

Conclusion: Tout idéal $I \neq \mathcal{O}_K$ est contenu dans un idéal maximal.

Démonstration: Soit $I \neq \mathcal{O}_K$ un idéal.

- * Si I est maximal, alors $I \subseteq \mathfrak{p} = I$.
- * Sinon, il existe un idéal J de $\mathcal{O}_K$ tel que $I \subsetneq J \subsetneq \mathcal{O}_K$. Comme $\mathcal{O}_K$ est noethérien, ce processus s'arrête à un moment, aboutissant à $I \subseteq \mathfrak{p} \leftarrow$ idéal maximal $\square$

Conclusion: Soit $I \neq \{0\}$ un idéal de $\mathcal{O}_K$. Alors $\Phi(I)$ est un réseau de rang n de $V = \mathbb{R}^{2n} \times \mathbb{C}^{2i}$ de covolume

$$\begin{aligned} V(\Phi(I)) &= |\mathcal{O}_K/I| V(\Phi(\mathcal{O}_K)) \\ &= \frac{|\mathcal{O}_K/I|}{2^{2n}} \sqrt{|\text{disc}(K)|} \end{aligned}$$

De plus, il existe un élément non nul

$a \in I$ de taille

$$\lambda(a) \leq \left(\frac{2}{\pi}\right)^{\frac{n}{2}} |\text{disc}(K)|^{\frac{1}{2n}} |\mathcal{O}_K/I|^{\frac{1}{n}}$$

En particulier, il existe $a \in I$ non nul

de norme

$$|N_K(a)| \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\text{disc}(K)|} |\mathcal{O}_K/\mathfrak{I}|$$

Démonstration: on a $\Phi(\mathfrak{I}) \subset \Phi(\mathcal{O}_K)$ et ce dernier est un réseau de rang n . Comme $\mathcal{O}_K/\mathfrak{I}$ est fini, $\Phi(\mathfrak{I})$ est aussi de rang n et son volume est égal à

$$\begin{aligned} V(\Phi(\mathfrak{I})) &= |\mathcal{O}_K/\mathfrak{I}| V(\Phi(\mathcal{O}_K)) \\ &= \frac{|\mathcal{O}_K/\mathfrak{I}| \sqrt{|\text{disc}(K)|}}{2^{r_2}} \end{aligned}$$

par le travail qu'on a déjà fait.

Montrons $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ de la norme $\|(z_1, \dots, z_{r_1+r_2})\| = \max_{1 \leq j \leq r_1+r_2} |z_j|$. Le volume de sa boule unité $(-1, 1)^{r_1} \times B(0, 1)^{r_2}$ est égal à $2^{r_1} \pi^{r_2}$. D'après le théorème de Minkowski, le réseau $\Phi(\mathfrak{I})$ contient un élément non nul $\Phi(a)$ de norme

$$\begin{aligned} \|\Phi(a)\| &\leq 2 \left(\frac{V(\Phi(\mathfrak{I}))}{\text{vol}(B)} \right)^{1/n} \\ &\leq \left(2^{\frac{n-r_1}{2r_2}} \pi^{-r_2} 2^{-r_2} |\mathcal{O}_K/\mathfrak{I}| \sqrt{|\text{disc}(K)|} \right)^{1/n} \end{aligned}$$

$$\leq \left(\frac{2}{\pi}\right)^{22/n} |\text{disc}(K)|^{1/2n} |\mathcal{O}_K/\mathfrak{I}|^{1/n}.$$

Car a est un entier algébrique et que tous ces conjugués sont de module $\leq$ cette quantité, on trouve

$$N_K(a) \leq \left(\frac{2}{\pi}\right)^{22} \sqrt{|\text{disc}(K)|} |\mathcal{O}_K/\mathfrak{I}|$$

□

Définition: Soit $\mathfrak{I}$ un idéal non nul de $\mathcal{O}_K$. On appelle norme de $\mathfrak{I}$ le cardinal

$$N(\mathfrak{I}) = |\mathcal{O}_K/\mathfrak{I}|.$$

Proposition: Pour tout idéal non nul $\mathfrak{I}$ de $\mathcal{O}_K$ et tout élément non nul a de $\mathcal{O}_K$,

$$N(a\mathfrak{I}) = |N_K(a)| \cdot N(\mathfrak{I})$$

En particulier, $N(a\mathcal{O}_K) = |N_K(a)|$.

Démonstration: Soit $(z_1, \dots, z_n)$ une base de $\mathfrak{I}$. Alors $(az_1, \dots, az_n)$ est une base de $a\mathfrak{I}$ et il suffit de vérifier

$$V(\Phi(a\mathfrak{I})) = |N_K(a)| V(\Phi(\mathfrak{I}))$$

⑥

Cette formule résulte de l'égalité

$$(*) \operatorname{disc}(az_1, \dots, az_n) = N_K(a)^2 \operatorname{disc}(z_1, \dots, z_n)$$

car on a vu que le discriminant d'un ordre A de K et le norme f d'un élément fondamental de $\Phi(A)$ sont reliés par

$$|\operatorname{disc}(A)| = 4^{n-2} \operatorname{nl}(f)^2.$$

Pour démontrer $(*)$, on écrit :

$$\operatorname{disc}(az_1, \dots, az_n) = \det(\varphi_i(az_j))^2$$

$$= \det(\varphi_i(a) \varphi_i(z_j))^2$$

$$= \underbrace{(\varphi_1(a) \dots \varphi_n(a))}_{N_K(a)}^2 \det(\varphi_i(z_j))^2$$

$$= N_K(a)^2 \operatorname{disc}(z_1, \dots, z_n) \quad \square$$

Corollaire : Pour qu'un idéal non nul I de $\mathcal{O}_K$ soit principal, il faut et il suffit qu'il existe $a \in I$ tel que

$$N_K(a) = \pm N(I)$$

Dans ce cas, l'élément a est un générateur de l'idéal I , c'est-à-dire $I = a\mathcal{O}_K$.

Démonstration: Si $I = a\mathcal{O}_K$ est principal, alors

$$N(I) = N(a\mathcal{O}_K) = |N_K(a)|$$

et donc $a \in I$ satisfait à $N_K(a) = \pm N(I)$.

Réciproquement, si $a \in I$ satisfait à

$$N_K(a) = \pm N(I), \text{ alors avec } a\mathcal{O}_K \subset I,$$

on trouve l'inégalité

$$N(I) = |\mathcal{O}_K/I| \leq |\mathcal{O}_K/a\mathcal{O}_K| = |N_K(a)|$$

car $\mathcal{O}_K/a\mathcal{O}_K \rightarrow \mathcal{O}_K/I$ est une

surjection, ce qui implique

$$|\mathcal{O}_K/I| = |\mathcal{O}_K/a\mathcal{O}_K|$$

donc $\mathcal{O}_K/a\mathcal{O}_K \cong \mathcal{O}_K/I$, c'est-à-dire
 $I = a\mathcal{O}_K$. En particulier, A est principal. $\square$

Groupe de classes d'idéaux

Soit $\mathcal{I}_K$ l'ensemble des idéaux non nuls de $\mathcal{O}_K$. On définit

$I \sim J$ s'il existe des éléments

non nuls $a, b \in \mathcal{O}_K$ tels que
 $aI = bJ$

C'est une relation d'équivalence:

$$* I \sim I \quad (a=b=1)$$

$$* I \sim J \Rightarrow J \sim I$$

$$* \text{Si } I \sim J \text{ et } J \sim H, \text{ alors}$$

$$aI = bJ$$

$$acI = bdH$$

$$cJ = dH$$

$$\Rightarrow I \sim H$$

Notation: $\mathcal{O}(K)$ l'ensemble des classes d'équivalence.

Lemme: $\mathcal{O}_K$ est principal $\Leftrightarrow \mathcal{O}(K)$ est réduit à un seul élément

Preuve: En effet, si $\mathcal{O}_K$ est principal, alors tout idéal non nul est de la forme $I = a\mathcal{O}_K$ avec $a \in \mathcal{O}_K$ non nul, donc $I \sim \mathcal{O}_K$.

Réciproquement, si $I \sim \mathcal{O}_K$, il existe $a, b \in \mathcal{O}_K$ tels que $aI = b\mathcal{O}_K$. Comme $b \in aI$, il existe $w \in I$ tel que $b = aw$, c'est-à-dire $aI = aw\mathcal{O}_K$, donc $I = w\mathcal{O}_K$. $\square$

Proposition: Posons $c = \left(\frac{2}{\pi}\right)^{n_2} \sqrt{|\text{disc}(K)|}$

Tout idéal non nul de $\mathcal{O}_K$ est équivalent à un idéal de norme $\leq c^n$. En particulier, l'ensemble $\text{Bl}(K)$ est fini.

Démonstration: Pour tout entier $1 \leq t \leq c^n$, les idéaux de $\mathcal{O}_K$ contenant t sont en bijection avec les idéaux de $\mathcal{O}_K/t\mathcal{O}_K$, qui est un anneau fini. (En effet, tout idéal de R/I est de la forme J/I pour un idéal J de R tel que $I \subseteq J \subseteq R$). Démontrons que tout idéal non nul de $\mathcal{O}_K$ est équivalent à un de ces idéaux.

Soit I un tel idéal. Il existe un élément non nul $a \in I$ tel que

$$|N_K(a)| \leq \mathfrak{N}(a)^n = \left(\frac{2}{\pi}\right)^{n_2} \sqrt{|\text{disc}(K)|} |\mathcal{O}_K/I| \\ = c N(I)$$

on a alors $a\mathcal{O}_K \subset I \subset \mathcal{O}_K$, ce qui implique que le cardinal de $I/a\mathcal{O}_K$ est $\leq c$.

$$z_j = \sum_{i=1}^n a_{ij} z_i$$

Soit $Q = X^n + q_1 X^{n-1} + \dots + q_n \in I'[\bar{X}]$

le polynôme caractéristique de la matrice (a_{ij}) .

Alors $Q(1) = 0$ car 1 est valeur propre.

M a alors

$$1 = -q_1 - \dots - q_n \in I',$$

c'est-à-dire $I' = \mathcal{O}_K$, d'où $I = a\mathcal{O}_K$. $\square$

lemma: Pour tout idéal non nul I de $\mathcal{O}_K$ il existe $k \leq h_K$ tel que I^k soit principal.

preuve: Comme $\mathcal{O}_K$ est de cardinal h_K , parmi les idéaux $\mathcal{O}_K, I, I^2, \dots, I^{h_K}$ il y en a au moins deux qui ont la même classe, disons I^m et I^{m+p} avec $0 \leq m < m+p \leq h_K$. Il existe donc $a, b \in \mathcal{O}_K$ tels que $a I^m = b I^{m+p} = b I^p I^m$. D'après le lemme, $b I^p = a \mathcal{O}_K$, ce qui veut dire que I^p est principal. $\square$

Preuve du théorème: $\mathcal{O}(K)$ est fini. Tout ce qui reste à montrer c'est que I idéal non nul admet un inverse. D'après le lemme I^t est principal pour un certain t . En écrivait $I^t = I \cdot I^{t-1}$, on voit que $I \cdot I^{t-1} \sim \mathcal{O}_K$, donc que I^{t-1} est l'inverse de l'idéal I $\square$

Proposition: Si I, I', J sont des idéaux non nuls de $\mathcal{O}_K$ tels que $I \cdot J = I' \cdot J$, alors $I = I'$.

Preuve: En effet, soit J' un idéal non nul de $\mathcal{O}_K$ tel que $J J'$ soit principal, disons $J J' = a \mathcal{O}_K$. Alors:

$$I J J' = I' J J'$$

donc $a I = a I'$, c'est-à-dire $I = I'$ $\square$