FAIRE EN PRIORITE LES PARTIES 2 et 5

UL 111

SESSION 2001
Filière MP

MATHÉMATIQUES

(Épreuve commune aux ENS : Ulm et Lyon)

DURÉE : 6 heures

La calculatrice n'est pas autorisée

Énoncé saisi par M. Quercia (michel.quercia@prepas.org) d'après le texte original.

Avertissement

La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite en particulier le candidat à produire des raisonnements précis et concis. Le candidat peut 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 **1** n'est utilisée que dans la partie **6**. Les parties **4** et **5** sont mutuellement indépendantes ainsi qu'essentiellement du reste du problème : seules les formules équivalentes obtenues dans les questions **4.5** et **5.6** sont utilisées dans la partie **6**.

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 $\zeta = \exp(\frac{2i\pi}{n})$, on notera τ_n la somme

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

1. Préliminaires

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

1.1. 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 $x, y/x$, $x \in (\mathbb{Z}/p\mathbb{Z})^*$].

1.2. En déduire les égalités

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

2. Généralités

2.1. 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 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 $\mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$ l'ensemble des combinaisons linéaires à coefficients entiers des v_i, $i = 1, \ldots, n$.

2.2. 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

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

[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.*

2.3. Montrer que le composé et la somme de deux endomorphismes entiers f, g de V qui commutent (*ie* 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 **2.2** 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 K un corps de nombres, muni de sa structure de $\mathbb{Q}$-espace vectoriel de dimension finie. On dira que $x \in K$ est *entier* si l'endomorphisme de multiplication

$$m_x : \begin{cases} K & \longrightarrow & K \\ y & \longmapsto & xy \end{cases}$$

est entier. On note $\mathcal{O}_K$ l'ensemble des éléments de K qui sont entiers, qui est donc un sous-anneau de K d'après la question **2.3.**

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

3. 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

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

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

3.2. Soit $D' \in \mathbb{Q}^*$. Montrer que $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$ si et seulement si $D/D' \in \mathbb{Q}^2$.

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

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

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

3.5. 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

$$\omega = \begin{cases} (1+\sqrt{d})/2 & \text{si } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{sinon.} \end{cases}$$

3.6. Montrer que l'application

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

est un isomorphisme de groupes abéliens.

4. Un calcul analytique de τ_n

On se donne n entier $\geqslant 1$. Pour $k = 0, \ldots, n-1$, on note f_k la fonction

$$f_k : \begin{cases} [0,1] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & \exp\left(\frac{2i\pi(t+k)^2}{n}\right) \end{cases}$$

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

4.1. Montrer que la suite de terme général

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

converge vers τ_n.

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

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

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

4.4. Comparer I_n et I_1.

4.5. Montrer la formule

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

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

5. Un calcul algébrique de τ_n

Soit n un entier impair > 1 et ζ le complexe $\zeta = \exp(\frac{2i\pi}{n})$.
Soit V le $\mathbb{C}$-espace vectoriel de dimension n 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

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

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

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

5.2. Diagonaliser $\varphi \circ \varphi$.

On remarque que

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

est la trace de φ.

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

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

5.4. Montrer les égalités $a + b = (n+1)/2$ et $c + d = (n-1)/2$ ainsi que $(a-b)^2 + (c-d)^2 = 1$.

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

5.6. 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 **4.5**).

6. Réciprocité quadratique

On considère deux nombres premiers impairs distincts, p, q. On note L le corps de nombres $\mathbb{Q}[\exp(\frac{2i\pi}{p})]$ 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

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

Première méthode

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

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

6.3. 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 **3.6**].

6.4. Montrer l'égalité (1).

Seconde méthode

6.5. Montrer qu'il existe une unique bijection

$$\phi : \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/pq\mathbb{Z}$$

telle que

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

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

6.6. Montrer la formule

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

6.7. En déduire l'égalité (1) [Utiliser les formules obtenues aux questions **4.5** ou **5.6**].

6.8. 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 **6.2**].

Une application

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

6.9. 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 $\mathbb{Z}/\ell\mathbb{Z}$. Montrer que n est le carré d'un entier.