TD 4 : Décomposition des nombres premiers et groupe des classes

Exercice 1. [Décomposition dans le cas quadratique]

Soit $d \neq 0, 1$ un entier relatif sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$.

(a) Rappeler une base entière de $\mathcal{O}_K$, et en déduire comment calculer la décomposition de tout $p\mathcal{O}_K$.

(b) Établir les différents types de décomposition de $p\mathcal{O}_K$ (ramifié, inerte ou totalement décomposé) suivant la congruence de d modulo p.

(c) Rappeler quel est le discriminant de K, et retrouver le lien avec les nombres premiers ramifiés.

Exercice 2. [Cas cyclotomique]

Soit $n \geq 3$, $\zeta_n = e^{2i\pi/n}$ et $K = \mathbb{Q}(\zeta_n)$. On rappelle que le polynôme minimal de ζ_n est le polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$ et que l'anneau des entiers de $\mathbb{Q}(\zeta_n)$ est $\mathbb{Z}[\zeta_n]$.

(a) Pour p un nombre premier ne divisant pas n, décrire les diviseurs irréductibles de Φ_n modulo p.

(b) En déduire la forme de la décomposition de $p\mathcal{O}_K$ en fonction de p modulo n.

Exercice 3. [Finitude du groupe de classes]

Soit K un corps de nombres de degré d et $\mathrm{Cl}(\mathcal{O}_K)$ son groupe de classes, on va montrer ci-dessous que celui-ci est fini.

On fixe $\alpha_1, \cdots, \alpha_d$ une $\mathbb{Z}$-base de $\mathcal{O}_K$, $\sigma_1, \cdots, \sigma_d$ les plongements de K dans $\mathbb{C}$, et la constante

$$G = \prod_{i=1}^{d} \left(\sum_{j=1}^{d} |\sigma_i(\alpha_j)| \right).$$

(a) Soit I un idéal non nul de $\mathcal{O}_K$, et m l'entier tel que $m^d \leq N(I) < (m+1)^d$. Montrer par un principe des tiroirs qu'il existe des entiers $n_1, \cdots, n_d$ non tous nuls avec $|n_i| \leq m$ pour tout i tels que

$$\alpha = n_1\alpha_1 + \cdots + n_d\alpha_d \in I.$$

(b) Montrer que $N_{K/\mathbb{Q}}(\alpha) \leq GN(I)$.

(c) En déduire que toute classe d'idéaux dans $\mathrm{Cl}(\mathcal{O}_K)$ a un représentant de norme au plus G, et en conclure que le groupe de classes est fini *(plus tard dans le cours, on verra une borne bien meilleure que G).*

(d) Avec cette borne, en déduire un algorithme pour calculer le groupe de classes, et l'utiliser pour montrer que $\mathbb{Z}[\sqrt{d}]$ est principal si $-2, -1, 2, 3$ (choisir un de ces cas).

(e) Montrer que $(2) = (2-\sqrt{6})^2$, $(3) = (3-\sqrt{6})^2$, $(5) = (\sqrt{6}-1)(\sqrt{6}+1)$ et que (7) est premier dans l'anneau $\mathbb{Z}[\sqrt{6}]$. En appliquant l'algorithme précédent (et en décomposant (11)), montrer que $\mathrm{Cl}(\mathbb{Z}[\sqrt{6}]) = \mathbb{Z}/2\mathbb{Z}$.

Exercice 4. [Nombres premiers totalement ramifiés]

On rappelle qu'un nombre premier p est totalement ramifié dans le corps de nombres K de degré d si $p\mathcal{O}_K = \mathfrak{P}^d$, autrement dit si le nombre de ramification de p est maximal. Supposons qu'il existe un tel nombre premier p.

On fixe $\alpha \in \mathfrak{P}\backslash\mathfrak{P}^2$ et $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ son polynôme caractéristique.

(a) Montrer que $(\alpha) = \mathfrak{P}I$ avec I un idéal de $\mathcal{O}_K$ premier à $\mathfrak{P}$, et en déduire que a_0 est divisible par p mais pas par p^2.

(b) On va montrer par récurrence que p divise $a_0, \cdots, a_i$ pour tout $i \leq d-1$. Supposons que c'est le cas à l'étape $i < d-1$. Montrer que

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_{i+1}\alpha^{i+1} \equiv 0 \mod p\mathcal{O}_K,$$

et en déduire que $a_{i+1}\alpha^{d-1} \in p\mathcal{O}_K$.

(c) En considérant les normes, en déduire que p divise a_{i+1}.

(d) En conclure que P est un polynôme d'Eisenstein.