§2. Formes quadratiques réduites

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

LEMME 2. *Il n'y a qu'un nombre fini de triplets de nombres entiers* (a, b, c) *tels que* $b^2 - 4ac = -d$ *et* $|b| \leqslant a \leqslant c$.

Démontrons le lemme 1. Soit $ax^2 + bxy + cy^2$ une forme quadratique appartenant à la classe C considérée. Par hypothèse cette forme est positive, de sorte que $a > 0$ et $c > 0$. Les changements de variables $(x, y) \mapsto (x - \varepsilon y, y)$ et $(x, y) \mapsto (x, y - \varepsilon x)$, où ε est le signe de b, ont pour effet de remplacer (a, b, c) par $(a, b - 2\varepsilon a, a + c - |b|)$ et par $(a + c - |b|, b - 2\varepsilon c, c)$. Si donc $|b| > a$ ou $|b| > c$, on peut remplacer $ax^2 + bxy + cy^2$ par une forme équivalente pour laquelle la quantité $a + c$ est strictement plus petite. Après un nombre fini de substitutions de ce type, on trouve une forme $ax^2 + bxy + cy^2$ dans C pour laquelle $|b| \leqslant a$ et $|b| \leqslant c$. Cette forme, ou la forme $cx^2 - bxy + ay^2$ qui s'en déduit par le changement de variables $(x, y) \mapsto (y, -x)$, remplit les conditions du lemme 1.

Démontrons le lemme 2. Si (a, b, c) sont comme dans l'énoncé de ce lemme, on a

$$d = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2, \tag{3}$$

de sorte que a ne peut prendre qu'un nombre fini de valeurs; il en est alors de même de b et de c, puisque $|b| \leqslant a$ et $c = (b^2 + d)/4a$.

§ 2. FORMES QUADRATIQUES RÉDUITES [1]

Dans ce paragraphe, nous montrons comment la *théorie de la réduction* de Gauss permet de sélectionner un représentant dans chaque classe C de formes quadratiques de discriminant $-d$.

Nous savons déjà que C contient une forme quadratique $ax^2 + bxy + cy^2$ telle que $|b| \leqslant a \leqslant c$ (lemme 1 du § 1). Peut-il y avoir plusieurs formes de ce type dans C? En fait, la seule autre possible est $ax^2 - bxy + cy^2$, lorsqu'elle est dans C. Ceci vient du fait que $|b|$ est déterminé par a et c (on a $b^2 - 4ac = -d$), et que a, c sont caractérisés par le fait que pour toute forme quadratique $q \in C$, on a

$$a = \inf\big(q(\mathbf{u})\big) \qquad (\mathbf{u} \neq 0 \text{ dans } \mathbf{Z}^2)\,; \tag{4}$$

$$ac = \inf\big(q(\mathbf{u})q(\mathbf{v})\big) \qquad (\mathbf{u}, \mathbf{v} \text{ non colinéaires dans } \mathbf{Z}^2)\,. \tag{5}$$

Il nous suffit en effet de vérifier (4) et (5) pour une seule forme quadratique $q \in C$, par exemple la forme $ax^2 + bxy + cy^2$ elle-même. Mais

[1] C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 171 et 172.

pour celle-ci, on a $q(1, 0) = a$, $q(0, 1) = c$ et $q(x, y) \geqslant ax^2 - |b||xy| + cy^2 \geqslant (2a-|b|)|xy| + (c-a)y^2$, d'où

$$(6) \qquad \begin{aligned} &q(x, 0) \geqslant a\,, && \text{si} \quad x \neq 0 \\ &q(0, y) \geqslant c\,, && \text{si} \quad y \neq 0 \\ &q(x, y) \geqslant (2a-|b|) + (c-a) = a + c - |b| \geqslant c && \text{si} \quad xy \neq 0\,, \end{aligned}$$

et donc les égalités (4) et (5).

Voyons maintenant dans quels cas la forme $ax^2 - bxy + cy^2$ appartient à la classe C:

Lemme. *Pour que la forme* $q(x, y) = ax^2 + bxy + cy^2$ *(avec* $|b| \leqslant a \leqslant c$*) soit équivalente à la forme* $q'(x, y) = ax^2 - bxy + cy^2$, *il faut et il suffit que l'on ait* $a = |b|$, $a = c$ *ou* $b = 0$.

On a $q(x, y) = q'(x \pm y, y)$ si $a = \pm b$, $q(x, y) = q'(y, -x)$ si $a = c$, $q(x, y) = q'(x, y)$ si $b = 0$. Supposons $0 < |b| < a < c$. S'il existe $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$ tel que $q'(x, y) = q(\alpha x + \beta y, \gamma x + \delta y)$, on a $q(\alpha, \gamma) = a$ et $q(\beta, \delta) = c$, d'où $\gamma = 0$ puis $\beta = 0$ en appliquant (6), et finalement $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm I$, ce qui est absurde.

L'étude qui précède nous conduit à adopter la définition suivante: une forme quadratique $ax^2 + bxy + cy^2$ est dite *réduite* si l'on a

$$\begin{aligned} &|b| \leqslant a \leqslant c \\ &b \geqslant 0 \quad \text{si} \quad a \text{ est égal à } |b| \text{ ou à } c\,. \end{aligned}$$

Nous avons alors prouvé le théorème suivant:

Théorème. *Chaque classe de formes quadratiques de discriminant* $-d$ *contient une unique forme réduite.*

La démonstration du lemme 1 du § 1 fournit en fait un algorithme permettant d'obtenir la forme quadratique réduite équivalente à une forme donnée.

Exemple. Appliqué à la forme quadratique $9x^2 + 43xy + 53y^2$ (représentée par (9, 43, 53) pour abréger), cet algorithme s'écrit

$$(9, 43, 53) \sim (9, 25, 19) \sim (9, 7, 3) \sim (5, 1, 3) \sim (3, -1, 5)$$

et $3x^2 - xy + 5y^2$ est la forme réduite cherchée.