Université Paris-Saclay 2022-2023
M1 M.F., Orsay Arithmétique

T.D. 6 : Corps de nombres

Les exercices soulignés sont ceux qui seront corrigés en TD ; ils sont à chercher en priorité. Les exercices 3 et 4 pourront être utilisés pour résoudre les suivants.

Exercice 1 Soit A un anneau factoriel et K son corps des fractions. Montrer que tout élément de K entier sur A est un élément de A.

Exercice 2 Soient A, B, C trois anneaux commutatifs unitaires. On suppose C entier sur B et B entier sur A. Montrer que C est entier sur A.

Exercice 3 Soient k un corps de nombres, L une extension finie de k, et $x \in L$. On note $\mathrm{Tr}_{M'/M}$ (resp. $\mathrm{N}_{M'/M}$) l'application trace (resp. norme) relative à une extension M'/M.

1. Soit K une extension finie de k contenue dans L, telle que $x \in K$. Démontrer qu'en posant $n = [L : K]$ on a
$$\mathrm{Tr}_{L/k}(x) = n\mathrm{Tr}_{K/k}(x) \qquad \text{et} \qquad \mathrm{N}_{L/k}(x) = \big(\mathrm{N}_{K/k}(x)\big)^n \,.$$
2. Notons μ_x le polynôme minimal de x sur k, et χ_x le polynôme caractéristique de la multiplication par x (vue comme endomorphisme du k-espace vectoriel L). Démontrer que χ_x est une puissance de μ_x, et en déduire que $\mu_x = \frac{\chi_x}{\mathrm{pgcd}(\chi_x, \chi_x')}$.
3. Notons $d = [L : k]$, et $\sigma_1, \ldots, \sigma_d$ les plongements de L dans $\mathbf{C}$ fixant k (point par point). Montrer que pour tout $x \in L$ on a
$$\mathrm{Tr}_{L/k}(x) = \sum_{i=1}^{d} \sigma_i(x) \qquad \text{et} \qquad \mathrm{N}_{L/k}(x) = \prod_{i=1}^{d} \sigma_i(x)\,.$$

Exercice 4 Montrer que la famille formée par 1 et les $\sqrt{d}$, pour $d \geq 2$ sans facteur carré, est libre sur $\mathbf{Q}$. En déduire le degré de l'extension $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbf{Q}$ pour $p_1, \ldots, p_n$ premiers deux à deux distincts.

Exercice 5 Déterminer de plusieurs façons un polynôme non nul de $\mathbf{Q}[X]$ s'annulant en $\sqrt{2} + \sqrt{3}$: par une méthode directe, en appliquant la question 2 de l'exercice 3, et (pour ceux qui le connaissent) en utilisant le résultant.

Exercice 6 Montrer *via* un calcul de traces que $\sqrt{3} \notin \mathbf{Q}(\sqrt[4]{2})$.

Exercice 7 Soit $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Notons k l'un des corps $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ ou $\mathbf{Q}(\sqrt{6})$. Démontrer qu'un élément α de K est entier si et seulement si $\mathrm{Tr}_{K/k}(\alpha)$ et $\mathrm{N}_{K/k}(\alpha)$ sont des entiers de k. En déduire l'anneau d'entiers de K.

Exercice 8 Soit p un nombre premier impair et ζ une racine primitive p-ème de l'unité. Le but de cet exercice est de montrer que l'anneau d'entiers $\mathcal{O}_K$ de $K = \mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$. On note Tr (resp. N) l'application trace (resp. norme) relative à l'extension $K/\mathbf{Q}$.

1. Soit $j \in \mathbf{N}$. En séparant le cas $p \mid j$ du cas $p \nmid j$, calculer $\mathrm{Tr}(\zeta^j)$. En déduire que $p\mathcal{O}_K \subset \mathbf{Z}[\zeta]$.
2. Déterminer le polynôme minimal de $\zeta - 1$; en déduire $\mathrm{N}(\zeta - 1)$.
3. Démontrer enfin que $\mathcal{O}_K = \mathbf{Z}[\zeta - 1] = \mathbf{Z}[\zeta]$.

Exercice 9 Soit K/k une extension finie de corps de nombres.

1. Démontrer le lemme de Dedekind : si $\chi_1, \ldots, \chi_n \colon G \to F^\times$ sont des morphismes de groupes 2 à 2 distincts d'un groupe G vers le groupe multiplicatif d'un corps F alors la famille $(\chi_1, \ldots, \chi_n)$ est F-libre.
2. En utilisant l'exercice 3, relier le discriminant d'une k-base $(\beta_1, \ldots, \beta_n)$ de K au déterminant de la matrice $[\sigma_i(\beta_j)]_{i,j}$ où $\sigma_1, \ldots, \sigma_n$ sont les plongements complexes de K qui induisent l'identité sur k.
3. Soit θ un nombre complexe algébrique sur k de degré n. On note $K = k(\theta)$. Montrer que le discriminant de la famille $(\theta^i)_{0 \le i \le n-1}$ vaut $(-1)^{n(n-1)/2}\mathrm{N}_{K/k}(P'(\theta))$ où P est le polynôme minimal de θ sur k.

Exercice 10

1. Soit K un corps de nombres de degré n sur $\mathbf{Q}$ et soit α_i, β_j, $1 \le i, j \le n$, des entiers algébriques de K. On suppose que
$$\mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \cdots + \mathbf{Z}\alpha_n \supseteq \mathbf{Z}\beta_1 + \mathbf{Z}\beta_2 + \cdots + \mathbf{Z}\beta_n\,,$$
et que les $\mathbf{Z}$-modules des membres de droite et de gauche sont libres. Montrer que $\frac{\Delta(\beta_1,\ldots,\beta_n)}{\Delta(\alpha_1,\ldots,\alpha_n)}$ est un carré dans $\mathbf{Z}$.
2. Calculer l'anneau des entiers de $K = \mathbf{Q}(\theta)$ où θ vérifie $\theta^3 + 2\theta + 1 = 0$.

Exercice 11 Soit K un corps de nombres de degré n sur $\mathbf{Q}$.

1. Soit $\mathfrak{P}$ un idéal maximal de $\mathcal{O}_K$. Montrer que $\mathfrak{P} \cap \mathbf{Z} = p\mathbf{Z}$ où p est un nombre premier.
2. Soit p un nombre premier. Montrer que l'idéal $p\mathcal{O}_K$ se décompose sous la forme
$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}\,,$$
où les $\mathfrak{P}_i$ sont les idéaux maximaux $\mathfrak{P}$ de $\mathcal{O}_K$ tels que $\mathfrak{P} \cap \mathbf{Z} = p\mathbf{Z}$, et les e_i sont des entiers naturels non nuls tels que $n = \sum_i e_i f_i$ avec $f_i = [\mathcal{O}_K/\mathfrak{P}_i : \mathbf{F}_p]$.

Exercice 12 Soit $K = \mathbf{Q}(\sqrt{d})$ un corps quadratique, où l'on suppose d sans facteur carré. On note δ_K le discriminant de K.

1. Soit p un nombre premier. Montrer que
   — si $\left(\dfrac{\delta_K}{p}\right) = 0$ alors $p\mathcal{O}_K = \mathfrak{P}^2$ pour un idéal maximal $\mathfrak{P}$ de $\mathcal{O}_K$ de norme p.
   — si $\left(\dfrac{\delta_K}{p}\right) = 1$ alors $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ pour des idéaux maximaux $\mathfrak{P}_1 \neq \mathfrak{P}_2$ de $\mathcal{O}_K$, de même norme p.
   — si $\left(\dfrac{\delta_K}{p}\right) = -1$ alors $p\mathcal{O}_K$ est un idéal maximal de $\mathcal{O}_K$ de norme p^2.
2. Soit $K = \mathbf{Q}(\sqrt{-5})$. Factoriser $p\mathcal{O}_K$ en produit d'idéaux premiers lorsque $p = 2, 3, 5, 7, 11, 29$. (On *ne* demande *pas* de déterminer systématiquement si les idéaux premiers apparaissant sont principaux.)

Dans les exercices qui suivent, on pourra utiliser sans démonstration la *borne de Minkowski* : soit K un corps de nombres de degré n sur $\mathbf{Q}$, r_1 le nombre de plongements complexes de K qui sont à valeurs réelles, et $r_2 = (n - r_1)/2$ (justifier que c'est un entier) ; alors toute classe d'idéaux de K contient un idéal entier $\mathfrak{a}$ dont la norme vérifie :

$$\mathrm{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc} K|}\,.$$

Exercice 13 Soit $K = \mathbf{Q}(\sqrt{-14})$.

1. En utilisant la borne de Minkowski, donner un ensemble (aussi petit que possible) $S = \{p_1, \ldots, p_s\}$ de nombres premiers tel que les idéaux premiers factorisant les $p_i\mathcal{O}_K$ engendrent le groupe des classes d'idéaux de K.
2. En utilisant la question 1 de l'exercice 12, donner le type de factorisation de chacun des idéaux $p_i\mathcal{O}_K$, $1 \leq i \leq s$.
3. En déduire que le groupe des classes de K est cyclique d'ordre 4. (Il pourra être utile de calculer la norme de $2 + \sqrt{-14}$.)

Exercice 14 Soit $K = \mathbf{Q}(\sqrt{-30})$.

1. Reprendre les questions 1 et 2 de l'exercice 13.
2. Montrer que les idéaux premiers qui factorisent les $p_i\mathcal{O}_K$ sont tous d'ordre 2 dans le groupe des classes de K.
3. En calculant $\mathrm{N}_{K/\mathbf{Q}}(\sqrt{-30})$, écrire une relation entre les idéaux premiers qui factorisent les $p_i\mathcal{O}_K$. En déduire la structure du groupe des classes de K.

Exercice 15 Soit $K = \mathbf{Q}(\sqrt{82})$.

1. Reprendre les questions 1 et 2 de l'exercice 13. En déduire un ensemble à deux éléments qui engendre le groupe des classes.
2. En calculant la norme de $10 + \sqrt{82}$, montrer qu'en fait le groupe des classes est engendré par un des idéaux premiers divisant $3\mathcal{O}_K$.
3. Montrer que l'idéal premier $\mathfrak{p}_2$ divisant 2 n'est pas principal. En déduire la structure de $\mathcal{C}l(K)$.

Exercice 16 (*extrait de l'examen de 2013*) Soit $K = \mathbf{Q}(\sqrt{35})$ et Δ_K son discriminant.

1. Quelle est la valeur de Δ_K ? Déterminer tous les $\omega \in \mathcal{O}_K$ tels que $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\omega$.
2. Rappeler pourquoi la norme $\mathrm{N}(\mathfrak{A})$ de tout idéal $\mathfrak{A}$ non nul de $\mathcal{O}_K$ vérifie $\mathrm{N}(\mathfrak{A}) \in \mathfrak{A}$.
3. En utilisant la question 1 de l'exercice 12, prouver qu'il existe des idéaux premiers de $\mathcal{O}_K$ notés $\mathfrak{P}_2$, $\mathfrak{P}_3$, $\mathfrak{P}_5$ tels qu'on ait les égalités entre idéaux :
$$2\mathcal{O}_K = \mathfrak{P}_2^2,\ 3\mathcal{O}_K = \mathfrak{P}_3,\ 5\mathcal{O}_K = \mathfrak{P}_5^2\,.$$
Vérifier les égalités $\mathfrak{P}_2 = 2\mathcal{O}_K + (1+\sqrt{35})\mathcal{O}_K$ et $\mathfrak{P}_5 = 5\mathcal{O}_K + \sqrt{35}\mathcal{O}_K$. Quel est l'ensemble des idéaux $\mathfrak{a}$ tels que $\mathrm{N}(\mathfrak{a}) \leq 5$?
4. Prouver que $\mathcal{C}l(K)$ est cyclique d'ordre 2.
5. Prouver que $\xi = 7 + \sqrt{35}$ est irréductible dans $\mathcal{O}_K$.
6. L'idéal $\xi\mathcal{O}_K$ est-il premier ? Si non, le décomposer en produit d'idéaux premiers.