§1. FINITUDE DU NOMBRE DE CLASSES

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **25.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'exposé est divisé en deux parties:

Les résultats exposés dans la première partie sont dus pour l'essentiel à Gauss [1]). On y montre pour commencer qu'il n'y a qu'un nombre *fini* de classes de formes quadratiques de discriminant $\Delta < 0$ donné (§ 1). On donne un algorithme simple permettant d'obtenir un *système de représentants* de ces classes, et de calculer le *nombre* $\tilde{h}(\Delta)$ *de telles classes* (§ 2 et § 3). Une des découvertes fondamentales de Gauss est l'existence d'une structure de *groupe abélien* naturelle sur l'ensemble $Cl(\Delta)$ des classes de formes quadratiques *primitives* de discriminant Δ (*primitives* signifie *telles que* $\mathrm{pgcd}(a, b, c) = 1$): cette structure de groupe est décrite au § 4; le lien avec l'arithmétique des *corps quadratiques imaginaires* est exposé aux § 4 et § 5.

En dressant une table des nombres de classes, Gauss constate expérimentalement que ces nombres semblent tendre vers $+\infty$ lorsque le discriminant tend vers $-\infty$ (en satisfaisant à (2)). Il faudra attendre plus de cent ans, avec les travaux de Heilbronn en 1934, pour voir cette assertion démontrée. Se pose alors la question de dresser, pour les petites valeurs de h entier $\geqslant 1$, la liste complète des $\Delta < 0$ tels que $\tilde{h}(\Delta) = h$. C'est essentiellement l'histoire (sans démonstrations) des progrès récents obtenus sur cette question qui fait l'objet de la seconde partie de l'exposé. Nous expliquerons le rôle joué par les courbes elliptiques dans ces progrès.

I. La classification de Gauss des formes quadratiques

§ 1. Finitude du nombre de classes [2])

Théorème. *Soit* d *un entier* $\geqslant 1$. *Il n'y a qu'un nombre fini de classes de formes quadratiques de discriminant* $-d$.

Ce théorème résulte des deux lemmes suivants:

Lemme 1. *Toute classe contient une forme quadratique* $ax^2 + bxy + cy^2$ *telle que* $|b| \leqslant a \leqslant c$.

---

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, 1801 (Werke, t. I), Section cinquième. (Traduction française par A.-C.-M. Poullet-Delisle, parue en 1807.) Dans cet ouvrage, Gauss suppose les formes $ax^2 + bxy + cy^2$ paires, c'est-à-dire telles que b soit pair. Le cas général s'y ramène facilement, en remplaçant $ax^2 + bxy + cy^2$ par $2ax^2 + 2bxy + 2cy^2$ lorsque b est impair.

[2]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 174.

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

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

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

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.