

Factorisation d'idéaux

Lemme: Soient I et J des idéaux non nuls de $\mathcal{O}_K$. on a

$$I \subset J \Leftrightarrow \text{Il existe un idéal } J' \text{ de } \mathcal{O}_K \text{ tel que } I = J \cdot J'$$

Preuve:

$\boxed{\Leftarrow}$ Si $I = J \cdot J'$, alors I est l'idéal engendré par les produits $a \cdot b$ avec $a \in J, b \in J'$. Comme J est un idéal, $ab \in J$ et $I \subset J$.

$\boxed{\Rightarrow}$ Soit H un idéal tel que $J \cdot H$ soit un idéal principal, disons $\alpha \mathcal{O}_K$ (par exemple, on peut prendre pour H une puissance convenable de J). Comme $I \subset J$, $I \cdot H \subset \alpha \mathcal{O}_K$. La partie $J' = \frac{1}{\alpha} I \cdot H$ est un idéal de $\mathcal{O}_K$, satisfaisant à $\alpha J \cdot J' = I \cdot J \cdot H = \alpha I$, d'où $I = J \cdot J'$ $\square$

Théorème: Tout idéal non nul de $\mathcal{O}_K$ s'écrit de façon unique à l'ordre près comme produit d'idéaux maximaux.

Démonstration: (Existence) Soit I un idéal non nul de $\mathcal{O}_K$. on démontre par récurrence sur $N(I)$ qu'il existe des idéaux maximaux $p_1, \dots, p_t$ de $\mathcal{O}_K$ tels que $I = p_1 \dots p_t$.
Si $N(I) = 1$, alors $I = \mathcal{O}_K$ et on prend le produit vide ($t=0$).

Si $N(I) \geq 2$, alors $I \neq \mathcal{O}_K$ et il reste un idéal maximal p_1 de $\mathcal{O}_K$ tel que $I \subset p_1$. D'après le lemme, il reste un idéal I_1 tel que $I = p_1 I_1$. On a $I \subset I_1$ et l'inclusion est stricte car si $I = I_1$, alors $I = p_1 I$ impliquant $p_1 = \mathcal{O}_K$ d'après le lemme de la dernière fois. On a donc $N(I_1) < N(I)$ et par récurrence il existe des idéaux maximaux $p_2, \dots, p_t$ tels que $I_1 = p_2 \dots p_t$, d'où $I = p_1 \dots p_t$.

(Unité) Il faut démontrer que si

$$p_1 \dots p_t = q_1 \dots q_s \quad (p_i, q_j \text{ maximaux}),$$

alors $t=s$ et il existe une permutation σ de $\{1, \dots, t\}$ telle que $q_i = p_{\sigma(i)}$.

par récurrence sur t , si $t=0$, alors $I = \mathcal{O}_K$.
Si $s > 0$, alors $I = Q_1 \dots Q_s$ implique $I \subset Q_1$,
ce qui est absurde car $Q_1 \neq \mathcal{O}_K$.

Lemme: Soit $\mathcal{Q}$ un idéal premier de $\mathcal{O}_K$
et soient $I_1, \dots, I_n$ des idéaux de $\mathcal{O}_K$ tels
que $I_1 \dots I_n \subset \mathcal{Q}$. Alors il existe $j \in \{1, \dots, n\}$
tel que $I_j \subset \mathcal{Q}$.

Preuve: Il suffit de traiter le cas $n=2$.
(En effet, le cas $n=0$ ne se produit pas; le
cas $n=1$ est évident, et on se ramène à $n=2$
par récurrence). Si $I_1 I_2 \subset \mathcal{Q}$ mais que
 $I_1 \not\subset \mathcal{Q}$, $I_2 \not\subset \mathcal{Q}$, on choisit des éléments
 $a_1 \in I_1 \setminus \mathcal{Q}$, $a_2 \in I_2 \setminus \mathcal{Q}$. Alors $a_1 a_2 \in I_1 I_2 \subset \mathcal{Q}$,
en contradiction avec le fait que $\mathcal{Q}$ est premier $\square$

Traitons le cas $t > 0$. Si $P_1 \dots P_t = Q_1 \dots Q_s$,
alors $Q_1 \dots Q_s \subset P_t$. Par le lemme, il existe
 $j \in \{1, \dots, s\}$ tel que $Q_j \subset P_t$, d'où $Q_j = P_t$
car c'est un idéal maximal. Quant à $\tilde{c}$
rendre les Q_i , on peut supposer $j=s$.

On a alors $p_1 \dots p_{t-1} p_t = q_1 \dots q_{s-1} p_t$,
 d'où $p_1 \dots p_{t-1} = q_1 \dots q_{s-1}$ par la propriété de
 simplification des idéaux. Par récurrence,
 $t=s$ et il reste la permutation voulue $\square$

Conclusion: Si $\mathcal{O}_K$ est factoriel, alors il
 est principal.

Preuve: Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$.
 Soit a un élément non nul de $\mathfrak{p}$ tel
 que $|N_K(a)|$ soit minimal.

On veut: a est irréductible

En effet, si $a = a_1 a_2$, alors soit $a_1 \in \mathfrak{p}$
 soit $a_2 \in \mathfrak{p}$ car $\mathfrak{p}$ est maximal. Supposons
 que $a_1 \in \mathfrak{p}$. Comme $N_K(a) = N_K(a_1) N_K(a_2)$,
 la minimalité de $|N_K(a)|$ entraîne $|N_K(a_2)| = 1$,
 c'est-à-dire a_2 est une unité.

Si $\mathcal{O}_K$ est factoriel, l'idéal engendré par
 un élément irréductible a est premier non
 nul, donc maximal. Alors $a \mathcal{O}_K \subset \mathfrak{p}$ implique

$\mathfrak{p} = a \mathcal{O}_K$ par maximalité de $a \mathcal{O}_K$.

Soit maintenant un idéal I quelconque. Par le théorème, $I = p_1 \dots p_t$ pour des idéaux maximaux p_i et comme chacun est premier, il en va de même pour I . $\square$

Multiplativité des normes d'idéaux

Théorème : Soient I et J des idéaux non nuls de $\mathcal{O}_K$. Alors $N(IJ) = N(I) \cdot N(J)$

On commence par quelques lemmes traitant des cas particuliers.

Lemme : Si $I + J = \mathcal{O}_K$, alors $N(IJ) = N(I)N(J)$.

Preuve : Considérons le morphisme d'anneaux

$$\varphi: \mathcal{O}_K \rightarrow \mathcal{O}_K/I \times \mathcal{O}_K/J$$

on va démontrer qu'il est surjectif de noyau IJ , d'où une isomorphie

$$\mathcal{O}_K/IJ \simeq \mathcal{O}_K/I \times \mathcal{O}_K/J$$

puis $N(IJ) = N(I)N(J)$ en prenant le cardinal des deux côtés.

Surjectivité: comme $I + J = \mathcal{O}_K$, il existe $a \in I$ et $b \in J$ tels que $1 = a + b$. Si $w, z \in \mathcal{O}_K$, alors

$$\begin{aligned}\varphi(bz + aw) &= ([bz + aw]_I, [bz + aw]_J) \\ &= ([bz]_I, [aw]_J) \\ &= ([z - az]_I, [w - bw]_J) \\ &= ([z]_I, [w]_J)\end{aligned}$$

Noyau: Soit $z \in \ker \varphi = I \cap J$. Écrivons $z = z(a + b) = az + zb$. Comme $z \in J$, $az \in I \cdot J$. Comme $z \in I$, $zb \in I \cdot J$, donc $z \in I \cdot J$. Réciproquement, si $z \in I \cdot J$, alors $z \in I$ et $z \in J$. $\square$

Lemme: Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$. Alors $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$ pour tout $e \geq 0$.

Preuve: Au vu de la suite $\mathfrak{p}^{e+1} \subset \mathfrak{p}^e \subset \mathcal{O}_K$, $N(\mathfrak{p}^{e+1}) = N(\mathfrak{p}^e) \cdot |\mathfrak{p}^e / \mathfrak{p}^{e+1}|$ et il suffit donc de montrer $N(\mathfrak{p}) = |\mathfrak{p} / \mathfrak{p}^{e+1}|$.

L'inclusion $\mathfrak{p}^{e+1} \subset \mathfrak{p}^e$ est stricte par l'unicité de la décomposition en produit d'idéaux premiers. Soit $a \in \mathfrak{p}^e \setminus \mathfrak{p}^{e+1}$. Soit

$$\varphi: \mathcal{O}_K \longrightarrow \mathcal{P}^e / \mathcal{P}^{e+1}$$

$$z \longmapsto [az]_{\mathcal{P}^{e+1}}$$

qui est une surjection de groupes abéliens. Son noyau $\mathcal{A} = \ker \varphi$ est un idéal car

$$\varphi(1z) = [a1z]_{\mathcal{P}^{e+1}} = [1]_{\mathcal{P}^{e+1}} [az]_{\mathcal{P}^{e+1}} = 0$$

pour tout $1 \in \mathcal{O}_K$. Il contient $\mathcal{P}$, d'où $\mathcal{P} \subset \mathcal{A} \subsetneq \mathcal{O}_K$, donc $\mathcal{P} = \mathcal{A}$ car $\mathcal{P}$ est maximal.

Démontrons que φ est surjectif. Soit $\mathcal{J} = \mathcal{P}^{e+1} + a\mathcal{O}_K$. Comme $\mathcal{J}$ contient $\mathcal{P}^{e+1}$, il existe un idéal $\mathcal{J}'$ tel que $\mathcal{P}^{e+1} = \mathcal{J}\mathcal{J}'$. On a donc $\mathcal{J} = \mathcal{P}^f$ pour $0 \leq f \leq e+1$ par la décomposition en produits d'idéaux. Comme $\mathcal{J}$ est contenu dans $\mathcal{P}^e$, on a $f \geq e$. Comme $a \notin \mathcal{P}^{e+1}$, $\mathcal{J}$ n'est pas égale à $\mathcal{P}^{e+1}$. Donc $\mathcal{J} = \mathcal{P}^e$.

Soit $x \in \mathcal{P}^e = \mathcal{J}$. Il existe $z \in \mathcal{P}^{e+1}$ et $w \in \mathcal{O}_K$ tels que $x = z + aw$. Alors

$$[x]_{\mathcal{P}^{e+1}} = [aw]_{\mathcal{P}^{e+1}} = \varphi(w)$$

et φ est surjectif. De l'isomorphisme

$$\mathcal{O}_K / \mathcal{P} \simeq \mathcal{P}^e / \mathcal{P}^{e+1}$$

on déduit l'égalité $|\mathcal{P}^e / \mathcal{P}^{e+1}| = N(\mathcal{P})$ $\square$

Démonstration du théorème: Il suffit de démontrer que si $I = p_1^{m_1} \dots p_t^{m_t}$ est la décomposition en produit d'idéaux maximaux, alors

$$N(I) = N(p_1)^{m_1} \dots N(p_t)^{m_t}$$

Pour $t=1$, c'est le lemme précédent.

Soit $I = \underbrace{p_1^{m_1}}_{I_1} \underbrace{p_2^{m_2} \dots p_t^{m_t}}_{I_2} = I_1 I_2$. Montrons

que $I_1 + I_2 = \mathcal{O}_K$. Comme $p_1^{m_1} \subset I_1 + I_2$, on a $I_1 + I_2 = p_1^e$ pour un entier $0 \leq e \leq m_1$. D'ailleurs, I_2 n'est pas contenu dans p_1 (car sinon il serait dans la décomposition). En particulier, $I_1 + I_2$ n'est pas contenu dans p_1 , donc $e=0$ et $I_1 + I_2 = \mathcal{O}_K$. On a donc:

$$\begin{aligned} N(I) &= N(I_1 I_2) = N(I_1) N(I_2) \\ &= N(p_1)^{m_1} N(I_2) \end{aligned}$$

et par récurrence on a le théorème est démontré □

Corollaire: Soit $c = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\text{disc}(K)|}$. Le groupe $\mathcal{O}_K^\times$ est engendré par les unités

d'idéaux premiers de norme $\leq c$.

Démonstration: Soit I un idéal non nul de $\mathcal{O}_K$. Il existe un idéal H tel que IH soit principal, disons $IH = b \mathcal{O}_K$. L'idéal H contient un élément non nul $a \in H$ de norme $|N_K(a)| \leq c \cdot N(H)$. On considère alors $J = \frac{a}{b} I$. C'est un idéal de $\mathcal{O}_K$ car $aI \subset IH \subset b \mathcal{O}_K$, équivalent à I , de norme

$$N(J) = \frac{|N_K(a)| N(I)}{|N_K(b)|}$$

Par la multiplicité des normes,

$$N(IH) = N(I) N(H) = |N_K(b)|,$$

$$\text{d'où } N(J) = \frac{|N_K(a)|}{N(H)} \leq c \quad \square$$

Remarque: on peut améliorer cette borne en remplaçant c par la constante de Minkowski

$$m_K = \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\text{disc}(K)|} \frac{n!}{n^n}$$

(En effet, $m_K \leq c_K$ car $r_2 \leq n/2$ et

$$2^{n/2} \frac{n!}{n^n} \leq 1 \quad \text{pour tout } n \geq 2)$$

Calcul d'un groupe de classes

Soit $n \geq 1$. Pour calculer $l(k)$, il faut savoir trouver explicitement les idéaux maximaux de $\mathcal{O}_K$ dont le norme est égale à n . On procède ainsi :

Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$.

- * $\mathcal{O}_K/\mathfrak{p}$ est un corps fini, donc de cardinal une puissance d'un nombre premier p .

- * Si $n = p^f$, alors $p \in \mathfrak{p}$ car $\mathcal{O}_K/\mathfrak{p}$ est de caractéristique p .

- * Supposons $\mathcal{O}_K = \mathbb{Z}[\alpha]$ avec α de polynôme minimal $A \in \mathbb{Z}[X]$. Alors

$$\mathcal{O}_K = \mathbb{Z}[X]/A\mathbb{Z}[X]$$

et $\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}[X]/I$ pour un idéal

I qui contient $\mathfrak{p}$ et A (l'image inverse de $\mathfrak{p}$ par $\mathbb{Z}[X] \rightarrow \mathcal{O}_K$). L'image J de I dans $\mathbb{F}_p[X]$ est un idéal (car la réduction modulo p est surjective). On a $J = (R(X))$,

d'où $\mathbb{Z}[X]/I \cong \mathbb{F}_p[X]/(R(X))$ et le

polynôme R est donc irréductible dans $\mathbb{F}_p[x]$.
 Comme $A \in I$, sa réduction modulo p est dans J ,
 donc R divise A . on en déduit

$$P = (p, \tilde{R}(x))$$

pour $\tilde{R} \in \mathbb{Z}[x]$ un polynôme de valuation R
 modulo p .

* $\mathcal{O}_K/p \simeq \mathbb{F}_p[x]/(R(x))$ a donc cardinal

$$N(p) = p^{\deg R}$$

* Réciproquement, tout facteur irréductible de
 A modulo p définit un idéal $P = (p, \tilde{R}(x))$.

Conclusion: les idéaux maximaux de $\mathcal{O}_K$
 de norme p sont en bijection avec
 les facteurs irréductibles de degré f de
 $A(x)$ modulo p .

Exemple: $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

le discriminant est $\text{disc}(K) = -20$.

$\mathcal{O}_K$ est engendré par les idéaux
 maximaux de norme $\leq \left(\frac{2}{\pi}\right)^1 \sqrt{20} = \frac{4\sqrt{5}}{\pi} \approx 2,8...$

Il suffit donc de déterminer les idéaux

maximale de $m=2$.

le polynôme minimal de $\sqrt{-5}$ est X^2+5 ,
qui est $(X+1)^2 \pmod{2}$. Les facteurs irréductibles
sont $X+1$ et le seul idéal maximal de
 $m=2$ est donc $M=(2, 1+\sqrt{-5})$.

Cet idéal n'est pas principal car il n'y
a pas d'élément de $m=2$ dans $\mathcal{O}_K$.

En effet, $N_K(X+y\sqrt{-5}) = X^2+5y^2$ est
 ≥ 5 si $y \neq 0$ et un carré si $y=0$.

L'idéal M^2 est engendré par

$$4, 2+2\sqrt{-5}, (1+\sqrt{-5})^2 = -4+2\sqrt{-5},$$

d'où

$$M^2 = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})$$

$$= (4, 2\sqrt{-5}, 2)$$

$$= (2, 2\sqrt{-5})$$

$$= 2 \mathbb{Z}[\sqrt{-5}]$$

c'est-à-dire M^2 est principal.

Par conséquent, $\text{cl}(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/2\mathbb{Z}$
en tant que groupe abélien.