Université Paris Cité (Diderot Paris 7)

Cours d'arithmétique (M1), janvier-avril 2026

Feuille TD4 : Décompositions d'idéaux, géométrie des nombres

Décompositions d'idéaux.

Exercice 1. Soit K un corps de nombres. On suppose qu'il existe $\theta \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\theta]$. Soient μ le polynôme minimal de θ et p un nombre premier. On écrit la décomposition en produit d'irréductibles de la réduction $\overline{\mu}$ de μ modulo p :

$$\overline{\mu} = \overline{\mu}_1^{e_1} \dots \overline{\mu}_r^{e_g},$$

où les $\overline{\mu}_i \in \mathbb{F}_p[X]$ sont des polynômes irréductibles non associés deux à deux. Pour chaque $1 \leq i \leq g$, on introduit un relèvement μ_i de $\overline{\mu}_i$ à $\mathbb{Z}[X]$ et on pose $\mathfrak{p}_i := (p, \mu_i(\theta))$. Montrer que $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont des idéaux premiers deux à deux distincts de $\mathcal{O}_K$ tels que $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$.

Exercice 2. On prend $K = \mathbb{Q}(\sqrt[3]{2})$ et on rappelle que $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ (exercice 15 du TD2). Soit p un nombre premier. Quelles sont les factorisations possibles de l'idéal $p\mathcal{O}_K$? Donner un exemple concret pour chaque possibilité.

Exercice 3. Soient $n \geq 3$ et $K = \mathbb{Q}(\zeta_n)$, où ζ_n est une racine primitive n-ième de l'unité. On rappelle que $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ (exercice 17 du TD3). Soient p un nombre premier et f_p l'ordre de la classe de p modulo $\frac{n}{p^{v_p(n)}}$. Montrer qu'il existe $r := \frac{\varphi(n)}{f_p \varphi(p^{v_p(n)})}$ idéaux premiers deux à deux distincts de $\mathcal{O}_K$ tels que :

$$p\mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^{\varphi(p^{v_p(n)})}.$$

Exercice 4.

1. Soient $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$. Soit p un nombre premier. Montrer que $p\mathcal{O}_K$ est le carré d'un idéal premier si, et seulement si, p divise le discriminant de K. Dans ce cas, on dit que l'extension $K/\mathbb{Q}$ *ramifie* en p.
2. Soit K un corps de nombres. On suppose qu'il existe $\theta \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\theta]$. On dit qu'un nombre premier p *ramifie* dans $\mathcal{O}_K$ si, dans la factorisation de l'idéal $p\mathcal{O}_K$, il y a au moins un exposant différent de 1. Montrer que p ramifie si, et seulement si, p divise le discriminant de K.

Exercice 5. Soit K un corps de nombres. Soit $(x_1, \dots, x_n)$ une base de K telle que $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}x_i$. On définit :

$$I := \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subset \mathbb{Z}\}.$$

1. (a) Montrer qu'il existe une base $(x_1^*, \dots, x_n^*)$ de K telle que, pour $1 \leq i, j \leq n$:

$$\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j^*) = \delta_{ij}.$$

   (b) Montrer que $I = \bigoplus_{i=1}^n \mathbb{Z}x_i^*$.

   (c) Déduire que I est un idéal fractionnaire, c'est-à-dire qu'il existe un entier $m > 0$ tel que mI est un idéal de $\mathcal{O}_K$.

2. Soit $\mathcal{D} := I^{-1} = \{x \in K : xI \subset \mathcal{O}_K\}$. On dit que $\mathcal{D}$ est la *différente* de K. Montrer que $\mathcal{D}$ est un idéal de $\mathcal{O}_K$.

3. (a) Soit $B = (b_{ij})_{1 \leq i,j \leq n}$ la matrice de passage de la base $(x_1^*, \dots, x_n^*)$ vers la base $(x_1, \dots, x_n)$. Montrer que $\det(B)$ est le discriminant Δ_K de K.

(b) Déduire que $[\mathcal{O}_K : \mathcal{D}] = |\Delta_K|$.

(c) Soient p un nombre premier et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Soit $e \geq 0$ tel que $p\mathcal{O}_K = \mathfrak{p}^e\mathfrak{a}$ pour un certain idéal $\mathfrak{a}$ premier avec $\mathfrak{p}$. On suppose que $e \geq 2$. On dit alors que l'extension $K/\mathbb{Q}$ *ramifie* en p.

i. Montrer que $\frac{1}{p} \cdot \mathfrak{p}\mathfrak{a} \subset I$.

ii. Déduire que $\mathfrak{p}^{e-1}$ divise $\mathcal{D}$.

iii. Conclure que p divise Δ_K.

Il est possible de montrer une réciproque à cet énoncé : si p divise Δ_K, alors l'extension $K/\mathbb{Q}$ ramifie en p. Mais ce résultat est plus difficile à établir.

Géométrie des nombres.

Exercice 6. Soit p un nombre premier congru à 1 modulo 4. On rappelle que, dans ce cas, il existe $u \in \mathbb{Z}$ tel que $u^2 \equiv -1 \mod p$.

1. On pose :
$$L := \{(a, b) \in \mathbb{Z}^2 : a \equiv ub \mod p\}.$$
Montrer que L intersecte le disque ouvert de centre 0 et de rayon $\sqrt{2p}$ ailleurs qu'en 0.
2. Conclure qu'il existe $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$.

Exercice 7. Soit n un entier naturel. On cherche à montrer que n est somme de quatre carrés.

1. Expliquer pourquoi on peut supposer que n est sans facteurs carrés. On fera cette hypothèse dans toute la suite de l'exercice.
2. Montrer qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $u^2 + v^2 + 1 \equiv 0 \mod n$.
3. On pose :
$$L := \{(a, b, c, d) \in \mathbb{Z}^4 : c \equiv au + bv \mod n, d \equiv av - bu \mod n\}.$$
Montrer que L intersecte la boule ouverte de centre 0 et de rayon $\sqrt{2n}$ dans $\mathbb{R}^4$ ailleurs qu'en 0.
4. Conclure.

Exercice 8. Soit $K = \mathbb{Q}(\sqrt{-5})$.

1. Montrer que $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$.
2. Trouver toutes les solutions entières de l'équation $x^2 + 5 = y^3$.

Exercice 9. Soit p un nombre premier tel que $p \equiv -1 \mod 12$. On pose $K := \mathbb{Q}(\sqrt{p})$.

1. Montrer qu'il existe deux idéaux premiers distincts $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de $\mathcal{O}_K$ tels que :
$$3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2.$$
2. Montrer que l'ordre de $\mathfrak{p}_1$ dans Cl_K est au moins $\lfloor \log_3(p) \rfloor$.

Exercice 10. Montrer que l'anneau des entiers de $K := \mathbb{Q}(\sqrt{-19})$ est principal.

Exercice 11. L'anneau des entiers de $K := \mathbb{Q}(\sqrt{14})$ est-il principal ?

Exercice 12. On considère un corps quadratique réel $K = \mathbb{Q}(\sqrt{d})$ avec d sans facteur carré, et Δ_K son discriminant.

1. Montrer que si $\Delta_K < 36$, alors $\mathcal{O}_K$ est principal si et seulement si les idéaux divisant 2 sont principaux.

2. En déduire que l'anneau $A_d = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est principal pour $d = 2, 3, 5, 6, 7$.
3. On regarde le cas $d = 10$. Montrer que $2\mathcal{O}_K = \mathfrak{p}^2$ pour un certain idéal $\mathfrak{p}$ non principal. En utilisant la borne de Minkowski, calculer le groupe des classes de $\mathcal{O}_K$.

Exercice 13. On considère un corps quadratique imaginaire $K = \mathbb{Q}(i\sqrt{d})$ avec d sans facteur carré et Δ_K son discriminant.

1. Si $d = p$ est premier avec $p \equiv 1 \mod 4$, montrer que $2\mathcal{O}_K = \mathfrak{p}^2$ et que $\mathfrak{p}$ n'est pas principal, produisant un élément d'ordre deux dans le groupe des classes.
2. On regarde le cas $d = 23$. Montrer que $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ avec $\mathfrak{p}_i$ non principal. En utilisant la borne de Minkowski, montrer que le groupe des classes est $\mathbb{Z}/3\mathbb{Z}$, les deux éléments non triviaux étant les classes de $\mathfrak{p}_1$ et $\mathfrak{p}_2$.
3. Si le discriminant Δ_K a au moins deux facteurs premiers, montrer que le groupe des classes contient un élément d'ordre deux et est donc non trivial.

Exercice 14. Soit $z \in \mathbb{C}$ une racine de $P(T) := T^5 - T + 1$. L'anneau des entiers de $K := \mathbb{Q}(z)$ est-il principal ?

Exercice 15. Soit $\omega = \sqrt[3]{2}$ et $K = \mathbb{Q}(\omega)$.

1. Montrer que le rang de $\mathcal{O}_K^\times$ est égal à 1 et que, si on note $N_1 \subset \mathcal{O}_K^\times$ le sous-groupe des unités de norme 1, le groupe N_1 est isomorphe à $\mathbb{Z}$ et $\mathcal{O}_K^\times = \{\pm 1\} \cdot N_1$.
2. Soit $\epsilon = \omega - 1$, vérifier que ϵ est une unité et qu'elle engendre N_1.
3. Montrer que $\mathcal{O}_K = \mathbb{Z}[\omega]$ est principal

Exercice 16. On veut prouver que le groupe des classes de $K = \mathbb{Q}(\zeta)$ avec $\zeta = \exp(2\pi i/23)$ a un groupe des classes non trivial, contenant $\mathbb{Z}/3\mathbb{Z}$.

1. Montrer que $k = \mathbb{Q}(i\sqrt{23})$ est un sous-corps de K et $[K : k] = 11$. [Indication : utiliser la théorie de Galois pour montrer que K contient un unique corps quadratique, ou bien utiliser la somme de Gauss
$$S = \sum_{a \in \mathbb{F}_{23}} \left(\frac{a}{23}\right) \zeta^a,$$
où $\left(\frac{a}{23}\right)$ désigne le symbole de Legendre, et montrer $S^2 = -23$.]
2. L'ordre de 2 modulo 23 est égal à 11. En déduire (Cf exercice 13, item 2) que $2\mathcal{O}_k = \mathfrak{p}_1\mathfrak{p}_2$ et $\mathfrak{p}_i\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$ vérifiant $N_{K/k}(\mathfrak{p}_i\mathcal{O}_K) = \mathfrak{p}_i^{11}$.
3. Conclure en montrant que 3 divise l'ordre de la classe de $\mathfrak{p}_i\mathcal{O}_K$.

Exercice 17. Soit p un nombre premier, on pose $\zeta_p := e^{2i\pi/p}$ et $x_p = \cos(2\pi/p)$. On considère $K = \mathbb{Q}(\zeta_p)$ et $K_0 = \mathbb{Q}(x_p)$.

1. On rappelle que $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Montrer que $\mathcal{O}_{K_0} = \mathbb{Z}[2x_p]$.
2. Montrer que $\mathbb{Z}[\zeta_p]^\times = \langle \zeta_p \rangle \times \mathbb{Z}[2x_p]^\times$.
3. Lorsque $p = 5$, calculer $\mathbb{Z}[\zeta_p]^\times$.

Exercice 18. Soit K un corps de nombres.

1. Soit I un idéal non nul de $\mathcal{O}_K$. Soient $m \geq 1$ et $a \in \mathcal{O}_K$ tels que $I^m = (a)$. En posant $L := K(\sqrt[m]{a})$, montrer que l'idéal $I\mathcal{O}_L$ est principal.
2. Montrer qu'il existe une extension finie L de K telle que, pour tout idéal I de $\mathcal{O}_K$, l'idéal $I\mathcal{O}_L$ de $\mathcal{O}_L$ est principal.

Exercice 19.

1. (a) Montrer que $|\Delta_K| > 1$ pour tout corps de nombres $K \neq \mathbb{Q}$.
   (b) Montrer que $|\Delta_K|$ tend vers l'infini lorsque K décrit des corps de nombres dont le degré tend vers l'infini.
2. Dans cette question, il est utile de connaître un peu de théorie de Galois. Soit $\Delta > 0$.
   (a) Montrer qu'il existe une constante $C_0(\Delta) > 0$ telle que, pour tout corps de nombres K de discriminant Δ_K avec $|\Delta_K| < \Delta$, on a $|\Delta_{K(i)}| < C_0(\Delta)$.
   (b) Montrer qu'il existe une constante $C_1(\Delta) > 0$ telle que, pour tout corps de nombres K de discriminant Δ_K avec $|\Delta_K| < \Delta$, il existe un plongement $\tau_0 : K(i) \to \mathbb{C}$ et un élément $x \in \mathcal{O}_{K(i)}$ vérifiant les propriétés suivantes :

$$|\mathrm{Im}(\tau_0(x))| < C(\Delta), \quad |\mathrm{Re}(\tau_0(x))| < 1, \quad \forall \tau \in \mathrm{Hom}_{\mathbb{Q}}(K(i), \mathbb{C}) \setminus \{\tau_0, \overline{\tau}_0\},\ |\tau(x)| < 1.$$

   (c) Dans le contexte de la question précédente, montrer que $K(i) = \mathbb{Q}(x)$.
   (d) En déduire qu'il existe un nombre fini de corps de nombres K de discriminant Δ_K avec $|\Delta_K| < \Delta$. Ce résultat s'appelle le **théorème d'Hermite**.