Théorie des nbrs 2 2023/2024
T.D. 1

On note $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$ le sous-anneau des entiers algébriques. Pour $x \in \overline{\mathbb{Q}}$, on note $\mathrm{P}_x \in \mathbb{Q}[\mathrm{T}]$ son polynôme minimal sur $\mathbb{Q}$. Rappelons que $x \in \overline{\mathbb{Q}}$ est entier ssi $\mathrm{P}_x \in \mathbb{Z}[\mathrm{T}]$. L'implication "si" est tautologique. Pour l'implication "seulement si", observer que si $\mathrm{P} \in \mathbb{Z}[\mathrm{T}]$ est un polynôme unitaire qui annule x alors $\mathrm{P}_x | \mathrm{P}$ dans $\mathbb{Q}[\mathrm{T}]$. En particulier les racines $x = x_1, \ldots, x_r$ de P_x sont des entiers algébriques. Comme $\overline{\mathbb{Z}}$ est un anneau, les fonctions symmétriques élémentaires $\mathrm{S}_r^1(\underline{x}), \ldots, \mathrm{S}_r^r(\underline{x})$ en les $x_1, \ldots, x_r$ sont encore dand $\overline{\mathbb{Z}}$. Mais $\mathrm{S}_r^1(\underline{x}), \ldots, \mathrm{S}_r^r(\underline{x})$ sont aussi dans $\mathbb{Q}$ donc dans $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Exercice 1. Soit z un nombre algébrique de polynôme minimal

$$\mathrm{P} = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0.$$

(1) Soit $d \in \mathbf{Z}$. Démontrer que dz est un entier algébrique si et seulement si $d^i a_{n-i} \in \mathbf{Z}$ pour tout $i = 1, \ldots, n$.

(2) Supposons que z ne soit pas nul. Démontrer que $1/z$ est un entier algébrique si et seulement si $\frac{a_1}{a_0}, \ldots, \frac{a_{n-1}}{a_0}, \frac{1}{a_0} \in \mathbf{Z}$.

(1) Notons que $deg(\mathrm{P}_{dz})\mathbb{Q}(dz) = \mathbb{Q}(z) = deg(\mathrm{P}_z)$. Par ailleurs, dz est annulé par $\mathrm{P}(\frac{\mathrm{X}}{d}) = \frac{1}{d^n}(\mathrm{X}^n + \sum_{0 \le k \le n-1} a_k d^{n-k}\mathrm{X}^k)$ donc $\mathrm{P}_{dz} | \mathrm{P}(\frac{\mathrm{X}}{d})$ dans $\mathbb{Q}[\mathrm{T}]$ *i.e.* il existe $a \in \mathbb{Q}$ tel que $\mathrm{P}_{dz} = a\mathrm{P}(\frac{\mathrm{X}}{d})$. Mais comme P_{dz} est unitaire, cela impose $a = d^n$ et $\mathrm{P}_{dz} = \mathrm{X}^n + \sum_{0 \le k \le n-1} a_k d^{n-k}\mathrm{X}^k$.

(2) C'est le même genre d'argument. Là encore, notons que $deg(\mathrm{P}_{1/z})\mathbb{Q}(1/z) = \mathbb{Q}(z) = deg(\mathrm{P}_z)$. Par ailleurs, $1/z$ est annulé par $\mathrm{X}^n\mathrm{P}(1/\mathrm{X}) = a_0\mathrm{X}^n + \sum_{1 \le k \le n-1} a_k\mathrm{X}^{n-k} + 1$ donc $\mathrm{P}_{1/z} | \mathrm{X}^n\mathrm{P}(1/\mathrm{X})$ dans $\mathbb{Q}[\mathrm{T}]$ *i.e.* il existe $a \in \mathbb{Q}$ tel que $\mathrm{P}_{1/z} = a\mathrm{X}^n\mathrm{P}(1/\mathrm{X})$. Mais comme $\mathrm{P}_{1/z}$ est unitaire, cela impose $aa_0 = 1$ et $\mathrm{P}_{1/z} = \mathrm{X}^n + \sum_{1 \le k \le n-1} \frac{a_k}{a_0}\mathrm{X}^k + \frac{1}{a_0}$.

Exercice 2. (1) Est-ce que $\frac{2}{3+\sqrt{13}}$ est un entier algébrique ?

(2) Déterminer le polynôme minimal du nombre algébrique $\frac{-2+\sqrt{2}+i\sqrt{2}}{2}$. Est-ce un entier algébrique ?

(1) Comme $x = \frac{2}{3+\sqrt{13}} = \frac{\sqrt{13}-3}{2} \notin \mathbb{Q}$, $[\mathbb{Q}(x) : \mathbb{Q}] \ge 2$. Par ailleurs, x est annulé par

$$\mathrm{P}(\mathrm{T}) = (\mathrm{T} - \frac{\sqrt{13}-3}{2})(\mathrm{T} - \frac{-\sqrt{13}-3}{2}) = \mathrm{T}^2 + 3\mathrm{T} - 1 \in \mathbb{Z}[\mathrm{T}].$$

Donc $\mathrm{P} = \mathrm{P}_x$ et $x \in \overline{\mathbb{Z}}$.

(2) On a $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{2}+i\sqrt{2}) = \mathbb{Q}(\sqrt{2}, i)$. En effet $(\sqrt{2}+i\sqrt{2})^2 = 2+4i-2 = 4i$ donc $i \in \mathbb{Q}(x)$ et $(\sqrt{2}+i\sqrt{2})^{-1} = \frac{\sqrt{2}-i\sqrt{2}}{4}$ donc $\sqrt{2} - i\sqrt{2} \in \mathbb{Q}(x)$ donc $(\sqrt{2}+i\sqrt{2}) + (\sqrt{2}-i\sqrt{2}) = 2\sqrt{2} \in \mathbb{Q}(x)$ donc $\sqrt{2} \in \mathbb{Q}(x)$. Cela montre déjà que $\mathbb{Q}(x) \supset \mathbb{Q}(\sqrt{2}, i)$. Or $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \times 2 = 4$ (pour voir que $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)] = 2$, observer que le polynôme minimal $\mathrm{P}_{\sqrt{2}} = \mathrm{T}^2 - 2$ de $\sqrt{2}$ sur $\mathbb{Q}$ reste irréductible sur $\mathbb{Q}(i)$). Donc $4 | [\mathbb{Q}(x) : \mathbb{Q}]$. Par ailleurs, x est annulé par

$$\begin{aligned}\mathrm{P}(\mathrm{T}) &= ((\mathrm{T}+1) - \tfrac{\sqrt{2}+i\sqrt{2}}{2})((\mathrm{T}+1) + \tfrac{\sqrt{2}+i\sqrt{2}}{2})((\mathrm{T}+1) - \tfrac{\sqrt{2}-i\sqrt{2}}{2})((\mathrm{T}+1) + \tfrac{\sqrt{2}-i\sqrt{2}}{2}) \\ &= (\mathrm{T}-1)^4 + 8(\mathrm{T}-1)^2 + 1 \in \mathbb{Z}[\mathrm{T}]\end{aligned}$$

donc $\mathrm{P}_x | \mathrm{P}$. Donc $\mathrm{P}_x = \mathrm{P}$ (et $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{2}, i)$) et $x \in \overline{\mathbb{Z}}$.

Exercice 3. Soient $a, b \in \mathbf{Z}$ des entiers sans facteur carré distincts et $n \geq 1$ un entier. Démontrer que $\frac{\sqrt{a}+\sqrt{b}}{n}$ est un entier algébrique si et seulement si soit $n = 1$, soit $n = 2$ et $a \equiv b \bmod 4$.

$x = \frac{\sqrt{a}+\sqrt{b}}{n}$ sur $\mathbb{Q}$ est annulé par

$$\mathrm{P}(\mathrm{T}) = (\mathrm{T}-\frac{\sqrt{a}+\sqrt{b}}{n})(\mathrm{T}+\frac{\sqrt{a}+\sqrt{b}}{n})(\mathrm{T}-\frac{\sqrt{a}-\sqrt{b}}{n})(\mathrm{T}+\frac{\sqrt{a}-\sqrt{b}}{n}) = \mathrm{T}^4-\frac{2(a+b)}{n^2}\mathrm{T}^2+\frac{(a-b)^2}{n^4}.$$

Donc $\mathrm{P}_x|\mathrm{P}$. Pour montrer que $\mathrm{P}_x = \mathrm{P}$, il faut montrer que $[\mathbb{Q}(x) : \mathbb{Q}] = 4$. Pour cela, observons que $(nx)^2 = a + 2\sqrt{ab} + b \in \mathbb{Q}(x)$ et $(nx)^3 = (a+b)(\sqrt{a}+\sqrt{b}) + 2(a\sqrt{b}+b\sqrt{a}) \in \mathbb{Q}(x)$ donc $a\sqrt{b}+b\sqrt{a} \in \mathbb{Q}(x)$ donc $\sqrt{a} = \frac{1}{b-a}((a\sqrt{b}+b\sqrt{a}) - a(\sqrt{b}+\sqrt{a})) \in \mathbb{Q}(x)$ et, de même, $\sqrt{b} \in \mathbb{Q}(x)$ donc $\mathbb{Q}(x) \supset \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Or $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})][\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 \times 2 = 4$ (pour voir que $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] = 2$, observer que, sinon, $u\sqrt{a} = v\sqrt{b}+w$ avec $0 \neq u, v, w \in \mathbb{Z}$ donc $u^2a = v^2b + 2vw\sqrt{b} + w$ donc $vw = 0$ donc $v = 0$ et $\sqrt{a} \in \mathbb{Q}$: contradiction, ou $w = 0$ et $u^2a = v^2b$ donc $a = b$ - car a, b sont sans facteurs carrés : contradiction). Donc $\mathrm{P}_x = \mathrm{P}$ et $x \in \overline{\mathbb{Z}}$ ssi (*) $\frac{2(a+b)}{n^2}, \frac{(a-b)^2}{n^4} \in \mathbb{Z}$. Notons (**) la condition $n = 1$ ou $n = 2$ et $a \equiv b \bmod 4$. On vérifie immédiatement que (**) $\Rightarrow$ (*). Réciproquement, (*) équivaut à $2(a+b) = cn^2$ et $a-b = dn^2$ avec $c, d \in \mathbb{Z}$. Notons d'abord que si $p > 2$ est un nbr premier divisant n on doit avoir $p^2|a-b, a+b$ donc $p^2|2a, 2b$ donc $p^2|a, b$, ce qui contredit le fait que a, b sont sans facteur carré. Donc $n = 2^m$. Mais alors $2^{2m-1}|a+b$, $2^{2m}|a-b$, ce qui implique $2^{2m-1}|2a, 2b$ donc $2^{2m-2}|a, b$. Là encore, comme a, b sont sans facteur carré, ce n'est possible que si $m = 0, 1$. Si $m = 0$, on est dans le cas $n = 1$. Si $m = 1$, on a $n = 2$ et $a - b = 4d \equiv 0 \bmod 4$.

Exercice 4.

(1) Soit $\mathrm{P} = a_n\mathrm{X}^n + \cdots + a_0 \in \mathbf{Z}[\mathrm{X}]$ un polynôme à coefficients entiers de degré n. Soit r un nombre rationnel, écrit sous la forme $r = u/v$ avec $u, v \in \mathbf{Z}$ premiers entre eux, satisfaisant à $\mathrm{P}(r) = 0$. Montrer que u divise a_0 et v divise a_n.

(2) Soit x un nombre rationnel. Montrer que $2\cos(\pi x)$ est un entier algébrique.

(3) Soit $x \in [0, 1]$ un nombre rationnel tel que $\cos(\pi x)$ soit aussi rationnel. Montrer que x appartient à l'ensemble $\{0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1\}$.

(1) Par hypothèse, $v^n\mathrm{P}(u/v) = a_nu^n + uv\sum_{1\leq k\leq n-1} a_ku^{k-1}v^{n-k-1} + a_0v^n = 0$. Donc, en réduisant modulo u et en utilisant que v est inversible dans $\mathbb{Z}/u$, on a $a_0 \equiv 0 \bmod u$. De même, en réduisant modulo v et en utilisant que u est inversible dans $\mathbb{Z}/v$, on a $a_n \equiv 0 \bmod v$.

(2) Notons $x = u/v$ avec $u, v \in \mathbb{Z}$ premiers entre eux. Alors $exp(-i\pi x), exp(i\pi x)$ sont racines de $\mathrm{T}^{2b} - 1$ donc dans $\overline{\mathbb{Z}}$. Comme $\overline{\mathbb{Z}}$ est un anneau, on en déduit $2cos(\pi x) = exp(-i\pi x) + exp(i\pi x) \in \overline{\mathbb{Z}}$.

(3) D'après (2), $2\cos(\pi x) \in \overline{\mathbb{Z}}$. Si on suppose de plus $\cos(\pi x) \in \mathbb{Q}$, alors $2\cos(\pi x) \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ donc $\cos(\pi x)$ est de la forme $\frac{a}{2}$ avec $a \in \mathbb{Z}$ et la contrainte $-1 \leq \frac{a}{2} \leq 1$, ce qui ne laisse comme possibilités que $a \in \{-2, -1, 0, 1, 2\}$ donc $\cos(\pi x) \in \{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\}$ *i.e.* $x \in \{0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1\}$.
Autre argument : Notons $x = u/v$ avec $u, v \in \mathbb{Z}$ premiers entre eux et $w = exp(i\pi x)$; c'est une racine n-ième de 1 avec $n = v$ si $2|u$ et $n = 2v$ sinon. Notons également $\mathrm{P} := (\mathrm{T} - exp(i\pi x))(\mathrm{T} - exp(-i\pi x)) = \mathrm{T}^2 - 2cos(\pi x)\mathrm{T} + 1$. Par hypothèse, $\mathrm{P} \in \mathbb{Q}[\mathrm{T}]$ et $\mathrm{P}(w) = 0$ donc $\Phi_n|\mathrm{P}$ et, en particulier, $\varphi(n) \leq 2$ donc $n \in \{1, 2, 3, 4\}$ et, comme $x \in [0, 1]$, $x \in \{0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1\}$. La condition $cos(\pi x) \in \mathbb{Q}$ élimine $x = \frac{1}{4}$ ($cos(\pi/4) = \sqrt{2}/2$) et $x = \frac{3}{4}$ ($cos(3\pi/4) = -\sqrt{2}/2$).

Exercice 5 (Polynômes cyclotomiques)**.** Soit $n \geq 1$ un entier. Le $n$ième *polynôme cyclotomique* est le polynôme unitaire dont les racines sont les racines primitives $n$ièmes de l'unité dans $\mathbf{C}$:

$$\Phi_n(\mathrm{X}) = \prod_{\substack{1\leq a\leq n\\(a,n)=1}} (\mathrm{X} - e^{\frac{2\pi i a}{n}}).$$

(1) Écrire $\Phi_n(\mathrm{X})$ pour $n = 1, 2, 3, 4$ et pour n un nombre premier. Quel est le degré de Φ_n ?

(2) Démontrer l'égalité

$$\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d(\mathrm{X}).$$

Qu'est-ce qu'on obtient en prenant les degrés des deux côtés de l'égalité ?

(3) Démontrer par récurrence sur n que Φ_n est un polynôme unitaire à coefficients entiers.

(4) Soit p un nombre premier. Démontrer l'égalité $\Phi_{p^m}(\mathrm{X}) = \Phi_p(\mathrm{X}^{p^{m-1}})$ pour tout $m \geq 1$.

(5) Démontrer que le polynôme Φ_n est *palindromique*, c'est-à -dire satisfait à

$$\mathrm{X}^{\deg(\Phi_n)}\Phi_n(\mathrm{X}^{-1}) = \Phi_n(\mathrm{X}).$$

Notons $\mu_n \subset \mathbb{C}^\times$ le sous-groupe des racines $n$ième de 1 et $\mathrm{U}_n \subset \mu_n$ le sous-ensemble des racines primitives $n$ièmes de 1 *i.e.* des $\in \mu_n$ d'ordre $|\langle\omega\rangle|$ exactement n. On a rappelé que si $\omega \in \mathrm{U}_n$, le morphisme de groupes $\mathbb{Z} \to \mu_n$, $k \mapsto \omega^k$ se factorise en un isomorphisme de groupes $\mathbb{Z}/n\tilde{\to}\mu_n$, qui se restreint en une bijection $(\mathbb{Z}/n)^\times\tilde{\to}\mathrm{U}_n$ (utiliser Bézout) ou encore que

$$\mathrm{U}_n = \{\omega^k \mid k \in \mathbb{Z},\ (k,n) = 1\} = \{\omega^k \mid k \in \mathbb{Z},\ 1 \leq k \leq n-1,\ (k,n) = 1\}.$$

(1) $\Phi_1 = \mathrm{T} - 1$, $\Phi_2 = \mathrm{T} + 1$, $\Phi_3 = \mathrm{T}^2 + \mathrm{T} + 1$, $\Phi_4 = \mathrm{T}^2 + 1$, $\Phi_p = \mathrm{T}^{p-1} + \cdots + 1$. Si $n = p$ est premier, $\mathrm{U}_p = \mu_\mathrm{P} \sqcup \{1\}$ donc

$$(\mathrm{T}-1)(\sum_{0\leq k\leq p-1} \mathrm{T}^k) = \mathrm{T}^p - 1 = \prod_{\omega\in\mathrm{U}_p} (\mathrm{T} - \omega) = (\mathrm{T}-1)\Phi_p,$$

donc $\Phi_p = \sum_{0\leq k\leq p-1} \mathrm{T}^k$. Par déf, le degré de Φ_n est $|\mathrm{U}_n| = |(\mathbb{Z}/n)^\times| =: \varphi(n)$ (indicatrice d'Euler). On a rappelé que si $n = \prod_p p^{v_p(n)}$ est la décomposition de n en produit d'irréductibles dans $\mathbb{Z}$ alors $\varphi(n) = \prod_p (p-1)p^{v_p(n)-1}$.

(2) Par définition μ_n est l'ensemble des zéros de $\mathrm{T}^n - 1$. Or $\mu_n = \sqcup_{d|n}\mathrm{U}_d$ donc

$$\mathrm{T}^n - 1 = \prod_{d|n}\prod_{\omega\in\mathrm{U}_d} (\mathrm{T} - \omega) = \prod_{d|n} \Phi_d.$$

En prenant les degrés, on obtient $n = \sum_{d|n} \varphi(d)$.

(3) Ok pour Φ_1. Si Φ_k est unitaire et dans $\mathbb{Z}[\mathrm{T}]$ pour $k \leq n$ alors $\mathrm{T}^{n+1}-1 = \Phi_{n+1}\prod_{d|n+1,d\leq n} \Phi_d$. Par hypothèse de rec., $\Psi_{n+1} := \prod_{d|n+1,d\leq n} \Phi_d$ est unitaire et dans $\mathbb{Z}[\mathrm{T}]$ donc de contenu 1. Donc Φ_{n+1} est unitaire (puisque $1 = \mathrm{CD}(\mathrm{T}^n-1) = \mathrm{CD}(\Phi_{n+1})\mathrm{CD}(\Psi_{n+1}) = \mathrm{CD}(\Phi_{n+1})$) et de contenu 1 par multiplicativité du contenu ($1 = \mathrm{C}_\mathbb{Z}(\mathrm{T}^n-1) = \mathrm{C}_\mathbb{Z}(\Phi_{n+1})\mathrm{C}_\mathbb{Z}(\Psi_{n+1}) = \mathrm{C}_\mathbb{Z}(\Phi_{n+1})$) donc dans $\mathbb{Z}[\mathrm{T}]$.
Autre argument : comme Ψ_{n+1} est à coefficients entiers unitaire donc de coefficient dominant inversible, on peut donc effectuer la division euclidienne de $\mathrm{T}^{n+1} - 1$ par Ψ_{n+1} dans $\mathbb{Z}[\mathrm{T}]$: il existe un unique couple $\mathrm{Q}, \mathrm{R} \in \mathbb{Z}[\mathrm{T}]$ tq $\mathrm{T}^{n+1} - 1 = \Psi_{n+1}\mathrm{Q} + \mathrm{R}$ avec $deg(\mathrm{R}) < deg(\Psi_{n+1})$. Mais $\mathrm{T}^{n+1} - 1 = \Psi_{n+1}\mathrm{Q} + \mathrm{R}$ est aussi la division euclidienne de $\mathrm{T}^{n+1} - 1$ par Ψ_{n+1} dans $\mathbb{Q}[\mathrm{T}]$, donc par unicité du quotient et du reste, on a $\mathbb{Z}[\mathrm{T}] \ni \mathrm{Q} = \Phi_{n+1}$ et $\mathrm{R} = 0$.

(4) Soit p un nombre premier. Notons $\Psi_{p,m} := \Phi_p(\mathrm{T}^{p^{m-1}})$. Si $\omega \in \mu_{p^m}$ alors $\omega^{p^{m-1}} \in \mu_p$ donc $\Psi_{p,m}(\omega) = \Phi_p(\omega^{p^{m-1}}) = 0$. Donc $\Phi_{p^m} | \Psi_{p,m}$. Mais comme Φ_{p^m}, $\Psi_{p,m}$ sont unitaires de même degré (car $\varphi(p^m) = p^{m-1}(p-1)$; cela se vérifie en observant que le nbr de multiples de p dans $\{0, \dots, p^m - 1\}$ est p^{m-1}), cela impose $\Phi_{p^m} = \Psi_{p,m}$.
Autre argument : On utilise la relation de (2) pour $n = p^m$, $n = p^{m-1}$ et $n = p$:

$$(*)\quad (\mathrm{T}^{p^{m-1}} - 1)\Phi_p(\mathrm{T}^{p^{m-1}}) = (\mathrm{T}^{p^{m-1}})^p - 1 = \mathrm{T}^{p^m} - 1 = \prod_{d|p^m} \Phi_d = \prod_{0\le k\le m} \Phi_{p^k}$$

$$(**)\quad (\mathrm{T}^{p^{m-1}} - 1) = \prod_{d|p^{m-1}} \Phi_d = \prod_{0\le k\le m-1} \Phi_{p^k}$$

En remplaçant $(\mathrm{T}^{p^{m-1}} - 1)$ dans (*) par son expression (**) et en simpifiant, on obtient l'égalité souhaitée.

(5) En utilisant $\mathrm{T}^n - 1 = \prod_{d|n} \prod_{\omega \in \mathrm{U}_d} (\mathrm{T} - \omega) = \prod_{d|n} \Phi_d$, on démontre par récurrence sur n que $\Phi_n(0) = 1$. On a alors

$$\mathrm{T}^{\varphi(n)}\Phi_n(\mathrm{T}^{-1}) = \prod_{\omega \in \mathrm{U}_n} (1 - \omega \mathrm{T}) = \prod_{\omega \in \mathrm{U}_n} (-\omega)\Phi_n = \Phi_n(0)\Phi_n = \Phi_n$$

Exercice 6 (Irréductibilité des polynômes cyclotomiques)**.** Soit $n \ge 3$.

(1) Soit ω une racine primitive $n$ème de l'unité et soit P son polynôme minimal. Montrer que $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ et qu'il existe $\mathrm{Q} \in \mathbf{Z}[\mathrm{X}]$ unitaire tel que $\Phi_n = \mathrm{PQ}$.

(2) Soit p un nombre premier ne divisant pas n. Montrer que $\Phi_n(\omega^p) = 0$.

(3) Supposons que $\mathrm{Q}(\omega^p) = 0$. Montrer que P divise le polynôme $\mathrm{Q}(\mathrm{X}^p)$.

(4) Toujours sous l'hypothèse $\mathrm{Q}(\omega^p) = 0$, démontrer que Φ_n a un facteur carré modulo p et aboutir à une contradiction. Conclure que ω^p est racine de P.

(5) Démontrer l'égalité $\Phi_n = \mathrm{P}$ et en déduire que Φ_n est irréductible dans $\mathbf{Q}[\mathrm{X}]$.

(1) Par définition, ω est racine de $\mathrm{T}^n - 1$ donc algébrique sur $\mathbb{Z}$; en particulier, son polynôme minimal P sur $\mathbb{Q}$ est dans $\mathbb{Z}[\mathrm{T}]$ et unitaire. Comme $\Phi_n(\omega) = 0$, on a $\mathrm{P} | \Phi_n$ dans $\mathbb{Q}[\mathrm{T}]$ *i.e.* il existe $\mathrm{Q} \in \mathbb{Q}[\mathrm{T}]$ tel que $\Phi_n = \mathrm{PQ}$. Le même argument que dans l'exo 5 (3) mq Q est en fait dans $\mathbb{Z}[\mathrm{T}]$ et unitaire.

(2) Soit p un nombre premier ne divisant pas n. Alors $\omega^p \in \mathrm{U}_p$. En effet, il existe $u, v \in \mathbb{Z}$ tq $up + vn = 1$ donc $(\omega^p)^u = \omega$; en particulier l'ordre de ω divise (donc est égal à) celui de ω^p.

(3) Comme P est le polynôme minimal de ω, $\mathrm{Q}(\omega^p) = 0$ implique $\mathrm{P} | \mathrm{Q}(\mathrm{T}^p)$.

(4) Supposons tjs $\mathrm{Q}(\omega^p) = 0$. Alors $\mathrm{P} | \mathrm{Q}(\mathrm{T}^p)$ implique $\overline{\mathrm{P}} | \overline{\mathrm{Q}}(\mathrm{T}^p) = \overline{\mathrm{Q}}(\mathrm{T})^p$. En particulier, tout facteur irréductible Π de $\overline{\mathrm{P}}$ divise $\overline{\mathrm{Q}}^p$ donc $\overline{\mathrm{Q}}$. Mais comme $\overline{\Phi}_n = \overline{\mathrm{PQ}}$, $\Pi^2 | \overline{\Phi}_n$. Ce n'est pas possible car $\overline{\Phi}_n | \mathrm{T}^n - 1$ mais, dans $\mathbb{F}_p[\mathrm{T}]$, on a $(\mathrm{T}^n - 1)' = n\mathrm{T}^{n-1} \neq 0$ (rappelons que p ne divise pas n) donc $\mathrm{T}^n - 1$ est séparable sur $\mathbb{F}_p[\mathrm{T}]$. Donc $\mathrm{Q}(\omega^p) \neq 0$, ce qui impose $\mathrm{P}(\omega^p) = 0$ par (1), (2).

(5) Fixons $\omega \in \mu_n$. On peut alors écrire tout élément de U_n sous la forme ω^m avec $(n, m) = 1$. Ecrivons $m = p_1 \cdots p_r$ avec $p_1, \dots, p_r$ des nombres premiers (éventuellement égaux) ne divisant pas n. On montre par rec. sur r que $\mathrm{P}(\omega^m) = 0$. Si $r = 1$, on vient de le voir. Si c'est vrai pour $s \le r$, on applique le cas $r = 1$ avec $\omega := \omega^{p_1 \cdots p_r}$ et $p := p_{r+1}$. On obtient ainsi que tous les éléments de U_n sont racines de P. Autrement dit, $\Phi_n | \mathrm{P}$.

Exercice 7 (Un théorème de Kronecker)**.** Soit $P \in \mathbf{Z}[X]$ un polynôme unitaire à coefficients entiers. On suppose que toutes les racines complexes de P sont de module ≤ 1.

(1) Soit α une racine complexe de P. Démontrer que α^n est un entier algébrique de module ≤ 1 pour tout entier n.

(2) En déduire que $\alpha = 0$ ou α est une racine de l'unité.

(3) Supposons P irréductible. Démontrer que $P = X$ ou P est un polynôme cyclotomique.

(1) Par hypothèse $\alpha \in \overline{\mathbb{Z}}$ donc, comme $\overline{\mathbb{Z}}$ est un anneau, $\alpha^n \in \overline{\mathbb{Z}}$. Par hypothèse aussi $|\alpha| \leq 1$ donc $|\alpha^n| = |\alpha|^n \leq 1$.

(2) Supposons $\alpha \neq 0$. Notons $\alpha_1 = \alpha, \ldots, \alpha_r$ les racines de $P_\alpha = T^n + \sum_{1\leq i\leq r} a_i T^{r-i}$ et considérons le polynôme $P_n = \prod_{1\leq i\leq r}(T-\alpha_i^n) = T^r + \sum_{1\leq i\leq r}(-1)^i S_i^r(\alpha_1^n, \ldots, \alpha_r^n)T^{r-i}$. Mais comme les $S_i^r(\alpha_1^n, \ldots, \alpha_r^n)$, $i = 1, \ldots, r$ sont des fonctions symétriques en les $\alpha_1, \ldots, \alpha_r$, il existe $\Sigma_1, \ldots \Sigma_r \in \mathbb{Z}[T_1, \ldots, T_r]$ tels que $S_i^r(\alpha_1^n, \ldots, \alpha_r^n) = \Sigma_i(a_1, \ldots, a_r)$ et, en particulier, $S_i^r(\alpha_1^n, \ldots, \alpha_r^n) \in \mathbb{Z}$, $i = 1, \ldots, r$. Donc $P_n \in \mathbb{Z}[T]$. de plus $deg(P_n) \leq r = deg(P_\alpha)$ et pour chaque $i = 1, \ldots, r$, $|S_i^r(\alpha_1^n, \ldots, \alpha_r^n)| \leq |\{1 \leq j_1 < \cdots < j_i \leq r\}| = N(r, i)$. Cela montre qu'il n'y a qu'un nbr fini de possibilités pour les P_n, $n \geq 1$ donc, en particulier, pour les α^n, $n \geq 1$. Donc il existe $n > m$ tel que $\alpha^m = \alpha^n$ ou, encore $\alpha^{n-m} = 1$.
Autre argument (utilise un peu de théorie de Galois) : Au lieu des P_n, $n \in \mathbb{Z}$, on peut considérer les polynômes minimaux Π_n de α^n sur $\mathbb{Q}$, $n \in \mathbb{Z}$. Comme $\mathbb{Q}(\alpha^n) \subset \mathbb{Q}(\alpha)$, on a $deg(\Pi_n) \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(\Pi_1)$ et comme $\alpha^n \in \overline{\mathbb{Z}}$, $\Pi_n \in \mathbb{Z}[T]$. Pour majorer les coefficients de Π_n indépendemment de n, il faut savoir que les racines de Π_n sont les $\sigma(\alpha^n) = \sigma(\alpha)^n$, pour $\sigma \in Gal(\overline{\mathbb{Q}}|\mathbb{Q})$ et que $\sigma(\alpha)$ est aussi une racine de P donc l'un des α_i, $i = 1, \ldots, r$.

(3) Supposons P irréductible donc $P = P_\alpha$. Si $\alpha = 0$, $P = X$ et si $\alpha \in \mu_n$, $P_\alpha = \Phi_n$.

Exercice 8 (Corps cyclotomiques)**.** Soient $n \geq 1$ un entier et $\omega = \exp(2\pi i/n)$.

(1) Calculer le degré du corps de nombres $\mathbb{Q}(\omega)$.

(2) Déterminer tous les plongements complexes de $\mathbf{Q}(\omega)$, ainsi que les nombres r_1 et r_2 des plongements réels et de paires de plongements complexes.

(1) Comme $\Phi_n(\omega = 0)$ et $\Phi_n \in \mathbb{Q}[T]$ est unitaire irréductible sur $\mathbb{Q}$, on a $\Phi_n = P_\omega$ donc $[\mathbf{Q}(\omega) : \mathbb{Q}] = deg(\Phi_n) = \varphi(n)$.

(2) Les plongements complexes de $\mathbb{Q}(\omega)$ correspondent aux racines de Φ_n. Plus précisément, pour tout $1 \leq u \leq n$, $(u, n) = 1$, on a un unique morphisme de corps

$$\mathbb{Q}(\omega) \overset{\omega \leftarrow \overline{T}}{\xleftarrow{\sim}} \mathbb{Q}[T]/P_\omega \overset{\overline{T} \to \omega^u}{\hookrightarrow} \mathbb{C}.$$

Si $n \geq 3$, aucun de ces plongements n'est réel. Autrement dit $r_1 = 0$, $r_2 = \varphi(n)/2$ (Si $n = 1, 2$, on a $\mathbb{Q}(\omega) = \mathbb{Q}$ donc $r_1 = 1$, $r_2 = 0$).

Exercice 9. Soit K le corps de nombres $\mathbf{Q}(\alpha)$ où α est une racine du polynôme $P = X^3 + X - 3$.

(1) Démontrer, par au moins deux méthodes différentes, que P est irréductible. Conclure que K est de degré 3.

(2) Calculer les polynômes caractéristiques de la multiplication par α et par α^2 dans K. En déduire les valeurs de la norme $N_K(\alpha^2)$ et la trace $Tr_K(\alpha^2)$.

(3) Démontrer que, pour tout $x \in \mathbf{Q}$, la norme de $x - \alpha$ est égale à $\mathrm{P}(x)$.

(1) Par réduction modulo 2 (car $\mathrm{T}^3 + \mathrm{T} + 1$ n'a pas de racines dans $\mathbb{F}_2$) ou directement, en observant que $\mathrm{T}^3 + \mathrm{T} + 1$ n'a pas de racine dans $\mathbb{Q}$ car sinon, il existerait $a, b \in \mathbb{Z}$ premiers entre eux tq $a^3 + a^2 b = 3b^3$, donc $b | a^3$: contradiction. En particulier, $\mathrm{P} = \mathrm{P}_\alpha$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(\mathrm{P}) = 3$.

(2) Notons $\mathrm{L}_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$, $x \mapsto \alpha x$ et $\mathrm{L}_{\alpha^2} : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$, $x \mapsto \alpha^2 x$. Dans la $\mathbb{Q}$-base $1, \alpha, \alpha^2$ de $\mathbb{Q}(\alpha)$, la matrice de L_α est la matrice compagnon $\mathrm{C}(\mathrm{P})$ de P et donc celle de $\mathrm{L}_{\alpha^2} = (\mathrm{L}_\alpha)^2)$ est $\mathrm{C}(\mathrm{P})^2$ donc

$$\mathrm{N}_{\mathbb{Q}(\alpha)}(\alpha^2) = 9, \quad \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha^2) = -2.$$

(3) Pour tout $x \in \mathbf{Q}$, la matrice de $\mathrm{L}_{x-\alpha} = \mathrm{L}_x - \mathrm{L}_\alpha$ dans $1, \alpha, \alpha^2$ est $x\mathrm{I}d - \mathrm{C}(\mathrm{P})$ donc

$$\mathrm{N}_{\mathbb{Q}(\alpha)}(x - \alpha) = det(x\mathrm{I}d - \mathrm{C}(\mathrm{P})) = \chi_{\mathrm{C}(\mathrm{P})}(x) = \mathrm{P}(x).$$