



# Entiers algébriques. Loi de réciprocité quadratique.

E.N.S Ulm et Lyon 2001

## Avertissement

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 obtenues dans les questions 4.5 et 5.6 sont utilisées dans la partie 6.

## Notations

Soit  $\zeta$  un nombre complexe. On note  $\mathbb{Q}[\zeta]$  le  $\mathbb{Q}$ -espace vectoriel engendré par  $\{\zeta^n \mid n \in \mathbb{N}\}$  : c'est une  $\mathbb{Q}$ -algèbre. On note  $\mathbb{Z}[\zeta]$  le sous-groupe additif de  $\mathbb{Q}[\zeta]$  engendré par  $\{\zeta^n \mid n \in \mathbb{N}\}$ . Un sous-corps de  $\mathbb{C}$  qui est de dimension finie en tant que  $\mathbb{Q}$ -espace vectoriel est appelé corps de nombre.

Soient  $n, k$  deux entiers. Si  $\zeta$  est une racine  $n^{\text{e}}$  de l'unité, le complexe  $\zeta^k$  ne dépend que de la classe  $x$  de  $k$  dans  $\mathbb{Z}/n\mathbb{Z}$  et sera noté  $\zeta^x$ .

Dans le cas particulier où  $\zeta = e^{\frac{2i\pi}{n}}$  on notera  $\tau_n$  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 
$$\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x = \begin{cases} -y^{\frac{p-1}{2}} & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}} & \text{sinon.} \end{cases} \quad \boxed{[S]}$$

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

1.2. En déduire les égalités 
$$y^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } y \text{ est un carré} \\ -1 & \text{sinon} \end{cases} \quad \boxed{[S]}$$

## 2. Généralités

2.1. Montrer que les deux propositions suivantes sont équivalentes :

(i) Il existe un polynôme unitaire à coefficients rationnels annulant  $\zeta$  ;

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

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

2.2. Montrer que les deux propositions suivantes sont équivalentes :

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

(ii) Il existe un entier  $n$  et une famille génératrice  $(v_1, v_2, \dots, v_n)$  de  $V$  telle que  $f\langle \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n \rangle \subset \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$ . [S]

[Indication : Pour (ii)  $\implies$  (i) on pourra introduire une matrice carrée  $A$  dont les coefficients  $a_{ij}$  vérifient  $f(v_j) = \sum_{i=1}^n a_{ij}v_i$  pour tout  $j \in \llbracket 1, n \rrbracket$  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 (i.e  $f \circ g = g \circ f$ ) sont entiers.

[Indication : On pourra montrer qu'on peut choisir un entier  $n$  et des vecteurs  $v_1, \dots, v_n$  comme dans (ii) de 2.2 qui conviennent à la fois pour  $f$  et  $g$ ].

Donner un exemple de deux endomorphismes entiers dont le composé n'est pas entier.

[S]

Soit  $K$  un corps de nombres, muni de sa structure de  $\mathbb{Q}$ -espace vectoriel de dimension finie. On dira qu  $x \in K$  est entier lorsque l'endomorphisme de multiplication  $K \longmapsto K$  est

$$y \longmapsto xy$$

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

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

### 3. Entiers des corps quadratiques

Soit  $D \in \mathbb{Q}$  qui n'est pas le carré d'un rationnel. Si  $D < 0$  on notera  $\sqrt{D}$  le complexe  $i\sqrt{|D|}$ . Un corps de la forme  $\mathbb{Q}[\sqrt{D}]$  est dit corps quadratique. On remarque que  $(1, \sqrt{D})$  est une base de  $\mathbb{Q}[\sqrt{D}]$ . On note  $\sigma$  l'automorphisme du corps  $\mathbb{Q}[\sqrt{D}]$  défini par  $\mathbb{Q}[\sqrt{D}] \longmapsto \mathbb{Q}[\sqrt{D}]$ .

$$a + b\sqrt{D} \longmapsto a - b\sqrt{D}$$

**3.1.** Montrer que les seuls automorphismes du corps  $\mathbb{Q}[\sqrt{D}]$  sont l'identité et  $\sigma$ . [S]

**3.2.** Soit  $D' \in \mathbb{Q}^*$ . Montrer que  $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$  si et seulement si  $\frac{D}{D'}$  est le carré d'un rationnel. [S]

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

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

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

**3.5.** Montrer que  $x \in \mathcal{O}_K$  si et seulement si  $x \in K$  et  $\begin{cases} x + \sigma(x) \in \mathbb{Z} \\ x\sigma(x) \in \mathbb{Z} \end{cases}$ . [S]

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

3.6. Montrer que l'application  $\varphi : \mathbb{Z}^2 \rightarrow \mathcal{O}_K$  est un isomorphisme de groupes additifs.  
 $(p, q) \mapsto p + q\omega$

[S]

#### 4. Un calcul analytique de $\tau_n$

On se donne un entier  $n \in \mathbb{N}^*$ . Pour  $k \in \llbracket 1, n-1 \rrbracket$  on note  $f_k$  la fonction

$$f_k : [0, 1] \rightarrow \mathbb{C} \quad \text{et} \quad f = \sum_{k=0}^n f_k \\ t \mapsto \exp\left(\frac{2i\pi(k+t)^2}{n}\right)$$

4.1. Montrer que la suite de terme général  $u_k = \sum_{m=-k}^k \int_0^1 f(t) e^{-2i\pi mt} dt$  converge vers  $\tau_n$ .

[S]

4.2. Montrer que la fonction de  $\mathbb{R}_+$  dans  $\mathbb{C}$   $x \mapsto \int_{-x}^x e^{\frac{2i\pi t^2}{n}} dt$  admet une limite  $I_n$  quand  $x \rightarrow +\infty$ .

[S]

4.3. Montrer que  $\tau_n + f\left(\frac{1}{2}\right) = 2I_n$ .

[S]

4.4. Comparer  $I_n$  et  $I_1$ .

[S]

4.5. Montrer la formule  $\tau_n = \frac{1 + i^{-n}}{1 + i^{-1}} \sqrt{n}$ .

[S]

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

[S]

#### 5. Un calcul algébrique de $\tau_n$

Soit  $n$  un entier impair  $\geq 3$ , et  $\zeta$  le complexe  $\zeta = e^{\frac{2i\pi}{n}}$ . Soit  $V$  le  $\mathbb{C}$ -espace vectoriel des applications de  $\mathbb{Z}/n\mathbb{Z}$  vers  $\mathbb{C}$ . Soit  $\varphi$  l'endomorphisme de  $V$  qui à tout  $f \in V$  associe

$$\varphi(f) : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C} \\ x \mapsto \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y) \zeta^{xy}$$

5.1. Soit  $f \in V$ . Montrer l'égalité  $\varphi \circ \varphi(f)(x) = nf(-x)$  pour tout  $x \in \mathbb{Z}/n\mathbb{Z}$ .

[S]



5.2. Montrer que  $\varphi$  est diagonalisable et localiser son spectre. [S]

On observe que  $\tau_n = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \zeta^{x^2}$  est la trace de  $\varphi$ .

5.3. Montrer que  $|\tau_n| = \sqrt{n}$ . [S]

On note  $a, b, c$  et  $d$  la multiplicité de  $\sqrt{n}, -\sqrt{n}, i\sqrt{n}$  et  $-i\sqrt{n}$  dans le polynôme caractéristique de  $\varphi$ .

5.4. Montrer que  $a + b = \frac{n+1}{2}$ ,  $c + d = \frac{n-1}{2}$  et que  $(a-b)^2 + (c-d)^2 = 1$ . [S]

5.5. Calculer  $\text{Dét } \varphi$ . [S]

5.6. En déduire les valeurs de  $a, b, c$  et  $d$  en fonction de  $n$  et la formule  $\tau_n = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 \pmod{4} \\ i\sqrt{n} & \text{si } n \equiv 3 \pmod{4} \end{cases}$

(compatible avec le résultat de 4.5). [S]

## 6. Réciprocité quadratique

On considère deux nombres premiers impairs distincts  $p, q$ . On note  $L$  le corps de nombres  $\mathbb{Q}[e^{\frac{2i\pi}{p}}]$  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 de  $q$  modulo  $p$  est un carré et  $-1$  sinon. On se propose de montrer par deux méthodes différentes que

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

Première méthode

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

6.2. Montrer la relation  $\tau_p^q - \left(\frac{q}{p}\right) \tau_p \in q\mathcal{O}_L \cap K = q\mathcal{O}_K$ . [S]

6.3. Soit  $n \in \mathbb{Z}$ . Montrer que si  $n\tau_p \in q\mathcal{O}_K$  alors  $q$  divise  $n$ . [S]

[Indication : utiliser le résultat de 3.6].

6.4. Montrer l'égalité (1). [S]

Seconde méthode

6.5. Montrer que l'on définit bien une application  $\Phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/pq\mathbb{Z}$  par la formule

$$\Phi(x \bmod p, y \bmod q) = qx + py \bmod pq, \quad \text{pour tout } (x, y) \in \mathbb{Z}^2, \quad [S]$$

et que cette application  $\Phi$  est bijective.



6.6. Montrer la formule

$$\tau_{pq} = \binom{p}{q} \binom{q}{p} \tau_p \tau_q. \quad [S] \quad (2)$$

6.7. Dédurre de (2) l'égalité (1) en utilisant le résultat de 5.6. [S]

6.8. Dans cette question  $K$  désigne le corps quadratique  $\mathbb{Q}[i]$ . En étudiant  $(1+i)^q$  dans  $\mathcal{O}_K$ , montrer l'égalité

$$\binom{2}{q} = (-1)^{\frac{q^2-1}{8}}. \quad [S]$$



## Corrigé du problème

### 1. Préliminaires

1.1. Soit  $y \in (\mathbb{Z}/p\mathbb{Z})^*$ . Si  $y$  n'est pas un carré, pour tout  $x \in (\mathbb{Z}/p\mathbb{Z})^*$ ,  $x \neq yx^{-1}$ . Il y a  $\frac{p-1}{2}$  paires  $\{x, yx^{-1}\}$  distinctes formant une partition de  $(\mathbb{Z}/p\mathbb{Z})^*$  et ainsi  $\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x = y^{\frac{p-1}{2}}$ .

Si  $y$  est un carré, il existe exactement deux éléments  $\pm x_0$  de  $(\mathbb{Z}/p\mathbb{Z})^*$  dont le carré est  $y$  (car  $\mathbb{Z}/p\mathbb{Z}$  est un anneau intègre et  $x^2 - x_0^2 = (x - x_0)(x + x_0)$ ). Dans ce cas on obtient une partition de  $(\mathbb{Z}/p\mathbb{Z})^*$  en deux singletons  $\{x_0\}$ ,  $\{-x_0\}$  et  $\frac{p-3}{2}$  paires  $\{x, yx^{-1}\}$  distinctes.

On a donc  $\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x = -x_0^2 y^{\frac{p-3}{2}} = -y^{\frac{p-1}{2}}$ . [Q]

1.2. On peut choisir le carré  $y_0 = 1_{\mathbb{Z}/p\mathbb{Z}}$  (noté simplement 1) qui donne  $\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x = -1$ , donc

$$y^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } y \text{ est un carré} \\ -1 & \text{sinon} \end{cases} \quad \text{[Q]}$$

### 2. Généralités

2.1. Si la condition (i) est vérifiée, la  $\mathbb{Q}$ -algèbre  $\mathbb{Q}[\zeta]$  est de dimension finie sur  $\mathbb{Q}$  égale au degré du polynôme minimal de  $\zeta$ . Cette  $\mathbb{Q}$  algèbre est intègre puisqu'elle est incluse dans  $\mathbb{C}$  qui est un corps. Toute algèbre intègre de dimension finie étant un corps,  $\mathbb{Q}[\zeta]$  est un corps de nombres lorsque la condition (i) est vérifiée.

Réciproquement, si la condition (ii) est vérifiée,  $\mathbb{Q}[\zeta]$  est de dimension finie sur  $\mathbb{Q}$  donc l'idéal annulateur dans  $\mathbb{Q}[X]$  de  $\zeta$  n'est pas nul et la condition (i) est vérifiée. [Q]

2.2. Supposons la condition (i) vérifiée : il existe une famille  $(a_1, a_2, \dots, a_p) \in \mathbb{Z}^p$  telle que

$$f^p = \sum_{k=1}^p a_k f^{p-k}.$$

Considérons alors une famille génératrice  $(g_1, g_2, \dots, g_q)$  du  $\mathbb{Q}$ -espace de type fini  $V$  et posons  $v_{i(p-k+1)} = f^{p-k}(g_i)$  pour tout  $(k, i) \in \llbracket 1, p \rrbracket \times \llbracket 1, q \rrbracket$ . Par construction, la famille  $(v_1, v_2, \dots, v_{pq})$  est génératrice de  $V$  et vérifie  $f(v_j) \in \sum_{r=1}^{pq} \mathbb{Z}v_r$

pour tout  $j \in \llbracket 1, pq \rrbracket$ . La condition (ii) est alors vérifiée.

Réciproquement, supposons la condition (ii) est vérifiée : on peut trouver une famille

$$(v_1, v_2, \dots, v_n)$$

génératrice de  $V$  et une matrice  $A \in \mathcal{M}_n(\mathbb{Z})$  telle que  $f(v_j) = \sum_{i=1}^n a_{ij} v_i$

pour tout  $j \in \llbracket 1, n \rrbracket$ . Le théorème de Cayley-Hamilton permet d'affirmer que le polynôme caractéristique  $\chi_A$  est un polynôme annulateur de  $A$ . En actionnant la matrice  $\tilde{\chi}_A(A)$  sur les vecteurs colonnes canoniques de  $\mathbb{Q}^n$  on obtient  $\tilde{\chi}_A(f)(v_j) = O_V$  pour tout

$j \in \llbracket 1, n \rrbracket$ . L'endomorphisme  $\tilde{\chi}_A(f)$  de  $V$  s'annule sur une famille génératrice de  $V$  : c'est donc l'endomorphisme nul. Ainsi  $\chi_A$  est un polynôme unitaire annulateur de  $f$  et par construction  $\chi_A \in \mathbb{Z}[X]$ . Donc (ii)  $\implies$  (i). [Q]

**2.3.** Considérons deux endomorphismes entiers de  $V$  qui commutent. On peut trouver des familles génératrices finies  $u$  et  $v$  associées à  $f$  et  $g$  respectivement et vérifiant la condition imposée dans 2.2.(ii) :  $f(u_i) \in \sum_j \mathbb{Z}u_j$  et  $g(v_i) \in \sum_j \mathbb{Z}v_j$ . Par linéarité de  $f$  et  $g$ ,  $f \circ g(u_i) = g \circ f(u_i) \in \sum_j \mathbb{Z}g(u_j)$  et  $f \circ g(v_i) = g \circ f(v_i) \in \sum_j \mathbb{Z}f(v_j)$  si bien qu'en notant  $w$  la famille obtenue en réunissant les vecteurs de  $u$ ,  $v$ ,  $f \circ u$  et  $f \circ v$ , on obtient une famille génératrice de  $V$  vérifiant la condition (ii) aussi bien pour  $f \circ g$  que pour  $f + g$  : les endomorphismes  $f \circ g$  et  $f + g$  sont donc entiers.

L'exemple  $V = \mathbb{Q}[i]$   $f(x + iy) = x$  et  $g(x + iy) = \frac{1+i}{2}(x + y)$  ( $x, y \in \mathbb{Q}^2$ ) donne deux projecteurs, donc des endomorphismes entiers de  $V$  tels que le composé  $f \circ g$  défini par  $f \circ g(x + iy) = \frac{x+y}{2}$  n'est pas entier (c'est la moitié d'un projecteur). [Q]

**2.4.** Soit  $x \in \mathcal{O}_K \cap \mathbb{Q}$ . Il existe alors un polynôme unitaire  $P = X^p - \sum_{k=1}^p a_k X^{p-k}$  à coefficients

dans  $\mathbb{Z}$  annulateur de  $m_x$ . Donc le rationnel  $x = \frac{m}{n}$  est racine de  $P$  :  $m^p = \sum_{k=1}^p a_k m^{p-k} n^k$ .

On peut choisir les entiers relatifs  $m$  et  $n$  étrangers, et comme  $n$  divise  $\sum_{k=1}^p a_k m^{p-k} n^k = m^p$  en étant étranger avec  $m^p$ , il faut que  $|n| = 1$ . On a donc  $x = \pm m \in \mathbb{Z}$ . On en déduit que  $\mathcal{O}_K \cap \mathbb{Q} \subset \mathbb{Z}$ . L'inclusion inverse est immédiate. [Q]

### 3. Entiers des corps quadratiques

**3.1.** Un automorphisme  $f$  du corps  $\mathbb{Q}[\sqrt{D}]$  doit conserver 1, par suite  $f$  induit l'identité sur  $\mathbb{Q}$ . Ainsi  $f(\sqrt{D})^2 = f(D) = D$  donc  $f(\sqrt{D}) = \pm\sqrt{D}$  si bien que l'application  $\mathbb{Q}$ -linéaire  $f$  coïncide avec l'identité ou avec  $\sigma$  sur la base  $(1, \sqrt{D})$  de  $\mathbb{Q}[\sqrt{D}]$ . Les seuls automorphismes du corps  $\mathbb{Q}[\sqrt{D}]$  sont donc l'identité et  $\sigma$  (on vérifie sans difficulté que  $\sigma$  est bien un automorphisme de corps). [Q]

**3.2.** Soit  $D' \in \mathbb{Q}^*$  et  $\sigma'$  l'automorphisme associé de  $\mathbb{Q}[\sqrt{D'}]$ . Supposons que  $\mathbb{Q}[\sqrt{D'}] = \mathbb{Q}[\sqrt{D}]$ . Alors  $\sigma = \sigma'$  (d'après 3.1.) donc en écrivant  $\sqrt{D'} = a + b\sqrt{D}$  avec  $(a, b) \in \mathbb{Q}^2$  on a aussi  $-\sqrt{D'} = a - b\sqrt{D}$  ce qui exige  $a = 0$ . On a donc  $\sqrt{D'} = b\sqrt{D}$  et alors  $\frac{D'}{D} = b^2$  est un carré dans  $\mathbb{Q}$ .

Réciproquement si  $\frac{D'}{D}$  est le carré d'un rationnel  $b$  on a  $\frac{\sqrt{D'}}{\sqrt{D}} = \pm b \neq 0$  si bien que les  $\mathbb{Q}$ -droites engendrées par  $\sqrt{D'}$  et  $\sqrt{D}$  sont les mêmes. Dès lors  $\mathbb{Q}[\sqrt{D'}] = \mathbb{Q}[\sqrt{D}]$ . [Q]

**3.3.** Écrivons  $d = \frac{m}{n}$  avec  $m$  et  $n$  entiers relatifs étrangers. Soit  $d$  l'entier relatif du signe de  $D$  et dont la valeur absolue est le produit des facteurs premiers de  $m$  et de  $n$  dont l'exposant est impair dans la décomposition de  $m$  et  $n$  en produit de facteurs premiers. Par construction  $\frac{D}{d}$  est le carré d'un rationnel, donc, par 3.2.,  $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{d}]$ , et  $d$  n'est divisible par aucun autre carré dans  $\mathbb{Z}$  que 1 ( $d$  est sans facteur carré autre que 1).

Si  $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$  avec  $(d, d') \in \mathbb{Z}^2$  et  $d$  et  $d'$  sans facteur carré autre que 1 alors d'après 3.2., on peut écrire  $\frac{d'}{d} = \frac{a^2}{b^2}$  avec  $a$  et  $b$  entiers relatifs étrangers. L'égalité  $d'b^2 = da^2$  montre que  $b^2$  divise  $da^2$  et comme  $b^2$  et  $a^2$  sont étrangers, le théorème de Gauss dit que  $b^2$  divise  $d$ . Comme  $d$  est sans facteur carré autre que 1,  $b^2 = 1$  et  $d' = da^2$ . De même  $a^2 = 1$  puisque  $d'$  est sans facteur carré autre que 1. Ainsi  $d = d'$ . [Q]

**3.4.** Soit  $(1, \delta)$  une base du corps  $K$  regardé comme  $\mathbb{Q}$ -espace vectoriel de dimension 2. Alors il existe  $(a, b) \in \mathbb{Q}^2$  tel que  $\delta^2 = a\delta + b$ . En posant  $D = a^2 + 4b$  on obtient un élément de  $\mathbb{Q}$  qui n'est pas un carré et tel que  $\delta \in \mathbb{Q}[\sqrt{D}]$ .  $K$  et  $\mathbb{Q}[\sqrt{D}]$  sont deux plans tels que  $K \subset \mathbb{Q}[\sqrt{D}]$  : ils sont égaux et  $K$  est un corps quadratique. [Q]

**3.5.** Soit  $x \in \mathcal{O}_K$ . Alors  $x$  est racine d'un polynôme unitaire  $P \in \mathbb{Z}[X]$  et comme  $0 = \sigma(\tilde{P}(x)) = \tilde{P}(\sigma(x))$ , on a aussi  $\sigma(x) \in \mathcal{O}_K$  (cf 2.2.(ii)). Comme  $\mathcal{O}_K$  est un sous-anneau de  $K$  on a  $x + \sigma(x) \in \mathcal{O}_K \cap \mathbb{Q}$  et  $x\sigma(x) \in \mathcal{O}_K \cap \mathbb{Q}$ . Or  $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$  d'après 2.4. Donc  $x + \sigma(x) = s$  et  $x\sigma(x) = p$  sont des entiers relatifs.

Réciproquement, si  $x + \sigma(x) = s$  et  $x\sigma(x) = p$  sont des entiers relatifs,  $x$  et  $\sigma(x)$  sont racines du polynôme unitaire  $P = X^2 - sX + p \in \mathbb{Z}[X]$ . En particulier  $x \in \mathcal{O}_K$  d'après 2.2.(ii). [Q]

**3.6.** Soit  $x \in \mathcal{O}_K$ . D'après 3.5.,  $x + \sigma(x)$  est un entier relatif. Donc  $x = a + b\sqrt{d}$  avec  $2a = a' \in \mathbb{Z}$  et  $b \in \mathbb{Q}$ . De même  $x - \sigma(x) = 2b\sqrt{d} \in \mathcal{O}_K$  donc  $4b^2d \in \mathbb{Z}$ . En écrivant  $b = \frac{p}{q}$ ,  $(p, q) \in \mathbb{Z}^2$  et  $p \wedge q = 1$ , on observe que  $q^2$  divise  $4p^2d$  et comme  $q^2 \wedge p^2 = 1$ ,  $q^2$  divise  $4d$ . Puisque  $d$  est sans facteur carré,  $|q| \leq 2$  donc  $2b = b' \in \mathbb{Z}$ . Ainsi  $a'^2 - b'^2d = 4x\sigma(x) \equiv 0 \pmod{4}$ . Cela exige que  $a'$  et  $b'$  soient de même parité (en effet  $d$  n'est pas divisible par  $4 = 2^2$ ).

- Cas où  $a'$  et  $b'$  sont pairs :  $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ . Inversement  $\sqrt{d} \in \mathcal{O}_K$  donc  $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$ .

- Cas où  $a'$  et  $b'$  sont impairs :  $a = \frac{a'}{2} = u + \frac{1}{2}$  avec  $u \in \mathbb{Z}$  et de même  $b = v + \frac{1}{2}$  avec  $v \in \mathbb{Z}$ . Dans ce cas  $a'^2 - b'^2d \equiv 1 - d \equiv 0 \pmod{4}$  et en posant  $\omega = \frac{1 + \sqrt{d}}{2}$  on a  $x = (u - v) + (2v + 1)\omega \in \mathbb{Z}[\omega]$ . Inversement, lorsque  $d \equiv 1 \pmod{4}$ ,  $d = 1 - 4d'$  avec  $d' \in \mathbb{Z}$  et  $\omega\sigma(\omega) = \frac{1 - d}{4} = d' \in \mathbb{Z}$  et  $\omega + \sigma(\omega) = 1 \in \mathbb{Z}$  donc  $\omega \in \mathcal{O}_K$  et alors  $\mathbb{Z}[\omega] \subset \mathcal{O}_K$ .

En posant  $\omega = \frac{1 + \sqrt{d}}{2}$  ou  $\sqrt{d}$  selon que  $d$  est, ou n'est pas congru à 1 modulo 4, on a montré que  $\mathcal{O}_K = \mathbb{Z}[\omega]$ . L'application  $\varphi : \mathbb{Z}^2 \rightarrow \mathcal{O}_K = \mathbb{Z}[\omega]$  définie par  $\varphi(p, q) = p + q\omega$  est alors un isomorphisme de groupes additifs. [Q]



#### 4. Un calcul analytique de $\tau_n$

4.1. La fonction  $f$  est de classe  $\mathcal{C}^1$  sur  $[0, 1]$  et  $f(0) = f(1) = \tau_n$ . On peut donc appliquer le théorème de Dirichlet à la fonction 1-périodique et  $\mathcal{C}^1$  par morceaux associée à  $f$  :

$$\forall t \in [0, 1], \quad f(t) = \sum_{m=-\infty}^{+\infty} c_m(f) e^{2i\pi mt} \quad \text{où} \quad c_m(f) = \int_0^1 f(t) e^{-2i\pi mt} dt.$$

En particulier, pour  $t = 0$  :  $\tau_n = \sum_{m=-\infty}^{+\infty} c_m(f)$ . [Q]

4.2. La fonction  $g : \mathbb{R} \mapsto \mathbb{C}$  définie par  $g(t) = e^{\frac{2i\pi t^2}{n}}$  est paire et continue sur  $\mathbb{R}$  donc elle y est localement intégrable. Pour montrer que  $G_n(x) = \int_{-x}^x g(t) dt = 2 \int_0^x g(t) dt$  admet une limite quand le réel  $x$  tend vers  $+\infty$  il suffit de montrer que  $H_n(x) = \int_1^x g(t) dt$  admet une limite quand  $x \rightarrow +\infty$ . En intégrant par parties on a

$$H_n(x) = \frac{n}{4i\pi} \int_1^x \frac{1}{t} d\left(e^{\frac{2i\pi t^2}{n}}\right) = \frac{n}{4i\pi} \left[ \frac{1}{t} e^{\frac{2i\pi t^2}{n}} \right]_{t=1}^{t=x} + \frac{n}{4i\pi} \int_1^x e^{\frac{2i\pi t^2}{n}} \frac{dt}{t^2}.$$

Comme  $\frac{g(t)}{t^2} = O\left(\frac{1}{t^2}\right)$  est intégrable sur  $[1, +\infty[$  et  $\frac{g(x)}{x} = O\left(\frac{1}{x}\right) \xrightarrow{x \rightarrow +\infty} 0$ ,  $H_n(x)$  admet une limite quand  $x \rightarrow +\infty$ , ce qui assure l'existence de  $I_n = \lim_{x \rightarrow +\infty} \int_{-x}^x g(t) dt$ .

[Q]

4.3. Par la relation de Chasles

$$I_n = \lim_{p \rightarrow +\infty} \sum_{m=-p}^{p-1} \int_{mn}^{(m+1)n} g(t) dt = \lim_{p \rightarrow +\infty} \sum_{m=-p}^{p-1} \int_0^n e^{\frac{2i\pi(t+mn)^2}{n}} dt = \lim_{p \rightarrow +\infty} \sum_{m=-p}^{p-1} \int_0^n e^{\frac{2i\pi t^2}{n}} e^{4i\pi mt} dt.$$

À nouveau par la relation de Chasles

$$\int_0^n e^{\frac{2i\pi t^2}{n}} e^{4i\pi mt} dt = \sum_{k=0}^{n-1} \int_k^{k+1} e^{\frac{2i\pi t^2}{n}} e^{4i\pi mt} dt = \sum_{k=0}^{n-1} \int_0^1 e^{\frac{2i\pi(t+k)^2}{n}} e^{4i\pi mt} dt = c_{2m}(f).$$

On a donc  $I_n = \sum_{m=-\infty}^{+\infty} c_{2m}(f)$ . Or d'après 4.1,  $\tau_n = \sum_{m=-\infty}^{+\infty} c_m(f)$  et  $f\left(\frac{1}{2}\right) = \sum_{m=-\infty}^{+\infty} c_m(f)(-1)^m$ .

Il en résulte que  $\tau_n + f\left(\frac{1}{2}\right) = 2I_n$ . [Q]

4.4. Le changement de variable  $t = \sqrt{n}u$  dans l'intégrale définissant  $G_n(x)$  et un passage à la limite quand  $x \rightarrow +\infty$  donnent directement  $I_n = \sqrt{n}I_1$ . On a directement  $\tau_1 = 1$  et lorsque  $n = 1$ ,  $f\left(\frac{1}{2}\right) = f_0\left(\frac{1}{2}\right) = e^{\frac{i\pi}{2}} = i$ . Donc  $2I_n = \sqrt{n}2I_1 = \sqrt{n}(1+i)$ . [Q]

4.5. Distinguons deux cas selon la parité de  $n$ .

• Cas où  $n = 2p$  :  $\tau_n = \sum_{k=0}^{n-1} e^{\frac{2i\pi k^2}{n}} = \sum_{k=0}^{p-1} e^{\frac{i\pi k^2}{p}} + \sum_{k=0}^{p-1} e^{\frac{i\pi(k+p)^2}{p}} = (1 + (-1)^p) \sum_{k=0}^{p-1} e^{\frac{i\pi k^2}{p}}$ . De

même  $f\left(\frac{1}{2}\right) = \sum_{k=0}^{n-1} e^{\frac{i\pi(2k+1)^2}{2n}} = \sum_{k=0}^{p-1} e^{\frac{i\pi(2k+1)^2}{4p}} + \sum_{k=0}^{p-1} e^{\frac{i\pi(2k+1+2p)^2}{4p}} = (1 - (-1)^p) \sum_{k=0}^{p-1} e^{\frac{i\pi(2k+1)^2}{4p}}$ .

Donc si  $n \equiv 2 \pmod{4}$ ,  $\tau_n = 0$  et si  $n \equiv 0 \pmod{4}$ ,  $f\left(\frac{1}{2}\right) = 0$  et  $\tau_n = \sqrt{n}(1+i)$ .

• Cas où  $n = 2p + 1$  :  $\tau_n = \sum_{k=0}^{n-1} e^{\frac{2i\pi k^2}{n}} = 1 + \sum_{k=1}^p e^{\frac{2i\pi k^2}{n}} + \sum_{k=1}^p e^{\frac{2i\pi(n-k)^2}{n}} = 1 + 2 \sum_{k=1}^p e^{\frac{2i\pi k^2}{n}}$ .

$f\left(\frac{1}{2}\right) = \sum_{k=0}^{n-1} e^{\frac{i\pi(2k+1)^2}{2n}} = \sum_{k=1}^p e^{\frac{i\pi(n-2k)^2}{2n}} + i^n + \sum_{k=1}^p e^{\frac{i\pi(n+2k)^2}{2n}} = i^n \left(1 + 2 \sum_{k=1}^p e^{\frac{2i\pi k^2}{n}}\right) = i^n \tau_n$ .

Alors  $\tau_n + f\left(\frac{1}{2}\right) = \tau_n(1+i^n) = \sqrt{n}(1+i)$ . Ainsi  $\tau_n = \sqrt{n} \frac{1+i}{1+i^n} = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 \pmod{4} \\ i\sqrt{n} & \text{si } n \equiv 3 \pmod{4} \end{cases}$ .

En remarquant que  $\frac{1+i}{1+i^n} = \frac{1+i^{-n}}{1+i^{-1}}$  on observe que la formule  $\tau_n = \sqrt{n} \frac{1+i^{-n}}{1+i^{-1}}$

obtenue dans le cas  $n$  impair est aussi valable dans le cas  $n$  pair. [Q]

4.6. Soit  $d$  un entier supérieur ou égal à 2 sans diviseur carré.

• Si  $d \equiv 1 \pmod{4}$ , alors  $\sqrt{d} = \tau_d \in \mathbb{Q}[\zeta]$  où  $\zeta = e^{\frac{2i\pi}{d}}$  est une racine  $d^e$  de l'unité. Dans ce cas  $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta]$ . De plus  $i\sqrt{d} \in \mathbb{Q}[\zeta']$  où  $\zeta' = e^{\frac{i\pi}{d}}$  est une racine de l'unité et alors  $\mathbb{Q}[i\sqrt{d}] \subset \mathbb{Q}[\zeta']$ .

• Si  $d \equiv 3 \pmod{4}$ , on obtient les inclusions  $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta']$  et  $\mathbb{Q}[i\sqrt{d}] \subset \mathbb{Q}[\zeta]$ .

• Si  $d \equiv 2 \pmod{4}$ , alors  $d = 2(2p+1)$  et par l'un des deux cas précédents, il existe une racine de l'unité  $\zeta = e^{\frac{2i\pi}{n}}$  telle que  $\sqrt{2p+1} \in \mathbb{Q}[\zeta]$ . Comme  $\sqrt{2} \in \mathbb{Q}[e^{\frac{i\pi}{4}}]$  et  $i\sqrt{2} \in \mathbb{Q}[e^{\frac{i\pi}{4}}]$  les nombres  $\sqrt{d}$  et  $i\sqrt{d}$  appartiennent à  $\mathbb{Q}[\zeta']$  où  $\zeta' = e^{\frac{2i\pi}{n'}}$  avec  $n' = n \vee 8$ . Les deux corps quadratiques  $\mathbb{Q}[\sqrt{d}]$  et  $\mathbb{Q}[i\sqrt{d}]$  sont alors inclus dans  $\mathbb{Q}[\zeta']$ .

On a ainsi prouvé que, pour tout corps quadratique  $K$ , il existe une racine de l'unité  $\zeta$  telle que  $K \subset \mathbb{Q}[\zeta]$ . [Q]

## 5. Un calcul algébrique de $\tau_n$

5.1.  $\varphi^2(f)(x) = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \varphi(f)(y) \zeta^{xy} = \sum_{(y,z) \in (\mathbb{Z}/n\mathbb{Z})^2} f(z) \zeta^{zy} \zeta^{xy} = \sum_{z \in \mathbb{Z}/n\mathbb{Z}} f(z) \sum_{y \in \mathbb{Z}/n\mathbb{Z}} (\zeta^{z+x})^y$ . Or

pour toute racine  $n^e$  de l'unité  $\xi \neq 1$ ,  $\sum_{y \in \mathbb{Z}/n\mathbb{Z}} \xi^y = \frac{1-\xi^n}{1-\xi} = 0$ , donc  $\varphi^2(f)(x) = n f(-x)$ .

[Q]

5.2. D'après 5.1, un polynôme annulateur de  $\varphi^2$  est  $X^2 - n^2$  : ce polynôme est scindé avec pour racines simples  $\pm n$ . Donc  $\varphi^2$  est diagonalisable avec spectre inclus dans  $\{-n, n\}$ . Comme  $n$  est non nul on en déduit que  $\varphi$  est diagonalisable avec spectre inclus dans  $\{-\sqrt{n}, \sqrt{n}, -i\sqrt{n}, i\sqrt{n}\}$ . [Q]

$$5.3. |\tau_n|^2 = \tau_n \overline{\tau_n} = \sum_{(x,y) \in (\mathbb{Z}/n\mathbb{Z})^2} \zeta^{x^2} \zeta^{-y^2} = \sum_{(x,y) \in (\mathbb{Z}/n\mathbb{Z})^2} \zeta^{(x-y)(x+y)}. \text{ Comme on suppose } n \text{ impair,}$$

2 est inversible dans  $\mathbb{Z}/n\mathbb{Z}$  donc on réalise une bijection de  $(\mathbb{Z}/n\mathbb{Z})^2$  sur lui-même en

$$\text{posant } \begin{cases} u = x - y \\ v = x + y \end{cases} \begin{cases} x = \frac{u+v}{2} \\ y = \frac{-u+v}{2} \end{cases} \text{ On a donc } |\tau_n|^2 = \sum_{(u,v) \in (\mathbb{Z}/n\mathbb{Z})^2} \zeta^{uv}. \text{ Or on a vu que si}$$

$$\zeta^u \neq 1 \text{ la somme } \sum_{v \in \mathbb{Z}/n\mathbb{Z}} (\zeta^u)^v \text{ est nulle. Donc } |\tau_n|^2 = n \text{ et } |\tau_n| = \sqrt{n}. \quad [\text{Q}]$$

5.4. La trace de  $\varphi$  est la somme de ses valeurs propres répétées avec leur multiplicité. Donc  $\tau_n = \sqrt{n}(a - b + i(c - d))$  et comme  $|\tau_n|^2 = n$  on en déduit que  $(a - b)^2 + (c - d)^2 = 1$ .

Par construction  $c - d$  est la dimension de l'espace propre pour  $\varphi^2$  associé à la valeur propre  $-n$ . D'après 5.1 cet espace propre est celui des applications impaires de  $\mathbb{Z}/n\mathbb{Z}$  dans  $\mathbb{C}$ . Le seul élément  $x \in \mathbb{Z}/n\mathbb{Z}$  vérifiant  $x = -x$  est 0 car  $n$  est impair. Donc la dimension du sous-espace de  $V$  constitué des applications impaires est  $\frac{n-1}{2}$ . On en conclut que

$$c + d = \frac{n-1}{2} \text{ et } a + b = n - (c + d) = \frac{n+1}{2}. \quad [\text{Q}]$$

5.5. La matrice de  $\varphi$  relativement à la base canonique de  $V$  est  $M = (\zeta^{pq})_{(p,q) \in [0, n-1]^2}$ . Le déterminant de  $\varphi$  est donc le déterminant de Van der Monde associé à la famille  $(1, \zeta, \dots, \zeta^{n-1})$ . Ainsi  $\text{Dét } \varphi = \prod_{0 \leq p < q < n} (\zeta^q - \zeta^p)$ . Il y a  $C_n^2$  facteurs dans ce produit

chaque facteur ayant pour argument  $\frac{\pi}{2} + \frac{(p+q)\pi}{n}$ . Un calcul simple donne

$$\frac{2}{n} \sum_{0 \leq p < q < n} (p+q) = \frac{1}{n} \left( \sum_{(p,q) \in [0, n-1]^2} (p+q) - \sum_{p=0}^{n-1} (p+p) \right) = \frac{1}{n} (n^2(n-1) - n(n-1)) = (n-1)^2$$

et comme  $(n-1)^2$  est multiple de 4,  $\frac{\pi}{n} \sum_{0 \leq p < q < n} (p+q) \equiv 0 \pmod{2\pi}$ . Il en résulte que

$$\text{Dét } \varphi = i^{\frac{n(n-1)}{2}} n^{\frac{n}{2}}. \quad [\text{Q}]$$

5.6. D'après 5.4 il n'y a que deux possibilités :

- $a = b = \frac{n+1}{4}$  et  $c - d = \pm 1$ , auquel cas  $n \equiv -1 \pmod{4}$ . Il faut alors d'après 5.5 que  $i^{\frac{n(n-1)}{2}} = (-1)^b i^{c-d}$ . Or  $i^{\frac{n(n-1)}{2}} = i^{1-2b} = (-1)^b i$ . Le seul choix possible est donc  $c - d = 1$ . Sachant que  $c + d = \frac{n-1}{2}$  il vient  $a = b = c = \frac{n+1}{4}$  et  $d = \frac{n-3}{4}$ . Dans ce cas  $\tau_n = \sqrt{n}(a - b + i(c - d)) = i\sqrt{n}$ .
- $c = d = \frac{n-1}{4}$  et  $a - b = \pm 1$ , auquel cas  $n \equiv 1 \pmod{4}$ . Cette fois  $i^{\frac{n(n-1)}{2}} = (-1)^c$  et par 5.4 il faut que  $b$  et  $c$  soient de même parité. La condition  $a + b = \frac{n+1}{2}$  donne

la seule possibilité  $a - b = 1$  avec  $b = c = d = \frac{n-1}{4}$  et  $a = \frac{n+3}{4}$ . Dans ce cas  $\tau_n = \sqrt{n}(a - b + i(c - d)) = \sqrt{n}$ . [Q]

## 6. Réciprocité quadratique

**6.1.** Soit  $x \in \mathcal{O}_L \cap K$ . L'endomorphisme  $m_{x,L} = x \text{Id}_L$  de  $L$  laisse stable  $K \subset L$  et il existe un polynôme unitaire  $P \in \mathbb{Z}[X]$  annulateur de  $m_{x,L}$ . Ce polynôme annule aussi la restriction  $m_{x,K} = x \text{Id}_K$  de  $m_{x,L}$  à  $K$  donc  $x \in \mathcal{O}_K$ .

Réciproquement soit  $x \in \mathcal{O}_K$ . Le polynôme unitaire  $P_x = X^2 - (x + \sigma(x))X + x\sigma(x)$  est à coefficients entiers d'après 3.5 et comme  $\tilde{P}_x(m_{x,L}) = \tilde{P}_x(x) \text{Id}_L$ , la relation  $\tilde{P}(x) = 0$  montre que  $m_{x,L}$  est annulé par  $P_x$  donc  $x \in \mathcal{O}_L$ . Il en résulte que  $\mathcal{O}_L \cap K = \mathcal{O}_K$ . [Q]

**6.2.** Posons  $\zeta = e^{\frac{2i\pi}{p}}$ . On a  $\tau_p = \sum_{k=1}^p \zeta^{k^2}$  donc  $\tau_p^q = \sum_{n_1+\dots+n_p=q} \frac{q!}{n_1! \dots n_p!} \prod_{k=1}^p \zeta^{k^2 n_k}$ . Dans cette

somme tous les coefficients  $\frac{q!}{n_1! \dots n_p!}$  sont des entiers divisibles par  $q$  dès que tous les entiers  $n_k$  sont différents de  $q$  car  $q$  étant premier,  $q$  est étranger avec  $n_1!, \dots, n_p!$  (théorème de Gauss). Comme les puissances de  $\zeta$  sont éléments de l'anneau  $\mathcal{O}_L$ , on en déduit que  $\tau_p^q - \sum_{k=1}^p \zeta^{k^2 q} \in q\mathcal{O}_L$ . Par ailleurs l'application  $x \mapsto x^2 q$  de  $\mathbb{Z}/p\mathbb{Z}$  dans lui

même induit une permutation de l'ensemble des carrés de  $\mathbb{Z}/p\mathbb{Z}$  si  $\binom{q}{p} = 1$  et induit une bijection de l'ensemble des carrés de  $\mathbb{Z}/p\mathbb{Z}$  sur son complémentaire si  $\binom{q}{p} = -1$ . Comme

la somme des racines  $p^e$  de l'unité est nulle, il vient  $\sum_{k=1}^p \zeta^{k^2 q} = \binom{q}{p} \sum_{k=1}^p \zeta^{k^2} = \binom{q}{p} \tau_p$ . On

en conclut que  $\tau_p^q - \binom{q}{p} \tau_p \in q\mathcal{O}_L \cap K = q\mathcal{O}_K$ . [Q]

**6.3.** Si  $n\tau_p \in q\mathcal{O}_K$  il existe  $(a, b) \in \mathbb{Z}^2$  tel que  $n\tau_p = q(a + b\omega)$  où  $\omega \in \left\{ \tau_p, \frac{1 + \tau_p}{2} \right\}$  (cf 3.6). Il en résulte que  $qb \in \{n, 2n\}$  et comme  $q$  est étranger avec 2, on déduit du théorème de Gauss que  $q$  divise  $n$ . [Q]

**6.4.** D'après 5.6,  $\tau_p^q - \binom{q}{p} \tau_p = n\tau_p$  avec  $n = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^{\frac{q-1}{2}} - \binom{q}{p}$ . Or par 6.2 et 6.3,  $n \equiv 0 \pmod{q}$  et par 1.2,  $p^{\frac{q-1}{2}} \equiv \binom{p}{q} \pmod{q}$ , donc  $(-1)^{\frac{p-1}{2} \frac{q-1}{2}} \binom{p}{q} \equiv \binom{q}{p} \pmod{q}$ . Il s'agit là d'une congruence modulo  $q$  entre entiers relatifs égaux à  $\pm 1$  et  $q > 2$  : on a donc une égalité, que l'on peut écrire sous la forme  $\binom{p}{q} \binom{q}{p} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$ . [Q]

6.5. Pour  $n \in \mathbb{N}^*$ , soit  $\mathcal{O}_n$  la surjection canonique de  $\mathbb{Z}$  sur  $\mathbb{Z}/n\mathbb{Z}$ . Si  $(x, x') \in \mathbb{Z}^2$  et  $(y, y') \in \mathbb{Z}^2$  vérifient respectivement  $\mathcal{O}_p(x) = \mathcal{O}_p(x')$  et  $\mathcal{O}_q(y) = \mathcal{O}_q(y')$  alors  $q(x - x') + p(y - y')$  est multiple de  $pq$  donc  $\mathcal{O}_{pq}(qx + py) = \mathcal{O}_{pq}(qx' + py')$ . On définit donc bien une application  $\Phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \mapsto \mathbb{Z}/pq\mathbb{Z}$  par la formule :  $\Phi(X, Y) = \mathcal{O}_{pq}(qx + py)$  pour tout  $(x, y) \in X \times Y$ . Comme  $p$  et  $q$  sont étrangers, le théorème de Bézout montre que pour tout  $z \in \mathbb{Z}$  il existe  $(x, y) \in \mathbb{Z}^2$  tel que  $z = qx + py$  donc  $\Phi(\mathcal{O}_p(x), \mathcal{O}_q(y)) = \mathcal{O}_{pq}(z)$ . L'application  $\Phi$  est donc surjective, et comme la source et le but de  $\Phi$  ont le même cardinal  $pq$ ,  $\Phi$  est bijective. [Q]

6.6. Grâce à la bijection  $\Phi$  précédente on a

$$\begin{aligned} \tau_{pq} &= \sum_{Z \in \mathbb{Z}/pq\mathbb{Z}} e^{\frac{2i\pi Z^2}{pq}} = \sum_{(X,Y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}} e^{\frac{2i\pi(qX+pY)^2}{pq}} = \sum_{(X,Y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}} e^{\frac{2i\pi qX^2}{p}} e^{\frac{2i\pi pY^2}{q}} \\ &= \sum_{X \in \mathbb{Z}/p\mathbb{Z}} e^{\frac{2i\pi qX^2}{p}} \sum_{Y \in \mathbb{Z}/q\mathbb{Z}} e^{\frac{2i\pi pY^2}{q}} \end{aligned}$$

On a déjà vu en 6.2 pourquoi  $\sum_{X \in \mathbb{Z}/p\mathbb{Z}} e^{\frac{2i\pi qX^2}{p}} = \begin{pmatrix} q \\ p \end{pmatrix} \tau_p$  si bien que  $\tau_{pq} = \begin{pmatrix} p \\ q \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} \tau_p \tau_q$ .

[Q]

6.7. • Supposons  $\frac{p-1}{2}$  et  $\frac{q-1}{2}$  de même parité :

– Ou bien  $p$  et  $q \equiv 1 \pmod{4}$  : alors  $\tau_{pq} = \sqrt{pq} = \tau_p \tau_q$  (cf 5.6) et  $\begin{pmatrix} p \\ q \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} = 1$  (cf 6.6).

– Ou bien  $p$  et  $q \equiv 3 \pmod{4}$  : alors  $\tau_{pq} = \sqrt{pq} = -\tau_p \tau_q$  (cf 5.6) et  $\begin{pmatrix} p \\ q \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} = -1$  (cf 6.6).

• Supposons  $\frac{p-1}{2}$  et  $\frac{q-1}{2}$  de parité contraire : alors  $pq \equiv 3 \pmod{4}$  et  $\tau_{pq} = i\sqrt{pq} = i\tau_p \tau_q$  (cf 5.6) donc  $\begin{pmatrix} p \\ q \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} = 1$  (cf 6.6).

Dans tous les cas  $\begin{pmatrix} p \\ q \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$ . [Q]

6.8. Par la formule du binôme et le fait que le nombre premier  $q$  divise  $C_q^k$  pour  $k \in \llbracket 1, q-1 \rrbracket$ , le complexe  $z_q = (1+i)^q - (1+i^q)$  est élément de  $q\mathbb{Z}[i]$ .

• Si  $q \equiv 1 \pmod{4}$ , alors  $z_q = (1+i) \left( 2^{\frac{q-1}{2}} (-1)^{\frac{q-1}{4}} - 1 \right) \in q\mathbb{Z}[i]$ . Cela exige que  $2^{\frac{q-1}{2}} (-1)^{\frac{q-1}{4}} \equiv 1 \pmod{q}$ , et comme  $2^{\frac{q-1}{2}} \equiv \begin{pmatrix} 2 \\ q \end{pmatrix} \pmod{q}$ , on a  $\begin{pmatrix} 2 \\ q \end{pmatrix} = (-1)^{\frac{q-1}{4}}$  avec  $\frac{q+1}{2}$  impair. Donc  $\begin{pmatrix} 2 \\ q \end{pmatrix} = (-1)^{\frac{q-1}{4} \frac{q+1}{2}} = (-1)^{\frac{q^2-1}{8}}$ .

• Si  $q \equiv -1 \pmod{4}$ , alors  $z_q = (1-i) \left( 2^{\frac{q-1}{2}} (-1)^{\frac{q+1}{4}} - 1 \right) \in q\mathbb{Z}[i]$ . Comme ci-dessus on obtient  $\begin{pmatrix} 2 \\ q \end{pmatrix} = (-1)^{\frac{q+1}{4}}$  avec  $\frac{q-1}{2}$  impair. Donc  $\begin{pmatrix} 2 \\ q \end{pmatrix} = (-1)^{\frac{q+1}{4} \frac{q-1}{2}} = (-1)^{\frac{q^2-1}{8}}$ .



Dans tous les cas  $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$ . [Q]

