UL 111

SESSION 2001
Filière MP

MATHÉMATIQUES

(Épreuve commune aux ENS : Ulm et Lyon)

Corrigé de M. Quercia (michel.quercia@prepas.org)

1. Préliminaires

1.1. Soit π le produit à calculer. On a $x \neq y/x$ si et seulement si $x^2 \neq y$. Donc si y n'est pas un carré, les $p-1$ facteurs du produit se regroupent en $(p-1)/2$ couples $x \times (y/x) = y$ et $\pi = y^{(p-1)/2}$.

Par contre, si y est un carré, $y = a^2 = (-a)^2$ et seuls $a, -a$ sont racines carrées de y car pour $x \neq \pm a$ on a $x^2 - y = x^2 - a^2 = (x-a)(x+a) \neq 0$. De plus $a \neq -a$ car a est non nul et p est impair. Donc les $p-3$ facteurs de π autres que a et $-a$ se regroupent deux par deux en couples de produit y et $\pi = y^{(p-3)/2} a(-a) = -y^{(p-1)/2}$.

1.2. On sait que $y^{(p-1)/2} = \mp\pi$ selon que y est un carré ou non, et $y = 1$ est un carré donc $1 = 1^{(p-1)/2} = -\pi$ d'où le résultat.

2. Généralités

2.1. S'il existe $P \in \mathbb{Q}[X]$ unitaire annulant ζ : $\zeta^n + a_{n-1}\zeta^{n-1} + \ldots + a_0\zeta^0 = 0$ alors par récurrence sur $p \in \mathbb{N}$, ζ^p est combinaison linéaire à coefficients rationnels de $\zeta^0, \ldots, \zeta^{n-1}$ donc $\mathbb{Q}[\zeta] = \text{vect}(\zeta^0, \ldots, \zeta^{n-1})$ est une $\mathbb{Q}$-algèbre de dimension finie. Il reste à prouver que tout élément x non nul de $\mathbb{Q}[\zeta]$ admet un inverse multiplicatif dans $\mathbb{Q}[\zeta]$. Or l'application $y \longmapsto xy$ est un endomorphisme de $\mathbb{Q}[\zeta]$, injectif donc surjectif, et par conséquent il existe $y \in \mathbb{Q}[\zeta]$ tel que $xy = 1$ c'est-à-dire $x^{-1} = y \in \mathbb{Q}[\zeta]$. Ainsi $\mathbb{Q}[\zeta]$ est un sous-corps de $\mathbb{C}$ de dimension finie sur $\mathbb{Q}$.

Réciproquement, soit $\zeta \neq 0$ tel que $\mathbb{Q}[\zeta]$ est un corps de nombres : alors $\zeta^{-1} \in \mathbb{Q}[\zeta]$ donc il existe $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{Q}$ tels que $\zeta^{-1} = a_0\zeta^0 + \ldots + a_n\zeta^n$. Quitte à diminuer n on peut supposer $a_n \neq 0$ car $\zeta^{-1} \neq 0$, d'où $P = X^{n+1} + \frac{a_{n-1}}{a_n}X^n + \ldots + \frac{a_0}{a_n}X - \frac{1}{a_n}$ est un polynôme annulateur de ζ, unitaire et à coefficients rationnels. Pour $\zeta = 0$ le polynôme $P = X$ est un annulateur unitaire à coefficients rationnels (et $\mathbb{Q}[0] = \mathbb{Q}$ est un corps de nombres).

2.2. Supposons que f admet un annulateur unitaire à coefficients entiers, soit : $f^k = a_0 f^0 + \ldots + a_{k-1} f^{k-1}$ avec $a_i \in \mathbb{Z}$. Soit $(u_1, \ldots, u_p)$ une famille génératrice de V, et $u_{i,j} = f^j(u_i)$ pour $i \in [\![1, p]\!]$ et $j \in [\![0, k[\![$. Alors $W = \sum_{i=1}^{p} \sum_{j=0}^{k-1} \mathbb{Z} u_{i,j}$ est stable par f et la famille $(u_{i,j})_{i \leqslant p,\ j<k}$ engendre V car elle contient $(u_1, \ldots, u_p)$.

Réciproquement, supposons qu'il existe un sous-groupe $\mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$ stable par f et tel que $(v_1, \ldots, v_n)$ engendre V. On note A la matrice définie dans l'indication et χ_A son polynôme caractéristique. On a par récurrence sur k :

$$A^k \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} f^k(v_1) \\ \vdots \\ f^k(v_n) \end{pmatrix},$$

et $\chi_A(A) = 0$ donc $\chi_A(f)(v_i) = 0$ pour tout i ce qui implique que $\chi_A(f) = 0$ car $(v_1, \ldots, v_n)$ est génératrice. $(-1)^n \chi_A$ est ainsi un polynôme unitaire, annulant f, et à coefficients entiers car A est à coefficients entiers.

2.3. Soient f, g entiers commutant. On choisit une famille $(v_1, \ldots, v_n)$ adaptée à f (c'est-à-dire $(v_1, \ldots, v_n)$ engendre vectoriellement V et le sous-groupe engendré, W, est stable par f). Soit par ailleurs $g^p = a_0 g^0 + \ldots + a_{p-1} g^{p-1}$ une relation de dépendance entre les puissances de g à coefficients entiers. On note $v_{i,j} = g^j(v_i)$ pour $i \in [\![1, n]\!]$ et $j \in [\![0, p[\![$ et on considère la famille (vectoriellement génératrice) $(v_{i,j})_{i \leqslant n,\ j<p}$. Le sous-groupe qu'elle engendre est :

$$X = \sum_{j=0}^{p-1} \sum_{i=1}^{n} \mathbb{Z} g^j(v_i) = \sum_{j=0}^{p-1} g^j(W).$$

W est stable par f et f et g commutent donc X est aussi stable par f. Par ailleurs,

$$g(X) = \sum_{j=1}^{p-1} g^j(W) + g^p(W) \subset \sum_{j=0}^{p-1} g^j(W) = X$$

car g^p est combinaison linéaire à coefficients entiers de $g^0, \ldots, g^{p-1}$. La famille $(v_{i,j})_{i\leqslant n,\ j<p}$ est donc adaptée à la fois à f et à g. On alors $(f+g)(X) \subset X$ et $(f\circ g)(X) \subset X$ ce qui prouve que $f+g$ et $f\circ g$ sont entiers (de même que tout endomorphisme de l'anneau engendré par f et g).

Contre-exemple avec $f\circ g \neq g\circ f$: Soient $f, g \in \mathcal{L}(\mathbb{Q}^2)$ de matrices $F = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ et $G = \frac{1}{2}\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)$ dans la base canonique de $\mathbb{Q}^2$. f et g sont entiers car $F^2 = F$ et $G^2 = G$. On montre que $h = f\circ g$ de matrice $H = \frac{1}{2}\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right)$ n'est pas entier : $H^2 = \frac{1}{2}H$ donc s'il existait une relation : $H^n = a_0H^0 + \ldots + a_{n-1}H^{n-1}$ avec $a_i \in \mathbb{Z}$ alors on aurait $\frac{1}{2^{n-1}}H = \frac{\text{entier}}{2^{n-2}}H + a_0I$ ce qui est absurde. On peut montrer de même que $k = f+g$ n'est pas entier à partir de la relation : $(k-\mathrm{id})^2 = \frac{1}{2}\mathrm{id}$.

2.4. Soit $x \in K$. Pour tout polynôme $P \in \mathbb{Z}[X]$ on a $P(m_x) = m_{P(x)}$ et $P(m_x) = 0 \iff m_{P(x)} = 0 \iff P(x) = 0$. Donc x est entier au sens de l'énoncé si et seulement s'il existe une relation $x^n = a_0x^0 + \ldots + a_{n-1}x^{n-1}$ avec $a_i \in \mathbb{Z}$. En particulier si $x \in \mathbb{Z}\cap K = \mathbb{Z}$ alors $x^1 = x$ donc x est entier. Ceci prouve $\mathbb{Z} \subset \mathcal{O}_K \cap \mathbb{Q}$.

Réciproquement, considérons $x = p/q \in \mathcal{O}_K \cap \mathbb{Q}$ avec $p, q \in \mathbb{Z}$ premiers entre eux et une relation algébrique : $x^n = a_0x^0 + \ldots + a_{n-1}x^{n-1}$ avec $a_i \in \mathbb{Z}$. On a donc $p^n/q^n = \alpha/q^{n-1}$ avec $\alpha \in \mathbb{Z}$ d'où $q \mid p^n$. Mais $q\wedge p = 1$ donc $q = \pm 1$ et $x \in \mathbb{Z}$.

3. Entiers des corps quadratiques

3.1. Dans la définition de σ il est sous-entendu que a, b désignent des rationnels. On vérifie sans peine que σ ainsi défini est bien un isomorphisme de corps. Considérons un isomorphisme quelconque f du corps $\mathbb{Q}[\sqrt{D}]$: $f(1) = 1$ par définition d'un morphisme de corps, et l'ensemble des $x \in K$ tels que $f(x) = x$ est un sous-corps de K donc $f(a) = a$ pour tout $a \in \mathbb{Q}$ et f est $\mathbb{Q}$-linéaire. On a aussi $f(\sqrt{D})^2 = f(\sqrt{D}^2) = f(D) = D$ donc $f(\sqrt{D}) = \pm\sqrt{D}$. Ainsi f coïncide avec id ou avec σ sur la base $(1, \sqrt{D})$ et, par $\mathbb{Q}$-linéarité, $f = \mathrm{id}$ ou $f = \sigma$.

3.2. Si $D/D' \in \mathbb{Q}^2$ (c'est-à-dire $D/D' = t^2$ avec $t \in \mathbb{Q}$) alors D' est non carré, $\sqrt{D'} = \pm(\sqrt{D})/t \in \mathbb{Q}[\sqrt{D}]$ et $\sqrt{D} = \pm t\sqrt{D'} \in \mathbb{Q}[\sqrt{D'}]$ d'où $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$.

Si D' est non carré et $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}] = K$ alors K admet trois isomorphismes de corps : id, σ et σ' associé au changement de signe de $\sqrt{D'}$. D'après la question précédente on a $\sigma = \sigma'$ donc $\sigma(\sqrt{D'}) = -\sqrt{D'}$ ce qui implique $\sqrt{D'} = b\sqrt{D}$ avec $b \in \mathbb{Q}$ d'où $D/D' = 1/b^2 \in \mathbb{Q}^2$.

3.3. Soit $D = \pm p_1^{\alpha_1}\ldots p_n^{\alpha_n}$ une décomposition de D en facteurs premiers ($p_i \in \mathbb{N}$, $p_1, \ldots, p_n$ premiers distincts, $\alpha_i \in \mathbb{Z}$). On pose $\beta_i = \alpha_i \bmod 2 \in \{0, 1\}$ et $d = \pm p_1^{\beta_1}\ldots p_n^{\beta_n} \in \mathbb{Z}$. Alors d est sans facteurs carrés et D/d est un carré par construction donc $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{d}]$.

Unicité de d : soient $d, d' \in \mathbb{Z}$ sans facteurs carrés tels que $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$: on a $d/d' \in \mathbb{Q}^2$ soit $d/d' = p^2/q^2$ avec p, q entiers premiers entre eux, et $p^2d' = q^2d$. Comme p^2 est premier à q^2 on en déduit $p^2 \mid d$, mais d est sans facteur carré donc $p^2 = 1$ et de même $q^2 = 1$ d'où finalement $d = d'$.

3.4. Soit $(1, x)$ une base de K sur $\mathbb{Q}$: il existe $\alpha, \beta \in \mathbb{Q}$ tels que $x^2 = \alpha + \beta x$ soit $(x-\beta/2)^2 = \alpha + \beta^2/4 = D$. Si D est le carré d'un rationnel, $D = r^2$, alors on obtient $x - \beta/2 = \pm r$ donc $x \in \mathbb{Q}$ ce qui est absurde ($(1, x)$ est $\mathbb{Q}$-libre)). Donc D est non carré et $\sqrt{D} = \pm(x-\beta/2) \in K$ d'où $\mathbb{Q}[\sqrt{D}] \subset K$ puis $\mathbb{Q}[\sqrt{D}] = K$ par comparaison des dimensions.

3.5. Si $x \in \mathcal{O}_K$ alors $x \in K$ et x annule un polynôme $P \in \mathbb{Z}[X]$ unitaire. Comme P est à coefficients entiers on a $P(\sigma(x)) = \sigma(P(x)) = 0$ donc $\sigma(x) \in \mathcal{O}_K$. $\mathcal{O}_K$ est un anneau donc $u = x + \sigma(x)$ et $v = x\sigma(x)$ appartiennent aussi à $\mathcal{O}_K$ et u et v sont invariants par σ car $\sigma^2 = \mathrm{id}$ donc $u, v \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Réciproquement, soit $x \in K$ tel que $u = x + \sigma(x)$ et $v = x\sigma(x)$ soient entiers. Alors x et $\sigma(x)$ sont les racines du polynôme $X^2 - uX + v$ donc $x \in \mathcal{O}_K$.

3.6. Le caractère morphisme et l'injectivité sont évidents. Il reste à prouver que $\mathcal{O}_K$ est le groupe engendré par 1 et ω ; notons H ce groupe.

Si $d \equiv 1 \pmod 4$ alors $\omega^2 = \dfrac{1+d}{4} + \dfrac{\sqrt{d}}{2} = \dfrac{d-1}{4} + \omega$ et $\dfrac{d-1}{4} \in \mathbb{Z}$ donc $\omega \in \mathcal{O}_K$. Si $d \not\equiv 1 \pmod 4$ alors $\omega^2 = d$ donc là aussi $\omega \in \mathcal{O}_K$. Dans les deux cas on conclut $H \subset \mathcal{O}_K$.

Réciproquement, Soit $x = a + b\sqrt{d} \in \mathcal{O}_K$ avec $a, b \in \mathbb{Q}$. On a $x + \sigma(x) = 2a \in \mathbb{Z}$, soit $a = p/2$ avec $p \in \mathbb{Z}$ et $x\sigma(x) = a^2 - db^2 = q \in \mathbb{Z}$ donc $4db^2 = p^2 - 4q$. Écrivons $2b = u/v$ avec $u, v \in \mathbb{Z}$ premiers entre eux et $v > 0$: $du^2 = v^2(p^2 - 4q)$ donc v^2 divise du^2 et $u^2 \wedge v^2 = 1$, d est sans facteur carré d'où $v = 1$, $b = u/2$ et $du^2 \equiv p^2 \pmod 4$.

Si $d \equiv 1 \pmod 4$ on obtient $u^2 \equiv p^2 \pmod 4$ donc u et p ont même parité, $x = a + b\sqrt{d} = \dfrac{p-u}{2} + u\omega \in H$.

Si $d \equiv 2 \pmod 4$ on obtient p pair, puis u pair car $4 \not| d$ donc $x = \dfrac{p}{2} + \dfrac{u}{2}\omega \in H$.

Si $d \equiv 3 \pmod 4$ et p est impair alors $p^2 \equiv 1 \pmod 4$ ce qui n'est pas le cas de du^2 quelque soit la parité de u, ce cas est impossible.

Si $d \equiv 3 \pmod 4$ et p est pair alors u est aussi pair et $x = \dfrac{p}{2} + \dfrac{u}{2}\omega \in H$.

Le cas $d \equiv 0 \pmod 4$ est impossible, d est sans facteur carré.

Dans tous les cas possibles on a obtenu $x \in H$ donc $\mathcal{O}_K \subset H$ ce qui achève la démonstration.

4. Un calcul analytique de τ_n

4.1. f est de classe $\mathcal{C}^1$, $f(0) = f(1) = \tau_n$ (car $x \longmapsto x+1$ est une permutation de $\mathbb{Z}/n\mathbb{Z}$) donc la fonction g, prolongée de f à $\mathbb{R}$ par 1-périodicité, est continue de classe $\mathcal{C}^1$ par morceaux, sa série de Fourier S_g converge normalement vers g sur $\mathbb{R}$. En écrivant $S_g(0) = g(0) = \tau_m$ on obtient la convergence demandée.

4.2. $$\int_{t=-x}^{x} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t = \Big[n\frac{\exp(2i\pi t^2/n)-1}{4i\pi t}\Big]_{t=-x}^{x} + n\int_{t=-x}^{x} \frac{\exp(2i\pi t^2/n)-1}{4i\pi t^2}\,\mathrm{d}t$$
$$\xrightarrow[x\to+\infty]{} n\int_{t=-\infty}^{+\infty} \frac{\exp(2i\pi t^2/n)-1}{4i\pi t^2}\,\mathrm{d}t = I_n \text{ (intégrale absolument convergente).}$$

4.4. Par changement de variable $t = u\sqrt{n}$ on obtient $I_n = I_1\sqrt{n}$.

4.5.
$$\begin{aligned}
u_k &= \sum_{m=-k}^{k}\sum_{\ell=0}^{n-1}\int_{t=0}^{1} \exp\Big(\frac{2i\pi(t+\ell)^2}{n}\Big)\exp(-2i\pi mt)\,\mathrm{d}t \\
&= \sum_{m=-k}^{k}\sum_{\ell=0}^{n-1}\int_{t=0}^{1} \exp\Big(\frac{2i\pi(t+\ell)^2}{n}\Big)\exp(-2i\pi m(t+\ell))\,\mathrm{d}t \\
&= \sum_{m=-k}^{k}\int_{t=0}^{n} \exp\Big(\frac{2i\pi t^2}{n}\Big)\exp(-2i\pi mt)\,\mathrm{d}t \\
&= \sum_{m=-k}^{k}\int_{t=0}^{n} \exp\Big(\frac{2i\pi(t^2-mnt)}{n}\Big)\,\mathrm{d}t \\
&= \sum_{m=-k}^{k}\int_{t=0}^{n} \exp\Big(\frac{2i\pi(t-mn/2)^2 - 2i\pi m^2n^2/4}{n}\Big)\,\mathrm{d}t \\
&= \sum_{m=-k}^{k}\int_{t=0}^{n} (-i)^{m^2n}\exp\Big(\frac{2i\pi(t-mn/2)^2}{n}\Big)\,\mathrm{d}t \\
&= \sum_{m=-k}^{k}\int_{t=-mn/2}^{-(m-2)n/2} (-i)^{m^2n}\exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t.
\end{aligned}$$

Pour m pair : $(-i)^{m^2 n} = 1$ et pour m impair : $(-i)^{m^2 n} = (-i)^n$ car $m^2 \equiv 1 \pmod 4$. Prenons k pair, $k = 2p$ et séparons la somme en deux selon la parité de m. Il vient :

$$\begin{aligned}
u_{2p} &= \sum_{m=-2p}^{2p} \int_{t=-mn/2}^{-(m-2)n/2} (-i)^{m^2 n} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t \\
&= \sum_{m=-p}^{p} \int_{t=-2mn/2}^{-(2m-2)n/2} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t + \sum_{m=-p+1}^{p-1} \int_{t=-(2m+1)n/2}^{-(2m-1)n/2} (-i)^n \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t \\
&= \int_{t=-pn}^{(p+1)n} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t + \int_{t=-(2p-1)n/2}^{(2p-1)n/2} (-i)^n \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t \\
&= \int_{t=pn}^{(p+1)n} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t + \int_{t=-pn}^{pn} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t + \int_{t=-(2p-1)n/2}^{(2p-1)n/2} (-i)^n \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t \\
&\xrightarrow[p\to\infty]{} (1 + (-i)^n) I_n
\end{aligned}$$

car $\displaystyle\int_{t=pn}^{(p+1)n} \exp\Big(\frac{2i\pi t^2}{n}\Big)\,\mathrm{d}t \xrightarrow[p\to\infty]{} 0$ par adaptation de la démonstration faite en **4.2.**

On a donc $\tau_n = (1 + (-i)^n) I_n = (1 + i^{-n})\sqrt{n}\, I_1 = \dfrac{1 + i^{-n}}{1 + i^{-1}} \sqrt{n}\, \tau_1 = \dfrac{1 + i^{-n}}{1 + i^{-1}} \sqrt{n}$.

4.6. On note $K = \mathbb{Q}[\sqrt{n}]$ où n est un entier sans facteur carré. La question précédente montre que $\sqrt{n} \in \mathbb{Q}[i, \zeta]$ avec $\zeta = \exp(\frac{2i\pi}{n})$ donc $K \subset \mathbb{Q}[i, \zeta] \subset \mathbb{Q}[\xi]$ avec $\xi = \exp(\frac{2i\pi}{4n})$.

5. Un calcul algébrique de τ_n

5.1. $\varphi \circ \varphi(f)(x) = \displaystyle\sum_{y \in \mathbb{Z}/n\mathbb{Z}} \varphi(f)(y) \zeta^{xy} = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \sum_{z \in \mathbb{Z}/n\mathbb{Z}} f(z) \zeta^{yz} \zeta^{xy} = \sum_{z \in \mathbb{Z}/n\mathbb{Z}} \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(z) \zeta^{y(x+z)}$.

Si $x + z \neq 0$ (dans $\mathbb{Z}/n\mathbb{Z}$) alors $\zeta^{x+z} \neq 1$ et $\displaystyle\sum_{y \in \mathbb{Z}/n\mathbb{Z}} \zeta^{y(x+z)} = \frac{\zeta^{n(x+z)} - 1}{\zeta^{x+z} - 1} = 0$.

Si $x + z = 0$ alors $\displaystyle\sum_{y \in \mathbb{Z}/n\mathbb{Z}} \zeta^{y(x+z)} = n$ d'où le résultat.

5.2. Soient P, I les sous-espaces de V constitués des fonctions paires, impaires.
Alors $P \oplus I = V$ et $\varphi \circ \varphi = n\mathrm{id}_P \oplus (-n)\mathrm{id}_I$.

trace de φ : V admet pour base la famille $(\delta_x)_{x \in \mathbb{Z}/n\mathbb{Z}}$ où $\delta_x(y) = \delta_{x,y}$ (symbole de Kronecker), et la composante sur δ_x de $\varphi(\delta_x)$ est ζ^{x^2} d'où la relation $\mathrm{tr}(\varphi) = \tau_n$.

5.3.

$$\begin{aligned}
|\tau_n|^2 = \tau_n \overline{\tau_n} &= \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \zeta^{x^2 - y^2} \\
&= \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \zeta^{(x-y)(x+y)} \\
&\text{(changement d'indice } z = x + y) \\
&= \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \sum_{z \in \mathbb{Z}/n\mathbb{Z}} \zeta^{(2x-z)z} \\
&= \sum_{z \in \mathbb{Z}/n\mathbb{Z}} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \zeta^{(2x-z)z} \\
&= \sum_{z \in \mathbb{Z}/n\mathbb{Z}} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \zeta^{2xz} \zeta^{-z^2} \\
&= \sum_{z \in \mathbb{Z}/n\mathbb{Z}} n \delta_{z,0} \zeta^{-z^2} \\
&= n.
\end{aligned}$$

5.4. D'après **5.1** on a $\varphi^4 = n^2\mathrm{id}_V$ donc φ annule le polynôme scindé à racines simples $X^4 - n^2$ ce qui prouve que φ est diagonalisable et $\mathrm{spec}(\varphi) \subset \{\pm\sqrt{n}, \pm i\sqrt{n}\}$.

Notons $V_{\sqrt{n}}, V_{-\sqrt{n}}, V_{i\sqrt{n}}, V_{-i\sqrt{n}}$ les sous-espaces propres correspondant, de dimensions a, b, c, d.

On a $V_{\sqrt{n}} \oplus V_{-\sqrt{n}} \subset \mathrm{Ker}(\varphi^2 - n\mathrm{id}) = P$ d'où $a + b \leqslant \dim P = \dfrac{n+1}{2}$ et de même $c + d \leqslant \dim I = \dfrac{n-1}{2}$. Mais $a + b + c + d = n = \dfrac{n+1}{2} + \dfrac{n-1}{2}$ donc les inégalités précédentes sont des égalités.

Enfin $\tau_n = \mathrm{tr}(\varphi) = ((a-b) + i(c-d))\sqrt{n}$ et $|\tau_n| = \sqrt{n}$ soit $(a-b)^2 + (c-d)^2 = 1$.

5.5. Soit $\mathcal{B} = (\delta_0, \ldots, \delta_{n-1})$ la base canonique de V. La matrice de φ dans cette base est $M = (\zeta^{(k-1)(\ell-1)})$, matrice de Vandermonde associée à la famille $(1, \zeta, \ldots, \zeta^{n-1})$. Donc, en notant $\xi = \exp(\frac{i\pi}{n})$:

$$\begin{aligned}
\det(\varphi) &= \prod_{k=1}^{n-1}\prod_{\ell=0}^{k-1}(\zeta^k - \zeta^\ell) \\
&= \prod_{k=1}^{n-1}\prod_{\ell=0}^{k-1}\xi^{k+\ell}(\xi^{k-\ell} - \xi^{\ell-k}) \\
&= \prod_{k=1}^{n-1}\prod_{\ell=0}^{k-1}\xi^{k+\ell}(2i\sin(k-\ell)\tfrac{\pi}{n}) \\
&= \prod_{k=1}^{n-1}\xi^{k(3k-1)/2}(2i)^k\prod_{\ell=0}^{k-1}\sin(k-\ell)\tfrac{\pi}{n} \\
&= \xi^{n(n-1)^2/2}(2i)^{n(n-1)/2}\prod_{k=1}^{n-1}\prod_{\ell=0}^{k-1}\sin(k-\ell)\tfrac{\pi}{n}.
\end{aligned}$$

Comme les sinus sont tous positifs, on en déduit $\arg(\det\varphi) \equiv \frac{\pi}{4}(n-1)(3n-2) \pmod{2\pi}$.

Mais on a aussi $\det(\varphi) = \sqrt{n}^n(-1)^b i^c(-i)^d = \sqrt{n}^n i^{2b+c-d}$ d'où $2b + c - d \equiv \dfrac{(n-1)(3n-2)}{2} \pmod 4$.

D'après la relation $(a-b)^2 + (c-d)^2 = 1$ on a quatre cas à considérer :

1) $a = b$, $c - d = 1$: alors $a = b = c = \dfrac{n+1}{4}$, $d = \dfrac{n-3}{4}$, $n = 4d+3$, $2b+c-d = 2d+3 \equiv (2d+1)(12d+7) \pmod 4$ ce qui est vérifié.
2) $a = b$, $d - c = 1$: alors $a = b = d = \dfrac{n+1}{4}$, $c = \dfrac{n-3}{4}$, $n = 4c+3$, $2b+c-d = 2c+1 \equiv (2c+1)(12c+7) \pmod 4$ ce qui est impossible.
3) $a - b = 1$, $c = d$: alors $a = \dfrac{n+3}{4}$, $b = c = d = \dfrac{n-1}{4}$. $n = 4d+1$, $2b + c - d = 2d \equiv 2d(12d+1) \pmod 4$, ce qui est vérifié.
4) $b - a = 1$, $c = d$: alors $b = \dfrac{n+3}{4}$, $a = c = d = \dfrac{n-1}{4}$. $n = 4d+1$, $2b + c - d = 2d + 2 \equiv 2d(12d+1) \pmod 4$, ce qui est impossible.

En conclusion, si $n \equiv 3 \pmod 4$ alors $a = b = c = \dfrac{n+1}{4}$, $d = \dfrac{n-3}{4}$;
si $n \equiv 1 \pmod 4$ alors $a = \dfrac{n+3}{4}$, $b = c = d = \dfrac{n-1}{4}$.

5.6. On a $\tau_n = ((a-b) + i(c-d))\sqrt{n}$, avec $\begin{cases} n \equiv 1 \pmod 4 \Longrightarrow a - b = 1,\ c - d = 0 \\ n \equiv 3 \pmod 4 \Longrightarrow a - b = 0,\ c - d = 1. \end{cases}$

6. Réciprocité quadratique

6.1. Soit $\mathcal{O}$ l'ensemble de tous les complexes racines d'un polynôme unitaire à coefficients entiers. On a, cf. **2.4** : $\mathcal{O}_L = \mathcal{O} \cap L$ d'où $\mathcal{O}_L \cap K = \mathcal{O} \cap L \cap K = \mathcal{O} \cap K = \mathcal{O}_K$.

6.2. Soit $\zeta = \exp(\frac{2i\pi}{p})$: $\zeta^p = 1$ donc $\zeta \in \mathcal{O}_L$ et $\tau_p = \zeta^{0^2} + \zeta^{1^2} + \ldots + \zeta^{(p-1)^2} \in \mathcal{O}_L$.

Lemme : soient $a_1, \ldots, a_n \in \mathcal{O}_L$. Alors $(a_1 + \ldots + a_n)^q - a_1^q - \ldots - a_n^q \in q\mathcal{O}_L$.
Démonstration : pour $n = 1$ la différence est nulle. Pour $n = 2$, $(a_1+a_2)^q - a_1^q - a_2^q = C_q^1 a_1^1 a_2^{q-1} + \ldots + C_q^{q-1} a_1^{q-1} a_2^1$ et tous les coefficients binomiaux $C_q^1, \ldots, C_q^{q-1}$ sont divisibles par q car q est premier. Pour n quelconque on établit le résultat par récurrence.

On en déduit $\tau_p^q - \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \zeta^{qx^2} \in q\mathcal{O}_L$. Notons $\mu = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \zeta^{qx^2}$: si q est un carré modulo p alors la liste $[qx^2,\ x \in \mathbb{Z}/p\mathbb{Z}]$ est une permutation de $[x^2,\ x \in \mathbb{Z}/p\mathbb{Z}]$ d'où $\mu = \tau_p = \left(\frac{q}{p}\right)\tau_p$.

Si q n'est pas un carré modulo p on partitionne $\mathbb{Z}/p\mathbb{Z}$ en : $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup C \cup N$ où C est l'ensemble des carrés non nuls et N l'ensemble des non carrés. L'application $\sigma : x \longmapsto x^2$ envoie $\mathbb{Z}/p\mathbb{Z}$ sur $\{0\} \cup C$ et chaque élément de C a exactement deux antécédents par σ car $x^2 = y^2 \iff x = \pm y$, d'où : $\tau_p = 1 + 2\sum_{x\in C} \zeta^x$.
De même, l'application $\sigma' : x \longmapsto qx^2$ envoie $\mathbb{Z}/p\mathbb{Z}$ sur $\{0\} \cup N$ et chaque élément de N a exactement deux antécédents par σ' d'où $\mu = 1 + 2\sum_{x\in N} \zeta^x$. On a alors : $\tau_p + \mu = 2 + 2\sum_{x\in C} \zeta^x + 2\sum_{x\in N} \zeta^x = 2\sum_{x\in\mathbb{Z}/p\mathbb{Z}} \zeta^x = 0$ d'où $\mu = -\tau_p = \left(\frac{q}{p}\right)\tau_p$.

Ainsi, dans tous les cas, $(\tau_p^q - \left(\frac{q}{p}\right)\tau_p)/q \in \mathcal{O}_L$ et $(\tau_p^q - \left(\frac{q}{p}\right)\tau_p)/q \in K$ car $\tau_p \in K$, d'où $\tau_p^q - \left(\frac{q}{p}\right)\tau_p \in q\mathcal{O}_K$.

6.3. Soit $n\tau_p = q(a + b\omega_p)$ où ω_p est le deuxième générateur du groupe $\mathcal{O}_K$ défini en **3.6** et $a, b \in \mathbb{Z}$.

Pour $p \equiv 1 \pmod 4$ on a : $n\sqrt{p} = q\left(a + b\frac{1+\sqrt{p}}{2}\right)$ soit $b = -2a, n = -qa$ et $q \mid n$.

Pour $p \equiv 3 \pmod 4$ on a : $n\sqrt{-p} = q\left(a + b\frac{1+\sqrt{-p}}{2}\right)$ soit $b = -2a, n = -qa$ et $q \mid n$.

6.4. On a d'après **5.6** : $\tau_p = \sqrt{(-1)^{\frac{p-1}{2}}p}$ donc $\tau_p^q = \left((-1)^{\frac{p-1}{2}}p\right)^{\frac{q-1}{2}}\tau_p$ et $\left(\left((-1)^{\frac{p-1}{2}}p\right)^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)\right)\tau_p \in q\mathcal{O}_K$ d'où $\left(\frac{q}{p}\right) \equiv \left((-1)^{\frac{p-1}{2}}p\right)^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod q$.
Les deux membres extrêmes valent ± 1 et $q > 2$ donc ils sont égaux, ce qui donne (1).

6.5. Comme le couple $((x \bmod q), (y \bmod p))$ décrit $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ quand (x, y) décrit $\mathbb{Z}^2$, si ϕ existe alors elle est unique.

Pour démontrer l'existence, considérons $\varphi : \begin{cases} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/pq\mathbb{Z} \\ (x,y) & \longmapsto & (xp+yq) \bmod pq. \end{cases}$

On a $\varphi(x,y) = \varphi(x',y') \iff pq \mid (x-x')p + (y-y')q \iff \begin{cases} p \mid (x-x')p + (y-y')q \\ q \mid (x-x')p + (y-y')q \end{cases} \iff \begin{cases} p \mid y-y' \\ q \mid x-x' \end{cases}$
car p et q sont premiers entre eux. On peut alors définir l'application quotient :

$$\phi : \begin{cases} \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/pq\mathbb{Z} \\ (X,Y) & \longmapsto & \varphi(x,y) \end{cases}$$

où x est un représentant de X et y un représentant de Y. Le calcul précédent montre que ϕ est bien définie ($\phi(X,Y)$ ne dépend pas des représentants x et y choisis) et est injective. Les ensembles de départ et d'arrivée ayant même cardinal fini, ϕ est bijective.

6.6. On note $\zeta = \exp(\frac{2i\pi}{pq})$, $\zeta_p = \exp(\frac{2i\pi}{p})$ et $\zeta_q = \exp(\frac{2i\pi}{q})$.

$$\begin{aligned}
\tau_{pq} &= \sum_{z\in\mathbb{Z}/pq\mathbb{Z}} \zeta^{z^2} \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta^{(xp+yq)^2} \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta^{x^2p^2+y^2q^2+2xypq} \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta^{x^2p^2+y^2q^2} \\
&= \Big(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \zeta^{x^2p^2}\Big)\Big(\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta^{y^2q^2}\Big) \\
&= \Big(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \zeta_q^{px^2}\Big)\Big(\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta_p^{qy^2}\Big).
\end{aligned}$$

On a vu en **6.2** que $\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta_p^{qy^2} = \left(\frac{q}{p}\right)\tau_p$ et on a de même $\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \zeta_q^{px^2} = \left(\frac{p}{q}\right)\tau_q$ d'où le résultat.

6.7. Immédiat.

6.8. $\mathcal{O}_K = \mathbb{Z}[i]$ car $-1 \equiv 3 \pmod 4$. On note dans ce qui suit : $x \equiv y \pmod q$ pour : $x - y \in q\mathbb{Z}[i]$.

D'après la formule du binôme : $(1+i)^q \equiv 1+i^q \pmod q$ et aussi : $(1+i)^q = (2i)^{\frac{q-1}{2}}(1+i) \equiv \binom{2}{q} i^{\frac{q-1}{2}}(1+i) \pmod q$

D'où $\binom{2}{q}(1+i) \equiv i^{\frac{1-q}{2}}(1+i^q) \pmod q$ ce qui implique l'égalité de ces deux quantités car elles ont même module, $\sqrt{2}$ (q est impair), donc leur distance est au plus $2\sqrt{2} < q$. On a donc :

$$\binom{2}{q} = i^{\frac{1-q}{2}} \frac{1+i^q}{1+i}$$

et on vérifie pour chaque valeur possible de q mod 8 que cette expression est égale à $(-1)^{\frac{q^2-1}{8}}$.

6.9. Soit $n \in \mathbb{Z}$ non carré, on montre qu'il existe une infinité de nombres premiers ℓ tels que $n \bmod \ell$ ne soit pas un carré dans $\mathbb{Z}/\ell\mathbb{Z}$. Décomposons n en facteurs premiers : $n = (-1)^{\alpha_0} 2^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ où les p_i sont des entiers naturels impairs premiers distincts et les α_i sont entiers naturels. Puisque n n'est pas un carré, l'un des α_i est impair.

1) S'il existe $i \geqslant 2$ tel que α_i est impair, par exemple si α_2 est impair : Soit $x \in \mathbb{Z}$ non carré modulo p_2 (x existe car le nombre de carrés distincts dans $\mathbb{Z}/p_2\mathbb{Z}$ est $(p_2+1)/2 < p_2$). D'après le théorème de Dirichlet et le lemme des restes chinois il existe une infinité de nombres ℓ premiers vérifiant les congruences simultanées :

$$\ell \equiv 1 \pmod 8, \qquad \ell \equiv x \pmod{p_2}, \qquad \ell \equiv 1 \pmod{p_i},\ i > 2.$$

Donc -1 et 2 sont des carrés modulo ℓ, et ℓ est un carré modulo $p_3, \dots, p_k$, $\ell \equiv 1 \bmod 4$ d'où $p_3, \dots, p_k$ sont des carrés modulo ℓ d'après la loi de réciprocité quadratique. Par contre ℓ n'est pas un carré modulo p_2 et donc, par réciprocité quadratique, p_2 n'est pas un carré modulo ℓ. Ainsi, n est congru modulo ℓ au produit d'un carré par une puissance impaire d'un non carré, c'est un non carré modulo ℓ.

2) Si α_1 est impair : on considère de même les nombres premiers ℓ vérifiant :

$$\ell \equiv 5 \pmod 8, \qquad \ell \equiv 1 \pmod{p_i},\ i > 1.$$

Pour un tel ℓ, $-1, p_2, \dots, p_k$ sont des carrés modulo ℓ tandis que 2 n'en est pas un et donc n non plus.

3) Si α_0 est impair et tous les autres α_i sont pairs : alors tout entier ℓ premier tel que $\ell \equiv 3 \pmod 4$ convient car $-n$ est un carré modulo ℓ et -1 n'en est pas un.