Composition de mathématiques
ENS Paris-Lyon 2001 – MP

Avertissement

La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite en particulier les candidat(e)s à produire des raisonnements précis et concis. Les candidat(e)s peuvent utiliser les résultats énoncés dans les questions ou parties précédentes. 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.4 et V.6 sont utilisées dans la partie VI.

Notations

Soit ζ un nombre complexe. On note $\mathbf{Q}[\zeta]$ le $\mathbf{Q}$-espace vectoriel engendré par $\{\zeta^n \mid n \in \mathbf{N}\}$: c'est une $\mathbf{Q}$-algèbre. On note $\mathbf{Z}[\zeta]$ le sous-groupe additif de $\mathbf{Q}[\zeta]$ engendré par $\{\zeta^n \mid n \in \mathbf{N}\}$.
Un sous-corps de $\mathbf{C}$ qui est de dimension finie (vu comme $\mathbf{Q}$-espace vectoriel) est appelé un corps de nombres.
Soit 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 $\mathbf{Z}/n\mathbf{Z}$ et sera noté ζ^x. Dans le cas particulier où $\zeta = \exp(\frac{2i\pi}{n})$, on notera τ_n la somme

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

PARTIE I - Préliminaires

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

I.1. Montrer l'égalité $\displaystyle\prod_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x = \begin{cases} -y^{(p-1)/2} & \text{si } y \text{ est un carré,} \\ y^{(p-1)/2} & \text{sinon.} \end{cases}$

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

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

PARTIE II - Généralités

II.1. Montrer que les deux propositions suivantes sont équivalentes :

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

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

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

II.2. 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

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

[Indication : pour $(ii) \Longrightarrow (i)$, 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*.

II.3. Montrer que le composé 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 II.2 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.

Soit $\mathbf{K}$ un corps de nombres, muni de sa structure de $\mathbf{Q}$-espace vectoriel de dimension finie. On dira que $x \in \mathbf{K}$ est *entier* si l'endomorphisme de multiplication $m_x : \mathbf{K} \to \mathbf{K}$, $y \mapsto xy$, est entier. On note $\mathcal{O}_\mathbf{K}$ l'ensemble des éléments de $\mathbf{K}$ qui sont entiers, qui est donc un sous-anneau de $\mathbf{K}$ d'après la question II.3.

II.4. Montrer l'égalité $\mathcal{O}_\mathbf{K} \cap \mathbf{Q} = \mathbf{Z}$.

PARTIE III - Entiers des corps quadratiques

Soit $D \in \mathbf{Q}$ 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 $\mathbf{Q}[\sqrt{D}]$ (avec D non carré) est dit corps quadratique. On remarque que $(1, \sqrt{D})$ est une base de $\mathbf{Q}[\sqrt{D}]$. On note σ l'isomorphisme de corps $\sigma : \mathbf{Q}[\sqrt{D}] \to \mathbf{Q}[\sqrt{D}]$, $a + b\sqrt{D} \mapsto a - b\sqrt{D}$ (pour a et b rationnels).

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

III.2. Soit $D' \in \mathbf{Q}^*$. Montrer que $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{D'}]$ si et seulement si D/D' est le carré d'un rationnel.

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

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

Soit d un entier sans facteur carré et $\mathbf{K} = \mathbf{Q}[\sqrt{d}]$.

III.5. Montrer que $x \in \mathcal{O}_\mathbf{K}$ si et seulement si $x \in \mathbf{K}$ et $\begin{cases} x + \sigma(x) \in \mathbf{Z} \\ x\sigma(x) \in \mathbf{Z}. \end{cases}$

Soit $\omega \in \mathcal{O}_\mathbf{K}$ défini par $\omega = \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{sinon.} \end{cases}$

III.6. Montrer que l'application de $\mathbf{Z}^2$ dans $\mathcal{O}_\mathbf{K}$, $(x, y) \mapsto x + y\omega$ est un isomorphisme de groupes abéliens.

PARTIE IV - Un calcul analytique de τ_n

On se donne n entier ≥ 1. Pour $k = 0, \ldots, n-1$, on note f_k la fonction de $[0;1]$ dans $\mathbf{C}$, $t \mapsto \exp\left(\dfrac{2i\pi(t+k)^2}{n}\right)$ et $f = f_0 + \cdots + f_{n-1}$.

IV.1. Montrer que la suite de terme général u_j donné par

$$u_j = \sum_{m=-j}^{j} \int_0^1 f(t) \exp(-2i\pi m t)\, \mathrm{d}t$$

converge vers τ_n.

IV.2. Montrer que la fonction de $\mathbf{R}_+$ dans $\mathbf{C}$ qui à un réel x associe

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

admet une limite I_n dans $\mathbf{C}$ en $+\infty$.

IV.3. Comparer I_n et I_1.

IV.4. Montrer la formule $\tau_n = \dfrac{1+i^{-n}}{1+i^{-1}}\sqrt{n}$.

IV.5. Soit $\mathbf{K}$ un corps quadratique. Montrer qu'il existe une racine de l'unité ξ telle que $\mathbf{K} \subset \mathbf{Q}[\xi]$.

PARTIE V - Un calcul algébrique de τ_n

Soit n un entier impair avec $n > 1$ et ζ le complexe $\zeta = \exp(\frac{2i\pi}{n})$.
Soit V le $\mathbf{C}$-espace vectoriel de dimension n des fonctions de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{C}$. Soit φ l'endomorphisme de V qui à la fonction f associe $\varphi(f)$ définie par $\varphi(f) : x \mapsto \displaystyle\sum_{y \in \mathbf{Z}/n\mathbf{Z}} f(y)\zeta^{xy}$.

V.1. Soit $f \in V$. Montrer l'égalité

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

V.2. Diagonaliser $\varphi \circ \varphi$.

On remarque que $\tau_n = \displaystyle\sum_{x \in \mathbf{Z}/n\mathbf{Z}} \zeta^{x^2}$ est la trace de φ.

V.3. Montrer que le module $|\tau_n|$ est $\sqrt{n}$.

On cherche à calculer τ_n.
Soit a, b, c, d les multiplicités respectives des valeurs propres $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$, $-i\sqrt{n}$ de φ.

V.4. Montrer les égalités $a + b = \dfrac{n+1}{2}$ et $c + d = \dfrac{n-1}{2}$ ainsi que $(a-b)^2 + (c-d)^2 = 1$.

V.5. En calculant $\det(\varphi)$, calculer a, b, c, d en fonction de n.

V.6. Montrer

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

(formule compatible avec la question IV.4).

PARTIE VI - Réciprocité quadratique

On considère deux nombres premiers impairs distincts, p, q. On note $\mathbf{L}$ le corps de nombres $\mathbf{Q}[\exp(\frac{2i\pi}{p})]$ et $\mathbf{K}$ le corps quadratique $\mathbf{Q}[\tau_p]$, qui est contenu dans $\mathbf{L}$. 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

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

Première méthode

VI.1. Montrer l'égalité $\mathcal{O}_L \cap \mathbf{K} = \mathcal{O}_{\mathbf{K}}$.

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

VI.3. Soit n un entier relatif. Montrer que si $n\tau_p$ est un élément de $q\mathcal{O}_{\mathbf{K}}$, alors q divise n.
[Indication : utiliser la question III.6.]

VI.4. Montrer l'égalité (1).

Seconde méthode

VI.5. Montrer qu'il existe une unique bijection φ de $\mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{Z}/pq\mathbf{Z}$ telle que

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

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

VI.6. Montrer la formule

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

VI.7. En déduire l'égalité (1).
[Utiliser les formules obtenues aux questions IV.4 ou V.6.]

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

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

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

Une application

On admet le résultat difficile suivant :
Étant donnés des entiers a, b non nuls premiers entre eux, l'ensemble $\{ak + b \,|\, k \in \mathbf{Z}\}$ contient une infinité de nombres premiers.

VI.9. 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 $\mathbf{Z}/\ell\mathbf{Z}$. Montrer que n est le carré d'un entier.

Composition de mathématiques – ENS Paris-Lyon 2001 – MP

PARTIE I - Préliminaires

I.1. L'application de $(\mathbf{Z}/p\mathbf{Z})^*$ dans lui-même donnée par $x \mapsto y/x$ est une bijection puisque c'est le cas pour le passage à l'inverse et pour la multiplication par y, car y est inversible. De plus cette bijection est involutive et ses points fixes sont exactement les x de $(\mathbf{Z}/p\mathbf{Z})^*$ tels que $x^2 = y$.

Donc si y n'est pas un carré, les $p-1$ facteurs du produit se regroupent en $(p-1)/2$ couples $(x, y/x)$ dont le produit vaut y, d'où l'assertion dans ce cas.

Si y est un carré, disons $y = a^2$. Alors $x^2 = y$ si et seulement si $x^2 = a^2$, i.e. $(x-a)(x+a) = 0$ ou encore $x = \pm a$. Comme p est impair, $a \neq -a$. Ainsi les $p-1$ facteurs du produit se regroupent en $(p-3)/2$ couples de produit y et le couple $(a, -a)$ dont le produit est $-a^2$, i.e. $-y$. D'où $\boxed{\displaystyle\prod_{x\in(\mathbf{Z}/p\mathbf{Z})^*} x = \begin{cases} -y^{(p-1)/2} & \text{si } y \text{ est un carré,} \\ y^{(p-1)/2} & \text{sinon.} \end{cases}}$

I.2. On applique ce qui précède à 1, qui est un carré puisque $1^2 = 1$, et on en déduit que le produit considéré précédemment vaut -1. Il en résulte $\boxed{\begin{cases} y^{(p-1)/2} = 1 & \text{si } y \text{ est un carré,} \\ y^{(p-1)/2} = -1 & \text{sinon.} \end{cases}}$

PARTIE II - Généralités

II.1. On considère le morphisme d'algèbres φ de $\mathbf{Q}[X]$ dans $\mathbf{Q}[\zeta]$ donné par $\varphi(P) = P(\zeta)$. Son noyau est un idéal de $\mathbf{Q}[X]$. S'il est nul, alors φ est injectif et en particulier $\mathbf{Q}[\zeta]$ est de dimension infinie. On en déduit $(ii) \Longrightarrow (i)$. Si cet idéal est non nul, puisque $\mathbf{Q}[X]$ est principal, on dispose de π_ζ un polynôme unitaire engendrant $\mathrm{Ker}(\varphi)$. Par division euclidienne on en déduit $\dim(\mathbf{Q}[\zeta]) = \deg(\pi_\zeta)$. De plus, pour x non nul dans $\mathbf{Q}[\zeta]$, l'application $y \mapsto xy$ est un endomorphisme de $\mathbf{Q}[\zeta]$, injectif par régularité de x dans $\mathbf{C}$, et donc surjectif puisque $\mathbf{Q}[\zeta]$ est de dimension finie. En particulier on dispose de y dans $\mathbf{Q}[\zeta]$ tel que $xy = 1$ i.e. x est inversible dans $\mathbf{Q}[\zeta]$ et donc $\mathbf{Q}[\zeta]$ est un corps de nombres. D'où $\boxed{(i) \Longleftrightarrow (ii).}$

II.2. Soit P un polynôme unitaire à coefficients entiers annulant f et $(u_1, \ldots, u_p)$ une famille génératrice de V. Pour $1 \leq i \leq p$ et $0 \leq j < \deg(P)$, on pose $u_{i,j} = f^j(u_i)$. Par construction, pour $1 \leq i \leq p$ et $0 \leq j < \deg(P) - 1$, $f(u_{i,j}) = u_{i,j+1}$ et, de plus, $f(u_{i,\deg(P)-1}) = f^{\deg(P)}(u_i) = (f^{\deg(P)} - P(f))(u_i)$, puisque $P(f) = 0$, et cette dernière expression est combinaison linéaire à coefficients entiers de $u_{i,0}$, …, $u_{i,\deg(P)-1}$ puisque P est unitaire et à coefficients entiers. Par linéarité, il en résulte $f\left(\sum_{i,j} \mathbf{Z}u_{i,j}\right) \subset \sum_{i,j} \mathbf{Z}u_{i,j}$.

Comme la famille $(u_{i,j})$ contient la famille (u_i), elle engendre V et on a donc $(i) \Longrightarrow (ii)$.

Réciproquement, soit $(v_1, \ldots, v_n)$ engendrant V et tel que $f(\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n) \subset \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n$. On dispose donc d'entiers $(a_{i,j})$ tels que $f(v_j) = \displaystyle\sum_{i=1}^{n} a_{i,j}v_i$ et on note $A = (a_{i,j})_{1\leq i,j\leq n}$.

Pour k dans $\mathbf{N}$, on note $A^k = (a_{i,j}^{(k)})$. Une récurrence immédiate montre qu'on a alors $f^k(v_j) = \displaystyle\sum_{i=1}^{n} a_{i,j}^{(k)} v_i$ et plus généralement si P est un polynôme à coefficients entiers et si $P(A) = (a_{i,j}^{(P)})$,

alors $P(f)(v_j) = \sum_{i=1}^{n} a_{i,j}^{(P)} v_i$. Soit alors χ_A le polynôme caractéristique de A. Puisque $\chi_A(A) = 0$, d'après le théorème de CAYLEY-HAMILTON, il vient $a_{i,j}^{(\chi_A)} = 0$ et donc $\chi_A(f)(v_j) = 0$. Comme $(v_1, \ldots, v_n)$ est génératrice, il en résulte $\chi_A(f) = 0$ et donc χ_A est un polynôme unitaire, annulant f, et à coefficients entiers puisque A est à coefficients entiers. On en déduit $\boxed{(i) \Longleftrightarrow (ii).}$

II.3. Soit f et g deux endomorphismes entiers commutant entre eux. On dispose d'une famille $(v_1, \ldots, v_n)$ engendrant V et telle que $f(\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n) \subset \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_n$. On dispose également de P un polynôme unitaire à coefficients entiers annulant g. On pose $v_{i,j} = g^j(v_i)$ pour $1 \leq i \leq n$ et $0 \leq j < \deg(P)$. La famille $(v_{i,j})$ est donc génératrice. Par construction, tout comme précédemment, on a directement, en posant $\Lambda = \sum_{i,j} \mathbf{Z}v_{i,j}$, $g(\Lambda) \subset \Lambda$. De plus

$$\Lambda = \sum_{j=0}^{\deg(P)-1} \left(\sum_{i=1}^{n} \mathbf{Z}v_{i,j} \right) = \sum_{j=0}^{\deg(P)-1} g^j \left(\sum_{i=1}^{n} \mathbf{Z}v_i \right)$$

et donc, puisque f et g commutent,

$$\begin{aligned} f(\Lambda) &= \sum_{j=0}^{\deg(P)-1} g^j \circ f \left(\sum_{i=1}^{n} \mathbf{Z}v_i \right) \\ &\subset \sum_{j=0}^{\deg(P)-1} g^j \left(\sum_{i=1}^{n} \mathbf{Z}v_i \right) = \Lambda \, . \end{aligned}$$

Il vient alors $(f+g)(\Lambda) \subset f(\Lambda) + g(\Lambda) \subset \Lambda + \Lambda = \Lambda$ et $(f \circ g)(\Lambda) \subset f(\Lambda) \subset \Lambda$ et donc $\boxed{f+g \text{ et } f \circ g \text{ sont entiers.}}$

Soit $V = \mathscr{M}_{2,1}(\mathbf{Q})$, $f = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$ et $g = \begin{pmatrix} 1/2 & 1/4 \\ 1 & 1/2 \end{pmatrix}$. On a $f^2 + f = g^2 - g = 0$ d'après le théorème de CAYLEY-HAMILTON puisque $-\operatorname{Tr}(f) = \operatorname{Tr}(g) = 1$ et $\det(f) = \det(g) = 0$. Comme $\operatorname{Tr}(f+g) = 0$ et $\det(f+g) = -\frac{1}{2}$, $X^2 - \frac{1}{2}$ est un polynôme annulateur de $f+g$ et, puisque $f+g$ n'est pas scalaire, c'est son polynôme minimal. Soit alors P un polynôme unitaire à coefficients entiers annulant $f+g$. Alors $X^2 - \frac{1}{2}$ divise P et on dispose de Q dans $\mathbf{C}[X]$ tel que $P = (X^2 - \frac{1}{2})Q$. On écrit $Q = a_0 + a_1 X + \cdots + a_n X^n$. Alors, puisque P est à coefficients entiers, $-\frac{1}{2}a_0$ et $-\frac{1}{2}a_1$ sont entiers, puisque ce sont les coefficients de P de degrés 0 et 1. Autrement dit a_0 et a_1 sont des entiers pairs. Les coefficients de P de degrés 2 et 3 sont alors $-\frac{1}{2}a_2 + a_0$ et $-\frac{1}{2}a_3 + a_1$ et il en résulte que a_2 et a_3 sont des entiers pairs. Une récurrence directe montre que tous les coefficients de Q sont des entiers pairs, ce qui contredit le fait que le coefficient dominant de P est 1.

De même $f \circ g$ est annulé par $X^2 + \frac{1}{2}X$ et une écriture $P = (X^2 + \frac{1}{2}X)Q$ avec P à coefficients

entiers, impose à Q d'être à coefficients entiers pairs et n'est donc pas compatible avec P unitaire. Il en résulte que $\boxed{f+g \text{ et } fg \text{ ne sont pas entiers.}}$

II.4. Soit x dans $\mathbf{K}$ et P dans $\mathbf{C}[X]$, on a $P(m_x) = m_{P(x)}$ et donc x est entier si et seulement s'il est annulé par un polynôme unitaire à coefficients entiers. En particulier tout entier relatif est entier. Par ailleurs si p et q sont deux entiers premiers entre eux et si P est un polynôme à coefficients entiers, unitaire, annulant p/q, alors $P(p/q) = 0$. Si on écrit $P = X^{\deg(P)} + Q$, alors Q est de degré strictement inférieur à $\deg(P)$ et on a $0 = q^{\deg(P)}P(p/q) = p^{\deg(P)} + q.q^{\deg(P)-1}Q(p/q)$ et donc, puisque $q^{\deg(P)-1}Q(p/q)$ est entier, q divise $p^{\deg(P)}$. Comme q est premier à p, il en résulte $q = \pm 1$ et donc $p/q \in \mathbf{Z}$. Par conséquent $\boxed{\mathbf{Z} = \mathcal{O}_\mathbf{K} \cap \mathbf{Q}.}$

PARTIE III - Entiers des corps quadratiques

III.1. Par construction σ est un isomorphisme d'espaces vectoriels puisque la base $(1, \sqrt{D})$ de $\mathbf{Q}[\sqrt{D}]$ est envoyée sur la base $(1, -\sqrt{D})$. Pour vérifier que c'est un isomorphisme de corps, il suffit donc de vérifier que c'est un morphisme d'anneaux et plus simplement qu'il préserve les produits des éléments de la base. Par commutativité, on se restreint aux produits 1.1, $1.\sqrt{D}$ et $\sqrt{D}.\sqrt{D}$. Comme $\sigma(1.1) = \sigma(1) = 1 = \sigma(1)\sigma(1)$, $\sigma(1.\sqrt{D}) = \sigma(\sqrt{D}) = -\sqrt{D} = \sigma(1)\sigma(\sqrt{D})$ et $\sigma(\sqrt{D}\sqrt{D}) = \sigma(D) = D = (-\sqrt{D})^2 = \sigma(\sqrt{D})\sigma(\sqrt{D})$, σ est bien un isomorphisme de corps, tout comme l'identité.

Soit maintenant f un isomorphisme du corps $\mathbf{Q}[\sqrt{D}]$. Alors $f_{|\mathbf{Q}} = \mathrm{Id}_\mathbf{Q}$ puisque $f(1) = 1$, $f(p) = pf(1) = p$ et $qf(p/q) = f(p) = p$ si p et q sont entiers, avec $q \neq 0$. De plus $f(\sqrt{D})^2 = f(\sqrt{D}^2) = f(D) = D$ et donc $f(\sqrt{D}) = \pm\sqrt{D}$. Il en résulte, par linéarité, $f = \mathrm{Id}$ ou $f = \sigma$, i.e. les seuls isomorphismes de corps de $\mathbf{Q}[\sqrt{D}]$ sont $\boxed{\text{l'identité et } \sigma.}$

III.2. Soit r dans $\mathbf{Q}$ tel que $D = D'r^2$, alors $\sqrt{D} = \sqrt{D'}r$ et donc $\sqrt{D} \in \mathbf{Q}[\sqrt{D'}]$, d'où $\mathbf{Q}[\sqrt{D}] \subset \mathbf{Q}[\sqrt{D'}]$. Comme D n'est pas un carré, $D \neq 0$ et donc $r \neq 0$. Il en résulte $D' = D\dfrac{1}{r^2}$ et donc $\mathbf{Q}[\sqrt{D'}] \subset \mathbf{Q}[\sqrt{D}]$, d'où $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{D'}]$.

Réciproquement si $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{D'}]$, alors D' n'est pas un carré, car sinon on aurait $\mathbf{Q}[\sqrt{D'}] = \mathbf{Q}$, et σ est un isomorphisme de corps de $\mathbf{Q}[\sqrt{D'}]$. Comme σ n'est pas l'identité de $\mathbf{Q}[\sqrt{D'}]$, on a $\sigma(\sqrt{D'}) = -\sqrt{D'}$ et donc $\sqrt{D'} \in \mathrm{Ker}(\sigma + \mathrm{Id}) = \mathbf{Q}\sqrt{D}$, et D'/D est le carré d'un rationnel (non nul). Par conséquent,

$\boxed{\mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{D'}] \text{ si et seulement si } D/D' \text{ est le carré d'un rationnel (non nul).}}$

III.3. D'après ce qui précède, il s'agit de démontrer qu'il existe un unique entier relatif d sans facteur carré tel que D/d soit le carré d'un rationnel. Quitte à multiplier D par le carré de son dénominateur, on peut le supposer entier. On a alors $D = \pm\prod_p p^{v_p(D)}$, où p décrit les nombres premiers et où v_p désigne la valuation p-adique. La condition s'écrit $d = \pm\prod_p p^{a_p}$ avec, pour tout entier premier p, $a_p = 0$ ou $a_p = 1$ et $v_p(D) - a_p$ est pair et, de plus, $D/d > 0$. On en déduit que d est du signe de D et $|d|$ est le produit des entiers premiers divisant D à une puissance impaire. Et, réciproquement, un tel d convient, i.e.

$\boxed{\text{il existe un unique } d \text{ dans } \mathbf{Z}, \text{ sans facteur carré, tel que } \mathbf{Q}[\sqrt{D}] = \mathbf{Q}[\sqrt{d}].}$

III.4. Soit $(1, x)$ une base de $\mathbf{K}$ sur $\mathbf{Q}$. Puisque $x^2 \in \mathbf{K}$, on dispose de α et β dans $\mathbf{Q}$ tels que $x^2 = \alpha + \beta x$. Il en résulte $x \in \mathbf{Q}[\sqrt{D}]$ avec $4\alpha + \beta^2 = D$, et donc $\mathbf{K} \subset \mathbf{Q}[\sqrt{D}]$. Par dimension, on a donc égalité et donc D n'est pas un carré et ainsi $\boxed{\mathbf{K} \text{ est un corps quadratique.}}$

III.5. Soit x dans $\mathcal{O}_\mathbf{K}$. On dispose alors de P, polynôme dans $\mathbf{Z}[X]$, unitaire, annulant x. Comme P est à coefficients entiers on a $P\circ\sigma=\sigma\circ P$ et donc $P(\sigma(x))=0$. Il en résulte $\sigma(x)\in\mathcal{O}_\mathbf{K}$. Comme $\mathcal{O}_\mathbf{K}$ est un anneau d'après II.3, $x+\sigma(x)$ et $x\sigma(x)$ appartiennent aussi à $\mathcal{O}_\mathbf{K}$. Comme σ est une involution, ces deux éléments sont invariants par σ, i.e. appartiennent à $\mathrm{Ker}(\sigma-\mathrm{Id})$, c'est-à-dire $\mathbf{Q}$. D'après II.4, ce sont donc des entiers relatifs.

Réciproquement, soit $x\in K$ tel que $x+\sigma(x)$ et $x\sigma(x)$ soient entiers relatifs. Alors x et $\sigma(x)$ sont les racines du polynôme à coefficients entiers $X^2-(x+\sigma(x))X+x\sigma(x)$ et donc $x\in\mathcal{O}_\mathbf{K}$. D'où $\boxed{x\in\mathcal{O}_\mathbf{K}\iff x\in\mathbf{K}\text{ et }x+\sigma(x)\text{ et }x\sigma(x)\text{ sont entiers.}}$

III.6. Par construction, $(x,y)\mapsto x+y\omega$ est un morphisme du groupe $\mathbf{Z}^2$ dans $\mathbf{C}$. Il est injectif car son noyau est réduit à $(0,0)$ puisque ω n'est pas rationnel, vu que d n'est pas un carré. Si d n'est pas congru à 1 modulo 4, on a $\omega^2-d=0$ et donc ω est entier et donc l'image du morphisme étudié est incluse dans $\mathcal{O}_\mathbf{K}$. Sinon ω est racine de $X^2-X-\dfrac{d-1}{4}$ et est donc aussi entier puisque $(d-1)/4$ est alors entier relatif. Dans tous les cas, l'image du morphisme est donc incluses dans $\mathcal{O}_\mathbf{K}$.

Soit maintenant x dans $\mathbf{K}$. On dispose de a et b dans $\mathbf{Q}$ tels que $x=a+b\sqrt{d}$, de sorte que $x+\sigma(x)=2a$ et $x\sigma(x)=a^2-db^2$. D'après la question précédente, $x\in\mathcal{O}_\mathbf{K}$ si et seulement si $2a$ et a^2-db^2 sont entiers.

On dispose de u et v dans $\mathbf{Z}$ et $\mathbf{N}^*$ respectivement, et premiers entre eux, tels que $b=u/v$. On a donc $4du^2=4db^2v^2=v^2((2a)^2-4(a^2-db^2))$. On suppose maintenant $x\in\mathcal{O}_\mathbf{K}$. Alors v^2 divise $4du^2$. Comme $u\wedge v=1$, on a aussi $u^2\wedge v^2=1$ et donc v^2 divise $4d$. Comme d est sans facteur carré, le seul nombre premier pouvant diviser v est 2 et donc $v|2$. Si $v=1$, alors l'équation $4du^2=(2a)^2-4(a^2-db^2)$ entraîne que $(2a)^2$ est un entier pair, donc multiple de 4 et donc $2a$ est un entier pair, i.e. a est entier. Comme b aussi, on a $x\in\mathbf{Z}+\mathbf{Z}\omega$.

Si $v=2$, $b=u/2$ et $du^2=(2a)^2-4(a^2-db^2)\equiv(2a)^2\pmod 4$. Comme $u\wedge v=1$, u est impair et donc $u^2\equiv 1\pmod 4$ et donc d est un carré modulo 4. S'il est pair, il est donc nul modulo 4, ce qui contredit que d est sans facteur carré. Il en résulte que d est impair. Comme -1 n'est pas un carré modulo 4, on a alors $d\equiv 1\pmod 4$ et donc $2a$ est impair, tout comme $2b$. Il en résulte $x\in\mathbf{Z}+\mathbf{Z}\omega$ puisque dans ce cas $\omega=\dfrac{1=\sqrt{d}}{2}$. Par conséquent

$\boxed{(x,y)\mapsto x+y\omega\text{ est un isomorphisme de groupes abéliens entre }\mathbf{Z}^2\text{ et }\mathcal{O}_\mathbf{K}.}$

PARTIE IV - Un calcul analytique de τ_n

IV.1. Par définition f est de classe C^∞ en tant que somme de telles fonctions. On a de plus, en posant $\zeta=\exp(2i\pi/n)$,

$$f(0)=\sum_{k=0}^{n-1}\zeta^{k^2}=\tau_n\quad\text{et}\quad f(1)=\sum_{k=0}^{n-1}\zeta^{(k+1)^2}=\tau_n\,.$$

De plus, pour m dans $\mathbf{Z}$, on a $\displaystyle\int_0^1\exp(-2i\pi mt)\,\mathrm{d}t=\delta_{m,0}$, en utilisant le symbole de Kronecker. Par conséquent

$$\lim u_j=\tau_n\iff\lim\sum_{m=_k}^{k}\int_0^1(f(t)-f(0))\exp(-2i\pi mt)\,\mathrm{d}t=0\,,$$

i.e., par linéarité de l'intégrale,

$$\lim u_j = \tau_n \iff \lim \int_0^1 (f(t) - f(0)) \frac{\sin((2k+1)\pi t)}{\sin(\pi t)} \,\mathrm{d}t = 0$$

en prolongeant la fonction quotient de deux sinus par continuité en 0 et 1, i.e. par $2k+1$. Or, si g est une fonction de classe C^∞ sur un intervalle I contenant un certain réel a, sa fonction pente par rapport à a, i.e. $x \mapsto \dfrac{g(x)-g(a)}{x-a}$ prolongée par continuité en a par $g'(a)$, est de classe C^∞. En effet, d'après la formule de Taylor-Laplace, on a

$$\forall x \in I \qquad g(x) - g(a) = (x-a) \int_0^1 g'(a + t(x-a)) \,\mathrm{d}t$$

et donc en notant g_a la fonction pente, $\forall x \in I$, $g_a(x) = \displaystyle\int_0^1 g'(a+t(x-a)) \,\mathrm{d}t$. Soit maintenant K un segment contenant a et inclus dans I. Pour tout t dans $[0;1]$ la fonction $h_t : x \mapsto g'(a+t(x-a))$ est de classe C^∞ sur K et on a, pour k dans $\mathbf{N}$, $t \mapsto h_t^{(k)}(x)$ est continue sur $[0;1]$ et

$$\forall t \in [0;1] \quad \left|h_t^{(k)}(x)\right| = \left|t^k g^{(k+1)}(a+t(x-a))\right| \leq \sup_K \left|g^{(k+1)}\right|$$

et on peut donc appliquer le théorème de Leibniz de dérivation sous le signe somme puisque les fonctions constantes (positives) sont des fonctions continues, positives et intégrables sur le compact $[0;1]$. On en déduit que si g_1 et g_2 sont deux fonctions de classe C^∞ sur un intervalle I contenant un certain réel a, le rapport de leurs fonctions pente par rapport à a, i.e. $x \mapsto \dfrac{g_1(x)-g_2(a)}{g_2(x)-g_2(a)}$ prolongé par continuité en a par $\dfrac{g_1'(a)}{g_2'(a)}$, est de classe C^∞ partout où le quotient est défini (et donc aussi en a). En appliquant ceci à $I = [0;1]$, $a = 0$ ou $a = 1$ et $g_1 = f$ et $g_2 : t \mapsto \sin(\pi t)$, on en déduit que la fonction $t \mapsto \dfrac{f(t)-f(0)}{\sin(\pi t)}$ est prolongeable en une fonction de classe C^∞ sur $[0;1]$. On note φ ce prolongement. Il vient alors par intégration par parties

$$\int_0^1 \varphi(t)\sin((2k+1)\pi t) \,\mathrm{d}t = \frac{1}{2k+1}\left(-\left[\varphi(t)\cos((2k+1)\pi t)\right]_0^1 + \int_0^1 \varphi'(t)\cos((2k+1)\pi t) \,\mathrm{d}t\right)$$

et donc, par inégalité triangulaire et inégalité de la moyenne,

$$\left|\int_0^1 \varphi(t)\sin((2k+1)\pi t) \,\mathrm{d}t\right| \leq \frac{1}{2k+1}\left(2\sup_{[0;1]}|\varphi| + \sup_{[0;1]}|\varphi'|\right);.$$

Par encadrement, on en déduit $\boxed{\lim u_j = \tau_n.}$

IV.2. Soit g et h les fonctions définies sur $\mathbf{R}$ par $g(t) = \exp(2i\pi t^2/n) - 1$ et $h(t) = \dfrac{n}{4i\pi t}$. Alors g est de classe C^∞ sur $\mathbf{R}$ et h l'est sur $\mathbf{R}^*$. De plus $g'h$, gh et gh' sont toutes les trois prolongeables par continuité en 0, respectivement par 1, 0 et $-\dfrac{1}{2}$. Il en résulte, pour x dans $\mathbf{R}^*$,

$$\int_0^x \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t = n\frac{\exp(2i\pi x^2/n) - 1}{4i\pi x} + n\int_0^x \frac{\exp(2i\pi t^2/n) - 1}{4i\pi t^2} \,\mathrm{d}t$$

et donc, par parité de l'intégrande,

$$\int_{-x}^{x} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t = 2n\frac{\exp(2i\pi x^2/n)-1}{4i\pi x} + 2n\int_0^x \frac{\exp(2i\pi t^2/n)-1}{4i\pi t^2}\,\mathrm{d}t\,.$$

Comme l'intégrale

$$\int_0^{+\infty} \frac{\exp(2i\pi t^2/n)-1}{4i\pi t^2}\,\mathrm{d}t$$

est absolument convergente, puisque l'intégrande est prolongeable par continuité sur $\mathbf{R}_+$ et est dans $O(t^{-2})$ en l'infini, il s'ensuit que $\displaystyle\int_{-x}^{x} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t$ admet une limite en $+\infty$, à savoir I_n donné par $\boxed{2n\displaystyle\int_0^{+\infty} \frac{\exp(2i\pi t^2/n)-1}{4i\pi t^2}\,\mathrm{d}t.}$

IV.3. Par changement de variable affine bijectif, $t = u\sqrt{n}$, il vient directement $\boxed{I_n = I_1\sqrt{n}.}$

IV.4. Pour k dans $\mathbf{N}$, on a

$$u_k = \sum_{m=-k}^{k}\sum_{\ell=0}^{n-1}\int_0^1 \exp\left(\frac{2i\pi(t+\ell)^2}{n}\right)\exp(-2i\pi mt)\,\mathrm{d}t$$

ou encore, par 1-périodicité,

$$u_k = \sum_{m=-k}^{k}\sum_{\ell=0}^{n-1}\int_0^1 \exp\left(\frac{2i\pi(t+\ell)^2}{n}\right)\exp(-2i\pi m(t+\ell))\,\mathrm{d}t$$

et donc, par changement de variable affine et relation de Chasles,

$$u_k = \sum_{m=-k}^{k}\int_0^n \exp\left(\frac{2i\pi t^2}{n}\right)\exp(-2i\pi mt)\,\mathrm{d}t = \sum_{m=-k}^{k}\int_0^n \exp\left(\frac{2i\pi(t^2-mnt)}{n}\right)\mathrm{d}t\,.$$

Il vient

$$\begin{aligned} u_k &= \sum_{m=-k}^{k}\int_0^n \exp\left(\frac{2i\pi(t-mn/2)^2 - 2i\pi m^2n^2/4}{n}\right)\mathrm{d}t \\ &= \sum_{m=-k}^{k}\int_0^n (-i)^{m^2n}\exp\left(\frac{2i\pi(t-mn/2)^2}{n}\right)\mathrm{d}t \end{aligned}$$

i.e.

$$u_k = \sum_{m=-k}^{k}\int_{-mn/2}^{-(m-2)n/2} (-i)^{m^2n}\exp\left(\frac{2i\pi t^2}{n}\right)\mathrm{d}t\,.$$

Pour m pair, on a $(-i)^{m^2n} = 1$. Pour m impair, on a $m^2 \equiv 1 \pmod 4$ et donc $(-i)^{m^2n} = (-i)^n$. On applique ce qui précède à $k = 2p$, avec p dans $\mathbf{N}$. Il vient :

$$\begin{aligned}
u_{2p} &= \sum_{m=-2p}^{2p} \int_{-mn/2}^{-(m-2)n/2} (-i)^{m^2n} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t \\
&= \sum_{m=-p}^{p} \int_{-2mn/2}^{-(2m-2)n/2} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t + \sum_{m=-p+1}^{p-1} \int_{-(2m+1)n/2}^{-(2m-1)n/2} (-i)^n \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t \\
&= \int_{-pn}^{(p+1)n} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t + \int_{-(2p-1)n/2}^{(2p-1)n/2} (-i)^n \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t \\
&= \int_{pn}^{(p+1)n} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t + \int_{-pn}^{pn} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t + \int_{-(2p-1)n/2}^{(2p-1)n/2} (-i)^n \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t
\end{aligned}$$

Or $\displaystyle\int_{pn}^{(p+1)n} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t$ tend vers 0 quand p tend vers l'infini d'après les calculs menés en IV.2. Il en résulte que u_{2p} tend vers $(1 + (-i)^n)I_n$ quand p tend vers l'infini.

Il vient $\tau_n = (1 + (-i)^n)I_n$ et $1 = \tau_1 = (1 + i^{-1})I_1$. D'où, par IV.3, $\boxed{\tau_n = \dfrac{1 + i^{-n}}{1 + i^{-1}}\sqrt{n}.}$

IV.5. On dispose de d un entier sans facteur carré tel que $K = \mathbf{Q}[\sqrt{d}]$. Soit $\xi = \exp(i\pi/2d)$. On a donc $i = \xi^d$ et $\exp(2i\pi/d) = \xi^4$, d'où, d'après ce qui précède, $\sqrt{d} = \tau_d \dfrac{1 + i^{-1}}{1 + i^{-d}} \in \mathbf{Q}[\xi]$. Comme $\xi^{4d} = 1$, $\boxed{\text{il existe une racine de l'unité } \xi \text{ telle que } \mathbf{K} \subset \mathbf{Q}[\xi].}$

PARTIE V - Un calcul algébrique de τ_n

V.1. Soit f dans V et x dans $\mathbf{Z}/n\mathbf{Z}$. On a

$$\begin{aligned}
\varphi \circ \varphi(f)(x) &= \sum_{y \in \mathbf{Z}/n\mathbf{Z}} \varphi(f)(y)\zeta^{xy} \\
&= \sum_{y \in \mathbf{Z}/n\mathbf{Z}} \sum_{z \in \mathbf{Z}/n\mathbf{Z}} f(z)\zeta^{yz}\zeta^{xy} \\
&= \sum_{z \in \mathbf{Z}/n\mathbf{Z}} f(z) \left(\sum_{y \in \mathbf{Z}/n\mathbf{Z}} \left(\zeta^{x+z}\right)^y \right) \\
&= \sum_{z \in \mathbf{Z}/n\mathbf{Z}} f(z) \left(\sum_{k=0}^{n-1} \left(\zeta^{x+z}\right)^k \right) .
\end{aligned}$$

On a $\zeta^{x+z} = 1 \Leftrightarrow x + z = 0$ et dans ce cas la dernière somme vaut n. Sinon, on a affaire à la somme d'une suite géométrique, de somme $(1 - \zeta^{n(x+z)})/(1 - \zeta^{x+z})$, i.e. 0. Il vient donc $\boxed{\varphi \circ \varphi(f)(x) = nf(-x).}$

V.2. Soient P et I les sous-espaces de V constitués des fonctions paires et impaires respectivement. Alors la restriction de $\varphi\circ\varphi$ à P et I est scalaire, donc toute base de V formée d'une base de P concaténée à une base de I est une base de diagonalisation de $\varphi\circ\varphi$ et on a $\boxed{V=P\oplus I \text{ avec } P=\mathrm{Ker}(\varphi\circ\varphi-n\mathrm{Id}) \text{ et } I=\mathrm{Ker}(\varphi\circ\varphi+n\mathrm{Id}).}$

Remarque : comme une base de V est $(\delta_x)_{x\in\mathbf{Z}/n\mathbf{Z}}$, on a $\mathrm{Tr}(\varphi)=\sum_{x\in\mathbf{Z}/n\mathbf{Z}}\varphi(\delta_x)(x)$ et $\varphi(\delta_x)(x)=\zeta^{x^2}$, d'où la remarque de l'énoncé.

V.3. Comme n est impair, la formule IV.4 donne immédiatement le résultat, mais ce n'est pas l'esprit du problème.

On a
$$|\tau_n|^2=\tau_n\overline{\tau_n}=\sum_{x\in\mathbf{Z}/n\mathbf{Z}}\sum_{y\in\mathbf{Z}/n\mathbf{Z}}\zeta^{x^2-y^2}=\sum_{x\in\mathbf{Z}/n\mathbf{Z}}\sum_{y\in\mathbf{Z}/n\mathbf{Z}}\zeta^{(x-y)(x+y)}\,.$$

Or l'application $(x,y)\mapsto(x+y,x-y)$ est bijective de $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/n\mathbf{Z}$ dans lui-même puisque n est impair. Il vient :
$$|\tau_n|^2=\sum_{u\in\mathbf{Z}/n\mathbf{Z}}\left(\sum_{v\in\mathbf{Z}/n\mathbf{Z}}(\zeta^u)^v\right)=n$$
puisque la somme intérieure est non nulle uniquement si $u=0$ et vaut alors n. D'où $\boxed{|\tau_n|=\sqrt{n}.}$

V.4. D'après V.1 ou V.2 le polynôme simplement scindé X^4-n^2 annule φ et donc φ est diagonalisable et son spectre est inclus dans $\{\pm\sqrt{n},\pm i\sqrt{n}\}$. De plus, d'après V.2, $a+b$ est égal à $\dim(P)$ et $c+d$ à $\dim(I)$. Comme des bases respectives de ces espaces sont $(\delta_0,\delta_x+\delta_{-x})_{1\le x\le(n-1)/2}$ et $(\delta_x-\delta_{-x})_{1\le x\le(n-1)/2}$ (en confondant x avec sa classe dans $\mathbf{Z}/n\mathbf{Z}$), il vient $\boxed{a+b=\frac{n+1}{2} \text{ et } c+d=\frac{n-1}{2}.}$

De plus $\tau_n=\mathrm{Tr}(\varphi)=((a-b)+i(c-d))\sqrt{n}$ et donc, d'après 5.3, $a-b+i(c-d)$ est de module 1, i.e. $\boxed{(a-b)^2+(c-d)^2=1.}$

V.5. En confondant les entiers avec leurs représentants dans $\mathbf{Z}/n\mathbf{Z}$, une base de V est donnée par $(\delta_k)_{0\le k\le n-1}$, et la matrice de φ dans cette base est la matrice de Vandermonde $(\zeta^{(k-1)(\ell-1)})_{1\le k,\ell\le n}$. On note $\xi=\exp(\frac{i\pi}{n})$, de sorte que $\xi^2=\zeta$. Il vient
$$\det(\varphi)=\prod_{0\le\ell<k\le n-1}(\zeta^k-\zeta^\ell)=\prod_{0\le\ell<k\le n-1}\xi^{k+\ell}(\xi^{k-\ell}-\xi^{\ell-k})\,.$$

Or, dans cette expression, on a
$$\xi^{k-\ell}-\xi^{\ell-k}=2i\sin\left((k-\ell)\frac{\pi}{n}\right)$$
dont un argument est $\pi/2$ puisque le sinus est positif. Il en résulte qu'un argument de $\det(\varphi)$ est
$$\sum_{0\le\ell<k\le n-1}\left(\frac{(k+\ell)\pi}{n}+\frac{\pi}{2}\right)$$

i.e.

$$\sum_{k=1}^{n-1}\left(\left(k^2+\frac{k(k-1)}{2}\right)\frac{\pi}{n}+\frac{k\pi}{2}\right)$$

ou encore

$$\pi\left(\frac{3}{2}\frac{(n-1)n(2n-1)}{6n}-\frac{1}{2}\frac{(n-1)n}{2n}+\frac{(n-1)n}{4}\right)$$

soit $\frac{\pi}{4}(n-1)(3n-2)$.

Mais un de ses arguments est aussi $\frac{\pi}{2}(c+2b+3d)$ et il vient donc $2b+c-d\equiv\frac{(n-1)(3n-2)}{2}$ (mod 4).

On est donc invité à calculer modulo 4. Si $n\equiv 1 \pmod 4$, alors $(n+1)/2$ est impair et $(n-1)/2$ est pair. Il vient donc $a+b\equiv 1 \pmod 2$ et $c+d\equiv 0 \pmod 2$. Puisque $-1\equiv 1 \pmod 2$, on en tire $a-b\equiv 1 \pmod 2$ et $c-d\equiv 0 \pmod 2$. Comme $(a-b)^2+(c-d)^2=1$, il vient $|a-b|=1$ et $c=d$, d'où $\{a,b\}=\left\{\frac{n-1}{4},\frac{n+3}{4}\right\}$ et $c=d=\frac{n-1}{4}$. Par conséquent $2b\equiv\frac{(n-1)(3n-2)}{2}$ (mod 4). Comme $n\equiv 1 \pmod 4$, $3n-2\equiv 1 \pmod 4$ et il vient $2b\equiv\frac{(n-1)}{2} \pmod 4$. Par conséquent $b=(n-1)/4$ et on a $\boxed{\text{si } n\equiv 1 \pmod 4,\ a=\frac{n+3}{4} \text{ et } b=c=d=\frac{n-1}{4}.}$

Si maintenant $n\equiv 3 \pmod 4$, il vient $a=b=\frac{n+1}{4}$ et $[c-d|=1$. On a alors $3n-2\equiv -1$ (mod 4) et $2b=\frac{n+1}{2}$, d'où $c-d\equiv -\frac{n-1}{2}-\frac{n+1}{2}\equiv -n\equiv 1 \pmod 4$. Il vient $c-d=1$ et donc $\boxed{\text{si } n\equiv 3 \pmod 4,\ a=b=c=\frac{n+1}{4} \text{ et } d=\frac{n-3}{4}.}$

V.6. Comme $\tau_n=((a-b)+i(c-d))\sqrt{n}$, il vient

$\boxed{\text{si } n\equiv 1 \pmod 4,\ \tau_n=\sqrt{n} \text{ et, si } n\equiv 3 \pmod 4,\ \tau_n=i\sqrt{n}.}$

PARTIE VI - Réciprocité quadratique

VI.1. On a vu en II.4 que les entiers d'un corps sont exactement ses éléments annulés par un polynôme unitaire à coefficients entiers relatifs. Comme $\mathbf{K}\subset\mathbf{L}$, il vient directement

$\boxed{\mathcal{O}_{\mathbf{L}}\cap\mathbf{K}=\mathcal{O}_{\mathbf{K}}.}$

VI.2. Puisque q est premier les coefficients binomiaux $\binom{q}{k}$ sont divisibles par q pour $1\leq k\leq q-1$, car alors q divise l'entier $k!\binom{q}{k}$ et est premier avec $k!$. En particulier, si x et y sont dans $\mathcal{O}_{\mathbf{L}}$, alors $(x+y)^q-x^q-y^q$ est une somme d'entiers multiples de q multipliés par un produit d'éléments de $\mathcal{O}_{\mathbf{L}}$ et appartient donc à $q\mathcal{O}_{\mathbf{L}}$ puisque $\mathcal{O}_{\mathbf{L}}$ est un anneau. Une récurrence immédiate montre qu'il en est de même pour une somme finie quelconque.

Puisque ζ^{x^2} est une racine de l'unité, elle appartient à $\mathcal{O}_{\mathbf{L}}$ et donc $\tau_p\in\mathcal{O}_{\mathbf{L}}$. Par définition $\tau_p\in\mathbf{K}$ et il vient $\tau_p\in\mathcal{O}_{\mathbf{K}}$. La remarque précédente, donne également

$$\tau_p^q-\sum_{x\in\mathbf{Z}/p\mathbf{Z}}\zeta^{qx^2}\in q\mathcal{O}_{\mathbf{L}}\ .$$

Si q est un carré modulo p (nécessairement non nul car q est premier à p), alors $u \mapsto qu$ est une bijection de $\mathbf{Z}/p\mathbf{Z}$ dans lui-même qui envoie 0 sur 0, un non-carré sur un non-carré et un carré non nul sur un carré non nul. Il en résulte

$$\sum_{x\in\mathbf{Z}/p\mathbf{Z}} \zeta^{qx^2} = \sum_{x\in\mathbf{Z}/p\mathbf{Z}} \zeta^{x^2} = \tau_p$$

et comme $\left(\frac{q}{p}\right) = 1$, $\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in \mathcal{O}_\mathbf{L}$.
Si q n'est pas un carré modulo p, $u \mapsto qu$ est une bijection de $\mathbf{Z}/p\mathbf{Z}$ dans lui-même qui envoie 0 sur 0, un non-carré sur un carré non nul et un carré non nul sur un non carré. Il vient

$$\sum_{x\in\mathbf{Z}/p\mathbf{Z}} \zeta^{qx^2} + \sum_{x\in\mathbf{Z}/p\mathbf{Z}} \zeta^{x^2} = 2\sum_{u\in\mathbf{Z}/n\mathbf{Z}} \zeta^{u} = 0$$

puisque chaque ζ^u est obtenu deux fois : une fois dans chaque somme si $u = 0$, deux fois dans la première somme si ce n'est pas un carré et deux fois dans la seconde si c'est un carré non nul. Comme $\left(\frac{q}{p}\right) = -1$, $\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in \mathcal{O}_\mathbf{L}$.
Or $\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in \mathbf{K}$ car $\tau_p \in \mathbf{K}$ et donc aussi après division par q. On conclut grâce à VI.1,

$$\boxed{\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in \mathcal{O}_\mathbf{K}.}$$

VI.3. On a $\mathbf{K} = \mathbf{Q}[\sqrt{p}]$ si $p \equiv 1 \pmod 4$ et $\mathbf{K} = \mathbf{Q}[\sqrt{-p}]$ sinon. Comme p est premier, il est sans carré de sorte qu'en posant $\omega_p = \dfrac{1+\sqrt{p}}{2}$ si $p \equiv 1 \pmod 4$ et $\omega_p = \dfrac{1+i\sqrt{p}}{2}$ sinon, d'après III.6, $\mathcal{O}_\mathbf{K} = \mathbf{Z} \oplus \mathbf{Z}\omega_p$.
On suppose $n\tau_p \in q\mathcal{O}_\mathbf{K}$. On dispose alors de a et b dans $\mathbf{Z}$ tels que $n\tau_p = q(a + b\omega_p)$. Il vient alors, si $p \equiv 1 \pmod 4$, $n\sqrt{p} = q\left(a + b\dfrac{1+\sqrt{p}}{2}\right)$ et donc, par unicité de l'écriture (d'après III.6), $\dfrac{b}{2} = -a$ et $n = -qa$.

Si $p \equiv 3 \pmod 4$, il vient $in\sqrt{p} = q\left(a + b\dfrac{1+i\sqrt{p}}{2}\right)$ et donc, toujours par unicité de l'écriture, $\dfrac{b}{2} = -a$ et $n = -qa$. Il en résulte $\boxed{q \mid n.}$

VI.4. D'après V.6, on a

$$\tau_p^{q-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}}$$

et donc, en posant $n = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)$, on a $n\tau_p \in q\mathcal{O}_\mathbf{K}$. On a donc $n \equiv 0 \pmod q$, d'après ce qui précède, i.e.

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod q$$

d'après I.2. Comme $q > 1$ et comme les extrêmes valent ± 1 tous les deux, ils sont égaux, i.e.

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

VI.5. Par construction, si φ existe, elle est unique. Soit alors l'application de $\mathbf{Z}^2$ dans $\mathbf{Z}/pq\mathbf{Z}$ donnée par $(x,y) \mapsto px + qy \pmod p q$. Alors le résultat ne dépend que de la classe de x modulo q et de celle de y modulo p. Par ailleurs, soit (x,y) et (x',y') deux couples d'entiers tels que $px+qy \equiv px'+qy' \pmod{pq}$. Alors, en prenant les classes modulo p, il vient $qy \equiv qy' \pmod p$ et, puisque p et q sont premiers entre eux, q est inversible modulo p et donc $y \equiv y' \pmod p$. Mutatis mutandis il vient $x \equiv x' \pmod q$ et donc l'application ainsi construite est injective. Par cardinalité elle est donc bijective et ainsi $\boxed{\text{il est une unique telle bijection.}}$

VI.6. On note $\zeta = \exp(\frac{2i\pi}{pq})$, $\zeta_p = \zeta^q = \exp(\frac{2i\pi}{p})$ et $\zeta_q = \zeta^p = \exp(\frac{2i\pi}{q})$. Il vient, en utilisant la bijection précédente,

$$\tau_{pq} = \sum_{x\in\mathbf{Z}/q\mathbf{Z}} \sum_{y\in\mathbf{Z}/p\mathbf{Z}} \zeta^{(xp+yq)^2} = \sum_{x\in\mathbf{Z}/q\mathbf{Z}} \sum_{y\in\mathbf{Z}/p\mathbf{Z}} \zeta^{x^2p^2+y^2q^2+2xypq} = \sum_{x\in\mathbf{Z}/q\mathbf{Z}} \sum_{y\in\mathbf{Z}/p\mathbf{Z}} \zeta^{x^2p^2+y^2q^2}$$

et donc

$$\tau_{pq} = \left(\sum_{x\in\mathbf{Z}/q\mathbf{Z}} \zeta^{x^2p^2}\right)\left(\sum_{y\in\mathbf{Z}/p\mathbf{Z}} \zeta^{y^2q^2}\right) = \left(\sum_{x\in\mathbf{Z}/q\mathbf{Z}} \zeta_q^{px^2}\right)\left(\sum_{y\in\mathbf{Z}/p\mathbf{Z}} \zeta_p^{qy^2}\right) .$$

D'après les calculs effectués en VI.2, on en déduit $\boxed{\tau_{pq} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\tau_p\tau_q.}$

VI.7. D'après V.6, on a $\tau_{pq}/(\tau_p\tau_q) = 1$ si $p \equiv 1 \pmod 4$ ou $q \equiv 1 \pmod 4$, et le quotient est égal à -1 sinon. On en déduit directement $\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.}$

VI.8. D'après III.6, on a $\mathcal{O}_\mathbf{K} = \mathbf{Z}[i]$ car $-1 \equiv 3 \pmod 4$.
On a encore, d'après la formule du binôme, $(1+i)^q - 1 - i^q \in q\mathbf{Z}[i]$. Comme

$$(1+i)^q = (2i)^{\frac{q-1}{2}}(1+i) \quad \text{et} \quad 2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \pmod q$$

il vient

$$\left(\frac{2}{q}\right)(1+i) - i^{-\frac{q-1}{2}}(1+i^q) \in q\mathbf{Z}[i] .$$

Or, ces deux quantités ont même module, à savoir $\sqrt{2}$ puisque q est impair. Le module de leur différence est donc au plus $2\sqrt{2}$ d'après l'inégalité triangulaire. Comme les éléments non nuls de $q\mathbf{Z}[i]$ sont de module au moins égal à q et qu'on a $2\sqrt{2} < 3 \leq q$, il vient $\left(\frac{2}{q}\right) = i^{-\frac{q-1}{2}}\frac{1+i^q}{1+i}$, soit $\boxed{\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}.}$

VI.9. Le théorème admis est le grand théorème de Dirichlet. On décompose n en facteurs premiers sous la forme $n = n = (-1)^{\alpha_0}2^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ où les p_i sont des nombres premiers impairs distincts et les α_i des entiers naturels éventuellement nuls. On pose $m = 8p_2\cdots p_k$.

Pour p premier impair, on se donne x_p qui n'est pas un carré modulo p, ce qui est licite puisque l'ensemble des carrés de $\mathbf{Z}/p\mathbf{Z}$ est de cardinal $(p+1)/2$. On note $x_i = x_{p_i}$.
D'après le théorème chinois, on a un isomorphisme d'anneaux

$$\mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/p_2\mathbf{Z} \times \cdots \mathbf{Z}/p_k\mathbf{Z}$$

et on peut choisir un antécédent de y_i de $(1, \cdots, x_i, \cdots, 1)$, pour $2 \leq i \leq k$, un antécédent y_1 de $(5, 1, \cdots, 1)$ et y_0 un antécédent de $(3, 1, \cdots, 1)$. Par construction y_0, …, y_k sont premiers à m puisque premiers à 2 et à chacun des p_j.
On dispose donc, d'après le théorème admis, d'une infinité de nombres premiers congrus à y_i modulo m, et ce pour tout i dans $[\![0; k]\!]$. En particulier il en existe hors de S et donc on dispose de q_i tel que $q_i \notin S$, q_i premier et $q_i \equiv y_i \pmod{m}$. D'après le choix effectué, si $i \geq 1$, $y_i \equiv 1 \pmod 4$ et donc $q_i \equiv 1 \pmod 4$ (puisque $4 \mid m$). Par réciprocité quadratique, il vient alors

$$\left(\frac{p_i}{q_i}\right) = \left(\frac{q_i}{p_i}\right) = \left(\frac{y_i}{p_i}\right) = \left(\frac{x_i}{p_i}\right) = -1\,,$$

tandis que, pour $j \neq i$ et $j \geq 1$, $\left(\frac{p_j}{q_i}\right) = \left(\frac{q_i}{p_j}\right) = 1$. Enfin, puisque $q_i \equiv 1 \pmod 4$, -1 est un carré modulo 4 et il en résulte que n est, modulo q_i, un carré multiplié par $p_i^{\alpha_i}$. Comme p_i n'est pas un carré modulo q_i, α_i est pair. Il en résulte que, au signe près, n est un carré. Comme q est un carré modulo q_0, α_0 est également pair et donc $\boxed{n \text{ est un carré.}}$