 2$,
- $a | (b^2 - \Delta)/4$,
- $|b| \leq a \leq (b^2 - \Delta)/(4a)$.

Proposition

Soit $\langle a, b, c\rangle$ *une forme définie positive réduite. Alors,*

- $|b| \leq \sqrt{\Delta/3}$ *et* $b \equiv \Delta \pmod 2$,
- $a|(b^2 - \Delta)/4$,
- $|b| \leq a \leq (b^2 - \Delta)/(4a)$.

Corollaire

Pour $\Delta < 0$, *les ensembles* $\mathrm{Cl}(\Delta)$ *et* $\mathrm{Cl}(\Delta)^+$ *sont finis de cardinalités* h_Δ *et* h_Δ^+ *respectivement.*

Proposition

Soit $\langle a, b, c\rangle$ une forme définie positive réduite. Alors,

- $|b| \leq \sqrt{\Delta/3}$ *et* $b \equiv \Delta \pmod 2$,
- $a|(b^2 - \Delta)/4$,
- $|b| \leq a \leq (b^2 - \Delta)/(4a)$.

Corollaire

Pour $\Delta < 0$, les ensembles $\mathrm{Cl}(\Delta)$ et $\mathrm{Cl}(\Delta)^+$ sont finis de cardinalités h_Δ et h_Δ^+ respectivement.

Nous pouvons utiliser cette proposition, pour trouver toutes les formes quadratiques réduites définies positives.

Algorithme calculant toutes les formes quadratiques definies positives réduites de discriminant donné.

Soit

$$B = \{0 \leq b \leq \sqrt{|\Delta|/3}, b \equiv \Delta \pmod 2\},$$

et pour $b \in B$ posons

$$A_b = \{a \,|\, (b^2 - \Delta)/4, |b| \leq a \leq (b^2 - \Delta)/(4a)\}.$$

Alors,

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

où

$$n(a, b) = \begin{cases} 1 & \text{si } b = 0 \text{ ou si } a \in \{b, (b^2 - \Delta)/4a\}, \\ 2 & \text{sinon.} \end{cases}$$

Exemple.

$\Delta = -264 = 4(-2 \cdot 3 \cdot 11)$

b	$(b^2 - \Delta)/4$	a	c
0	66	$1, 2, 3, 6$	$66, 33, 22, 11$
2	67		
4	70	$5, 7$	$14, 10$
6	75		
8	82		

Par conséquent $h^+_\Delta = 8$, et

$$Cl(\Delta)^+ = \left\{ \begin{array}{llll} \langle 1, 0, 66\rangle, & \langle 2, 0, 33\rangle, & \langle 3, 0, 22\rangle, & \langle 6, 0, 11\rangle, \\ \langle 5, 4, 14\rangle, & \langle 5, -4, 14\rangle, & \langle 7, 4, 10\rangle, & \langle 7, -4, 10\rangle \end{array} \right\}.$$

Exemple.

$\Delta = -264 = 4(-2 \cdot 3 \cdot 11)$

b	$(b^2 - \Delta)/4$	a	c
0	66	$1, 2, 3, 6$	$66, 33, 22, 11$
2	67		
4	70	$5, 7$	$14, 10$
6	75		
8	82		

Par conséquent $h_\Delta^+ = 8$, et

$$Cl(\Delta)^+ = \left\{ \begin{array}{llll} \langle 1, 0, 66 \rangle, & \langle 2, 0, 33 \rangle, & \langle 3, 0, 22 \rangle, & \langle 6, 0, 11 \rangle, \\ \langle 5, 4, 14 \rangle, & \langle 5, -4, 14 \rangle, & \langle 7, 4, 10 \rangle, & \langle 7, -4, 10 \rangle \end{array} \right\}.$$

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

$\langle 5, 4, 14 \rangle \sim \langle 5, -4, 14 \rangle$, $\langle 7, 4, 10 \rangle \sim \langle 7, -4, 10 \rangle$, et $h_\Delta = 6$.

Formes indéfinies

Définition

Une forme quadratique indéfinie $f = \langle a, b, c\rangle$ *est dite* réduite *si*

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

Formes indéfinies

Définition

Une forme quadratique indéfinie $f = \langle a, b, c \rangle$ *est dite* réduite *si*

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

Observations: Si $\langle a, b, c \rangle$ est réduite, $\langle c, b, a \rangle$ l'est aussi. En outre, $|a| < \sqrt{\Delta}$, $|c| < \sqrt{\Delta}$ et $ac < 0$. Remarquons que

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

Formes indéfinies

Définition

Une forme quadratique indéfinie $f = \langle a, b, c \rangle$ *est dite* réduite *si*

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

Observations: Si $\langle a, b, c \rangle$ est réduite, $\langle c, b, a \rangle$ l'est aussi. En outre, $|a| < \sqrt{\Delta}$, $|c| < \sqrt{\Delta}$ et $ac < 0$. Remarquons que

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

Proposition

Si $|a| \leq |c|$ *et* $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$, *alors* $\langle a, b, c \rangle$ *est réduite.*

Proposition

Toute forme quadratique indéfinie f de discrminant Δ est proprement équivalente à une forme réduite de même discrminant.

Proposition

Toute forme quadratique indéfinie f de discrminant Δ est proprement équivalente à une forme réduite de même discrminant.

Démonstration: Si $\langle a, b, c\rangle$ n'est pas réduite, on chosit δ tel que $\sqrt{\Delta} - 2|c| < -b + 2c\delta < \sqrt{\Delta}$. Donc,

$$\langle c, -b + 2c\delta, a - b\delta + c\delta^2\rangle = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \langle a, b, c\rangle$$

et si $|a - b\delta + c\delta^2| < |c|$ le processus est répété.

Corollaire

Pour $\Delta > 0$, $\mathrm{Cl}(\Delta)$ et $\mathrm{Cl}(\Delta)^+$ sont finis du cardinalité h_Δ et h_Δ^+ respectivement.

Exemple.

$\Delta = 316 = 4 \cdot 79$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a \rvert$	$\lvert c \rvert$
2	15, 77	19, 77		
4	13, 77	21, 77		
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		
14	3, 77	31, 77	2, 3, 5, 6, 10, 15	15, 10, 6, 5, 3, 2
16	1, 77	33, 77	1, 3, 5, 15	15, 5, 3, 1

Les formes réduites sont:

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

Définition

Les formes $\langle a, b, a' \rangle$ *et* $\langle a', b', c' \rangle$ *sont dites* adjacentes par la droite *si* $b + b' \equiv 0 \pmod{2a'}$. *Les formes* $\langle c', b, c \rangle$ *et* $\langle a', b', c' \rangle$ *sont dites* adjacentes par la gauche *si* $b + b' \equiv 0 \pmod{2c'}$.

Proposition

Soit $f = \langle a, b, c \rangle$ *une forme quadratique indéfinie réduite. Alors, il existe une forme équivalente à* f *adjacente par la droite et une autre forme équivalente à* f *et adjacente par la gauche.*

Démonstration: Nous considérons $b + b' \equiv 0 \pmod{2ac}$, et les matrices $\begin{pmatrix} 0 & -1 \\ 1 & -(b+b')/2c \end{pmatrix}$ et $\begin{pmatrix} -(b+b')/2a & -1 \\ 1 & 0 \end{pmatrix}$.

Définition

Les formes $\langle a, b, a' \rangle$ *et* $\langle a', b', c' \rangle$ *sont dites* adjacentes par la droite *si* $b + b' \equiv 0 \pmod{2a'}$. *Les formes* $\langle c', b, c \rangle$ *et* $\langle a', b', c' \rangle$ *sont dites* adjacentes par la gauche *si* $b + b' \equiv 0 \pmod{2c'}$.

Proposition

Soit $f = \langle a, b, c \rangle$ *une forme quadratique indéfinie réduite. Alors, il existe une forme équivalente à* f *adjacente par la droite et une autre forme équivalente à* f *et adjacente par la gauche.*

Démonstration: Nous considérons $b + b' \equiv 0 \pmod{2ac}$, et les matrices $\begin{pmatrix} 0 & -1 \\ 1 & -(b+b')/2c \end{pmatrix}$ et $\begin{pmatrix} -(b+b')/2a & -1 \\ 1 & 0 \end{pmatrix}$.

Observation: L'esemble des formes quadratiques réduites de discriminant $\Delta > 0$ peut être partionné en cycles de formes adjacentes par la droite (ou par la gauche).

Théorème

Soit f et f' deux formes quadratiques indéfinies réduites. Alors, $f \approx f' \iff$ toutes les deux appartiennent au même cycle.

Une implication est déjà démontrée. Pour l'autre nous avons besoin des nombres quadratiques.

Formes quadratiques (Leçon 2)

Jorge Jiménez Urroz
(Universitat Politècnica de Catalunya)

École Cimpa, Bamako, Novembre 2010

Nombres quadratiques

Définition

Un nombre quadratique *est un nombre* α *de la forme* $x + y\sqrt{\Delta}$ *où* Δ *n'est pas un carré parfait de* $\mathbb{Q}$ *et où* $x, y \in \mathbb{Q}$. *Le* conjugué *de* α *est* $\alpha' = x - y\sqrt{\Delta}$.

Un nombre quadratique est donc un nombre qui est solution d'un polynôme irréductible de degré deux. Dans ce qui suit, Δ n'est pas un carré parfait.

Nombres quadratiques

Définition

Un nombre quadratique *est un nombre* α *de la forme* $x + y\sqrt{\Delta}$ *où* Δ *n'est pas un carré parfait de* $\mathbb{Q}$ *et où* $x, y \in \mathbb{Q}$. *Le* conjugué *de* α *est* $\alpha' = x - y\sqrt{\Delta}$.

Un nombre quadratique est donc un nombre qui est solution d'un polynôme irréductible de degré deux. Dans ce qui suit, Δ n'est pas un carré parfait.

Définition

Soit $\Delta > 0$. *Un nombre quadratique* α *est* réduit *si* $\alpha > 1$ *et* $-1 < \alpha' < 0$.

Définition

Soit $f = \langle a, b, c\rangle$ *de discriminant* $\Delta > 0$*. Alors, on asssocie à* f *les nombres réels*

$$\omega_1 = \frac{b+\Delta}{2|a|} \quad \text{et} \quad \omega_2 = \frac{b+\Delta}{2|c|}.$$

Définition

Soit $f = \langle a, b, c\rangle$ *de discriminant* $\Delta > 0$*. Alors, on asssocie à* f *les nombres réels*

$$\omega_1 = \frac{b+\Delta}{2|a|} \quad \textit{et} \quad \omega_2 = \frac{b+\Delta}{2|c|}.$$

Observation: f est réduite si et seulement si ω_1 et ω_2 sont réduits.

Définition

Soit $f = \langle a, b, c \rangle$ *de discriminant* $\Delta > 0$*. Alors, on asssocie à* f *les nombres réels*

$$\omega_1 = \frac{b+\Delta}{2|a|} \quad et \quad \omega_2 = \frac{b+\Delta}{2|c|}.$$

Observation: f est réduite si et seulement si ω_1 et ω_2 sont réduits.

Définition

Soit $\{a_i\}_{\mathbb{N}} \subset \mathbb{R}$*. Une* fraction continue α *est une expression de la forme* $\alpha = [a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}}$

Définition

Les a_i *sont dits les* quotients partiels *de la fraction continue* α. *Si* $a_0 \in \mathbb{Z}$ *et* $a_i \in \mathbb{N}$, *pour* $i > 0$, *alors la fraction continue est dite simple.*

Définition

Les a_i sont dits les quotients partiels *de la fraction continue α. Si $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}$, pour $i > 0$, alors la fraction continue est dite simple.*

Proposition

Soit α une fraction continue. Alors, le développement de α est infini si et seulement si α est irrationnel.

Démonstration: Soit $\alpha = a_0 + x_1$, avec $a_0 = [\alpha]$. Pour $i \geq 1$,

$$a_i = \begin{cases} 0 & \text{si } x_i = 0, \\ \left[\frac{1}{x_i}\right] & \text{si } x_i \neq 0, \end{cases}$$

et $x_{i+1} = \frac{1}{x_i} - a_i$. Si $\alpha \in \mathbb{Q}$, alors $x_i = \frac{p_i}{q_i}$ et $0 < q_i < q_{i-1}$.

Définition

Soit $\alpha = [a_0, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+l}}]$*. La barre horizontale veut dire que la suite des éléments se répète indéfiniment. De plus,* $a_0, \ldots, a_{k-1}$ *et* $a_k, \ldots, a_{k+l}$ *sont respectivement appelés la* prépériode *et la* période *de* α*.*

Si α est un nombre quadratique associé à une forme quadratique indéfinie de discriminant fondamental $\Delta > 0$, alors il existe $P_0, Q_0 \in \mathbb{Z}$, tels que

$$\alpha = \alpha_0 = \frac{P_0 + \sqrt{\Delta}}{2Q_0} \quad \text{avec} \quad 4Q_0 | (\Delta - P_0^2).$$

En ce cas $\alpha = [a_0, a_1, a_2, \ldots]$ où pour $i \geq 0$,

- $\alpha_i = \frac{P_i + \sqrt{\Delta}}{2Q_i}$,
- $a_i = [\alpha_i]$,
- $P_{i+1} = 2a_iQ_i - P_i$,
- $Q_{i+1} = \frac{\Delta - P_{i+1}^2}{4Q_i}$.

$$
\begin{aligned}
\alpha &= a_0 + \frac{P_0 - 2a_0Q_0 + \sqrt{\Delta}}{2Q_0} \\
&= a_0 + \frac{1}{\frac{2Q_0}{P_0 - 2a_0Q_0 + \sqrt{\Delta}}} \\
&= a_0 + \frac{1}{\frac{2Q_0(\sqrt{\Delta} - (P_0 - 2a_0Q_0))}{\Delta - (P_0 - 2a_0Q_0)^2}} \\
&= a_0 + \frac{1}{\frac{\sqrt{\Delta} + 2a_0Q_0 - P_0}{2(\Delta - (P_0 - 2a_0Q_0)^2)/4Q_0}} \\
&= \ldots
\end{aligned}
$$

Exemples

(1) Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\alpha_0 = \frac{4+\sqrt{40}}{6}$, nous avons:

.

Exemples

(1) Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\alpha_0 = \frac{4+\sqrt{40}}{6}$, nous avons:

- $\alpha_i = \frac{P_i+\sqrt{\Delta}}{2Q_i}$,
- $a_i = [\alpha_i]$,
- $P_{i+1} = 2a_iQ_i - P_i$,
- $Q_{i+1} = \frac{\Delta - P_{i+1}^2}{4Q_i}$.

Exemples

(1) Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\alpha_0 = \frac{4+\sqrt{40}}{6}$, nous avons:

- $\alpha_i = \frac{P_i+\sqrt{\Delta}}{2Q_i}$,
- $a_i = [\alpha_i]$,
- $P_{i+1} = 2a_iQ_i - P_i$,
- $Q_{i+1} = \frac{\Delta - P_{i+1}^2}{4Q_i}$.

$1 < \alpha_0 < 2, \quad a_0 = 1, \quad P_0 = 4, \quad Q_0 = 3;$
$P_1 = 2, \quad Q_1 = 3; \quad 1 < \alpha_1 = \frac{2+\sqrt{40}}{6} < 2, \quad a_1 = 1;$
$P_2 = 4 \quad Q_2 = 2, \quad 2 < \alpha_2 = \frac{4+\sqrt{40}}{4} < 3, \quad a_2 = 2;$
$P_3 = 4, \quad Q_3 = 3, \quad \alpha_3 = \frac{4+\sqrt{40}}{6}.$

Exemples

(1) Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\alpha_0 = \frac{4+\sqrt{40}}{6}$, nous avons:

- $\alpha_i = \frac{P_i+\sqrt{\Delta}}{2Q_i}$,
- $a_i = [\alpha_i]$,
- $P_{i+1} = 2a_iQ_i - P_i$,
- $Q_{i+1} = \frac{\Delta - P_{i+1}^2}{4Q_i}$.

$1 < \alpha_0 < 2, \quad a_0 = 1, \quad P_0 = 4, \quad Q_0 = 3;$
$P_1 = 2, \quad Q_1 = 3; \quad 1 < \alpha_1 = \frac{2+\sqrt{40}}{6} < 2, \quad a_1 = 1;$
$P_2 = 4 \quad Q_2 = 2, \quad 2 < \alpha_2 = \frac{4+\sqrt{40}}{4} < 3, \quad a_2 = 2;$
$P_3 = 4, \quad Q_3 = 3, \quad \alpha_3 = \frac{4+\sqrt{40}}{6}.$

i	0	1	2	...
P_i	4	2	4	...
Q_i	3	3	2	...
a_i	1	1	2	...

Donc, $\alpha_0 = [\overline{1, 1, 2}]$.

Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\beta_0 = \frac{6+\sqrt{40}}{2}$, nous avons:

Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\beta_0 = \frac{6+\sqrt{40}}{2}$, nous avons:

- $\alpha_i = \frac{P_i+\sqrt{\Delta}}{2Q_i}$,
- $a_i = [\alpha_i]$,
- $P_{i+1} = 2a_iQ_i - P_i$,
- $Q_{i+1} = \frac{\Delta - P_{i+1}^2}{4Q_i}$.

$6 < \beta_0 < 7, \quad a_0 = 6,\ P_0 = 6,\ Q_0 = 1;$
$P_1 = 6,\ Q_1 = 1,\ \beta_1 = \frac{6+\sqrt{40}}{2}$.

Avec $\Delta = 40 = 4 \cdot 5 \cdot 2$ et $\beta_0 = \frac{6+\sqrt{40}}{2}$, nous avons:

- $\alpha_i = \frac{P_i+\sqrt{\Delta}}{2Q_i}$,
- $a_i = [\alpha_i]$,
- $P_{i+1} = 2a_iQ_i - P_i$,
- $Q_{i+1} = \frac{\Delta - P_{i+1}^2}{4Q_i}$.

$6 < \beta_0 < 7, \quad a_0 = 6,\ P_0 = 6,\ Q_0 = 1;$
$P_1 = 6,\ Q_1 = 1,\ \beta_1 = \frac{6+\sqrt{40}}{2}$.

i	0	...
P_i	6	...
Q_i	1	...
a_i	6	...

Donc, $\beta_0 = [\overline{6}]$.

Formes réduites de discriminant $\Delta = 40$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a \rvert$	$\lvert c \rvert$
2	$4,32$	$8,32$	3	3
4	$2,32$	$10,32$	$3,2$	$2,3$
6	$0,32$	$12,32$	1	1

Formes réduites de discriminant $\Delta = 40$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a \rvert$	$\lvert c \rvert$
2	4, 32	8, 32	3	3
4	2, 32	10, 32	3, 2	2, 3
6	0, 32	12, 32	1	1

Les formes réduites de discriminant 40 sont:

$$\langle \pm 3, 2, \mp 3 \rangle, \quad \langle \pm 3, 4, \mp 2 \rangle, \quad \langle \pm 2, 4, \mp 3 \rangle, \quad \langle \pm 1, 6, \mp 1 \rangle.$$

Formes réduites de discriminant $\Delta = 40$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a \rvert$	$\lvert c \rvert$
2	4, 32	8, 32	3	3
4	2, 32	10, 32	3, 2	2, 3
6	0, 32	12, 32	1	1

Les formes réduites de discriminant 40 sont:

$$\langle \pm 3, 2, \mp 3 \rangle, \quad \langle \pm 3, 4, \mp 2 \rangle, \quad \langle \pm 2, 4, \mp 3 \rangle, \quad \langle \pm 1, 6, \mp 1 \rangle.$$

$$f_1 = \langle 3, 2, -3 \rangle \to \langle -3, 4, 2 \rangle \to \langle 2, 4, -3 \rangle \to \langle -3, 2, 3 \rangle \to$$
$$\to \langle 3, 4, -2 \rangle \to \langle -2, 4, 3 \rangle \to f_1.$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Formes réduites de discriminant $\Delta = 40$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a\rvert$	$\lvert c\rvert$
2	4, 32	8, 32	3	3
4	2, 32	10, 32	3, 2	2, 3
6	0, 32	12, 32	1	1

Les formes réduites de discriminant 40 sont:

$$\langle \pm 3, 2, \mp 3\rangle, \quad \langle \pm 3, 4, \mp 2\rangle, \quad \langle \pm 2, 4, \mp 3\rangle, \quad \langle \pm 1, 6, \mp 1\rangle.$$

$$f_1 = \langle 3, 2, -3\rangle \to \langle -3, 4, 2\rangle \to \langle 2, 4, -3\rangle \to \langle -3, 2, 3\rangle \to$$
$$\to \langle 3, 4, -2\rangle \to \langle -2, 4, 3\rangle \to f_1.$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

$$\omega_2(f_1) = \frac{2+\sqrt{40}}{6} = [\overline{1, 2, 1}]$$

$$f_2 = \langle 1, 6, -1 \rangle \to \langle -1, 6, 1 \rangle \to f_2$$

$$f_2 = \langle 1, 6, -1 \rangle \to \langle -1, 6, 1 \rangle \to f_2$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 6 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -6 \end{pmatrix}.$$

.

$$f_2 = \langle 1, 6, -1\rangle \to \langle -1, 6, 1\rangle \to f_2$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 6 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -6 \end{pmatrix}.$$

$\omega_2(f_2) = \frac{4+\sqrt{40}}{4} = [\overline{6}].$

$$f_2 = \langle 1, 6, -1\rangle \to \langle -1, 6, 1\rangle \to f_2$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 6 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -6 \end{pmatrix}.$$

$\omega_2(f_2) = \frac{4+\sqrt{40}}{4} = [\overline{6}].$

$h^+_\Delta = 2.$

(2) $\Delta = 60 = 4 \cdot 15$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a \rvert$	$\lvert c \rvert$
2	$5,74$	$9,74$		
4	$3,74$	$11,74$		
6	$1,74$	$13,74$	$1,2,3,6$	$6,3,2,1$

(2) $\Delta = 60 = 4 \cdot 15$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\|a\|$	$\|c\|$
2	$5,74$	$9,74$		
4	$3,74$	$11,74$		
6	$1,74$	$13,74$	$1,2,3,6$	$6,3,2,1$

Les formes réduites de discriminant 60 sont:

$$\langle \pm 1, 6, \mp 6 \rangle, \quad \langle \pm 2, 6, \mp 3 \rangle, \quad \langle \pm 3, 6, \mp 2 \rangle, \quad \langle \pm 6, 6, \mp 1 \rangle.$$

(2) $\Delta = 60 = 4 \cdot 15$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a\rvert$	$\lvert c\rvert$
2	5, 74	9, 74		
4	3, 74	11, 74		
6	1, 74	13, 74	1, 2, 3, 6	6, 3, 2, 1

Les formes réduites de discriminant 60 sont:

$$\langle \pm 1, 6, \mp 6\rangle, \quad \langle \pm 2, 6, \mp 3\rangle, \quad \langle \pm 3, 6, \mp 2\rangle, \quad \langle \pm 6, 6, \mp 1\rangle.$$

$$\frac{6+\sqrt{60}}{12} = [\overline{1, 6}], \qquad \frac{6+\sqrt{60}}{6} = [\overline{2, 3}],$$

$$\frac{6+\sqrt{60}}{4} = [\overline{3, 2}], \qquad \frac{6+\sqrt{60}}{2} = [\overline{6, 1}].$$

- $\frac{6+\sqrt{60}}{12} = [\overline{1,6}]$

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

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

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

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

$$\langle -2,6,3\rangle \to \langle 3,6,-2\rangle \to \langle -2,6,3\rangle, \quad \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}.$$

(3) Soit $\Delta = 145 = 5 \cdot 29$. Les formes réduites sont:

$$\langle \pm 6, 1, \mp 6 \rangle, \quad \langle \pm 5, 5, \mp 6 \rangle, \quad \langle \pm 6, 5, \mp 5 \rangle, \quad \langle \pm 3, 7, \mp 8 \rangle,$$
$$\langle \pm 4, 7, \mp 6 \rangle, \quad \langle \pm 6, 7, \mp 4 \rangle, \quad \langle \pm 8, 7, \mp 3 \rangle, \quad \langle \pm 2, 9, \mp 8 \rangle,$$
$$\langle \pm 4, 9, \mp 4 \rangle, \quad \langle \pm 8, 9, \mp 2 \rangle, \quad \langle \pm 1, 11, \mp 6 \rangle, \quad \langle \pm 2, 11, \mp 3 \rangle,$$
$$\langle \pm 3, 11, \mp 2 \rangle, \quad \langle \pm 6, 11, \mp 1 \rangle.$$

(3) Soit $\Delta = 145 = 5 \cdot 29$. Les formes réduites sont:

$$\langle \pm 6, 1, \mp 6\rangle, \quad \langle \pm 5, 5, \mp 6\rangle, \quad \langle \pm 6, 5, \mp 5\rangle, \quad \langle \pm 3, 7, \mp 8\rangle,$$
$$\langle \pm 4, 7, \mp 6\rangle, \quad \langle \pm 6, 7, \mp 4\rangle, \quad \langle \pm 8, 7, \mp 3\rangle, \quad \langle \pm 2, 9, \mp 8\rangle,$$
$$\langle \pm 4, 9, \mp 4\rangle, \quad \langle \pm 8, 9, \mp 2\rangle, \quad \langle \pm 1, 11, \mp 6\rangle, \quad \langle \pm 2, 11, \mp 3\rangle,$$
$$\langle \pm 3, 11, \mp 2\rangle, \quad \langle \pm 6, 11, \mp 1\rangle.$$

$f_1 = \langle 6, 1, -6\rangle, \quad \omega_2(f_1) = \frac{1+\sqrt{145}}{12} = [\overline{1, 11, 1}]$

$\langle 6, 1, -6\rangle \to \langle -6, 11, 1\rangle \to \langle 1, 11, -6\rangle \to \langle -6, 1, 6\rangle \to$
$\langle 6, 11, -1\rangle \to \langle -1, 11, 6\rangle \to f_1$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -11 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 11 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

$f_2 = \langle 5, 5, -6\rangle \quad \omega_2(f_2) = \frac{5+\sqrt{145}}{12} = [\overline{1, 2, 2, 1, 1}]$

$\langle 5, 5, -6\rangle \to \langle -6, 7, 4\rangle \to \langle 4, 9, -4\rangle \to \langle -4, 7, 6\rangle \to$
$\langle 6, 5, -5\rangle \to \langle -5, 5, 6\rangle \to \langle 6, 7, -4\rangle \to \langle -4, 9, 4\rangle \to$
$\langle 4, 7, -6\rangle \to \langle -6, 5, 5\rangle \to f_2$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

$f_3 = \langle 3, 7, -8 \rangle \quad \omega_2(f_3) = \frac{7+\sqrt{145}}{16} = [\overline{1, 5, 3}]$

$\langle 3, 7, -8 \rangle \to \langle -8, 9, 2 \rangle \to \langle 2, 11, -3 \rangle \to \langle -3, 7, 8 \rangle \to$
$\langle 8, 9, -2 \rangle \to \langle -2, 11, 3 \rangle \to f_3$

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -5 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -3 \end{pmatrix}.$$

$f_4 = \langle 8, 7, -3 \rangle \quad \omega_2(f_4) = \frac{7+\sqrt{145}}{6} = [\overline{3, 5, 1}]$

$\langle 8, 7, -3 \rangle \to \langle -3, 11, 2 \rangle \to \langle 2, 9, -8 \rangle \to \langle -8, 7, 3 \rangle \to$
$\langle 3, 11, -2 \rangle \to \langle -2, 9, 8 \rangle \to f_4.$

$$\begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -5 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -3 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Algorithme calculant le cycle des formes réduites proprement équivalentes à une forme quadratique donnée.

Soit $f_0 = \langle a_0, b_0, c_0 \rangle$ une forme quadratique de discriminant $\Delta > 0$. Alors, $\alpha_0 = \frac{b_0+\Delta}{2|c_0|} = [\overline{u_0, \dots u_{l-1}}]$ et le cycle des formes réduites proprement équivalentes a f_0 est formé des formes réduites $f_0 \dots f_{r-1}$ où

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

Pour $0 \leq i \leq r-2$,

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

Observation: Si l est impair, alors $f_l = \langle -a_0, b_0, -c_0 \rangle$.

Théorème

Deux formes quadratiques réduites de discriminant $\Delta > 0$ sont proprement équivalentes si et seulement si elles appartiemment au même cycle.

L'idée de la démonstration est d'observer que si $f \approx g$, alors $\omega_2(g)$ est un nombre réduit associé à une forme quadratique du cycle de f; par conséquent, f et g sont dans le même cycle.

Formes quadratiques
(Leçon 3)

Jorge Jiménez Urroz
(Universitat Politècnica de Catalunya)

École Cimpa, Bamako, Novembre 2010

Formes concordantes

Soit Δ un discriminant fondamental. On a

$$(x^2 + \Delta y^2)(z^2 + \Delta w^2) = (xz + \Delta yw)^2 + \Delta(xw - zy)^2.$$

Nous pouvons donc mutiplier certains formes quadratiques. Nous voulons donner une structure algébrique aux ensembles $Cl(\Delta)$ et $Cl(\Delta)^+$, en généralisant la multiplication ci-haut.

On voit que

$$(a_1x_1^2+bx_1y_1+a_2cy_1^2)(a_2x_2^2+bx_2y_2+a_1cy_2^2) = (a_1a_2X^2+bXY+cY^2)$$

où

$$\begin{cases} X = x_1x_2 - cy_1y_2, \\ Y = ax_1y_2 + a_2y_1x_2 + by_1y_2. \end{cases}$$

Définition

Les formes $f_1 = \langle a_1, b, ca_2 \rangle$ *et* $f_2 = \langle a_2, b, a_1 c > \rangle$ *sont dites* concordantes.

Observation: Deux formes concordantes ont le même discriminant.

Définition

Les formes $f_1 = \langle a_1, b, ca_2 \rangle$ *et* $f_2 = \langle a_2, b, a_1 c > \rangle$ *sont dites* concordantes.

Observation: Deux formes concordantes ont le même discriminant.

Définition

Sur l'ensemble des formes concordantes nous avons donc une loi de composition: $F = f_1 * f_2 = \langle a_1 a_2, b, c \rangle$.

Définition

Les formes $f_1 = \langle a_1, b, ca_2 \rangle$ *et* $f_2 = \langle a_2, b, a_1c > \rangle$ *sont dites* concordantes.

Observation: Deux formes concordantes ont le même discriminant.

Définition

Sur l'ensemble des formes concordantes nous avons donc une loi de composition: $F = f_1 * f_2 = \langle a_1a_2, b, c \rangle$.

Maintenant on veut montrer qu'il y a une forme concordante dans chaque classe d'équivalence de formes quadratiques.

Lemme

Soit f une forme primitive, et $M \neq 0$ entier. Alors f représente un entier m différent de zéro et tel que $pgcd(m, M) = 1$.

Lemme

Soit f une forme primitive, et $M \neq 0$ entier. Alors f représente un entier m différent de zéro et tel que pgcd$(m, M) = 1$.

Démonstration: Soit $2M = PQR$ avec les retrictions suivantes. Tout d'abord, $p|P$ si et seulement si $p|(a, 2M)$ mais $p \nmid c$. De plus, $p|Q$ si et seulement si $p|(a, c, 2M)$. Finalement, $p|R$ si et seulement si $p|2M$ mais $p \nmid a$. Alors $(aP^2 + bPR + cR^2, 2M) = 1$. Vérifiez que par définition $(P, Q) = (Q, R) = (P, R) = 1$, et qu'il n'est pas possible d'avoir $a + b + c = 0$.

Lemme

Soit $\{C_1, C_2\} \subset \mathrm{Cl}(\Delta)^+$, *et* $M \neq 0$ *entier. Alors, il existe une paire de formes concordantes* $f_1 = \langle a_1, b, a_2 c\rangle \in C_1$ *et* $f_2 = \langle a_2, b, a_1 c\rangle \in C_2$ *telles que* $pgcd(a_1, a_2) = pgcd(a_1 a_2, M) = 1$.

Lemme

Soit $\{C_1, C_2\} \subset \mathrm{Cl}(\Delta)^+$*, et* $M \neq 0$ *entier. Alors, il existe une paire de formes concordantes* $f_1 = \langle a_1, b, a_2 c\rangle \in C_1$ *et* $f_2 = \langle a_2, b, a_1 c\rangle \in C_2$ *telles que pgcd*$(a_1, a_2) =$*pgcd*$(a_1 a_2, M) = 1$*.*

Démonstration: Choisissons $F_1 = \langle a_1, b_1, c_1\rangle \in C_1$ tel que $\mathrm{pgcd}(a_1, M) = 1$. Prenons des entiers r, s tels que $(r, s) = 1$ et tels que $a_1 = f(r, s)$ est copremier avec M. Alors, il existe $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma f = F_1$ est la forme que nous désirons.

Lemme

Soit $\{C_1, C_2\} \subset \mathrm{Cl}(\Delta)^+$, et $M \neq 0$ entier. Alors, il existe une paire de formes concordantes $f_1 = \langle a_1, b, a_2 c\rangle \in C_1$ et $f_2 = \langle a_2, b, a_1 c\rangle \in C_2$ telles que pgcd$(a_1, a_2) =$pgcd$(a_1 a_2, M) = 1$.

Démonstration: Choisissons $F_1 = \langle a_1, b_1, c_1\rangle \in C_1$ tel que $\mathrm{pgcd}(a_1, M) = 1$. Prenons des entiers r, s tels que $(r, s) = 1$ et tels que $a_1 = f(r, s)$ est copremier avec M. Alors, il existe $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma f = F_1$ est la forme que nous désirons.

Puis choisissons $F_2 = \langle a_2, b_2, c_2\rangle \in C_2$ avec $(a_2, a_1 M) = 1$.

Lemme

Soit $\{C_1, C_2\} \subset \mathrm{Cl}(\Delta)^+$, et $M \neq 0$ entier. Alors, il existe une paire de formes concordantes $f_1 = \langle a_1, b, a_2 c\rangle \in C_1$ et $f_2 = \langle a_2, b, a_1 c\rangle \in C_2$ telles que pgcd$(a_1, a_2) =$pgcd$(a_1 a_2, M) = 1$.

Démonstration: Choisissons $F_1 = \langle a_1, b_1, c_1\rangle \in C_1$ tel que pgcd$(a_1, M) = 1$. Prenons des entiers r, s tels que $(r, s) = 1$ et tels que $a_1 = f(r, s)$ est copremier avec M. Alors, il existe $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma f = F_1$ est la forme que nous désirons.

Puis choisissons $F_2 = \langle a_2, b_2, c_2\rangle \in C_2$ avec $(a_2, a_1 M) = 1$. Ensuite, prenons des entiers n_1, n_2 tels que $a_1 n_1 - a_2 n_2 = \frac{b_1 - b_2}{2}$. Notez que $b_1 \equiv b_2 \equiv \Delta \pmod 2$.

Lemme

Soit $\{C_1, C_2\} \subset \mathrm{Cl}(\Delta)^+$, et $M \neq 0$ entier. Alors, il existe une paire de formes concordantes $f_1 = \langle a_1, b, a_2 c\rangle \in C_1$ et $f_2 = \langle a_2, b, a_1 c\rangle \in C_2$ telles que pgcd$(a_1, a_2) =$pgcd$(a_1 a_2, M) = 1$.

Démonstration: Choisissons $F_1 = \langle a_1, b_1, c_1\rangle \in C_1$ tel que pgcd$(a_1, M) = 1$. Prenons des entiers r, s tels que $(r, s) = 1$ et tels que $a_1 = f(r, s)$ est copremier avec M. Alors, il existe $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma f = F_1$ est la forme que nous désirons.

Puis choisissons $F_2 = \langle a_2, b_2, c_2\rangle \in C_2$ avec $(a_2, a_1 M) = 1$. Ensuite, prenons des entiers n_1, n_2 tels que $a_1 n_1 - a_2 n_2 = \frac{b_1 - b_2}{2}$. Notez que $b_1 \equiv b_2 \equiv \Delta \pmod 2$.

Les formes $f_j = \begin{pmatrix} 1 & 0 \\ n_j & 1 \end{pmatrix} F_j$ sont les formes demandées dans l'énoncé avec $b = b_j + 2a_j n_j$.

Proposition

Soient C_1, C_2 *deux classes d'équivalence propre de formes quadratiques de discriminant fondamental* Δ, *et soient* $f_1 \in C_1$ *et* $f_2 \in C_2$ *des formes concordantes. Soient* $g_1 \in C_1$ *et* $g_2 \in C_2$ *une autre paire de formes concordantes. Alors*

$$f_1 * f_2 \approx g_1 * g_2.$$

Proposition

Soient C_1, C_2 deux classes d'équivalence propre de formes quadratiques de discriminant fondamental Δ, et soient $f_1 \in C_1$ et $f_2 \in C_2$ des formes concordantes. Soient $g_1 \in C_1$ et $g_2 \in C_2$ une autre paire de formes concordantes. Alors

$$f_1 * f_2 \approx g_1 * g_2.$$

Démonstration: Soit $f_1 = \langle a_1, b, c_1 \rangle$, $f_2 = \langle a_2, b, c_2 \rangle$, $g_1 = \langle a_1', b', c_1' \rangle$ et $g_2 = \langle a_2', b', c_2' \rangle$.

- Cas 1: Soit $f_1 = g_1$ et $\mathrm{pgcd}(a_1, a_2') = 1$. Il existe $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\gamma f_2 = g_2$. Il est très facile de voir que $-sc_2 = ta_2'$. Or $a_1 | c_2$, de sorte que $a_1 | t$. La matrice $\gamma' = \begin{pmatrix} r & sa_1 \\ t/a_1 & u \end{pmatrix}$ est telle que $\gamma'(f_1 * f_2) = f_1 * g_2$.

• Cas 2: Soit $b = b'$ et $\text{pgcd}(a_1, a_2') = 1$. Dans ce cas, f_1 et g_2 sont concordantes, et deux applications du dernier cas montrent que

$$f_1 * f_2 \approx f_1 * g_2 \approx g_1 * g_2.$$

- Cas 2: Soit $b = b'$ et $\mathrm{pgcd}(a_1, a_2') = 1$. Dans ce cas, f_1 et g_2 sont concordantes, et deux applications du dernier cas montrent que

$$f_1 * f_2 \approx f_1 * g_2 \approx g_1 * g_2.$$

- Cas 3: Soit $\mathrm{pgcd}(a_1 a_2, a_1' a_2') = 1$. Soient B, n, n' tels que $b + 2a_1 a_2 n = b' + 2a_1' a_2' n' = B$. Considérons

$F_1 = \begin{pmatrix} 1 & 0 \\ a_2 n & 1 \end{pmatrix} f_1 = \langle a_1, B, C_1 \rangle,$

$F_2 = \begin{pmatrix} 1 & 0 \\ a_1 n & 1 \end{pmatrix} f_2 = \langle a_2, B, C_2 \rangle,$

$H_1 = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} (f_1 * f_2) = \langle a_1 a_2, B, C \rangle.$

• Cas 2: Soit $b = b'$ et $\mathrm{pgcd}(a_1, a_2') = 1$. Dans ce cas, f_1 et g_2 sont concordantes, et deux applications du dernier cas montrent que

$$f_1 * f_2 \approx f_1 * g_2 \approx g_1 * g_2.$$

• Cas 3: Soit $\mathrm{pgcd}(a_1 a_2, a_1' a_2') = 1$. Soient B, n, n' tels que $b + 2a_1 a_2 n = b' + 2a_1' a_2' n' = B$. Considérons

$F_1 = \begin{pmatrix} 1 & 0 \\ a_2 n & 1 \end{pmatrix} f_1 = \langle a_1, B, C_1 \rangle,$

$F_2 = \begin{pmatrix} 1 & 0 \\ a_1 n & 1 \end{pmatrix} f_2 = \langle a_2, B, C_2 \rangle,$

$H_1 = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} (f_1 * f_2) = \langle a_1 a_2, B, C \rangle.$

On voit que $a_1 a_2 | (B^2 - \Delta)/4$ et par conséquent F_1 et F_2 sont concordantes.

• Cas 2: Soit $b = b'$ et $\text{pgcd}(a_1, a_2') = 1$. Dans ce cas, f_1 et g_2 sont concordantes, et deux applications du dernier cas montrent que

$$f_1 * f_2 \approx f_1 * g_2 \approx g_1 * g_2.$$

• Cas 3: Soit $\text{pgcd}(a_1 a_2, a_1' a_2') = 1$. Soient B, n, n' tels que $b + 2a_1 a_2 n = b' + 2a_1' a_2' n' = B$. Considérons

$$F_1 = \begin{pmatrix} 1 & 0 \\ a_2 n & 1 \end{pmatrix} f_1 = \langle a_1, B, C_1 \rangle,$$

$$F_2 = \begin{pmatrix} 1 & 0 \\ a_1 n & 1 \end{pmatrix} f_2 = \langle a_2, B, C_2 \rangle,$$

$$H_1 = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} (f_1 * f_2) = \langle a_1 a_2, B, C \rangle.$$

On voit que $a_1 a_2 | (B^2 - \Delta)/4$ et par conséquent F_1 et F_2 sont concordantes. Similairement, les formes $G_1 = \langle a_1', B, C_1' \rangle$ et $G_2 = \langle a_2', B, C_2' \rangle$ sont corcordantes, et $H_2 = \langle a_1' a_2', B, C \rangle \approx g_1 * g_2$.

• Cas 2: Soit $b = b'$ et $\text{pgcd}(a_1, a_2') = 1$. Dans ce cas, f_1 et g_2 sont concordantes, et deux applications du dernier cas montrent que

$$f_1 * f_2 \approx f_1 * g_2 \approx g_1 * g_2.$$

• Cas 3: Soit $\text{pgcd}(a_1 a_2, a_1' a_2') = 1$. Soient B, n, n' tels que $b + 2a_1 a_2 n = b' + 2a_1' a_2' n' = B$. Considérons

$$F_1 = \begin{pmatrix} 1 & 0 \\ a_2 n & 1 \end{pmatrix} f_1 = \langle a_1, B, C_1 \rangle,$$

$$F_2 = \begin{pmatrix} 1 & 0 \\ a_1 n & 1 \end{pmatrix} f_2 = \langle a_2, B, C_2 \rangle,$$

$$H_1 = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} (f_1 * f_2) = \langle a_1 a_2, B, C \rangle.$$

On voit que $a_1 a_2 | (B^2 - \Delta)/4$ et par conséquent F_1 et F_2 sont concordantes. Similairement, les formes $G_1 = \langle a_1', B, C_1' \rangle$ et $G_2 = \langle a_2', B, C_2' \rangle$ sont corcordantes, et $H_2 = \langle a_1' a_2', B, C \rangle \approx g_1 * g_2$.

Nous concluons, grâce au dernier cas pour F_1, F_2, G_1, G_2, que

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

•Cas 4: D'après le lemme précédent, il existe deux formes concordantes $F_1 = \langle A_1, B, C_1 \rangle \in C_1$ et $F_2 = \langle A_2, B, C_2 \rangle \in C_2$ telles que $\mathrm{pgcd}(A_1 A_2, a_1 a_2 a'_1 a'_2) = 1$. Alors, nous pouvons appliquer deux fois le dernier cas, ce qui prouve que

$$f_1 * f_2 \approx F_1 * F_2 \approx g_1 * g_2.$$

Théorème

Soit $\Delta \neq 0$. L'ensemble des classes d'equivalence propre des formes quadratiques binaires de discriminant Δ est un groupe abélien fini. L'élément neutre du groupe est la classe principale. L'inverse de f est la classe de toute forme improprement équivalente à f.

Démonstration: Soit $f =< a, b, c >$.

- Commutativité: C'est clair par définition.

Théorème

Soit $\Delta \neq 0$. L'ensemble des classes d'equivalence propre des formes quadratiques binaires de discriminant Δ est un groupe abélien fini. L'élément neutre du groupe est la classe principale. L'inverse de f est la classe de toute forme improprement équivalente à f.

Démonstration: Soit $f =< a, b, c >$.

- Commutativité: C'est clair par définition.

- Elément neutre: On a $\begin{pmatrix} 1 & 0 \\ \frac{b-\varepsilon}{2} & 1 \end{pmatrix} f_0 = \langle 1, b, ac \rangle$, ce qui est une forme concordante avec $f = \langle a, b, c \rangle$, et $f * \langle 1, b, ac \rangle = f$.

Théorème

Soit $\Delta \neq 0$. L'ensemble des classes d'equivalence propre des formes quadratiques binaires de discriminant Δ est un groupe abélien fini. L'élément neutre du groupe est la classe principale. L'inverse de f est la classe de toute forme improprement équivalente à f.

Démonstration: Soit $f =< a, b, c >$.

- <u>Commutativité</u>: C'est clair par définition.

- <u>Elément neutre</u>: On a $\begin{pmatrix} 1 & 0 \\ \frac{b-\varepsilon}{2} & 1 \end{pmatrix} f_0 = \langle 1, b, ac \rangle$, ce qui est une forme concordante avec $f = \langle a, b, c \rangle$, et $f * \langle 1, b, ac \rangle = f$.

- <u>Inverse</u>: Nous avons $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \langle a, b, c \rangle = \langle c, b, a \rangle$, ce qui est une forme concordante avec f et $f * \langle c, b, a \rangle = \langle ac, b, 1 \rangle \approx f_0$.

•<u>Associativé</u>: Soient C_1, C_2, C_3 trois classes d'équivalence. Nous commençons par trouver, au moyen du lemme ci-dessus, des formres $g_i =< a_i, b_i, c_i >\in C_i$ telles que pgcd$(a_1, a_2) = 1$, $pgcd(a_1 a_2, a_3) = 1$.

•<u>Associativé</u>: Soient C_1, C_2, C_3 trois classes d'équivalence. Nous commençons par trouver, au moyen du lemme ci-dessus, des formres $g_i =< a_i, b_i, c_i >\in C_i$ telles que $\text{pgcd}(a_1, a_2) = 1$, $pgcd(a_1 a_2, a_3) = 1$.

Prenons ensuite des entiers n_j tels que $b_j + 2a_j n_j = B$ pour un entier B indépendant de j, et des formes $f_j = \begin{pmatrix} 1 & 0 \\ n_j & 1 \end{pmatrix} g_j = \langle a_j, B, C_j \rangle$. Alors,

$$f_1 * (f_2 * f_3) = f_1 * \langle a_2 a_3, B, C \rangle = \langle a_1 a_2 a_3, B, C/a_1 \rangle,$$

et

$$(f_1 * f_2) * f_3 = \langle a_1 a_2, B, C' \rangle * f_3 = \langle a_1 a_2 a_3, B, C/a_1 \rangle.$$

Algorithme du composition

Soient $f = \langle a, b, c \rangle$ et $f' = \langle a', b', c' \rangle$ de discriminant Δ.

Soit $\delta =$pgdc$\left(a, a', \frac{b+b'}{2}\right) = au + a'v + \frac{b+b'}{2}w$,

où les éléments u, v, w trouvés par Bezout ne sont pas uniques. Alors,

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

où $A = \frac{aa'}{\delta^2}$, $B = \frac{1}{\delta}(aub' + a'vb + w(bb' + \Delta)/2)$, et $C = \frac{B^2 - \Delta}{4A}$.

Exemple

$\Delta = -264 = 4(-2 \cdot 3 \cdot 11)$

b	$(b^2 - \Delta)/4$	a	c
0	66	$1, 2, 3, 6$	$66, 33, 22, 11$
2	67		
4	70	$5, 7$	$14, 10$
6	75		
8	82		

Par conséquent, $h^+_\Delta = 8$, et un ensemble de représentants de $Cl(\Delta)^+$ est donné par l'ensemble

$$\left\{ \begin{array}{llll} I = \langle 1, 0, 66 \rangle, & f_1 = \langle 2, 0, 33 \rangle, & f_2 = \langle 3, 0, 22 \rangle, & f_3 = \langle 6, 0, 11 \rangle, \\ f_4 = \langle 5, 4, 14 \rangle, & f_5 = \langle 5, -4, 14 \rangle, & f_6 = \langle 7, 4, 10 \rangle, & f_7 = \langle 7, -4, 10 \rangle \end{array} \right\}$$

Dénotons par $\mathcal{I}$ la classe de I et par C_i la classe de f_i.

- $C_1 * C_1 =?$

$\delta = 2 = 1 \cdot 2 + 0 \cdot 2 + 0 \cdot 0$; donc $u = 1, v = w = 0$. Alors, $A = 4$, $B = 0$, $C = 66$, et $C_1 * C_1 = \mathcal{I}$.

- $C_1 * C_1 = ?$

$\delta = 2 = 1 \cdot 2 + 0 \cdot 2 + 0 \cdot 0$; donc $u = 1, v = w = 0$. Alors, $A = 4$, $B = 0$, $C = 66$, et $C_1 * C_1 = \mathcal{I}$.

- $C_4 * C_4 = ?$

$\delta = 1 = 1 \cdot 5 + 0 \cdot 5 - 1 \cdot 4$; donc $u = 1, v = 0, w = -1$. Alors, $A = 25$, $B = 144$, $C = 210$. De plus,

$$\langle 25, 144, 210 \rangle \approx \langle 210, -144, 25 \rangle \approx \langle 25, -6, 3 \rangle \approx \langle 3, 0, 22 \rangle.$$

Donc, $C_4 * C_4 = C_2$.

- $C_2 * C_5 =?$

$\delta = 1 = 2 \cdot 3 - 1 \cdot 5 + 0 \cdot 2$, donc $u = 3, v = -1, w = 0$.
Alors $A = 15$, $B = -24$, $C = 14$. De plus,

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

Donc, $C_2 * C_5 = C_4$.

$Cl^+(-264)$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
$\mathcal{I}$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_1	C_1	$\mathcal{I}$	C_3	C_2	C_7	C_6	C_5	C_4
C_2	C_2	C_3	$\mathcal{I}$	C_1	C_5	C_4	C_7	C_6
C_3	C_3	C_2	C_1	$\mathcal{I}$	C_6	C_7	C_4	C_5
C_4	C_4	C_7	C_5	C_6	C_2	$\mathcal{I}$	C_1	C_3
C_5	C_5	C_6	C_4	C_7	$\mathcal{I}$	C_2	C_3	C_1
C_6	C_6	C_5	C_7	C_4	C_1	C_3	C_2	$\mathcal{I}$
C_7	C_7	C_4	C_6	C_5	C_3	C_1	$\mathcal{I}$	C_2

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
$\mathcal{I}$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_1	C_1	$\mathcal{I}$	C_3	C_2	C_7	C_6	C_5	C_4
C_2	C_2	C_3	$\mathcal{I}$	C_1	C_5	C_4	C_7	C_6
C_3	C_3	C_2	C_1	$\mathcal{I}$	C_6	C_7	C_4	C_5
C_4	C_4	C_7	C_5	C_6	C_2	$\mathcal{I}$	C_1	C_3
C_5	C_5	C_6	C_4	C_7	$\mathcal{I}$	C_2	C_3	C_1
C_6	C_6	C_5	C_7	C_4	C_1	C_3	C_2	$\mathcal{I}$
C_7	C_7	C_4	C_6	C_5	C_3	C_1	$\mathcal{I}$	C_2

$\mathrm{Cl}^+(-264) \not\simeq D_8$ car D_8 n'est pas abélien.

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
$\mathcal{I}$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_1	C_1	$\mathcal{I}$	C_3	C_2	C_7	C_6	C_5	C_4
C_2	C_2	C_3	$\mathcal{I}$	C_1	C_5	C_4	C_7	C_6
C_3	C_3	C_2	C_1	$\mathcal{I}$	C_6	C_7	C_4	C_5
C_4	C_4	C_7	C_5	C_6	C_2	$\mathcal{I}$	C_1	C_3
C_5	C_5	C_6	C_4	C_7	$\mathcal{I}$	C_2	C_3	C_1
C_6	C_6	C_5	C_7	C_4	C_1	C_3	C_2	$\mathcal{I}$
C_7	C_7	C_4	C_6	C_5	C_3	C_1	$\mathcal{I}$	C_2

$\mathrm{Cl}^+(-264) \not\simeq D_8$ car D_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq Q_8$ car Q_8 n'est pas abélien.

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
$\mathcal{I}$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_1	C_1	$\mathcal{I}$	C_3	C_2	C_7	C_6	C_5	C_4
C_2	C_2	C_3	$\mathcal{I}$	C_1	C_5	C_4	C_7	C_6
C_3	C_3	C_2	C_1	$\mathcal{I}$	C_6	C_7	C_4	C_5
C_4	C_4	C_7	C_5	C_6	C_2	$\mathcal{I}$	C_1	C_3
C_5	C_5	C_6	C_4	C_7	$\mathcal{I}$	C_2	C_3	C_1
C_6	C_6	C_5	C_7	C_4	C_1	C_3	C_2	$\mathcal{I}$
C_7	C_7	C_4	C_6	C_5	C_3	C_1	$\mathcal{I}$	C_2

$\mathrm{Cl}^+(-264) \not\simeq D_8$ car D_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq Q_8$ car Q_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq \mathbb{Z}/8\mathbb{Z}$ car il n'y a aucun élément d'ordre 8.

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
$\mathcal{I}$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_1	C_1	$\mathcal{I}$	C_3	C_2	C_7	C_6	C_5	C_4
C_2	C_2	C_3	$\mathcal{I}$	C_1	C_5	C_4	C_7	C_6
C_3	C_3	C_2	C_1	$\mathcal{I}$	C_6	C_7	C_4	C_5
C_4	C_4	C_7	C_5	C_6	C_2	$\mathcal{I}$	C_1	C_3
C_5	C_5	C_6	C_4	C_7	$\mathcal{I}$	C_2	C_3	C_1
C_6	C_6	C_5	C_7	C_4	C_1	C_3	C_2	$\mathcal{I}$
C_7	C_7	C_4	C_6	C_5	C_3	C_1	$\mathcal{I}$	C_2

$\mathrm{Cl}^+(-264) \not\simeq D_8$ car D_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq Q_8$ car Q_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq \mathbb{Z}/8\mathbb{Z}$ car il n'y a aucun élément d'ordre 8.
$\mathrm{Cl}^+(-264) \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, C_5 est d'ordre 4.

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
$\mathcal{I}$	$\mathcal{I}$	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_1	C_1	$\mathcal{I}$	C_3	C_2	C_7	C_6	C_5	C_4
C_2	C_2	C_3	$\mathcal{I}$	C_1	C_5	C_4	C_7	C_6
C_3	C_3	C_2	C_1	$\mathcal{I}$	C_6	C_7	C_4	C_5
C_4	C_4	C_7	C_5	C_6	C_2	$\mathcal{I}$	C_1	C_3
C_5	C_5	C_6	C_4	C_7	$\mathcal{I}$	C_2	C_3	C_1
C_6	C_6	C_5	C_7	C_4	C_1	C_3	C_2	$\mathcal{I}$
C_7	C_7	C_4	C_6	C_5	C_3	C_1	$\mathcal{I}$	C_2

$\mathrm{Cl}^+(-264) \not\simeq D_8$ car D_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq Q_8$ car Q_8 n'est pas abélien.
$\mathrm{Cl}^+(-264) \not\simeq \mathbb{Z}/8\mathbb{Z}$ car il n'y a aucun élément d'ordre 8.
$\mathrm{Cl}^+(-264) \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, C_5 est d'ordre 4.
$\mathrm{Cl}^+(-264) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq < C_1 > \times < C_5 >$.

Bibliographie

• D. Buell, *Binary quadratic forms*, Springer-Verlag, 1989. (C'est le premier volume à consulter. Les notes de cours sont basées sur ce volume; on y trouve aussi les preuves omises. Cependant ce volume contient plusieurs coquilles.)

• J. Buchmann, *Binary quadratic forms: an algorithmic approach*, Springer-Verlag, 2007.

• D. Cox, *Primes of the form* $x^2 + ny^2$, J. Wiley & sons, 1989. (Très beau volume traitant de la théorie du corps de classes. Le premier chapitre contient une introduction aux formes quadratiques binaires.)

• Alain Faisant, *L'équation diophantienne du second degré*. (En français.)

• D. Flath, *Introduction to Number Theory*, J. Wiley & sons, 1989.
(C'est une très belle introduction à la théorie des nombres, dans lequel on y trouve une belle présentation des formes quadratiques. Le volume se veut une préparation pour lire les *Disquisitiones Arithmeticae* de Gauss.)

• F. Gauss, *Disquisitiones Arithmeticae*, 1801.
La version originale est en latin, mais il existe des versions françaises et anglaises.)

• P. Ribenboim, *My numbers, my friends*, Springer-Verlag, 2000.
(Il contient un bon survol de la théorie des formes quadratiques, sans les preuves mais avec des exemples.