Théorie algébrique des nombres
Feuille d'exercices n°3

Dans ce qui suit, les anneaux considérés sont supposés commutatifs et unitaires.

Exercice 1. Soient A un anneau de Dedekind et I, J des idéaux fractionnaires non nuls. Donner, en fonction des décompositions de I et de J en produit de puissances d'idéaux premiers, donner les décompositions en produit de puissances d'idéaux premiers de IJ, $I \cap J$ et $I + J$. En déduire que $IJ = (I \cap J)(I + J)$. En particulier, si $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ sont des idéaux premiers non nuls deux à deux distincts, on a $\prod_{i=1}^{r} \mathfrak{p}_i^{n_i} = \bigcap_{i=1}^{r} \mathfrak{p}_i^{n_i}$ pour tout $n_1, \ldots, n_r \in \mathbf{N}$.

Exercice 2. Soient K un corps, $A = K[X, Y]$ et $I = XA + YA$. Montrer que $I^{-1} = A$, de sorte que I n'est pas inversible.

Exercice 3. Soient A un anneau intègre dans lequel tout idéal non nul est inversible. Montrer que A est de Dedekind (indication : on commencera par montrer que A est noethérien, puis que tout idéal non nul admet une factorisation en produit d'idéaux maximaux, unique à permuation près).

Exercice 4. Soit A un anneau intègre noethérien dont tout idéal maximal est inversible. Montrer que A est de Dedekind.

Exercice 5. Soient A un anneau de Dedekind, K son corps des fractions et $I \subset K$ un idéal fractionnaire. On veut montrer que I peut être engendré par deux éléments.

(1) Se ramener au cas où I est un idéal non nul de A.
(2) Soit $\alpha \in I \setminus \{0\}$. Montrer que les décompositions en produits d'idéaux premiers de I et αA s'écrivent $I = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$ et $\alpha A = \prod_{i=1}^{r} \mathfrak{p}_i^{m_i}$ avec $r \in \mathbf{N}$ et $m_i \geq n_i \geq 0$ pour tout $i \in \{1, \ldots, r\}$.
(3) Pour $i \in \{1, \ldots, r\}$, montrer qu'il existe $b_i \in \mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1}$, et justifier l'existence de $\beta \in A$ tel que $\beta \equiv b_i \mod \mathfrak{p}_i^{n_i+1}$ pour $i \in \{1, \ldots, r\}$.
(4) En déduire que $I = \alpha A + \beta A$.

Exercice 6. Soient A un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers. Montrer que A est principal.

Exercice 7. On pose $B = \mathbf{C}[X, Y]/(Y^2 - (X^3 - X))\,\mathbf{C}[X, Y]$. On veut montrer que B est un anneau de Dedekind. On pose $A = \mathbf{C}[X]$ et $K = \mathbf{C}(X) = \mathrm{Frac}(A)$. Soient $y \in \overline{K}$ une racine de $Y^2 - (X^3 - X)$, $L = K[y]$ et $\mathcal{O}_L$ l'anneau des éléments de L entiers sur A.

(1) Montrer que B est isomorphe à $A[y]$.
(2) Que vaut $\dim_K(L)$? Montrer que $\mathrm{Frac}(A[y]) = L$ et que $A[y] \subseteq \mathcal{O}_L$.
(3) Soit $z = a(X) + b(X)y \in \mathcal{O}_L$. En utilisant la trace, montrer que $a(X) \in A$ et qu'il existe $P \in A$ tel que $b(x) = \frac{P(X)}{X^3 - X}$.

(4) En utilisant la norme, montrer que $X^3 - X$ divise P^2. En déduire que $b(X) \in A$.
(5) Montrer que B est un anneau de Dedekind.

Exercice 8. Soit $K = \mathbf{Q}(\sqrt{5})$. On a $\mathcal{O}_K = \mathbf{Z}\left[\frac{1+\sqrt{5}}{2}\right]$: c'est un anneau de Dedekind. Posons $A = \mathbf{Z}\left[\sqrt{5}\right]$, c'est un sous-anneau de $\mathcal{O}_K$.

(1) Montrer que $K = \mathrm{Frac}(A)$. En déduire que A n'est pas de Dedekind.
(2) Montrer que $\mathfrak{p} = 2A + \left(1+\sqrt{5}\right)A$ est un idéal premier de A, et que l'idéal $2A$ n'est pas premier.
(3) Montrer que $\mathfrak{p}^2 = 2\mathfrak{p}$. En déduire que $\mathfrak{p}$ n'est pas inversible.
(4) Déterminer le polynôme minimal de $\frac{1+\sqrt{5}}{2}$ sur $\mathbf{Q}$, et montrer que $2\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$.
(5) Montrer que $2A$ ne peut pas s'écrire $2A = IJ$ où I et J sont deux idéaux propres de A (on regardera $IJ\mathcal{O}_K$). En particulier, l'idéal $2A$ n'a pas de décomposition en produit d'idéaux premiers de A.

Exercice 9. Soit $K = \mathbf{Q}(i\sqrt{5})$. On a $\mathcal{O}_K = \mathbf{Z}\left[i\sqrt{5}\right]$, c'est un anneau de Dedekind.

(1) Soit $I = 2\mathcal{O}_K + \left(1+i\sqrt{5}\right)\mathcal{O}_K$. Montrer que $I^2 = 2\mathcal{O}_K$. En déduire que $\mathcal{O}_K$ n'est pas principal.
(2) Donner la décomposition de $2\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$.

Exercice 10. Soient $\zeta = e^{\frac{2i\pi}{23}}$ et $K = \mathbf{Q}(\zeta)$. Le but de cet exercice est de prouver que $\mathcal{O}_K$ n'est pas principal.

(1) Montrer que $2^{23} - 1$ est divisible par 47 mais pas par 47^2. Calculer $\mathrm{N}_{K/\mathbf{Q}}(\zeta - 2)$.
(2) Soit $\mathfrak{a}$ l'idéal de $\mathcal{O}_K$ engendré par 47 et $\zeta - 2$. Montrer que pour tout $x \in \mathfrak{a}$, on a $47 \mid \mathrm{N}_{K/\mathbf{Q}}(x)$.
(3) Supposons qu'il existe $\alpha \in \mathcal{O}_K$ tel que $\mathfrak{a} = \alpha\mathcal{O}_K$. Montrer que $\mathrm{N}(\alpha)$ divise 47^{22} et $\mathrm{N}(\zeta - 2)$. En déduire $\mathrm{N}(\alpha)$.
(4) Montrer que K contient une unique extension quadratique L de $\mathbf{Q}$ et que $L = \mathbf{Q}\left(i\sqrt{23}\right)$.
(5) Soit $\beta = \mathrm{N}_{K/L}(\alpha)$. Montrer que $\beta \in \mathcal{O}_L$ et montrer $\mathrm{N}_{L/\mathbf{Q}}(\beta) = 47$.
(6) Montrer que $\mathcal{O}_L$ ne contient pas d'élément de norme 47 et conclure.

Exercice 11. Dans $A := \mathbf{Z}\left[i\sqrt{3}\right]$ on considère l'idéal $\mathfrak{a}$ engendré par 2 et $1 + i\sqrt{3}$. Montrer que $\mathfrak{a} \neq 2A$ et que $\mathfrak{a}^2 = 2\mathfrak{a}$. En déduire que les idéaux de $\mathbf{Z}\left[i\sqrt{3}\right]$ ne se factorisent pas de manière unique en produit d'idéaux premiers. Montrer que $\mathfrak{a}$ est l'unique idéal premier contenant 2. En déduire que $2A$ ne s'écrit pas comme un produit d'idéaux premiers.

Exercice 12.
(1) Étudier la décomposition dans $\mathbf{Q}[i]$ des nombres premiers 2, 3, 5. Donner un générateur pour chacun des idéaux premiers trouvés.
(2) Étudier la décomposition dans $\mathbf{Q}[i\sqrt{5}]$ des nombres premiers 2, 3, 5 et 11. Est-il possible de donner des générateurs pour les idéaux premiers qui apparaissent ?
(3) Étudier la décomposition dans $\mathbf{Q}[i\sqrt{3}]$ des nombres premiers 2, 3, 5 et 7.

Exercice 13.
(1) Soit α une racine de $X^3 - 2$. On a vu précédemment que l'anneau des entiers de $\mathbf{Q}[\alpha]$ est $\mathbf{Z}[\alpha]$. Étudier la décomposition dans $\mathbf{Z}[\alpha]$ des nombres premiers 2, 3, 5, 7 et 31 (on admettra que $X^3 - 2 \equiv (X-4)(X-7)(X+11) \mod 31\,\mathbf{Z}[X]$).

(2) Soit α une racine de $X^3 - X - 1$. On a vu précédemment que l'anneau des entiers de $\mathbf{Q}[\alpha]$ est $\mathbf{Z}[\alpha]$. Étudier la décomposition dans $\mathbf{Z}[\alpha]$ des nombres premiers 2, 3, 5 et 23.

Exercice 14. Soient $P = X^3 + X^2 - 2X + 8$, $x \in \mathbf{C}$ une racine de P et $K = \mathbf{Q}[x]$.

(1) Montrer que P est irréductible sur $\mathbf{Q}$.
(2) Montrer que le dicriminant de $\mathbf{Z}[x]$ vaut -2012.
(3) Quel est le polynôme minimal de $\frac{1}{x}$? En déduire que $y = \frac{4}{x} \in \mathcal{O}_K$. Exprimer y dans la base $(1, x, x^2)$.
(4) Soit $\Lambda = \mathbf{Z} + \mathbf{Z}\,x + \mathbf{Z}\,y$. Montrer que $\mathbf{Z}[x]$ est d'indice 2 dans Λ. En déduire le discriminant de Λ.
(5) En admettant que 503 est premier, montrer que $\mathcal{O}_K = \Lambda$.
(6) On définit trois applications

$$\begin{aligned} \phi_1 \colon \mathcal{O}_K &\to \mathbf{F}_2 \\ a + bx + cy &\mapsto a \mod 2\,\mathbf{Z} \end{aligned}$$

$$\begin{aligned} \phi_2 \colon \mathcal{O}_K &\to \mathbf{F}_2 \\ a + bx + cy &\mapsto a + b \mod 2\,\mathbf{Z} \end{aligned}$$

$$\begin{aligned} \phi_3 \colon \mathcal{O}_K &\to \mathbf{F}_2 \\ a + bx + cy &\mapsto a + c \mod 2\,\mathbf{Z} \end{aligned}$$

Montrer que ϕ_1, ϕ_2 et ϕ_3 sont des morphismes d'anneaux. (On pourra calculer xy, x^2 et y^2 modulo 2.)
(7) Pour $i \in \{1, 2, 3\}$, on pose $\mathfrak{p}_i = \mathsf{Ker}(\phi_i)$. Montrer que les $\mathfrak{p}_i$ sont des idéaux premiers deux à deux distincts, et que $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.
(8) En déduire qu'il n'existe aucun $z \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbf{Z}[z]$.