L'utilisation des calculatrices n'est pas autorisée pour cette épreuve. La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite donc le candidat à produire des raisonnements clairs, complets, précis et concis. Le candidat peut utiliser les résultats énoncés dans les questions ou les parties précédentes ; il veillera toutefois à préciser la référence du résultat utilisé. Chaque partie est d'ailleurs largement indépendante des précédentes, une fois admis les résultats qui y sont démontrés.
Plus précisément, la partie **I** n'est utilisée que dans la partie **VI**. Les parties **IV** et **V** sont mutuellement indépendantes ainsi qu'essentiellement du reste du problème : seules les formules équivalentes obtenues dans les questions **IV.9** et **V.5** sont utilisées dans la partie **VI**.

Objectif : L'objectif de ce sujet est de donner une démonstration de la loi de réciprocité quadratique.

Notations : Soit ζ un nombre complexe. On note $\mathbb{Q}[\zeta]$ le $\mathbb{Q}$-espace vectoriel engendré par $\{\zeta^n,\ n\in\mathbb{N}\}$: c'est une $\mathbb{Q}$-algèbre. On note $\mathbb{Z}[\zeta]$ le sous-groupe additif de $\mathbb{Q}[\zeta]$ engendré par $\{\zeta^n,\ n\in\mathbb{N}\}$.
Un sous-corps de $\mathbb{C}$ qui est de dimension finie (vu comme $\mathbb{Q}$-espace vectoriel) est appelé un *corps de nombres*.
Soient n,k deux entiers. Si ζ est une racine n-ème de l'unité, le complexe ζ^k ne dépend que de la classe x de k dans $\mathbb{Z}/n\mathbb{Z}$ et sera noté ζ^x. Dans le cas particulier où $\zeta=\exp(\dfrac{2i\pi}{n})$, on notera τ_n la somme

$$\tau_n=\sum_{x\in\mathbb{Z}/n\mathbb{Z}}\zeta^{x^2}.$$

I. Préliminaires

Soit p premier impair et $y\in(\mathbb{Z}/p\mathbb{Z})^*$. On dira que y est un carré s'il existe $x\in(\mathbb{Z}/p\mathbb{Z})^*$ tel que $y=x^2$.

(1) Montrer l'égalité

$$\prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*}x=\begin{cases}-y^{(p-1)/2} & \text{si } y \text{ est un carré,}\\ y^{(p-1)/2} & \text{sinon.}\end{cases}.$$

Indication : regrouper deux à deux dans le produit les termes $x, y/x$, pour $x\in(\mathbb{Z}/p\mathbb{Z})^*$.

(2) En déduire les égalités

$$\begin{cases}y^{(p-1)/2}=1 & \text{si } y \text{ est un carré,}\\ y^{(p-1)/2}=-1 & \text{sinon.}\end{cases}$$

II. Généralités

(1) Montrer que les deux propositions suivantes sont équivalentes :

(i) Il existe un polynôme P unitaire à coefficients rationnels annulant ζ.

(ii) La $\mathbb{Q}$-algèbre $\mathbb{Q}[\zeta]$ est un corps de nombres.

Soit K un corps de nombre. On dira qu'un élément $x\in K$ est un *entier algébrique* s'il existe un polynôme P unitaire à coefficients entiers qui annule x. Et on notera $\mathcal{O}_K$ l'ensemble des entiers algébriques de K.

(2) Montrer l'égalité $\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}$.

Avec des arguments de réduction, on peut démontrer que $\mathcal{O}_K$ est un sous-anneau de K. Cette partie est mise en partie VII et pourra être traitée à la maison (avec les outils de réduction). On admettra par la suite ce résultat.

III. Entiers des corps quadratiques

Soit $D\in\mathbb{Q}$ qui n'est pas le carré d'un rationnel. Si D est négatif, on notera $\sqrt{D}$ le complexe $i\sqrt{-D}$. Un corps de la forme $\mathbb{Q}[\sqrt{D}]$ (avec D non carré) est dit corps quadratique. On remarque que $(1,\sqrt{D})$ est une base de $\mathbb{Q}[\sqrt{D}]$. On note σ l'isomorphisme de corps

$$\sigma:\begin{cases}\mathbb{Q}[\sqrt{D}] & \to\mathbb{Q}[\sqrt{D}]\\ a+b\sqrt{D} & \mapsto a-b\sqrt{D}\end{cases}.$$

(1) Montrer que les seuls isomorphismes de corps de $\mathbb{Q}[\sqrt{D}]$ dans lui-même sont l'identité et σ.

(2) Soit $D'\in\mathbb{Q}^*$. Montrer que $\mathbb{Q}[\sqrt{D}]=\mathbb{Q}[\sqrt{D'}]$ si et seulement si $\dfrac{D}{D'}$ est un carré dans $\mathbb{Q}$.

(3) Montrer qu'il existe un unique $d\in\mathbb{Z}$ sans facteur carré tel que $\mathbb{Q}[\sqrt{D}]=\mathbb{Q}[\sqrt{d}]$.

(4) Soit K un sous-corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$. Montrer que K est un corps quadratique.

Dorénavant, on fixe d un entier sans facteur carré tel que $K=\mathbb{Q}[\sqrt{d}]$.

(5) Montrer que $x\in\mathcal{O}_K$ si et seulement si $x\in K$ et

$$\begin{cases}x+\sigma(x)\in\mathbb{Z}\\ x\sigma(x)\in\mathbb{Z}.\end{cases}$$

Soit $\omega \in \mathcal{O}_K$ défini par

$$\omega = \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{si } d \equiv 1[4] \\ \sqrt{d} & \text{sinon.} \end{cases}$$

(6) Montrer que l'application

$$\begin{cases} \mathbb{Z}^2 & \to \mathcal{O}_K \\ (x,y) & \mapsto x + y\omega \end{cases}$$

est un isomorphisme de groupes abéliens.

IV. Un calcul algébrique de τ_n

Soit $n > 1$ un entier impair et ζ le complexe $\zeta = \exp\left(\dfrac{2i\pi}{n}\right)$.

Soit V le $\mathbb{C}$-espace vectoriel des fonctions de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$. Soit φ l'endomorphisme de V qui à la fonction f associe $\varphi(f)$ définie par

$$\varphi(f) : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to \mathbb{C} \\ x & \mapsto \displaystyle\sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)\zeta^{xy}. \end{cases}$$

(1) Donner une base de V et montrer que sa dimension vaut n.

(2) Soit $f \in V$. Montrer l'égalité

$$\varphi \circ \varphi(f)(x) = nf(-x) \quad \text{pour tout } f \in V,\ x \in \mathbb{Z}/n\mathbb{Z}.$$

On note P et I les sous-espaces de V constitués des fonctions respectivement paires et impaires : $P = \{f \in V,\ \forall x \in \mathbb{Z}/n\mathbb{Z},\ f(-x) = f(x)\}$ et $I = \{f \in V,\ \forall x \in \mathbb{Z}/n\mathbb{Z},\ f(-x) = -f(x)\}$.
On rappelle que $V = P \oplus I$.

(3) Que vaut $\varphi \circ \varphi$ sur P ? Et sur I ?
Rappel : Si ψ est une symétrie d'un $\mathbb{C}$-espace vectoriel F de dimension finie, c'est-à-dire un endomorphisme vérifiant $\psi^2 = \mathrm{id}_F$ alors $F = \ker(\psi - \mathrm{id}_F) \oplus \ker(\psi + \mathrm{id}_F)$.

(4) Montrer que le module $|\tau_n|$ est $\sqrt{n}$.

(5) Expliquer que

$$\tau_n = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \zeta^{x^2}$$

est la trace de φ.
On cherche à calculer τ_n.

(6) Montrer que $V = P_1 \oplus P_2 \oplus I_1 \oplus I_2$, avec P_1, P_2, I_1 et I_2 des sous-espaces vectoriels stables par φ sur lesquels φ agit comme une homothétie de rapports respectifs $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$ et $-i\sqrt{n}$.

(7) On note a, b, c, d les dimensions respectives de P_1, P_2, I_1 et I_2. Montrer que $a + b = \dfrac{n+1}{2}$, $c + d = \dfrac{n-1}{2}$ et $(a-b)^2 + (c-d)^2 = 1$.

(8) En calculant $\det(\varphi)$, calculer a, b, c, d en fonction de n.

(9) Montrer

$$\tau_n = \begin{cases} \sqrt{n} & \text{si } n \equiv 1[4], \\ i\sqrt{n} & \text{si } n \equiv 3[4]. \end{cases}$$

V. Un calcul analytique de τ_n

On se donne $n \geq 1$ un entier. Pour $k \in [\![0, n-1]\!]$, on note f_k la fonction

$$f_k : \begin{cases} [0,1] & \to \mathbb{C} \\ t & \mapsto \exp\Big(\dfrac{2i\pi(t+k)^2}{n}\Big) \end{cases}$$

et $f = f_0 + \cdots + f_{n-1}$.

(1) Que vaut $f(0)$? Et $f(1)$?
On admet que, comme f est de classe $\mathcal{C}^2$, par un argument de série de Fourier, si on note $c_m = \displaystyle\int_0^1 f(t)\exp(-2i\pi mt)\ \mathrm{d}t$, alors pour tout $t \in \mathbb{R}$, $\displaystyle\sum_{m=-\infty}^{+\infty} c_m \exp(2i\pi mt) = f(t)$, avec sommabilité de la famille.

(2) En déduire que la suite de terme général $u_k = \displaystyle\sum_{m=-k}^{k} \int_0^1 f(t)\exp(-2i\pi mt)\ \mathrm{d}t$ converge vers τ_n.

(3) Montrer que la fonction de $\mathbb{R}^+$ dans $\mathbb{C}$ qui à un réel x associe

$$\int_{-x}^{x} \exp\Big(\frac{2i\pi t^2}{n}\Big)\ \mathrm{d}t$$

admet une limite $I_n \in \mathbb{R}$ en $+\infty$.

(4) Comparer I_n et I_1.

(5) Montrer la formule

$$\tau_n = \frac{1 + i^{-n}}{1 + i^{-1}}\sqrt{n}.$$

(formule compatible avec la question **IV.9***)*

(6) Soit K un corps quadratique. Montrer qu'il existe une racine de l'unité ξ telle que $K \subset \mathbb{Q}[\xi]$.

VI. Loi de réciprocité quadratique

On considère deux nombres premiers impairs distincts, p, q. On note L le corps de nombres $\mathbb{Q}\left[\exp\left(\frac{2i\pi}{p}\right)\right]$ et K le corps quadratique $\mathbb{Q}[\tau_p]$, qui est contenu dans L. On note $\left(\frac{q}{p}\right)$ l'entier qui vaut 1 si la classe q modulo p est un carré et -1 sinon. On se propose de montrer par deux méthodes différentes la formule, appelée loi de réciprocité quadratique :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{1}$$

Première méthode

(1) Montrer l'égalité $\mathcal{O}_L \cap K = \mathcal{O}_K$.

(2) Montrer la relation $\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in q\mathcal{O}_K$.

(3) Soit n un entier relatif. Montrer que si $n\tau_p$ est un élément de $q\mathcal{O}_K$, alors q divise n. *Indication : utiliser la question* **III.6**.

(4) Montrer l'égalité (1).

Seconde méthode

(5) Montrer qu'il existe une unique bijection $\phi : \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$ telle que

$$\phi((x \bmod q), (y \bmod p)) = (xp + yq) \bmod pq$$

pour tout $(x, y) \in \mathbb{Z}^2$.

(6) Montrer la formule

$$\tau_{pq} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\tau_p\tau_q.$$

(7) En déduire l'égalité (1) [Utiliser les formules obtenues aux questions **IV.9** ou **V.5**].

(8) On pose dans cette question $K = \mathbb{Q}[i]$. En étudiant $(1+i)^q$ dans $\mathcal{O}_K$, montrer l'égalité

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$$

Indication : on s'inspirera de la question **VI.2**.

(9) *Application (à chercher plus tard) :* On admet le résultat difficile suivant : Étant donnés des entiers a, b non nuls premiers entre eux, l'ensemble $\{ak+b,\ k \in \mathbb{Z}\}$ contient une infinité de nombres premiers. Soit n un entier relatif. Soit S un ensemble fini de nombres premiers. On suppose que pour tout nombre premier $\ell \notin S$, la classe de n modulo ℓ est un carré dans $\mathbb{Z}/\ell\mathbb{Z}$. Montrer que n est le carré d'un entier.

VII. $\mathcal{O}_K$ est un sous-anneau (avec de la réduction, à chercher plus tard)

Soit V un $\mathbb{Q}$-espace vectoriel de dimension finie et f un endomorphisme de V. Si $v_1, \ldots, v_n$ sont des éléments de V, on note $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ l'ensemble des combinaisons linéaires à coefficients entiers des v_i, $i = 1, \ldots, n$.

(1) Montrer que les deux propositions suivantes sont équivalentes :

(i) Il existe un polynôme P unitaire à coefficients entiers annulant f ;

(ii) Il existe un entier n et des vecteurs v_i, $i = 1., \ldots, n$ engendrant V tels que

$$f(\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n) \subset \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n.$$

Indication : pour *(ii)* $\Rightarrow$ *(i),* on pourra introduire une matrice carrée dont les coefficients $a_{i,j}$ vérifient

$$f(v_j) = \sum_{i=1}^{n} a_{i,j}v_i,\ j = 1, \ldots, n$$

et considérer son polynôme caractéristique].

Un tel endomorphisme est dit *entier.*

(2) Montrer que la composée et la somme de deux endomorphismes entiers f, g de V qui commutent (*i.e.* tels que $f \circ g = g \circ f$) sont entiers. *Indication :* on pourra montrer qu'on peut choisir un entier n, des vecteurs v_i, $i = 1, \ldots, n$ comme dans *(ii)* de la question précédente, qui conviennent à la fois pour f et g.
Montrer que ce n'est plus le cas en général si on ne suppose pas que les endomorphismes commutent.

(3) Soit K un corps de nombres, muni de sa structure de $\mathbb{Q}$-espace vectoriel de dimension finie. Expliquer que $x \in K$ est un entier algébrique si et seulement si l'endomorphisme de multiplication

$$m_x : \begin{cases} K & \to K \\ y & \mapsto xy \end{cases}$$

est entier. En déduire que l'ensemble $\mathcal{O}_K$ est un sous-anneau de K.