TD 2 : Corps de nombres et entiers algébriques

Exercice 1. [Traces et normes relatives]

Soit L/K une extension finie de corps de nombres. Pour tout $\alpha \in L$, on note m_α la multiplication par α dans L et

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}\, m_\alpha, \qquad N_{L/K}(\alpha) = \det m_\alpha.$$

Montrer (en considérant les automorphismes d'une extension galoisienne de M) que pour $K \subset L \subset M$ des extensions finies de corps de nombres et pour $\alpha \in M$, on a

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)) \qquad N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)).$$

Qu'en déduire quand $\alpha \in L$?

Exercice 2. [Calcul d'anneau d'entiers]

Soient $m, n \neq 1$ des entiers distincts sans facteur carré congrus à 1 modulo 4. On considère $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

(a) Montrer que $\alpha \in K$ est un entier algébrique si et seulement si sa trace et sa norme relative sur $\mathbb{Q}(\sqrt{m})$ sont des entiers algébriques.

(b) En considérant les traces relatives sur les corps intermédiaires, montrer que tout $\alpha \in \mathcal{O}_K$ est de la forme

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn}}{4}, \qquad a, b, c, d \in \mathbb{Z},\ a \equiv b \equiv c \equiv d \mod 2.$$

(b) En déduire qu'une base entière de K est

$$\left(1, \left(\frac{1+\sqrt{m}}{2}\right), \left(\frac{1+\sqrt{n}}{2}\right), \left(\frac{1+\sqrt{m}}{2}\right) \cdot \left(\frac{1+\sqrt{n}}{2}\right)\right).$$

Exercice 3. [Opérations de base et décomposition]

Soient I et J des idéaux non nuls de A, donner les décompositions de IJ, $I \cap J$ et $I + J$ en fonction de celles de I et J. En déduire que $IJ = (I \cap J)(I + J)$.

Exercice 4. [Valuations discrètes] Soit A un anneau de Dedekind de corps des fractions K.

Pour tout idéal premier non nul $\mathfrak{p}$ de A et tout $a \in A$ non nul, on note $v_\mathfrak{p}(a)$ la multiplicité de $\mathfrak{p}$ dans la décomposition de (a), et $v_\mathfrak{p}(0) = +\infty$.

(a) Montrer que chaque $v_\mathfrak{p}$ est une valuation discrète sur A qui s'étend sur K, et que l'anneau de valuation discrète associé est $A_\mathfrak{p}$.

(b) Montrer que $A = \cap_\mathfrak{p} A_\mathfrak{p}$.

(c) Montrer le lemme d'approximation : pour $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ des idéaux maximaux distincts de A, $x_1, \cdots, x_r$ des éléments de K et $n_1, \cdots, n_r \in \mathbb{Z}$, il existe $x \in K$ tel que $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ pour tout $1 \leq i \leq r$.

(d) En déduire que si A n'a qu'un nombre fini d'idéaux premiers, il est principal. Donner un exemple d'un tel anneau.

Exercice 5. [Anneaux de Dedekind]

(a) En trouvant un élément de $\mathbb{Q}[\sqrt{-3}]$ entier sur l'anneau $\mathbb{Z}[\sqrt{-3}]$, démontrer que ce dernier n'est pas de Dedekind.

(b) Donner deux exemples (pas trop similaires) d'anneaux de Dedekind qui ne sont pas des anneaux d'entiers de corps de nombres.

(c) Montrer qu'un anneau de Dedekind est factoriel si et seulement si il est principal.

Exercice 6. [Caractérisation des anneaux de Dedekind]

Soit A un anneau intègre de corps des fractions K.

(a) Supposons que pour tout idéal fractionnaire non nul I de A, $I \cdot I^{-1} = A$. Montrer que A est noethérien et que tout idéal non nul de A s'écrit de manière unique comme produit d'idéaux maximaux.

(b) Réciproquement, prouver que si tout idéal non nul de A s'écrit comme produit d'idéaux maximaux, tout idéal fractionnaire non nul de A est inversible.

(c) En déduire que ces deux conditions sont équivalentes à être un anneau de Dedekind.

Exercice 7. [Un exemple d'anneau d'entiers non monogène]

Soit $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ et $\alpha \in \mathcal{O}_K$ de polynôme minimal P sur $\mathbb{Q}$. Pour tout polynôme Q de $\mathbb{Z}[X]$, on notera $\overline{Q}$ sa réduction dans $\mathbb{F}_3[X]$.

(a) Montrer que 3 divise $Q(\alpha)$ dans $\mathbb{Z}[\alpha]$ si et seulement si $\overline{P}$ divise $\overline{Q}$ dans $\mathbb{F}_3[X]$.

On suppose désormais que $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

(b) Soient les entiers algébriques $\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$, $\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$, $\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$ et $\alpha_4 = (1-\sqrt{7})(1-\sqrt{10})$. Montrer que tous les $\alpha_i\alpha_j$ $(i \neq j)$ sont divisibles par 3 dans $\mathbb{Z}[\alpha]$, mais qu'aucune des puissances α_i^n ne l'est en considérant leur trace.

(c) Soient $P_i \in \mathbb{Z}[X]$, $1 \leq 4$ des polynômes tels que $P_i(\alpha) = \alpha_i$. Montrer que $\overline{P}$ divise les $\overline{P_iP_j}$ $(i \neq j)$ mais aucune des puissances $\overline{P_i}^n$. En déduire que pour tout i entre 1 et 4, $\overline{P}$ possède un facteur irréductible divisant $\overline{P_j}$ pour $j \neq i$ mais pas $\overline{P_i}$.

(d) En déduire que $\overline{P}$ a quatre facteurs irréductibles distincts, puis une contradiction. Ceci prouve que l'anneau $\mathcal{O}_K$ n'est pas de la forme $\mathbb{Z}[\alpha]$.

Exercice 8. [Entiers de Gauss]

(a) Rappeler quels sont les inversibles de $\mathbb{Z}[i]$. On note $N = |\cdot|^2$ sur $\mathbb{C}$.

(b) Montrer que N définit un stathme euclidien sur $\mathbb{Z}[i]$.

(c) Soit p un nombre premier. Montrer que p est réductible dans $\mathbb{Z}[i]$ si et seulement si il existe $\pi \in \mathbb{Z}[i]$ tel que $N(\pi) = p$, et que π est alors irréductible lui-même.

(d) En déduire que si p est congru à 3 modulo 4, il est irréductible dans $\mathbb{Z}[i]$.

(e) Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si X^2+1 est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

(f) En utilisant un critère sur les carrés de $(\mathbb{Z}/p\mathbb{Z})^*$, en déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \mod 4$.

(g) Déduire des résultats précédents quels sont les entiers de $\mathbb{Z}$ s'écrivant comme somme de deux carrés.