Entiers algébriques : correction

Exercice 1. On rappelle le résultat principal de l'exercice 4 du TD 4 (et sa preuve) :

> Si A est un anneau de corps des fractions K et que L/K est une extension algébrique, $s \in \mathrm{L}$ est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans la clôture intégrale $\mathrm{A_K}$ de A dans K.

– Si le polynôme minimal $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ de s est à coefficients dans $\mathrm{A_K}$, s est entier sur $\mathrm{A_K}$ et donc sur A, $\mathrm{A_K}$ étant entier sur A.
– Réciproquement, si $\mathrm{Q} \in \mathrm{A}[\mathrm{X}]$ est un polynôme unitaire tel que $\mathrm{Q}(s) = 0$, le polynôme minimal P divise Q. À ce titre, toutes ses racines dans une clôture algébrique $\overline{\mathrm{K}}$ sont entières sur A et il en va de même de ses coefficients (d'après les relations coefficients-racines et parce que les éléments entiers sur A forment un anneau). Les coefficients de P sont donc entiers sur A, ce qui signifie exactement $\mathrm{P} \in \mathrm{A_K}[\mathrm{X}]$.

1. Évidemment, si α est racine d'un polynôme unitaire $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$, α est algébrique.
   Si maintenant $\alpha \in \overline{\mathbf{Q}}$, on applique le résultat principal cité plus haut (à $\mathrm{A} = \mathbf{Z}$, $\mathrm{K} = \mathbf{Q}$ et $\mathrm{L} = \overline{\mathbf{Q}}$; dans ce cas, le cours garantit que $\mathrm{A_K} = \mathbf{Z}$) et on obtient bien
   $$\alpha \in \mathscr{O}_{\mathbf{C}} \text{ si et seulement si le polynôme minimal de A est dans } \mathbf{Z}[\mathrm{X}].$$
2. On va encore vouloir appliquer le même résultat (à $\mathrm{A} = \mathscr{O}_{\mathrm{K}}$, K et $\mathrm{L} = \overline{\mathbf{Q}}$). On remarque alors que la preuve de l'énoncé donné en ouverture n'utilise nulle part le fait que K est le corps des fractions de l'anneau A : il est simplement important que K contienne A. On peut donc obtenir directement le résultat sans vérifier que K est le corps des fractions de $\mathscr{O}_{\mathrm{K}}$:
   $$\alpha \in \mathscr{O}_{\mathbf{C}} \text{ si et seulement si le polynôme minimal de } \alpha \text{ sur K est dans } \mathscr{O}_{\mathrm{K}}[\mathrm{X}].$$
   Vérifions tout de même que $\mathrm{K} = \mathrm{Frac}\,\mathscr{O}_{\mathrm{K}}$, ce résultat étant utile. Pour cela, prenons $x \in \mathrm{K}$. Comme $\mathrm{K}/\mathbf{Q}$ est algébrique, il existe des coefficients rationnels (a_i) tels que
   $$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$
   Soit $\Delta \in \mathbf{Z}$ non nul tel que $\forall i, \Delta a_i \in \mathbf{Z}$. On a alors
   $$\Delta^n \left(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \right) = 0$$
   $$\text{ou encore : } (\Delta x)^n + \Delta a_{n-1}(\Delta x)^{n-1} + \cdots + \Delta^{n-1} a_1 (\Delta x) + \Delta^n a_0 = 0$$
   et Δx est annulé par le polynôme unitaire
   $$\mathrm{X}^n + \Delta a_{n-1}\mathrm{X}^{n-1} + \cdots + \Delta^{n_1} a_1 \mathrm{X} + \Delta^n a_0 \in \mathbf{Z}[\mathrm{X}].$$
   En particulier, on a prouvé que tout élément x de K s'écrivait sous la forme $\widetilde{x}/\Delta$, où $\widetilde{x} \in \mathscr{O}_{\mathrm{K}}$ et $\Delta \in \mathbf{Z} \setminus \{0\}$. Comme $\mathbf{Z} \subseteq \mathscr{O}_{\mathrm{K}}$, il s'ensuit que K est bien le corps des fractions de $\mathscr{O}_{\mathrm{K}}$.
3. On a vu (TD 1, exercice 8) que toute extension quadratique de $\mathbf{Q}$ s'écrit $\mathrm{K} = \mathbf{Q}(\sqrt{d})/\mathbf{Q}$, où $d \in \mathbf{Z}$ est sans facteur carré. Le cours affirme alors que
   $$\mathscr{O}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \mathbf{Z}[\sqrt{d}] & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \mathbf{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Exercice 2.

1. C'est tautologique. À vrai dire, $\mathrm{T}^{\mathrm{L}}_{\alpha}$ est même L-linéaire.
2. Si α_{K}, $\mathrm{T}^{\mathrm{L}}_{\alpha} = \alpha\,\mathrm{id}_{\mathrm{L}}$. On a donc
$$\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha) = \mathrm{tr}(\alpha\,\mathrm{id}_{\mathrm{L}}) = \alpha\cdot[\mathrm{L}:\mathrm{K}] \qquad \mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\alpha) = \mathrm{dét}(\alpha\,\mathrm{id}_{\mathrm{L}}) = \alpha^{[\mathrm{L}:\mathrm{K}]}.$$
3. Si $\alpha,\beta\in\mathrm{L}$ et $\lambda\in\mathrm{K}$, on a clairement $\mathrm{T}^{\mathrm{L}}_{\alpha+\lambda\beta} = \mathrm{T}^{\mathrm{L}}_{\alpha} + \lambda\mathrm{T}^{\mathrm{L}}_{\beta}$ et $\mathrm{T}^{\mathrm{L}}_{\alpha\beta} = \mathrm{T}^{\mathrm{L}}_{\alpha}\circ\mathrm{T}^{\mathrm{L}}_{\beta}$.
Il s'ensuit que $\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha+\lambda\beta) = \mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha) + \lambda\,\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\beta)$ et $\mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\alpha\beta) = \mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\alpha)\,\mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\beta)$.
4. Soit $(\beta_i)_{i=1}^{d}$ une L-base de M. On a donc $d = [\mathrm{M}:\mathrm{L}]$. En tant que L-espace vectoriel, M se décompose donc en une somme directe (de L-droites)
$$\mathrm{M} = \mathrm{L}\beta_1 \oplus \cdots \oplus \mathrm{L}\beta_d.$$
Puisque $\alpha\in\mathrm{L}$, la multiplication $\mathrm{T}^{\mathrm{L}}_{\alpha}$ préserve chacun des facteurs.
En outre, comme $\beta_i \neq 0$, la multiplication par β_i induit un isomorphisme L-linéaire
$$\varphi_i : \left(\mathrm{T}^{\mathrm{L}}_{\beta_i}\right)_{|\mathrm{L}} : \mathrm{L} \to \mathrm{L}\beta_i,$$
d'inverse $\varphi_i^{-1} = \left(\mathrm{T}^{\mathrm{L}}_{\beta_i^{-1}}\right)_{\mathrm{L}\beta_i}$ et l'on a
$$\varphi_i^{-1}\circ\left(\mathrm{T}^{\mathrm{M}}_{\alpha}\right)_{|\mathrm{L}\beta_i}\circ\varphi = \left(\mathrm{T}^{\mathrm{M}}_{\alpha}\right)_{|\mathrm{L}} = \mathrm{T}^{\mathrm{L}}_{\alpha},$$
ce qui n'est rien d'autre que le fait que $\alpha\beta_i = \beta_i\alpha$.
En particulier, on a
$$\mathrm{tr}_{\mathrm{K}}\left(\mathrm{T}^{\mathrm{M}}_{\alpha}\right)_{|\mathrm{L}\beta_i} = \mathrm{tr}_{\mathrm{K}}\,\mathrm{T}^{\mathrm{L}}_{\alpha} = \mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha)$$
$$\mathrm{dét}_{\mathrm{K}}\left(\mathrm{T}^{\mathrm{M}}_{\alpha}\right)_{|\mathrm{L}\beta_i} = \mathrm{dét}_{\mathrm{K}}\,\mathrm{T}^{\mathrm{L}}_{\alpha} = \mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\alpha).$$
On obtient donc
$$\mathrm{Tr}_{\mathrm{M}/\mathrm{K}}(\alpha) = \mathrm{tr}_{\mathrm{K}}\,\mathrm{T}^{\mathrm{M}}_{\alpha} = \sum_{i=1}^{d}\mathrm{tr}_{\mathrm{K}}\left(\mathrm{T}^{\mathrm{M}}_{\alpha}\right)_{|\mathrm{L}\beta_i} = d\,\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha)$$
$$\mathrm{Nm}_{\mathrm{M}/\mathrm{K}}(\alpha) = \mathrm{dét}_{\mathrm{K}}\,\mathrm{T}^{\mathrm{M}}_{\alpha} = \prod_{i=1}^{d}\mathrm{dét}_{\mathrm{K}}\left(\mathrm{T}^{\mathrm{M}}_{\alpha}\right)_{|\mathrm{L}\beta_i} = \mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\alpha)^d.$$
Remarque. En supposant simplement $\alpha\in\mathrm{M}$, on peut également démontrer les fomules dites *de transitivité*
$$\mathrm{Tr}_{\mathrm{M}/\mathrm{K}}(\alpha) = \mathrm{Tr}_{\mathrm{M}/\mathrm{L}}\left(\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(\alpha)\right) \qquad \mathrm{Nm}_{\mathrm{M}/\mathrm{K}}(\alpha) = \mathrm{Nm}_{\mathrm{M}/\mathrm{L}}\left(\mathrm{Nm}_{\mathrm{L}/\mathrm{K}}(\alpha)\right),$$
dont ce qu'on vient de démontrer n'est qu'un cas particulier.
5. On remarque que si $\mathrm{Q}\in\mathrm{K}[\mathrm{X}]$ est un polynôme et si $\alpha\in\mathrm{L}$, on a $\mathrm{Q}(\mathrm{T}^{\mathrm{L}}_{\alpha}) = \mathrm{T}^{\mathrm{L}}_{\mathrm{Q}(\alpha)}$. Comme en outre $\mathrm{T}^{\mathrm{L}}_{\beta}$ est nul si et seulement si β l'est, on obtient que le polynôme minimal de α est exactement le polynôme minimal de $\mathrm{T}^{\mathrm{L}}_{\alpha}$. Puisque son degré est déjà égal à la dimension de L, le théorème de Cayley-Hamilton entraîne que c'en est également le polynôme caractéristique.
Remarque. On peut aussi faire le calcul dans la base $(1,\alpha,\ldots,\alpha^{n-1})$ de $\mathrm{K}(\alpha)$: si on écrit $\mathrm{P} = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0 \in \mathrm{K}[\mathrm{X}]$ le polynôme minimal de α sur K, la matrice de $\mathrm{T}^{\mathrm{K}(\alpha)}_{\alpha}$ dans notre base est la matrice compagnon
$$\begin{pmatrix} & & -a_0 \\ 1 & & -a_1 \\ & \ddots & \vdots \\ & 1 & -a_{n-1} \end{pmatrix}$$
de P. En particulier, son polynôme caractéristique est bien P.

6. D'après la question précédente et les relations coefficients-racines, si on note $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynôme minimal de α sur K, on a

$$\begin{aligned} \mathrm{Tr}_{K(\alpha)/K}(\alpha) &= -a_{n-1} \text{ est bien la somme des racines de P et} \\ \mathrm{Nm}_{K(\alpha)/K}(\alpha) &= (-1)^n a_0 \text{ en est bien le produit.} \end{aligned}$$

Donc, d'un côté, grâce à la question 4, on a

$$\mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)]\,\mathrm{Tr}_{K(\alpha)/K}(\alpha) \qquad \mathrm{Nm}_{L/K}(\alpha) = \big(\mathrm{Nm}_{K(\alpha)/K}(\alpha)\big)^{[L:K(\alpha)]}.$$

De l'autre côté, si on note $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ les racines du polynôme minimal de α, on sait que $K(\alpha)$ a n plongements K-linéaires σ_i dans $\mathbf{C}$, caractérisés par $\sigma_i(\alpha) = \alpha_i$.
Chacun de ces σ_i plongements se prolonge en $[L : K(\alpha)]$ plongements différents de L dans $\mathbf{C}$, qui vérifient donc $\sigma(\alpha) = \alpha_i$. On a donc

$$\begin{aligned} \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \sigma(\alpha) &= \sum_{\sigma \in \mathrm{Hom}_K(K(\alpha),\mathbf{C})} \sum_{\substack{\tilde{\sigma} \in \mathrm{Hom}_K(L,\mathbf{C}) \\ \tilde{\sigma} \text{ prolonge } \sigma}} \tilde{\sigma}(\alpha) \\ &= [L : K(\alpha)] \sum_{i=1}^{n} \alpha_i = [L : K(\alpha)]\,\mathrm{Tr}_{K(\alpha)/K}(\alpha) = \mathrm{Tr}_{L/K}(\alpha). \\ \prod_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \sigma(\alpha) &= \prod_{\sigma \in \mathrm{Hom}_K(K(\alpha),\mathbf{C})} \prod_{\substack{\tilde{\sigma} \in \mathrm{Hom}_K(L,\mathbf{C}) \\ \tilde{\sigma} \text{ prolonge } \sigma}} \tilde{\sigma}(\alpha) \\ &= \prod_{i=1}^{n} \alpha_i^{[L:K(\alpha)]} = \big(\mathrm{Nm}_{K(\alpha)/K}(\alpha)\big)^{[L:K(\alpha)]} = \mathrm{Nm}_{L/K}(\alpha). \end{aligned}$$

7. D'après ce qui précède, si $\alpha \in \mathcal{O}_L$, les coefficients de son polynôme minimal (sur $\mathbf{Q}$), et en particulier $\mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ et $\mathrm{Nm}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$, doivent être des éléments de $\mathcal{O}_{\mathbf{Q}} = \mathbf{Z}$. Il en est alors de même de

$$\mathrm{Tr}_{L/\mathbf{Q}}(\alpha) = [L : \mathbf{Q}(\alpha)]\,\mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha) \qquad \text{et} \qquad \mathrm{Nm}_{L/\mathbf{Q}}(\alpha) = \mathrm{Nm}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)^{[L:\mathbf{Q}(\alpha)]}.$$

8. Dans la suite de l'exercice, on note simplement $\mathrm{Tr} = \mathrm{Tr}_{L/\mathbf{Q}}$ et $\mathrm{Nm} = \mathrm{Nm}_{L/\mathbf{Q}}$.
Supposons que $\alpha \in \mathcal{O}_L$ soit une unité de $\mathcal{O}_L$: on peut donc trouver $\beta \in \mathcal{O}_L$ tel que $\alpha\beta = 1$. On a donc une égalité (dans $\mathbf{Z}$, d'après la question précédente)

$$\mathrm{Nm}(\alpha) \cdot \mathrm{Nm}(\beta) = 1$$

et il s'ensuit que $\mathrm{Nm}(\alpha) \in \mathbf{Z}^\times = \{\pm 1\}$.
Réciproquement, supposons que $\mathrm{Nm}(\alpha) = \pm 1$. En écrivant le polynôme minimal (sur $\mathbf{Q}$) de α, on obtient donc des coefficients entiers (a_i) tels que

$$\alpha^n + a_{n_1}\alpha^{n-1} + \cdots + a_1\alpha \pm 1 = 0.$$

En multipliant par $\alpha^{-n} \in L$, on obtient donc

$$\pm\alpha^{-n} + a_1\alpha^{-(n-1)} + \cdots + a_{n-1}\alpha^{-1} + 1 = 0$$

et α^{-1} est bien racine d'un polynôme unitaire à coefficients entiers : $\alpha^{-1} \in \mathcal{O}_L$.

9. Un élément $\alpha \in \mathbf{Q}(\sqrt{d})$ s'écrit d'une façon unique $\alpha = x + y\sqrt{d}$, avec $x, y \in \mathbf{Q}$. Par exemple à cause de la question 6, on a

$$\mathrm{Tr}(\alpha) = \left(x + y\sqrt{d}\right) + \left(x - y\sqrt{d}\right) = 2x \quad \text{et} \quad \mathrm{Nm}(\alpha) = \left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right) = x^2 - dy^2.$$

Si $\alpha \in \mathscr{O}_\mathrm{L}$, ces deux nombres sont entiers d'après la question précédente.
Réciproquement, si ces deux nombres sont entiers, distinguons deux cas :
– Si $\alpha \in \mathbf{Q}$, c'est-à-dire si $y = 0$, $\mathrm{Tr}(\alpha) = 2\alpha$ et $\mathrm{Nm}(\alpha) = \alpha^2$. Ainsi, $\alpha^2 \in \mathbf{Z}$, ce qui n'est possible pour un nombre rationnel que si $\alpha \in \mathbf{Z}$ (si on veut, c'est une conséquence du fait que $\mathbf{Z}$ est intégralement clos).
– Si $\alpha \notin \mathbf{Q}$, on a $\mathrm{L} = \mathbf{Q}(\alpha)$. Ainsi, la question 5 entraîne que le polynôme minimal de α est

$$\mathrm{X}^2 - \mathrm{Tr}(\alpha)\mathrm{X} + \mathrm{Nm}(\alpha).$$

On a donc bien que $\alpha \in \mathscr{O}_\mathrm{L}$ si et seulement si $\mathrm{Tr}(\alpha)$ et $\mathrm{Nm}(\alpha)$ sont entiers.

10. On cherche donc à calculer les unités de l'anneau des entiers d'un $\mathrm{L} = \mathbf{Q}(\sqrt{d})$, avec d négatif et sans facteur carré. (Ces anneaux sont appelés *anneaux d'entiers quadratiques imaginaires,* pour des raisons évidentes.)
D'après ce qui précède, il est légitime de distinguer deux cas :
– Si d est congru à 2 ou 3 modulo 4, on a

$$\mathscr{O}_\mathrm{L} = \mathbf{Z}\left[\sqrt{d}\right] = \left\{x + y\sqrt{d} \,\middle|\, x, y \in \mathbf{Z}\right\}$$

et

$$\mathrm{Nm}\left(x + y\sqrt{d}\right) = x^2 - dy^2.$$

Si $d \neq -1$, on a donc $-d > 1$ et, d'après la question 8,

$$x + y\sqrt{d} \in \mathscr{O}_\mathrm{L}^\times \Leftrightarrow \mathrm{Nm}\left(x + y\sqrt{d}\right) = \pm 1 \Leftrightarrow \begin{cases} x^2 = 1 \\ y = 0 \end{cases} \Leftrightarrow x + y\sqrt{d} = \pm 1.$$

– Si d est congru à 1 modulo 4, on a

$$\mathscr{O}_\mathrm{L} = \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ \frac{x + y\sqrt{d}}{2} \;\middle|\; \begin{array}{l} x, y \in \mathbf{Z} \\ x \equiv y \pmod 2 \end{array} \right\}$$

et

$$\mathrm{Nm}\left(\frac{x + y\sqrt{d}}{2}\right) = \frac{x^2 - dy^2}{4}.$$

Si $d \neq -3$, on a donc $-d \geq 7$ et

$$\frac{x + y\sqrt{d}}{2} \in \mathscr{O}_\mathrm{L}^\times \Leftrightarrow \mathrm{Nm}\left(\frac{x + y\sqrt{d}}{2}\right) = \pm 1 \Leftrightarrow x^2 + dy^2 = \pm 4 \Leftrightarrow \begin{cases} x^2 = 4 \\ y = 0 \end{cases} \Leftrightarrow \frac{x + y\sqrt{d}}{2} = \pm 1.$$

– Dans le cas $d = -1$ (donc $\mathrm{L} = \mathbf{Q}(i)$), on a

$$\mathscr{O}_\mathrm{L} = \mathbf{Z}[i] = \left\{x + iy \,\middle|\, x, y \in \mathbf{Z}\right\}$$

et

$$\mathrm{Nm}(x + iy) = x^2 + y^2.$$

On a donc

$$x + iy \in \mathscr{O}_\mathrm{L}^\times \Leftrightarrow \mathrm{Nm}(x + iy) = \pm 1 \Leftrightarrow x^2 + y^2 = \pm 1 \Leftrightarrow (x, y) \in \{(\pm 1, 0), (0, \pm 1)\}.$$

On a donc

$$\mathscr{O}_\mathrm{L}^\times = \{\pm 1, \pm i\}.$$

– Dans le cas $d=-3$ (donc $\mathrm{L}=\mathbf{Q}(\zeta_3)$), on a

$$\mathscr{O}_\mathrm{L}=\mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]=\left\{\frac{x+y\sqrt{3}i}{2}\;\middle|\;\begin{array}{l}x,y\in\mathbf{Z}\\ x\equiv y\ (\mathrm{mod}\ 2)\end{array}\right\}$$

et

$$\mathrm{Nm}\left(\frac{x+iy}{2}\right)=\frac{x^2+3y^2}{4}.$$

On a donc

$$\frac{x+iy}{2}\in\mathscr{O}_\mathrm{L}^\times\Leftrightarrow\begin{cases}x,y\in\mathbf{Z}\\ x\equiv y\ (\mathrm{mod}\ 2)\\ x^2+3y^2=\pm4\end{cases}\Leftrightarrow(x,y)\in\{(\pm2,0),(\pm1,\pm1)\}$$

On a donc

$$\mathscr{O}_\mathrm{L}=\left\{\pm1,\pm\frac{1\pm\sqrt{3}}{2}\right\}=\left\{\zeta_6^k\,\middle|\,1\leq k\leq6\right\}.$$

Remarquons qu'*a posteriori*, ces résultats ne sont pas surprenants : si un corps de nombres contient une racine de l'unité ζ, celle-ci est racine d'un polynôme cyclotomique, donc entière sur $\mathbf{Z}$, et l'équation $\zeta^n=1$ entraîne qu'elle est une unité. On devait donc s'attendre à ce que les racines de l'unité de degré 2 sur $\mathbf{Q}$, c'est-à-dire $\pm\zeta_4=\pm i$, $\pm\zeta_3$ et $\pm\zeta_6$, apparussent quelque part.

Par ailleurs, un des premiers théorèmes de la théorie algébrique des nombres, le *théorème des unités de Dirichlet* affirme que si L est un corps de nombres arbitraire, $\mathscr{O}_\mathrm{L}^\times$ est un groupe (évidemment abélien) de type fini et en détermine la partie libre ; ce théorème a pour conséquence que $\mathbf{Q}$ et $\mathbf{Q}(\sqrt{d})$, avec $d<0$ sont les seuls corps de nombres L tels que $\mathscr{O}_\mathrm{L}^\times$ soit un groupe fini.

Exercice 3.

1. Commençons par calculer $\mathrm{Tr}(\zeta_p^j)$. Déjà, ζ_p^j ne dépend que de la classe de j modulo p. Si $j\not\equiv0\ (\mathrm{mod}\ p)$, ζ_p^j est une racine primitive p-ième de l'unité donc les $p-1=[\mathrm{L}:\mathbf{Q}]$ plongements $\sigma:\mathrm{L}\to\mathbf{C}$ envoient ζ_p^j sur les $p-1$ racines primitives $(\zeta_p^i)_{i=1}^p$ et

$$\mathrm{Tr}(\zeta_p^j)=\sum_{\sigma:\mathrm{L}\to\mathbf{C}}\sigma(\zeta_p^j)=\sum_{i=1}^{p}\zeta_p^j=\sum_{i=0}^{p}\zeta_p^j-1=-1.$$

Évidemment, si j est un multiple de p, $\zeta_p^j=1$ et sa trace est

$$\mathrm{Tr}(1)=[\mathrm{L}:\mathbf{Q}]=p-1.$$

On en déduit que

$$\mathrm{Tr}(\pi)=\mathrm{Tr}(1-\zeta_p)=\mathrm{Tr}(1)-\mathrm{Tr}(\zeta_p)=p-1-(-1)=p.$$

Par ailleurs,

$$\mathrm{Nm}(\pi)=\prod_{\sigma:\mathrm{L}\to\mathbf{C}}\sigma\left(1-\zeta_p\right)=\prod_{\sigma:\mathrm{L}\to\mathbf{C}}\left(1-\sigma(\zeta_p)\right)=\prod_{i=1}^{p-1}\left(1-\zeta_p^i\right)=\Phi_p(1)=p,$$

car $\Phi_p(\mathrm{X})=\mathrm{X}^{p-1}+\mathrm{X}^{p-2}+\cdots+\mathrm{X}+1$.

2. Si p ne divise pas b, ζ_p^b est une racine p-ième primitive. Il s'ensuit qu'on peut trouver un entier $n \leq p-1$ tel que $\zeta_p^a = \left(\zeta_p^b\right)^n$. En particulier,

$$\frac{1-\zeta_p^a}{1-\zeta_p^b} = \frac{1-\left(\zeta_p^b\right)^n}{1-\zeta_p^b} = 1+\zeta_p^b+\cdots+\left(\zeta_p^b\right)^{n-1} \in \mathbf{Z}[\zeta_p] \subseteq \mathscr{O}_\mathrm{L}.$$

De même si p ne divise pas a, $\dfrac{1-\zeta_p^b}{1-\zeta_p^a} \in \mathscr{O}_\mathrm{L}$. Il s'ensuit que si p ne divise ni a ni b,

$$\frac{1-\zeta_p^a}{1-\zeta_p^b} \in \mathscr{O}_\mathrm{L}^\times.$$

Remarque. Ces nombres sont ce que l'on appelle les *unités cyclotomiques*. En général, $\mathbf{Z}[\zeta_n]$ a d'autres unités.

En particulier, si $j \in \{1,\dots,p-1\}$, on a $\dfrac{1-\zeta_p^j}{\pi} = \dfrac{1-\zeta_p^j}{1-\zeta_p} \in \mathscr{O}_\mathrm{L}^\times$ et les éléments $1-\zeta_p^j$ et π sont associés dans $\mathscr{O}_\mathrm{L}$.

On a donc des unités u_j telles que $1-\zeta_p^j = u_j\pi$. Cela entraîne

$$p = \mathrm{Nm}(\pi) = \prod_{j=1}^{p-1}\left(1-\zeta_p^j\right) = \underbrace{u_1\cdots u_{p-1}}_{\in\mathscr{O}_\mathrm{L}^\times}\pi^{p-1}.$$

En résumé, p et π^{p-1} sont associés dans $\mathscr{O}_\mathrm{L}$, ce qui entraîne $p\mathscr{O}_\mathrm{L} = \pi^{p-1}\mathscr{O}_\mathrm{L}$.

3. D'après ce qui précède, $\pi\mathscr{O}_\mathrm{L}$ contient $\pi^{p-1}\mathscr{O}_\mathrm{L} = p\mathscr{O}_\mathrm{L}$ et donc p. Mais $\pi\mathscr{O}_\mathrm{L} \cap \mathbf{Z}$ est un idéal de $\mathbf{Z}$ (de manière générale, on vérifie sans difficulté que si I est un idéal d'un anneau B dont A est un sous-anneau, alors $\mathrm{I}\cap\mathrm{A}$ est un idéal de A). Par ailleurs, cet idéal ne contient pas 1 (cela entraînerait $\pi\mathscr{O}_\mathrm{L} = \mathscr{O}_\mathrm{L}$ et donc que π soit une unité, ce qui est impossible car $\mathrm{Nm}(\pi) = p$). L'ensemble $\pi\mathscr{O}_\mathrm{L} \cap \mathbf{Z}$ est donc un idéal strict de $\mathbf{Z}$ contenant le nombre premier p et on a

$$\pi\mathscr{O}_\mathrm{L} \cap \mathbf{Z} = p\mathbf{Z}.$$

4. (a) Si $j \in \{0,1,\dots,p-2\}$, on a

$$\mathrm{Tr}(\pi\zeta_p^j) = \mathrm{Tr}((1-\zeta_p)\zeta_p^j) = \mathrm{Tr}(\zeta_p^j) - \mathrm{Tr}(\zeta_p^{j+1}) = \begin{cases} (-1)-(-1) = 0 & \text{si } j \in \{1,\dots,p-2\} \\ p & \text{si } j = 0. \end{cases}$$

donc

$$\mathrm{Tr}(\pi x) = a_0\,\mathrm{Tr}(\pi) + a_1\,\mathrm{Tr}(\pi\zeta_p) + \cdots + a_{p-2}\,\mathrm{Tr}(\pi\zeta_p^{p-2}) = a_0 p.$$

(b) Déjà,

$$\mathrm{Tr}(\pi x) = \sum_\sigma \sigma(\pi x) = \sum_\sigma \sigma(\pi)\sigma(x),$$

la somme portant sur les plongements $\sigma : \mathrm{L} \to \mathbf{C}$. Or, $\sigma(\pi) = 1-\sigma(\zeta_p)$ est de la forme $1-\zeta_p^j$, pour un certain $j \in \{1,\dots,p-1\}$. D'après la question 2, cet élément de $\mathscr{O}_\mathrm{L}$ est associé à π.

Par ailleurs, les plongements de L dans $\mathbf{C}$ préservent le polynôme minimal des éléments et donc leur caractère entier. Si $x \in \mathscr{O}_\mathrm{L}$, on a donc pour tout σ, $\sigma(x) \in \mathscr{O}_\mathrm{L}$. Il s'ensuit que les $p-1$ facteurs $\sigma(\pi)\sigma(x)$ appartiennent tous à $\sigma(\pi)\mathscr{O}_\mathrm{L} = \pi\mathscr{O}_\mathrm{L}$. On a donc $\mathrm{Tr}(\pi x) \in \pi\mathscr{O}_\mathrm{L}$.

Enfin, si x est entier, il en est de même de πx donc $\mathrm{Tr}(\pi x) \in \mathbf{Z}$.

On a donc bien $\mathrm{Tr}(\pi x) \in \pi\mathscr{O}_\mathrm{L} \cap \mathbf{Z} = p\mathbf{Z}$.

Comme $\mathrm{Tr}(\pi x) = a_0 p$ d'après la question précédente, cela entraîne que $a_0 \in \mathbf{Z}$.

(c) On a donc déjà démontré que si

$$x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_L,$$

le coefficient a_0 est entier. En particulier, le nombre

$$\zeta_p^{-1}(x - a_0) = a_1 + a_2\zeta_p + \cdots + a_{p-2}\zeta_p^{p-3} \in \mathcal{O}_L$$

est encore dans $\mathcal{O}_L$, ce qui entraîne $a_1 \in \mathbf{Z}$. Par une récurrence immédiate, on obtient ainsi que tous les a_i sont entiers et donc que $x \in \mathbf{Z}[\zeta_p]$.

(d) Tout l'exercice a servi à démontrer que $\mathcal{O}_L \subseteq \mathbf{Z}[\zeta_p]$. Puisque ζ_p est clairement un entier algébrique, la réciproque est immédiate.

Remarque. De manière générale, si n est un entier quelconque, $\mathbf{Z}[\zeta_n]$ est exactement l'anneau $\mathcal{O}_{\mathbf{Q}(\zeta_n)}$ des entiers du corps cyclotomique.

Exercice 4.

1. Soit $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ les racines du polynôme caractéristique de $T = T_\alpha^{\mathbf{Q}(\alpha)}$ qui est égal, d'après la question 5 de l'exercice 2, au polynôme minimal de α sur $\mathbf{Q}$. En particulier, les α_i sont tous distincts et sont des entiers algébriques.

   Sur $\mathbf{C}$, la matrice T est semblable à la matrice diagonale $\mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_d)$. Sa puissance n-ième est donc semblable à la matrice diagonale $\mathrm{diag}(\alpha_1^n, \alpha_2^n, \ldots, \alpha_d^n)$.

   En particulier, d'après les relations coefficients-racines, les coefficients du polynôme caractéristique P_n de T^n sont au signe près les polynômes symétriques élémentaires

$$\sigma_k(\alpha_1^n, \ldots, \alpha_d^n) = \sum_{i_1 < i_2 < \cdots < i_k} \alpha_{i_1}^n \alpha_{i_2}^n \cdots \alpha_{i_k}^n.$$

   Cela entraîne du même coup que les coefficients de P_n sont des entiers algébriques (et donc des entiers usuels, puisqu'ils sont rationnels) et qu'en module,

$$|\sigma_k| \leq \sum_{i_1 < i_2 < \cdots < i_k} 1 = \binom{d}{k} \leq 2^d.$$

2. D'après la question précédente, les polynômes caractéristiques P_n vivent tous dans l'ensemble $\mathscr{P}_d$ des polynômes entiers unitaires de degré d à coefficients dans $\{-2^d, \ldots, 2^d\}$. Cet ensemble est fini.

   Ainsi, α^n vit dans l'ensemble $\bigcup_{P \in \mathscr{P}_d} Z_{\mathbf{C}}(P)$ des racines complexes de tels polynômes, et cet ensemble est également fini.

   D'après le principe des tiroirs, il existe deux entiers $n < m$ tels que $\alpha^n = \alpha^m$. On en déduit donc $\alpha^{m-n} = 1$, et α est une racine de l'unité.

3. Le nombre $z = \frac{3}{5} + \frac{4}{5}i$ est évidemment un nombre algébrique de polynôme minimal

$$(X - z)(X - \overline{z}) = X^2 - \frac{6}{5}X + 1.$$

   Comme $|z| = |\overline{z}| = 1$, ce nombre vérifie les hypothèses du résultat précédent (moins l'intégralité).

   Cependant, z n'est pas une racine de l'unité : en effet, vu son polynôme minimal, ce n'est même pas un entier algébrique.

Exercice 5.
Soit α un nombre de Pisot et $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ les racines de son polynôme minimal sur $\mathbf{Q}$.
Par intégralité de α (et donc de α^n), on a

$$\mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha^n) = \alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n \in \mathbf{Z}.$$

Comme $\forall i \in \{2, \ldots, d\}$, $|\alpha_i| < 1$, on a donc

$$d(\alpha^n, \mathbf{Z}) \leq |\alpha_2|^n + \cdots + |\alpha_d|^n \xrightarrow[n\to\infty]{} 0.$$