Finitude du nombre de classe, lien avec les classes de formes

Pascal Molin

Mars 2004

1 Classes d'idéaux entiers

On adopte les notations suivantes pour ce qui suit :
- $\mathbf{K}$ est un corps de nombres de dimension n.
- $\mathcal{O}_\mathbf{K}$ est son anneau des entiers, on a $\mathcal{O}_\mathbf{K} = \sum_{k=1}^{n} \mathbf{Z}\omega_i$.
- $\mathcal{I}(\mathcal{O}_\mathbf{K})$ désigne l'ensemble des idéaux de $\mathcal{O}_\mathbf{K}$.
- A et B sont des idéaux de $\mathcal{O}_\mathbf{K}$, $A = \sum \alpha_i \mathbf{Z}$.

Définition 1. *Soit I un idéal de $\mathcal{O}_\boldsymbol{K}$. $\mathcal{O}_\boldsymbol{K}/I$ est fini, et son cardinal est appelé la **norme** de I.*

Démonstration :
lemme : $I \cap \boldsymbol{Z} \neq \emptyset$.
En effet, soit $\alpha \in I, \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$ avec $(a_i) \in \mathbf{Z}$, donc $a_n \in I \cap \mathbf{Z}$.

Soit donc $a \in I \cap \mathbf{Z}$, on a $(a) \cap I$, donc une surjection $\mathcal{O}_\mathbf{K}/(a) \to \mathcal{O}_\mathbf{K}/I$. Montrons que $\#(\mathcal{O}_\mathbf{K}/(a)) = a^n$. Soit $\omega \in \mathcal{O}_\mathbf{K}$, $\omega = \sum(q_i a_i\omega_i + r_i\omega_i)$, $0 \leq r_i < a$. Donc on a un système de représentants des classes $C = \{\sum r_i\omega_i, 0 \leq r_i < a\}$, qui est de cardinal a^n. Donc $\mathcal{O}_\mathbf{K}/(a)$ est bien fini.

□

On introduit maintenant une relation d'équivalence sur les idéaux entiers.

Définition 2. *Deux idéaux entiers A et B sont dits équivalents s'il existe deux entiers algébriques α et β tels qu'on ait $(\alpha)A = (\beta)B$. On note alors $A \sim B$.*

On peut alors considérer l'ensemble des classes d'idéaux :

$$\mathcal{C}l(\mathcal{O}_\mathbf{K}) = \mathcal{I}(\mathcal{O}_\mathbf{K})/\sim$$

Théorème 1. *$\mathcal{C}l(\mathcal{O}_\boldsymbol{K})$ est un groupe fini pour la multiplication entre idéaux. On note son cardinal $h_\boldsymbol{K}$.*

Démonstration :

- le produit d'idéaux est compatible avec l'équivalence, si $(\alpha)A = (\beta)B$ et $(\alpha')A' = (\beta')B'$ alors $(\alpha\beta)AB = (\alpha'\beta')A'B'$.
- l'élément neutre est la classe des idéaux principaux. Si $(\alpha)A = (\beta)\mathcal{O}_\mathbf{K}$ alors $A = (\frac{\beta}{\alpha}) \subset \mathcal{O}_\mathbf{K}$ est principal, et la réciproque est évidente.

On a donc un monoïde, il reste donc à montrer l'existence d'un inverse et la finitude. L'existence d'un inverse a été démontrée lors de la dernière séance, mais peut aussi être déduite de la finitude, qui est l'objet du paragraphe suivant. On peut aussi démontrer simplement l'existence de l'inverse dans le cas des corps quadratiques $\mathbf{Q}(\sqrt{d})$ en remarquant que pour $A = u\mathbf{Z} + v\mathbf{Z}$, l'idéal $A\bar{A} = (u\bar{u}, v\bar{v}, u\bar{v}, \bar{u}v)$ est principal. En effet les nombres $u\bar{u}, v\bar{v}, u\bar{v} + \bar{u}v$ sont entiers relatifs car invariants par conjugaison, donc en notant n leur pgcd, on a $(n) \subset A\bar{A}$. Pour l'inclusion réciproque, il faut montrer que n divise $u\bar{v}$ et $\bar{u}v$; on remarque pour cela les quotients sont racines du polynôme unitaire $X^2 - \frac{u\bar{v}+\bar{u}v}{n}X + \frac{u\bar{u}v\bar{v}}{n^2}$, et sont donc rationnels et entiers algébriques, donc entiers, ce qui achève la démonstration. □

Le nombre de classes $h_{\mathbf{K}}$ vaut 1 pour les seuls anneaux principaux, et renseigne sur le caractère plus ou moins principal d'un anneau. La preuve de la finitude du nombre de classes explicite ce lien en majorant le nombre de classes à l'aide d'un nombre lié au caractère plus ou moins euclidien de l'anneau.

Donnons quelques exemples pour illustrer ce résultat et comprendre le mécanisme à l'origine de la finitude du nombre de classes.

Exemples

- $\mathbf{K} = \mathbf{Q}[i]$. Dans ce cas, l'anneau $\mathbf{Z}[i]$ est euclidien, donc principal, donc $h_{\mathbf{Q}[i]} = 1$.
  Le raisonnement est le suivant : On munit $\mathbf{Z}[i]$ d'une division euclidienne : soient α et $\beta \neq 0$ dans $\mathbf{Z}[i]$. Il s'agit de trouver un entier de Gauss ω tel que $|\alpha - \omega\beta| < |\beta|$.t à dire situé dans la boule unité centrée en $\frac{\alpha}{\beta} \in \mathbf{Q}(i)$. Or les parties réelles et imaginaires de tout élémemt du corps sont à distance inférieure à $\frac{1}{2}$ d'un entier, donc l'élément est à distance inférieure à $2 \times (\frac{1}{2})^2 = \frac{1}{2}$ d'un entier algébrique, et la division est possible.
  Ensuite, cette division euclidienne assure que tout élément d'un idéal est multiple d'un élément de module minimal, donc tout idéal est principal et le nombre de classes est $h_{\mathbf{Q}(i)} = 1$.
- $\mathbf{K} = \mathbf{Q}(i\sqrt{5})$. L'anneau des entiers $\mathbf{Z}[i\sqrt{5}]$ n'est cette fois pas principal, mais on peut le munir d'une division euclidienne approchée.
  Soit en effet $\gamma \in \mathbf{Q}(i\sqrt{5})$, on peut écrire $\gamma = E[\gamma]+u(\gamma)+iv(\gamma)\sqrt{5}$, où $E[\gamma]$ est l'entier algébrique le plus proche de γ. On a $|u(\gamma)| \leq \frac{1}{2}$ et $|v(\gamma)| \leq \frac{1}{2}$, ce qui donne $N(\gamma - E[\gamma]) \leq \frac{1}{4} + \frac{5}{4}$, ce qui ne convient pas. En revanche, si on a $|u(\gamma)| \leq \frac{1}{2}$ et $|v(\gamma)| \leq \frac{1}{3}$, alors $N(\gamma - E[\gamma]) \leq \frac{1}{4} + \frac{5}{9} < 1$. Sinon, 2γ vérifie ces conditions. Ainsi, pour tout couple $\alpha, \beta \in \mathbf{Z}[i\sqrt{5}], \beta \neq 0$, on a l'existence de $\omega \in \mathbf{Z}[i\sqrt{5}]$ tel que soit $N(\alpha-\omega\beta) < 1$, soit $N(2\alpha-\omega\beta) < 1$.
  En suivant le même raisonnement que dans le cas $\mathbf{Q}(i)$, on choisit pour chaque idéal entier A un élément $\beta \neq 0$ de A de norme minimale. Pour tout élément $\alpha \in A$,la division nous donne l'existence de ω tel que soit $\alpha = \omega\beta$, soit $2\alpha = \omega\beta$. Donc dans tous les cas, $2\alpha \in (\beta)$, soit $(2)A \subset (\beta)$. Contrairement à la situation précédente, A n'est pas équivalent à (β), mais l'est à $B = (\frac{1}{\beta})(2)A$. Tout idéal est donc équivalent à un idéal contenant

2, et nous pouvons déterminer ces idéaux.

$$\begin{array}{lll} \{B, (2) \subset B\} & \simeq \mathcal{I}(\mathbf{Z}(\sqrt{-5})/(2)) \simeq \mathcal{I}(\mathbf{Z}[X]/(2, X^2+5)) \simeq & \mathcal{I}(\mathbf{Z}/2\mathbf{Z}[X]/(X+1)^2) \\ (2) & \longleftarrow & (1) \\ (2, 1+\sqrt{-5}) & \longleftarrow & (1+X) \end{array}$$

Il reste à vérifier que $(2, 1+\sqrt{-5})$ n'est pas principal, or cet idéal a pour norme 2 qui ne peut correspondre à la norme d'un idéal principal, de la forme a^2+5b^2. Ainsi, $h_{\mathbf{Q}(\sqrt{-5})} = 2$.

Cas général de la finitude du nombre de classes

Proposition 1 (pseudo division euclidienne). *Soit $\boldsymbol{K}$ un corps de nombres.*

$$\exists M_{\boldsymbol{K}}, \forall \alpha, \beta \in \mathcal{O}_{\boldsymbol{K}}, \beta \neq 0, \exists t \in [1 \dots M_{\boldsymbol{K}}, \exists \omega \in \mathcal{O}_{\boldsymbol{K}}, |N(t\alpha - \omega\beta)| < |N(\beta)|.$$

Démonstration :
Il suffit de montrer que $\forall \gamma \in \mathbf{K}, \exists t \leq M_{\mathbf{K}}, |N(t\gamma - \omega)| < 1$. Soit donc $\gamma \in \mathbf{K}, \gamma = \sum \gamma_i \omega_i, \gamma_i \in \mathbf{Q}$. $|N(\gamma)| \leq |\prod(\sum \gamma_i \omega_i^{(j)}) \leq (\max|\gamma_i|)^n C$, où $C = \prod(\sum|\omega_i^{(j)}|)$.

Soit $d \in \mathbf{N}, d > \sqrt[n]{c}$ et $M_{\mathbf{K}} = d^n$. On écrit $\gamma_i = E[\gamma_i] + r(\gamma_i)$ où $0 \leq \gamma_i < 1$ et $E[\gamma] = \sum E[\gamma_i]\omega_i$ est un entier algébrique.

On envoie les $d^n + 1$ points $r(k\gamma) = (r(k\gamma_1), \dots r(k\gamma_n)), k \in [\![0; M]\!]$ dans le cube $[0; 1[^n$, que l'on subdivise en d^n sous-cubes de côté $1/d$. Par principe des tiroirs, deux d'entre eux au moins sont dans un même sous cube, donc il existe $k' > k$ tels que $r(k'\gamma) - r(k\gamma) = r(t\gamma) \in [0; 1/d[^n$, où $t = k' - k \in [\![1; M]\!]$. On a ainsi trouvé un point $t\gamma$ suffisemment proche de l'entier algébrique $E[t\gamma]$, et on a donc : $|N(t\gamma - E[t\gamma])| \leq (\frac{1}{d})^n \times C < 1$ par définition de C, ce qui constitue l'inégalité recherchée. □

Théorème 2. *Le nombre de classes d'idéaux de $\mathcal{O}_{\boldsymbol{K}}$ est fini.*

Démonstration :
Soient $A \in \mathcal{I}(\mathcal{O}_{\mathbf{K}})$ et $\beta \in A \setminus \{0\}$ tel que $|N(\beta)|$ soit minimale. $\forall \alpha \in A, \exists t \in [\![1; M_{\mathbf{K}}]\!], \exists \omega \in \mathcal{O}_{\mathbf{K}}, |N(t\alpha - \omega\beta)| < |N(\beta)|$, donc $t\alpha = \omega\beta$. Donc pour tout α, $M!\alpha \in (\beta)$, d'où $(M!)A \subset (\beta)$. En posant $B = (\frac{1}{\beta})(M!)A \in \mathcal{I}(\mathcal{O}_{\mathbf{K}})$, on a donc $A \sim B$. Or les idéaux entiers qui contiennent $M_{\mathbf{K}}!$ sont en nombre fini, car en bijection avec les idéaux de $\mathcal{O}_{\mathbf{K}}/(M!)$ qui est fini de cardinal $|N(M_{\mathbf{K}}!)| = (M_{\mathbf{K}}!)^n$. Ainsi, $\mathcal{C}l(\mathcal{O}_{\mathbf{K}})$ est fini. □

2 Lien avec les classes de formes quadratiques.

Rappels et notations :
Dans ce qui suit, $\mathbf{K}$ est un corps quadratique $\mathbf{Q}(\sqrt{d})$ de discriminant $\Delta_{\mathbf{K}}$ valant $-d$ (resp. $-4d$) si $d \equiv 1[4]$ (resp. $\equiv 2, 3[4]$).

On considère des formes quadratiques $f(x, y) = ax^2 + bxy + cy^2$, de même discriminant $\Delta_{\mathbf{K}} = b^2 - 4ac$, munies de la relation d'équivalence

$$f \sim g \Leftrightarrow \exists p, q, r, s \in \mathbf{N}, f(x, y) = g(px + qy, rx + sy) \text{ et } \begin{vmatrix} p & q \\ r & s \end{vmatrix} = \pm 1$$

On note $\mathcal{C}l(d)$ l'ensemble des classes de formes quadratiques.

Proposition 2. *A tout idéal $A = u\boldsymbol{Z} + v\boldsymbol{Z}$ de $\mathcal{O}_{\boldsymbol{K}}$, on associe la forme quadratique $f_{u,v} : x, y \longmapsto \frac{N(ux+vy)}{N(A)}$. Alors :*
- *$f_{u,v}$ a pour discriminant $\Delta_{\boldsymbol{K}}$.*
- *Si $A = u'\boldsymbol{Z} + v'\boldsymbol{Z}$, $f_{u',v'} \sim f_{u,v}$.*
- *Si $A \sim B$, alors $f_A \sim f_B$.*

Remarque : Le deuxième point permet de s'abstraire de la base, d'où l'écriture f_A dans le troisième.

Démonstration :

- $N(ux+vy) = N(u)^2x^2 + (u\bar{v} + \bar{u}v)xy + N(v)^2y^2$, donc $N(A)^2\Delta_f = (u\bar{v} + \bar{u}v)^2 - 4N(u)^2N(v)^2 = (u\bar{v} - \bar{u}v)^2 = \Delta(A) = N(A)^2\Delta_{\mathbf{K}}$.
- L'écriture du changement de base $(u', v') \to (u, v)$ fait apparaître un matrice orthogonale, ce qui correspond à l'équivalence des deux formes.
- Il suffit de vérifier l'équivalence pour A et $(\alpha)A$, qui s'obtient sans effort : $\frac{N(\alpha ux+\alpha vy)}{N((\alpha)A)} = \frac{N(\alpha)N(ux+vy)}{N(\alpha)N(A)}$. L'égalité entre la norme d'un entier et de l'idéal qu'il engendre a été traitée lors du précedent exposé, ainsi que la multiplicativité de la norme sur les idéaux qui est générale, mais s'obtient en outre aisément dans le cas particulier de la multiplication par un idéal principal en remarquant la suite exacte : $0 \to \mathcal{O}_{\mathbf{K}}/A \to \mathcal{O}_{\mathbf{K}}/(\alpha A) \to \mathcal{O}_{\mathbf{K}}/(\alpha) \to 0$

□

Cette proposition permet de définir cette application entre les ensembles quotients d'idéaux et de formes quadratiques, et d'énoncer le résultat suivant :

Théorème 3. *On a la surjection suivante :*

$$\begin{cases} \mathcal{C}l(\mathcal{O}_{\boldsymbol{K}}) & \to & \mathcal{C}l(\Delta_{\boldsymbol{K}}) \\ A & \mapsto & \frac{N_{/A}}{N(A)} \end{cases}$$

Démonstration :
L'application est surjective car la forme $ax^2 + bxy + cy^2$ est l'image de $a\mathbf{Z} + \frac{b+\sqrt{\Delta_{\mathbf{K}}}}{2}\mathbf{Z}$, qui est de norme a. □

Exemples :

	Nombre de classes	Formes	Idéaux
$\mathbf{Q}(i)$	$h_{\mathbf{Q}(i)} = 1$	$x^2 + y^2$	(1)
$\mathbf{Q}(\sqrt{-5})$	$h_{\mathbf{Q}(\sqrt{-5})} = 2$	$x^2 + 5y^2$	(1)
		$2x^2 + 2xy + 3y^2$	$(2, 1 + \sqrt{-5})$