

⑨ Factorisation dans les anneaux d'entiers

Soit A un anneau intègre.

Définition. on dit que A est euclidien

s'il existe une fonction

$$j: A \setminus \{0\} \longrightarrow \mathbb{N} = \{0, 1, \dots\}$$

«st euclidien»

telle que:

(1) pour tout $a \in A$ et tout $b \in A \setminus \{0\}$,
il existe $q, r \in A$ tels que

$$a = bq + r \quad \text{et} \quad j(r) < j(b) \\ \text{ou } r = 0.$$

pas
nécessaire

(2) $j(ab) \geq \max(j(a), j(b))$.

Les exemples les plus standards sont $A = \mathbb{Z}$
avec $j = |\cdot|$ et $A = k[X]$ pour un corps k
avec $j = \deg$.

Proposition: Soit A un anneau intègre.

A euclidien $\Rightarrow A$ principal $\Rightarrow A$ factoriel

Tout idéal est
de la forme πA .

Tout $x \in A$ non
nul ni inversible
s'écrit de
manière "unique"
 $\pi_1 \pi_2 \dots \pi_n$

(première implication)

Preuve: Soit A un anneau euclidien pour j
et soit I un idéal non nul. Alors $j(I \setminus \{0\})$
est un sous-ensemble non vide de $\mathbb{N}$, donc il
existe un élément $b \in I \setminus \{0\}$ de plus petit $j(b)$.
Soit $a \in I$. Écrivons $a = bq + r$. Comme
 $r = a - bq \in I$ et $j(r) < j(b)$, on a $a = bq$,
c'est-à-dire $I = bA$. $\square$

Exemples de $A = \mathcal{O}_K$ qui sont euclidiens
pour la norme $N_K: \mathcal{O}_K \rightarrow \mathbb{Z}$

Lemme: Si pour tout $z \in K$ il existe $a \in \mathcal{O}_K$
tel que $N_K(z - a) < 1$, alors $\mathcal{O}_K$ est un
anneau euclidien pour N_K .

Démonstration: Soient $a, b \in \mathcal{O}_K$ avec $b \neq 0$.
Appliquée à $z = \frac{a}{b} \in K$, l'hypothèse donne
l'existence de $q \in \mathcal{O}_K$ tel que $N_K(z - q) < 1$.
Soit $r = a - bq \in \mathcal{O}_K$. Alors $r = b(z - q)$,
donc $N_K(r) = N_K(b) N_K(z - q) < N_K(b)$,
ce qui montre que $\mathcal{O}_K$ est euclidien pour
la norme N_K . $\square$

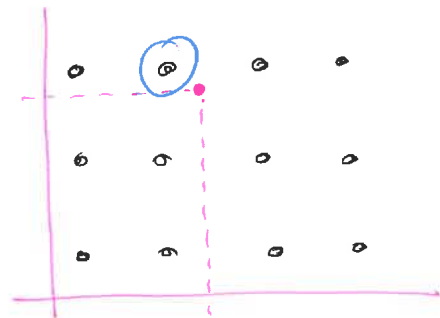
(2)

Exemple 1: $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$ est euclidien

En effet, si $z = x + iy \in \mathbb{Q}(i)$, on définit

$$= \xi + i\eta \quad \text{avec } \xi \text{ et } \eta$$

les entiers les plus proches de x et y respectivement et



$$N_K(z - a) = (x - \xi)^2 + (y - \eta)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

$$\text{car } |x - \xi| \leq \frac{1}{2} \text{ et } |y - \eta| \leq \frac{1}{2}$$

Exemple 2: $K = \mathbb{Q}(e^{\frac{2\pi i}{3}})$, $\mathcal{O}_K = \mathbb{Z}[e^{\frac{2\pi i}{3}}]$ est euclidien. Rappelons que la norme est donnée

$$\begin{aligned} N_K(a + b e^{\frac{2\pi i}{3}}) &= (a + b e^{\frac{2\pi i}{3}})(a + b e^{-\frac{2\pi i}{3}}) \\ &= a^2 + ab(e^{\frac{2\pi i}{3}} + e^{-\frac{2\pi i}{3}}) + b^2 \\ &= a^2 - ab + b^2 \end{aligned}$$

En effet, soit $z = x + iy \in K$ et $a = \xi + i\eta$ avec $\xi, \eta \in \mathbb{Z}$ les entiers les plus proches. Alors:

$$\begin{aligned} N_K(z - a) &= (x - \xi)^2 - (x - \xi)(y - \eta) + (y - \eta)^2 \\ &\leq \frac{3}{4} < 1. \end{aligned}$$

Exemple 3: $K = \mathbb{Q}(\sqrt{-19})$. Comme $-19 \equiv 1 \pmod{4}$,

son anneau d'entiers est $\mathcal{O}_K = \mathbb{Z} \left[\frac{1 + \sqrt{-19}}{2} \right]$. Il n'est pas euclidien. Par l'absurde, soit j un idéal sur $\mathcal{O}_K$. Soit $a \in \mathcal{O}_K$ non nul, non inversible tel que $j(a)$ soit minimal. Soit $z \in \mathcal{O}_K$. Alors $z = aq + r$ avec $r = 0$ ou $j(r) < j(a)$, c'est-à-dire $r = 0$ ou inversible. On en déduit que tout élément de $\mathcal{O}_K$ est ou nul ou à un élément nul ou inversible.

$$\Rightarrow |\mathcal{O}_K / (a)| \leq \underbrace{|\mathcal{O}_K^\times|}_{=3} + 1$$

lemme: $|\mathcal{O}_K / (a)| = N_K(a)$

preuve: $(a) \subset \mathcal{O}_K$ est un réseau de $\mathbb{C} \simeq \mathbb{R}^2$.
 En effet, a et aw forment une base $\mathbb{R}$ -base de $\mathbb{C}$. En particulier,

$$|\mathcal{O}_K / (a)| = \frac{V((a))}{V(\mathcal{O}_K)} = |a|^2 = N(a)$$

car multiplication par a est la conjugaison d'une rationnelle et d'une unité de norme 1.
 uppt $|a|$. □

(3)

Soit $a = x + y\omega$. Alors

$$\begin{aligned} N_K(a) &= \left(x + y \frac{1+\sqrt{-19}}{2}\right) \left(x + y \frac{1-\sqrt{-19}}{2}\right) \\ &= x^2 + xy + 5y^2 \end{aligned}$$

Si $|y| \geq 1$, alors

$$N_K(a) = \underbrace{(x^2 + xy + y^2)}_{\geq 0 \text{ car}} + 4y^2 \geq 4$$

$$(x+y)^2 = x^2 + 2xy + y^2 \geq 0$$

$$x^2 + xy + y^2 \geq -xy$$

Si $|y| = 0$, alors $|x| \geq 2$ car a n'est pas inversible, donc $N_K(a) \geq 4$. Par conséquent :

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ n'est pas euclidien

Remarque: Par une méthode similaire, on montre que $\mathcal{O}_K$ pour $K = \mathbb{Q}(\sqrt{-D})$ avec $D > 0$ est euclidien $\Leftrightarrow D \in \{1, 2, 3, 7, 11\}$. (C'est un résultat de Gauss et I. Sarnak, prouvé en 1971).

Remarque: Par contre, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ est principal.

I déaux d'un anneau d'entiers

Proposition. Soit K un corps de nombres de degré n . Soit $I \subset \mathcal{O}_K$ un idéal non nul. L'anneau $\mathcal{O}_K/I$ est fini et son cardinal $|\mathcal{O}_K/I|$ appartient à I .

Démonstration: Soit $a \in I \setminus \{0\}$. Alors il existe $b \in \mathcal{O}_K$ tel que $N_K(a) = ab$. Comme I est un idéal, $N_K(a) \in I$. Il y a donc une application surjective d'anneaux

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\quad} & \mathcal{O}_K/I \\ \downarrow & & \\ N_K(a) \mathcal{O}_K & \xrightarrow{\quad} & \\ \cong & & \\ (\mathbb{Z}/N_K(a)\mathbb{Z})^n & & \end{array}$$

Ce qui montre que $\mathcal{O}_K/I$ est fini.
Soit $N = |\mathcal{O}_K/I|$. Pour tout $a \in \mathcal{O}_K$, on a alors $N \cdot (a \bmod I) = 0$ par le théorème du degré. En posant $a=1$, on trouve $N \equiv 0 \bmod I$, c'est-à-dire $N \in I$. $\square$

Corollaire: Un idéal premier non nul de $\mathcal{O}_K$ est maximal.

(7)

Démonstration: Soit $I \neq 0$ un idéal premier de $\mathcal{O}_K$. Alors l'anneau $\mathcal{O}_K/I$ est intègre et fini. Si a n'est pas nul, $\mathcal{O}_K/I \rightarrow \mathcal{O}_K/I$ est injectif, donc bijectif car $\mathcal{O}_K/I$ est fini, ce qui signifie que a est inversible. Ainsi, $\mathcal{O}_K/I$ est un corps, c'est-à-dire I est un idéal maximal. $\square$

Corollaire: L'anneau $\mathcal{O}_K$ est noethérien, c'est-à-dire toute suite croissante d'idéaux

$$\dots \subset I_n \subset I_{n+1} \subset \dots$$

de $\mathcal{O}_K$ est arrêtée à partir d'un certain rang.

Démonstration: Par l'absurde, si (I_n) est une suite strictement croissante, pour tout n tel que $I_n \neq 0$, l'ensemble $\mathcal{O}_K/I_n$ est fini et l'inclusion $I_n \subset I_{n+1}$ donne lieu à une surjection $\mathcal{O}_K/I_n \twoheadrightarrow \mathcal{O}_K/I_{n+1}$, qui n'est pas injective car $I_n \neq I_{n+1}$. On a donc

$$|\mathcal{O}_K/I_{n+1}| < |\mathcal{O}_K/I_n|$$

et on obtient une suite d'entiers ≥ 0 strictement décroissante. $\square$

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, d'où l'on a $I \subseteq \mathfrak{p} \leftarrow$ idéal maximal $\square$

Conclusion: Soit $I \neq \{0\}$ un idéal de $\mathcal{O}_K$. Alors $\Phi(I)$ est un réseau de rang n de $V = \mathbb{R}^{2n} \times \mathbb{C}^{2n}$ 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 $\mathfrak{f}$ d'un diviseur premier $\mathfrak{p}$ de $\Phi(A)$ sont reliés par

$$|\operatorname{disc}(A)| = 4^{r_2} \operatorname{nl}(\mathfrak{f})^2.$$

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

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

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

Tout idéal non nul de $\mathcal{O}_K$ est équivalent à un idéal de norme $\leq c$. En particulier, l'ensemble $\mathcal{O}_K$ est fini.

Démonstration: