Théorie algébrique des nombres
Feuille d'exercices n°2

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

Exercice 1. Montrer que les éléments $\frac{2}{3+\sqrt{13}} \in \mathbf{C}$ et $\frac{-2+\sqrt{2}+i\sqrt{2}}{2} \in \mathbf{C}$ sont entiers sur $\mathbf{Z}$.

Exercice 2. Soient K un corps et A la sous-K-algèbre de $K[X,Y]$ engendrée par les monômes X^kY^{k+1} pour $k \in \mathbf{N}$. Montrer que $A[XY]$ est contenu dans un sous-A-module de type fini de $K[X,Y]$, mais que XY n'est pas entier sur A.

Exercice 3. Soient $A \subseteq B$ une extension d'anneaux avec A noethérien, $x \in B^\times$, et $y \in A[x] \cap A[x^{-1}]$. Montrer qu'il existe $n \in \mathbf{N}$ tel que le sous-A-module $M = A + Ax + \cdots + Ax^n \subseteq B$ soit stable par l'opération de multiplication par y. En déduire que y est entier sur A.

Exercice 4. Soient A un anneau intègre et $\alpha \in A \setminus \{0\}$. On suppose l'anneau $A/\alpha A$ réduit et l'anneau localisé $A[\alpha^{-1}]$ intégralement clos. Montrer que A est intégralement clos.

Exercice 5. Soient A un anneau et G un groupe fini d'automorphismes de A. Montrer que l'extension $A^G \subseteq A$ est entière.

Exercice 6. Soient $A \subseteq B$ une extension entière, $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ des idéaux premiers de B tels que $\mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A$. Montrer que $\mathfrak{p}_1 = \mathfrak{p}_2$.

Exercice 7. Soient A un anneau intègre, K son corps des fractions, L/K une extension algébrique de corps, B la clôture intégrale de A dans L et $S \subseteq A \setminus \{0\}$ une partie multiplicative. Montrer que la clôture intégrale du localisé $S^{-1}A$ dans L est le localisé $S^{-1}B$.

Exercice 8. Soient A un anneau intégralement clos, K son corps des fractions, et $P \in A[X]$ unitaire. Montrer que si P est réductible dans $K[X]$, alors P est réductible dans $A[X]$.

Exercice 9. On sait que l'anneau des entiers de $\mathbf{Q}\left(\sqrt{3}\right)$ (resp. de $\mathbf{Q}\left(\sqrt{7}\right)$) est $\mathbf{Z}\left[\sqrt{3}\right]$ (resp. $\mathbf{Z}\left[\sqrt{7}\right]$). Montrer que $\mathbf{Z}\left[\sqrt{3},\sqrt{7}\right]$ n'est pas l'anneau des entiers de $\mathbf{Q}\left(\sqrt{3},\sqrt{7}\right)$ (regarder $\frac{\sqrt{3}+\sqrt{7}}{2}$).

Exercice 10. Soient $\alpha \in \mathbf{C}$ une racine du polynôme $X^3 - 10 \in \mathbf{Q}[X]$ et $K = \mathbf{Q}(\alpha)$. Montrer que $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$ (on montrera que $\frac{1+\alpha+\alpha^2}{3} \in \mathcal{O}_K$).

Exercice 11. Soient $\alpha \in \mathbf{C}$ une racine du polynôme $X^3 - X - 4 \in \mathbf{Q}[X]$ et $K = \mathbf{Q}(\alpha)$. Montrer que $\left(1, \alpha, \frac{\alpha+\alpha^2}{2}\right)$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$.

Exercice 12. Soient $\alpha \in \mathbf{C}$ une racine du polynôme $X^5 - X - 1 \in \mathbf{Q}[X]$ et $K = \mathbf{Q}(\alpha)$. Montrer que $\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4\right)$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$.

Exercice 13. Soient $P(X) = X^3 - 3X + 1 \in \mathbf{Q}[X]$ et $\alpha \in \mathbf{C}$ une racine de P.

(1) Montrer que P est irréductible dans $\mathbf{Q}[X]$.
(2) Posons $K = \mathbf{Q}(\alpha)$. Calculer $\mathrm{D}(1, \alpha, \alpha^2)$. En déduire que $9\mathcal{O}_K \subseteq \mathbf{Z}[\alpha] \subseteq \mathcal{O}_K$.
(3) Montrer que $\alpha, \alpha+2 \in \mathcal{O}_K^\times$, que $(\alpha+1)^3 = 3\alpha(\alpha+2)$ et que $(\alpha+1)\mathcal{O}_K$ (resp. $(\alpha+1)\,\mathbf{Z}[\alpha]$) est un idéal premier de $\mathcal{O}_K$ (resp. de $\mathbf{Z}[\alpha]$).
(4) Montrer que $\mathbf{Z}[\alpha] \cap (\alpha+1)\mathcal{O}_K = (\alpha+1)\,\mathbf{Z}[\alpha]$. En déduire que $\mathbf{Z}[\alpha] \cap 3\mathcal{O}_K = 3\,\mathbf{Z}[\alpha]$, puis que l'application naturelle $\mathbf{Z}[\alpha]/3\,\mathbf{Z}[\alpha] \to \mathcal{O}_K/3\mathcal{O}_K$ est bijective, et que $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

Exercice 14. Soient $\alpha \in \mathbf{C}$ racine de $X^3 - 3X + 9$ et $K = \mathbf{Q}[\alpha]$. Calculer le discriminant de $(1, \alpha, \alpha^2)$. Montrer que $\beta = \frac{\alpha^2}{3} \in \mathcal{O}_K$ (on pourra calculer le polynôme caractéristique de β), et en déduire que $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\,\alpha + \mathbf{Z}\,\beta$.

Exercice 15. Soient p un nombre premier, $r \in \mathbf{N}_{>0}$ et $\zeta \in \mathbf{C}$ une racine primitive p^r-ième de l'unité. Posons $K = \mathbf{Q}(\zeta)$. On se propose de démontrer que $\mathcal{O}_K = \mathbf{Z}[\zeta]$.

(1) Montrer que si $\zeta' \in \mathbf{C}$ est une racine primitive p^r-ième de l'unité, alors
$$\frac{1-\zeta'}{1-\zeta} \in \mathbf{Z}[\zeta]$$
(2) Montrer la formule $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}$. En déduire que $\Phi_{p^r}(1) = p$. Démontrer que
$$p = u(1-\zeta)^{\varphi(p^r)}$$
où u est une unité de $\mathbf{Z}[\zeta]$ (et donc de $\mathcal{O}_K$). Montrer que $\pi = 1 - \zeta$ n'est pas inversible dans $\mathcal{O}_K$.
(3) Montrer que pour tout $m \in \{0, \ldots, r-1\}$, on a $\mathrm{N}_{K/\mathbf{Q}}\left(1-\zeta^{p^m}\right) = p^{p^m}$ (on pourra commencer par le cas $m = 0$, puis en déduire le cas général). Après avoir calculé $\Phi'_{p^r}(\zeta)$, en déduire que $\mathrm{N}_{K/\mathbf{Q}}\left(\Phi'_{p^r}(\zeta)\right) = \pm p^c$ pour un certain entier c. En déduire que $\#(\mathcal{O}_K/\,\mathbf{Z}[\zeta])$ est une puissance de p.
(4) Montrer que $\#\mathcal{O}_K/\pi^{\varphi(n)}\mathcal{O}_K = p^{\varphi(n)}$. En déduire $\#\mathcal{O}_K/\pi\mathcal{O}_K$, puis que le morphisme d'anneaux $\mathbf{Z}/p\,\mathbf{Z} \to \mathcal{O}_K/\pi\mathcal{O}_K$ est bijectif. Établir l'égalité $\mathcal{O}_K = \mathbf{Z}[\zeta] + \pi^k\mathcal{O}_K$ pour tout $k \in \mathbf{N}_{>0}$, puis conclure.

Exercice 16. Soient $\alpha = \sqrt[3]{2} \in \mathbf{R}$, $A = \mathbf{Z}[\alpha]$ et $K = \mathbf{Q}(\alpha)$. On veut montrer que $\mathcal{O}_K = A$.

(1) Montrer que $A \subseteq \mathcal{O}_K$ et donner une base de A sur $\mathbf{Z}$.
(2) Calculer le discriminant $\mathrm{D}(1, \alpha, \alpha^2)$.
(3) Soient $a, b, c \in \mathbf{Q}$ et $x = a + b\alpha + c\alpha^2 \in K$. Calculer $\mathrm{Tr}_{K/\mathbf{Q}}(x)$, $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha x)$ et $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha^2 x)$. En déduire que $6\mathcal{O}_K \subseteq A$.
(4) Soient $a, b, c \in \mathbf{Q}$ et $x = a + b\alpha + c\alpha^2 \in K$. Calculer le polynôme caractéristique de x. En déduire que $x \in \mathcal{O}_K$ si et seulement si
$$(*) \qquad \begin{cases} 3a \in \mathbf{Z} \\ 3a^2 - 6bc \in \mathbf{Z} \\ 6abc - a^3 - 2b^3 - 4c^3 \in \mathbf{Z} \end{cases}$$
En déduire que si $x \in \mathcal{O}_K$, on a $3b \in \mathbf{Z}$ (multiplier la troisième équation de $(*)$ par 18), puis que $3c \in \mathbf{Z}$, de sorte que $3\mathcal{O}_K \subseteq A$.

(5) Supposons toujours $x \in \mathcal{O}_K$. Notons $\overline{a}$, $\overline{b}$ et $\overline{c}$ les images dans $\mathbf{Z}/3\,\mathbf{Z}$ de $3a$, $3b$ et $3c$ respectivement. Montrer que $\overline{a}^2 + \overline{b}\overline{c} = 0$. Montrer que $\overline{a} = 0$ (raisonner par l'absurde : si $\overline{a} \neq 0$, montrer que $b + c \in \mathbf{Z}$, et de même que $a + b \in \mathbf{Z}$, puis éliminer a et c dans la troisième équation de $(*)$ pour arriver à une contradiction). En déduire que $a \in \mathbf{Z}$ et que $b \in \mathbf{Z}$ ou $c \in \mathbf{Z}$, puis conclure.

Exercice 17. Soit $P(X) = X^n + a_{n-1} + \cdots + a_1 X + a_0 \in \mathbf{Z}[X]$ un polynôme d'Eisenstein en p pour un certain premier p. On considère le corps de nombres $K = \mathbf{Q}[\theta]$ engendré par une racine θ de $P(X)$ dans $\mathbf{C}$.

(1) Vérifier que l'indice $[\mathcal{O}_K : \mathbf{Z}[\theta]]$ est fini.
(2) Soit $x = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \in \mathbf{Z}[\theta]$. Montrer que $\mathrm{N}_{K/\mathbf{Q}}(x) \equiv c_0^n \mod p\,\mathbf{Z}$ (on pourra considérer la matrice de la multiplication par x dans la base $(1, \theta, \ldots, \theta^{n-1})$).
(3) On souhaite montrer que l'indice $[\mathcal{O}_K : \mathbf{Z}[\theta]]$ est premier à p. Supposons que ce ne soit pas le cas.
   (a) Montrer que $\mathcal{O}_K$ contient un élément y de la forme $y = \frac{c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}}{p}$ où les c_i sont des entiers non tous divisibles par p.
   (b) Montrer que c_0 est divisible par p.
   (c) Montrer, de proche en proche, que tous les c_i sont divisibles par p, et conclure.
(4) Application : déterminer l'anneau des entiers $K = \mathbf{Q}[\theta]$, où $\theta \in \mathbf{C}$ est une racine du polynôme $P(X) = X^3 - 3$.

Exercice 18. Soient $\alpha \in \mathbf{C}$ un entier algébrique non nul dont tous les conjugués sont de module ≤ 1. Montrer que α est une racine de l'unité (théorème de Kronecker).