TD 1 : Corps de nombres et anneaux d'entiers

Nous rappelons que pour une extension finie de corps L/K et $\alpha \in L$, la trace et la norme de α relativement à cette extension sont respectivement la trace et le déterminant du morphisme de multiplication par α dans L en tant qu'application K-linéaire (en particulier, elles sont à valeurs dans K). On les notera $\mathrm{Tr}_{L/K}(\alpha)$ et $N_{L/K}(\alpha)$ ci-dessous.

Exercice 1. [Résultats généraux sur la trace et la norme]

(a) Pour une extension finie L/K, montrer que la trace $\mathrm{Tr}_{L/K}$ est K-linéaire et que $N_{L/K}$ est multiplicative, et décrire leurs restrictions à K.

(b) Montrer que pour une suite d'extensions finies de corps $K \subset L \subset M$, pour tout $\alpha \in M$, on a

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

(c) Soit L/K une extension finie séparable et $\alpha \in L$. Supposons que le polynôme minimal de α sur K est de degré n, on en note $\alpha_1, \cdots, \alpha_n$ les racines dans $\overline{K}$. Montrer que

$$\mathrm{Tr}_{L/K}(\alpha) = \frac{[L:K]}{n} \sum_{i=1}^{n} \alpha_i \qquad N_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \alpha_i \right)^{[L:K]/n}.$$

(d) Pour une extension finie $K/\mathbb{Q}$, montrer que $\alpha \in \mathcal{O}_K$ est inversible dans $\mathcal{O}_K$ si et seulement si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Que peut-on dire lorsque $N_{K/\mathbb{Q}}(\alpha)$ est un nombre premier ?

Exercice 2. [Corps quadratiques]

Dans tout l'exercice, d est un entier relatif sans facteur carré, différent de 0 et 1.

(a) Pour tous $a, b \in \mathbb{Q}$, calculer la trace et la norme de $a + b\sqrt{d}$ dans $\mathbb{Q}(\sqrt{d})$, puis son polynôme minimal dans $\mathbb{Q}$.

(b) En déduire que l'ensemble des entiers algébriques de $\mathbb{Q}(\sqrt{d})$, noté $\mathcal{O}_d$, est $\mathbb{Z}[\sqrt{d}]$ si d est congru à 2 ou 3 modulo 4, et $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si d est congru à 1 modulo 4.

(c) Déterminer $\mathcal{O}_d^*$ si $d < 0$. Sans preuve, que semble-t-il se passer pour $d > 0$? Étudier les premiers cas.

(d) Montrer que $\mathbb{Z}[i]$ est euclidien pour la norme usuelle, et calculer ses éléments irréductibles.

(e) Montrer que $\mathcal{O}_{-5}$ n'est pas factoriel.

(f) Montrer que tout corps de nombres de degré 2 est égal à un $\mathbb{Q}(\sqrt{d})$ et que ceux-ci sont non-isomorphes deux à deux.

Exercice 3.

Soit $\alpha = \sqrt[4]{2}$ et $K = \mathbb{Q}(\alpha)$. Soit p premier différent de 2. On va démontrer par l'absurde que $\sqrt{p} \notin K$, supposons donc qu'on peut écrire

$$\sqrt{p} = a + b\alpha + c\alpha^2 + d\alpha^3 \qquad a, b, c, d \in \mathbb{Q}.$$

(a) Montrer que $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}(\sqrt{p}) = 0$. En déduire que $a = 0$.

(b) En considérant $\sqrt{p}/\alpha$ et un corps intermédiaire bien choisi, montrer de la même manière que $b = 0$.

(c) Imiter l'idée pour obtenir $c = 0$, et trouver finalement une contradiction.

Remarque : cet exercice sera bien plus simple avec des résultats plus généraux donnés dans la suite du cours.

Exercice 4. [Anneaux d'entiers relatifs]

Soient A, B deux anneaux intègres commutatifs unitaires, avec $A \subset B$.

(a) Montrer que $b \in B$ est entier sur A si et seulement si la multiplication par B stabilise un certain A-module non nul de type fini inclus dans B.

(b) En déduire que l'ensemble des éléments de B entiers sur A est un anneau.

(c) Si K est un corps de nombres, montrer que tout élément de K entier sur $\mathcal{O}_K$ est déja dans $\mathcal{O}_K$. En déduire que tout anneau $A \subset K$ qui est un $\mathbb{Z}$-module de type fini est inclus dans $\mathcal{O}_K$.

Exercice 5. [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 $\mathbb{Z}[\alpha] = \mathcal{O}_K$. Soient les entiers algébriques

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10}), \quad \alpha_2 = (1+\sqrt{7})(1-\sqrt{10}),$$

$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10}), \quad \alpha_4 = (1-\sqrt{7})(1-\sqrt{10}).$$

(b) Montrer que tous les $\alpha_i\alpha_j$ $(i \neq j)$ sont divisibles par 3 dans $\mathbb{Z}[\alpha]$.

(c) Calculer la trace de chaque puissance α_i^n grâce à l'exercice 1, et en déduire qu'aucun d'entre eux n'appartient à $3\mathcal{O}_K$.

(d) Soient $P_i \in \mathbb{Z}[X]$, $1 \leq i \leq 4$ 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 $\overline{P_i}$.

(e) 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 $\mathbb{Z}[\alpha]$.