Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 34 (1988)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LE PROBLÈME DE GAUSS SUR LE NOMBRE DE CLASSES
Autor: Oesterlé, J.
Kapitel: §4. Le groupe des classes
DOI: https://doi.org/10.5169/seals-56588

L'étude des formes quadratiques se ramène facilement à celle des formes *primitives*, c'est-à-dire celles dont les coefficients ont 1 pour plus grand commun diviseur. En effet, si $-d < 0$ est congru à 0 ou à 1 modulo 4, il existe un plus grand entier F tel que $-d$ s'écrive $-d_0F^2$ avec $-d_0$ congru à 0 ou 1 modulo 4. Pour toute classe C de formes quadratiques de discriminant $-d$, il existe un diviseur $f \geqslant 1$ de F et une classe C' de formes quadratiques primitives de discriminant $-df^{-2}$ tels que $C = fC'$.

Les nombres de classes $\tilde{h}$ et les nombres de classes primitives h sont donc reliés par l'égalité

$$\tilde{h}(-d) = \sum_{f|F} h(-df^{-2}) . \tag{8}$$

Lorsque F est égal à 1, ce qui équivaut à dire que d n'est pas divisible par le carré d'un nombre premier impair et est congru à 3 (mod. 4), à 4 (mod. 16) ou à 8 (mod. 16), on dit que $-d$ est un *discriminant fondamental*. Toute forme de discriminant $-d$ est alors primitive et on a $\tilde{h}(-d) = h(-d)$.

§ 4. Le groupe des classes [1])

Cherchant à généraliser la formule classique

$$(x^2+y^2)(x'^2+y'^2) = (xx'-yy')^2 + (xy'+yx')^2 ,$$

Gauss se demande pour quels couples (q, q') de formes quadratiques, il existe une forme quadratique q'' telle que l'on ait une identité

$$q(x, y)q'(x', y') = q''(x'', y'') ,$$

où x'' et y'' sont des combinaisons linéaires à coefficients entiers de xx', xy', yx' et yy'.

Si l'on a une identité du type précédent, et si $-d$, $-d'$, $-d''$ désignent les discriminants de q, q', q'', le carré du déterminant de l'application linéaire $(x, y) \mapsto (x'', y'')$ (resp. $(x', y') \mapsto (x'', y'')$) est égal à $dq'(x', y')^2/d''$ (resp. $d'q(x, y)^2/d''$).

Gauss montre que lorsque q et q' sont des formes primitives de même discriminant $-d$, il est possible d'obtenir une identité du type ci-dessus, avec q'' forme primitive de discriminant $-d$, et

$$q'(x', y') = \det\big((x, y) \mapsto (x'', y'')\big) , \quad q(x, y) = \det\big((x', y') \mapsto (x'', y'')\big) .$$

---

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 234 à 243.

Il montre de plus que, sous ces conditions, la classe C'' de q'' ne dépend que des classes C, C' de q, q', et que la loi de composition qui à (C, C') associe C'' définit sur l'ensemble $Cl(-d)$ des classes de formes primitives de discriminant $-d$ une structure de groupe abélien.

De nos jours, on préfère introduire la loi de composition précédente en interprétant $Cl(-d)$ comme un ensemble de classes d'idéaux fractionnaires inversibles. Pour cela, introduisons l'ensemble $\mathcal{O}(-d)$ des nombres complexes de la forme $(u + iv\sqrt{d})/2$, où u et v sont des nombres entiers et $u \equiv vd \pmod 2$. C'est un sous-anneau de $\mathbf{C}$, dont le corps des fractions est $K = Q + Qi\sqrt{d}$.

Un *réseau* de K est un sous-groupe de K qui admet une base sur $\mathbf{Z}$ formée de deux éléments. On dit qu'un réseau L de K est un $\mathcal{O}(-d)$-*idéal fractionnaire inversible* si $\mathcal{O}(-d)$ est l'ensemble des $\alpha \in K$ tels que $\alpha L \subset L$. Cela équivaut à dire que L est stable par multiplication par les éléments de $\mathcal{O}(-d)$, et est un $\mathcal{O}(-d)$-module projectif (nécessairement de rang 1). On vérifie que cela équivaut aussi à l'existence d'un nombre rationnel $\lambda > 0$ tel que $L\overline{L} = \lambda\mathcal{O}(-d)$, avec $\overline{L}$ le réseau conjugué de L. Ce nombre λ est alors noté $N(L)$ et appelé *norme* de L.

Les $\mathcal{O}(-d)$-idéaux fractionnaires inversibles forment un *groupe abélien* pour la loi de composition $(L, L') \mapsto LL'$ (si $L\overline{L} = \lambda\mathcal{O}(-d)$ et $L'\overline{L'} = \lambda'\mathcal{O}(-d)$, on a $LL'(\overline{LL'}) = \lambda\lambda'\mathcal{O}(-d)$); son élément neutre est $\mathcal{O}(-d)$ et l'opposé de L est $N(L)^{-1}\overline{L}$. Les $\mathcal{O}(-d)$-idéaux fractionnaires inversibles de la forme $\lambda\mathcal{O}(-d)$ avec $\lambda \in K^\times$ sont dits *principaux* et forment un sous-groupe du groupe précédent. Le groupe quotient est *le groupe des classes de* $\mathcal{O}(-d)$-*idéaux fractionnaires inversibles.* Il s'identifie canoniquement au groupe $\mathrm{Pic}(\mathcal{O}(-d))$ des classes de $\mathcal{O}(-d)$-modules projectifs de rang 1.

Etant donné un $\mathcal{O}(-d)$-idéal fractionnaire inversible L, et une base (ω_1, ω_2) d'orientation positive de L sur $\mathbf{Z}$, la forme quadratique $q(x, y) = N(L)^{-1} \mid x\omega_1 + y\omega_2 \mid^2$ est à coefficients entiers, primitive et de discriminant $-d$: cela résulte facilement de l'égalité $L\overline{L} = N(L)\mathcal{O}(-d)$. Inversement, étant donnée une forme quadratique $ax^2 + bxy + cy^2$ primitive et de discriminant $-d$, le réseau L de K engendré par a et $(b + i\sqrt{d})/2$ est un $\mathcal{O}(-d)$-idéal fractionnaire inversible, car on a $L\overline{L} = a\mathcal{O}(-d)$. On vérifie que les constructions précédentes définissent par passage au quotient des *isomorphismes réciproques l'un de l'autre* entre le groupe des classes de $\mathcal{O}(-d)$-idéaux fractionnaires inversibles et $Cl(-d)$, muni de la structure de groupe définie par Gauss.

L'*élément neutre* de $Cl(-d)$ est la classe de la forme $x^2 + (d/4)y^2$ si $d \equiv 0 \pmod 4$, celle de la forme $x^2 + xy + ((d+1)/4)y^2$ si $d \equiv 3 \pmod 4$. L'*opposé* de la classe de $ax^2 + bxy + cy^2$ est celle de $ax^2 - bxy + cy^2$. Le lemme du § 2 permet donc de dresser la liste des éléments d'ordre $\leqslant 2$ de $Cl(-d)$ (appelés *classes ambiguës* ou *ambiges*); le nombre de ces éléments est [1])

$$(9)\qquad \begin{array}{lll} 2^{t-1} & \text{si} & d \not\equiv 12 \bmod 16 \quad \text{et} \quad d \not\equiv 0 \bmod 32 \\ 2^{t-2} & \text{si} & d \equiv 12 \bmod 16 \\ 2^{t} & \text{si} & d \equiv 0 \bmod 32\,, \end{array}$$

où t est le nombre de diviseurs premiers de d.

Pour calculer le produit des classes de deux formes quadratiques $ax^2 + bxy + cy^2$ et $a'x^2 + b'xy + c'y^2$ primitives de discriminant $-d$, on pose [2])

$$\delta = \operatorname{pgcd}(a, a', (b+b')/2)\,,$$

on choisit des entiers u, v et w tels que

$$ua + va' + w(b+b')/2 = \delta\,,$$

et on pose

$$a'' = aa'/\delta^2\,,\quad b'' = [uab' + va'b + w(bb' - d)/2]/\delta\,,\quad c'' = (b''^2 + d)/4a''\,.$$

La forme quadratique $a''x^2 + b''xy + c''y^2$ est alors à coefficients entiers, primitive et de discriminant $-d$, et sa classe est le produit cherché.

En effet, aux classes des deux formes quadratiques données correspondent les classes des $\mathcal{O}(-d)$-idéaux fractionnaires: $L = \mathbf{Z}a + \mathbf{Z}(b + i\sqrt{d})/2$ et $L' = \mathbf{Z}a' + \mathbf{Z}(b' + i\sqrt{d})/2$. L'idéal fractionnaire LL' est engendré par les quatre éléments

$$aa'\,,\ (ab' + ai\sqrt{d})/2\,,\ (a'b + a'i\sqrt{d})/2\,,\ (bb' - d + i(b+b')\sqrt{d})/4$$

et l'on a $N(LL') = aa'$. On vérifie facilement que $\omega_1 = (aa')/\delta$ et $\omega_2 = \delta(b'' + i\sqrt{d})/2$ forment une base de LL' sur $\mathbf{Z}$ d'orientation positive et que l'on a $(aa')^{-1} \mid x\omega_1 + y\omega_2 \mid^2 = a''x^2 + b''xy + c''y^2$, d'où le résultat.

Exemple. Le groupe $Cl(-347)$ est cyclique d'ordre 5 (cf. § 3, exemple). Il est engendré par la classe C de la forme réduite $3x^2 + xy + 29y^2$, et

---

[1]) C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 257 à 259.

[2]) C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 242; cf. aussi le n° 243 pour des méthodes plus rapides de calcul du produit.

$2C$, $3C$, $4C$, $5C$ sont les classes des formes réduites dont les coefficients sont (9, 7, 11), (9, −7, 11), (3, −1, 29) et (1, 1, 87) respectivement.

§ 5. Lien entre $h(-d)$ et $h(-df^2)$ [1])

Soient $-d$ un *discriminant fondamental* (cf. § 3), et f un entier $\geqslant 1$. Les nombres de classes primitives $h(-df^2)$ et $h(-d)$ sont liés par une formule simple. Pour l'établir, nous allons définir un homomorphisme de groupes

$$v: Cl(-df^2) \to Cl(-d)\,.$$

C'est dans le langage des idéaux fractionnaires que cet homomorphisme se définit le plus aisément: à la classe d'un $\mathcal{O}(-df^2)$-idéal fractionnaire L, v fait correspondre la classe de $\mathcal{O}(-d)L$, qui est un $\mathcal{O}(-d)$-idéal fractionnaire.

Pour tout $x \in \mathcal{O}(-d)$, inversible modulo $f\mathcal{O}(-d)$, le réseau $x\mathcal{O}(-d) \cap \mathcal{O}(-df^2)$ est un $\mathcal{O}(-df^2)$-idéal fractionnaire. L'application qui à x associe la classe de cet idéal définit par passage au quotient un homomorphisme de groupes

$$u: \big(\mathcal{O}(-d)/f\mathcal{O}(-d)\big)^\times \to Cl(-df^2)\,.$$

On démontre (en utilisant le fait que « la donnée d'un réseau équivaut à celle de ses localisés ») que la suite

$$\big(\mathcal{O}(-d)/f\mathcal{O}(-d)\big)^\times \xrightarrow{u} Cl(-df^2) \xrightarrow{v} Cl(-d) \to 0$$

est exacte, et que le noyau de u est engendré par les classes des entiers relatifs inversibles modulo f et des unités de $\mathcal{O}(-d)$.

Un argument de comptage permet d'en déduire la formule

$$h(-df^2) = h(-d)w^{-1}f \prod_{\substack{p \mid f \\ p \text{ premier}}} \big(1 - p^{-1}\chi(p)\big)$$

où l'on a posé

$$w = \begin{array}{llll} 3 & \text{si} & d = 3 & \text{et} \quad f \geqslant 2 \\ 2 & \text{si} & d = 4 & \text{et} \quad f \geqslant 2 \\ 1 & \text{sinon}\,, & & \end{array}$$

et où χ désigne le caractère de Dirichlet quadratique $n \mapsto \left(\dfrac{-d}{n}\right)$ associé

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 253 à 256.