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 $f_2 = \langle a_2, b, a_1c >\rangle$ 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 $pgcd(m, M) = 1$.

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 $pgcd(a_1, a_2) = pgcd(a_1 a_2, M) = 1$.

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 $(a_2, a_1 M) = 1$. 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

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

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 $\mathrm{pgcd}(a_1, a_2') = 1$. 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. 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.

• 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 $f * \langle 1, b, ac \rangle = f$.

• Inverse: 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 $f * \langle c, b, a \rangle = \langle ac, b, 1 \rangle \approx f_0$.

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

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 $C_1 * C_1 = \mathcal{I}$.

• $C_4 * C_4 =?$
$\delta = 1 = 1 \cdot 5 + 0 \cdot 5 - 1 \cdot 4$; 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, $C_2 * C_5 = C_4$.

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	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.

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	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.

Groupe de classes de formes quadratiques
Exemple

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	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.

Groupe de classes de formes quadratiques
Exemple

$\mathrm{Cl}^+(-264)$	$\mathcal{I}$	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.