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 ζ 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 ζ est une racine n^{e} 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 $\zeta = \mathrm{e}^{\frac{2i\pi}{n}}$ 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 $\displaystyle\prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x = \begin{cases} -y^{\frac{p-1}{2}} & \text{si y est un carré,} \\ y^{\frac{p-1}{2}} & \text{sinon.} \end{cases}$ [S]

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

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

2. Généralités

2.1. Montrer que les deux propositions suivantes sont équivalentes :

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

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

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

2.2. Montrer que les deux propositions suivantes sont équivalentes :

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

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

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

[Indication : Pour *(ii)* $\Longrightarrow$ *(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 $j \in [\![1, n]\!]$ 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 (*i.e* $f \circ g = g \circ f$) sont entiers.

[Indication : On pourra montrer qu'on peut choisir un entier n et des vecteurs $v_1, \cdots, v_n$ 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 $K \overset{y \,\longmapsto\, xy}{\longmapsto} K$ est 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 σ l'automorphisme du corps $\mathbb{Q}[\sqrt{D}]$ défini par $\mathbb{Q}[\sqrt{D}] \overset{a+b\sqrt{D} \,\longmapsto\, a-b\sqrt{D}}{\longmapsto} \mathbb{Q}[\sqrt{D}]$.

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

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

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

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

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

[S]

4. Un calcul analytique de τ_n

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

$$f_k : \begin{array}{ccc} [0\,,\,1] & \longmapsto & \mathbb{C} \\ t & \longmapsto & \exp\left(\frac{2i\pi(k+t)^2}{n}\right) \end{array} \qquad \text{et} \qquad f = \sum_{k=0}^{n} f_k\,.$$

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

[S]

4.2. Montrer que la fonction de $\mathbb{R}_+$ dans $\mathbb{C}$ $x \longmapsto \displaystyle\int_{-x}^{x} \mathrm{e}^{\frac{2i\pi t^2}{n}}\,\mathrm{d}t$ admet une limite I_n quand $x \to +\infty$. [S]

4.3. Montrer que $\tau_n + f\left(\dfrac{1}{2}\right) = 2I_n$. [S]

4.4. Comparer I_n et I_1. [S]

4.5. Montrer la formule $\tau_n = \dfrac{1+i^{-n}}{1+i^{-1}}\sqrt{n}$. [S]

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

5. Un calcul algébrique de τ_n

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

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

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]

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

5.2. Montrer que φ 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 φ.

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 $-\sqrt{n}$ dans le polynôme caractéristique de φ.

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

5.5. Calculer Dét φ. [S]

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

(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

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

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 $\Phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \longmapsto \mathbb{Z}/pq\mathbb{Z}$ 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 Φ est bijective.

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

6.6. Montrer la formule

$$\tau_{pq} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\tau_p\tau_q\,. \quad [\text{S}] \tag{2}$$

6.7. Déduire 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

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}\,. \quad [\text{S}]$$

♦ ♦
♦

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

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

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

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

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 ζ. 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 ζ n'est pas nul et la condition *(i)* est vérifiée. [Q]

2.2. Supposons la condition *(i)* vérifiée : il existe une famille $(a_1\,,\,a_2\,,\,\ldots\,,\,a_p) \in \mathbb{Z}^p$ telle que $f^p = \displaystyle\sum_{k=1}^{p} a_k f^{p-k}$. Considérons alors une famille génératrice $(g_1\,,\,g_2\,,\,\ldots\,,\,g_q)$ du $\mathbb{Q}$-espace de type fini V et posons $v_{i(p-k+1)} = f^{p-k}(g_i)$ pour tout $(k\,,\,i) \in [\![\,1\,,\,p\,]\!] \times [\![\,1\,,\,q\,]\!]$. Par construction, la famille $(v_1\,,\,v_2\,,\,\ldots\,,\,v_{pq})$ est génératrice de V et vérifie $f(v_j) \in \displaystyle\sum_{r=1}^{pq} \mathbb{Z}v_r$ pour tout $j \in [\![\,1\,,\,pq\,]\!]$. La condition *(ii)* est alors vérifiée.
Réciproquement, supposons la condition *(ii)* est vérifiée : on peut trouver une famille $(v_1\,,\,v_2\,,\,\ldots\,,\,v_n)$ génératrice de V et une matrice $A \in \mathcal{M}_n(\mathbb{Z})$ telle que $f(v_j) = \displaystyle\sum_{i=1}^{n} a_{ij} v_i$ pour tout $j \in [\![\,1\,,\,n\,]\!]$. Le théorème de Cayley-Hamilton permet d'affirmer que le polynôme caractéristique χ_A est un polynôme annulateur de A. En actionnant la matrice $\widetilde{\chi}_A(A)$ sur les vecteurs colonnes canoniques de Q^n on obtient $\widetilde{\chi}_A(f)(v_j) = O_V$ pour tout

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

$j \in [\![1\,,\,n]\!]$. L'endomorphisme $\widetilde{\chi}_A(f)$ de V s'annule sur une famille génératrice de V : c'est donc l'endomorphisme nul. Ainsi χ_A est un polynôme unitaire annulateur de f et par construction $\chi_A \in \mathbb{Z}[X]$. Donc *(ii)* $\Longrightarrow$ *(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 $f\circ g(v_i) = g\circ f(v_i) \in \sum_j \mathbb{Z}f(u_j)$ 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 $g(x+iy) = \dfrac{1+i}{2}(x+y)$ $(x\,,\,y) \in \mathbb{Q}^2$ donne deux projecteurs,donc des endomorphismes entiers de V tels que le composé $f\circ g$ défini par $f\circ g(x+iy) = \dfrac{x+y}{2}$ 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 $x = \dfrac{m}{n}$ 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 σ 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 σ (on vérifie sans difficulté que σ est bien un automorphisme de corps). [Q]

3.2. Soit $D' \in \mathbb{Q}^*$ et σ' 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 $\dfrac{D'}{D} = b^2$ est un carré dans $\mathbb{Q}$.

Réciproquement si $\dfrac{D'}{D}$ est le carré d'un rationnel b on a $\dfrac{\sqrt{D'}}{\sqrt{D}} = \pm b \neq 0$ 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]

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

3.3. Écrivons $d = \dfrac{m}{n}$ 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 $\dfrac{D}{d}$ 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 $\dfrac{d'}{d} = \dfrac{a^2}{b^2}$ 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 $0 = \sigma\big(\widetilde{P}(x)\big) = \widetilde{P}\big(\sigma(x)\big)$, 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 $b = \dfrac{p}{q}$, $(p\,,\,q) \in \mathbb{Z}^2$ et $p \wedge q = 1$, on observe que q^2divise $4p^2d$ et comme $q^2 \wedge p^2 = 1$, q^2 divise $4d$. Puisque d est sans facteur carré, $|q| \leqslant 2$ donc $2b = b' \in \mathbb{Z}$. Ainsi $a'^2 - b'^2d = 4x\sigma(x) \equiv 0 \quad [4]$. 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 : $a = \dfrac{a'}{2} = u + \dfrac{1}{2}$ avec $u \in \mathbb{Z}$ et de même $b = v + \dfrac{1}{2}$ avec $v \in \mathbb{Z}$. Dans ce cas $a'^2 - b'^2d \equiv 1 - d \equiv 0 \quad [4]$ et en posant $\omega = \dfrac{1+\sqrt{d}}{2}$ on a $x = (u-v) + (2v+1)\omega \in \mathbb{Z}[\omega]$. Inversement, lorsque $d \equiv 1 \quad [4]$, $d = 1 - 4d'$ avec $d' \in \mathbb{Z}$ et $\omega\sigma(\omega) = \dfrac{1-d}{4} = d' \in \mathbb{Z}$ 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 $\omega = \dfrac{1+\sqrt{d}}{2}$ 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 $\varphi : \mathbb{Z}^2 \longmapsto \mathcal{O}_K = \mathbb{Z}[\omega]$ définie par $\varphi(p\,,\,q) = p + q\omega$ est alors un isomorphisme de groupes additifs. [Q]

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

4. Un calcul analytique de τ_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 :

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

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

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

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

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

[Q]

4.3. Par la relation de Chasles

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

À nouveau par la relation de Chasles

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

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

Il en résulte que $\tau_n+f\left(\dfrac{1}{2}\right)=2I_n$. [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 $x\to+\infty$ donnent directement $I_n=\sqrt{n}\,I_1$. On a directement $\tau_1=1$ et lorsque $n=1$, $f\left(\dfrac{1}{2}\right)=f_0\left(\dfrac{1}{2}\right)=\mathrm{e}^{\frac{i\pi}{2}}=i$. Donc $2I_n=\sqrt{n}\,2I_1=\sqrt{n}\,(1+i)$. [Q]

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

4.5. Distinguons deux cas selon la parité de n.

- Cas où $n=2p$: $\tau_n=\sum_{k=0}^{n-1}\mathrm{e}^{\frac{2i\pi k^2}{n}}=\sum_{k=0}^{p-1}\mathrm{e}^{\frac{i\pi k^2}{p}}+\sum_{k=0}^{p-1}\mathrm{e}^{\frac{i\pi(k+p)^2}{p}}=\left(1+(-1)^p\right)\sum_{k=0}^{p-1}\mathrm{e}^{\frac{i\pi k^2}{p}}$. De même $f\left(\frac{1}{2}\right)=\sum_{k=0}^{n-1}\mathrm{e}^{\frac{i\pi(2k+1)^2}{2n}}=\sum_{k=0}^{p-1}\mathrm{e}^{\frac{i\pi(2k+1)^2}{4p}}+\sum_{k=0}^{p-1}\mathrm{e}^{\frac{i\pi(2k+1+2p)^2}{4p}}=\left(1-(-1)^p\right)\sum_{k=0}^{p-1}\mathrm{e}^{\frac{i\pi(2k+1)^2}{4p}}$.
  Donc si $n\equiv 2\ [4]$, $\tau_n=0$ et si $n\equiv 0\ [4]$, $f\left(\frac{1}{2}\right)=0$ et $\tau_n=\sqrt{n}\,(1+i)$.
- Cas où $n=2p+1$: $\tau_n=\sum_{k=0}^{n-1}\mathrm{e}^{\frac{2i\pi k^2}{n}}=1+\sum_{k=1}^{p}\mathrm{e}^{\frac{2i\pi k^2}{n}}+\sum_{k=1}^{p}\mathrm{e}^{\frac{2i\pi(n-k)^2}{n}}=1+2\sum_{k=1}^{p}\mathrm{e}^{\frac{2i\pi k^2}{n}}$.
  $f\left(\frac{1}{2}\right)=\sum_{k=0}^{n-1}\mathrm{e}^{\frac{i\pi(2k+1)^2}{2n}}=\sum_{k=1}^{p}\mathrm{e}^{\frac{i\pi(n-2k)^2}{2n}}+i^n+\sum_{k=1}^{p}\mathrm{e}^{\frac{i\pi(n+2k)^2}{2n}}=i^n\left(1+2\sum_{k=1}^{p}\mathrm{e}^{\frac{2i\pi k^2}{n}}\right)=i^n\tau_n$.
  Alors $\tau_n+f\left(\frac{1}{2}\right)=\tau_n(1+i^n)=\sqrt{n}\,(1+i)$. Ainsi $\tau_n=\sqrt{n}\,\dfrac{1+i}{1+i^n}=\begin{cases}\sqrt{n} & \text{si } n\equiv 1\ [4],\\ i\sqrt{n} & \text{si } n\equiv 3\ [4].\end{cases}$
  En remarquant que $\dfrac{1+i}{1+i^n}=\dfrac{1+i^{-n}}{1+i^{-1}}$ on observe que la formule $\tau_n=\sqrt{n}\,\dfrac{1+i^{-n}}{1+i^{-1}}$ 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 $d\equiv 1\ [4]$, alors $\sqrt{d}=\tau_d\in\mathbb{Q}[\zeta]$ où $\zeta=\mathrm{e}^{\frac{2i\pi}{d}}$ 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 $\zeta'=\mathrm{e}^{\frac{i\pi}{2d}}$ est une racine de l'unité et alors $\mathbb{Q}[i\sqrt{d}]\subset\mathbb{Q}[\zeta']$.
- Si $d\equiv 3\ [4]$, on obtient les inclusions $\mathbb{Q}[\sqrt{d}]\subset\mathbb{Q}[\zeta']$ et $\mathbb{Q}[i\sqrt{d}]\subset\mathbb{Q}[\zeta]$.
- Si $d\equiv 2\ [4]$, alors $d=2(2p+1)$ et par l'un des deux cas précédents, il existe une racine de l'unité $\zeta=\mathrm{e}^{\frac{2i\pi}{n}}$ telle que $\sqrt{2p+1}\in\mathbb{Q}[\zeta]$. Comme $\sqrt{2}\in\mathbb{Q}[\mathrm{e}^{\frac{i\pi}{4}}]$ et $i\sqrt{2}\in\mathbb{Q}[\mathrm{e}^{\frac{i\pi}{4}}]$ les nombres $\sqrt{d}$ et $i\sqrt{d}$ appartiennent à $\mathbb{Q}[\zeta']$ où $\zeta'=\mathrm{e}^{\frac{2i\pi}{n'}}$ 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 ζ telle que $K\subset\mathbb{Q}[\zeta]$. [Q]

5. Un calcul algébrique de τ_n

5.1. $\varphi^2(f)(x)=\sum_{y\in\mathbb{Z}/n\mathbb{Z}}\varphi(f)(y)\zeta^{xy}=\sum_{(y,z)\in\left(\mathbb{Z}/n\mathbb{Z}\right)^2}f(z)\zeta^{zy}\zeta^{xy}=\sum_{z\in\mathbb{Z}/n\mathbb{Z}}f(z)\sum_{y\in\mathbb{Z}/n\mathbb{Z}}(\zeta^{(z+x)})^y$. Or pour toute racine n^{e} de l'unité $\xi\neq 1$, $\sum_{y\in\mathbb{Z}/n\mathbb{Z}}\xi^y=\dfrac{1-\xi^n}{1-\xi}=0$, donc $\varphi^2(f)(x)=n\,f(-x)$.

[Q]

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

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

5.3. $|\tau_n|^2 = \tau_n\overline{\tau_n} = \sum_{(x,y)\in\left(\mathbb{Z}/n\mathbb{Z}\right)^2} \zeta^{x^2}\zeta^{-y^2} = \sum_{(x,y)\in\left(\mathbb{Z}/n\mathbb{Z}\right)^2} \zeta^{(x-y)(x+y)}$. Comme on suppose n impair, 2 est inversible dans $\mathbb{Z}/n\mathbb{Z}$ donc on réalise une bijection de $\left(\mathbb{Z}/n\mathbb{Z}\right)^2$ sur lui même en posant $\begin{cases} u = x-y \\ v = x+y \end{cases}$ $\begin{cases} x = \dfrac{u+v}{2} \\ y = \dfrac{-u+v}{2} \end{cases}$ On a donc $|\tau_n|^2 = \sum_{(u,v)\in\left(\mathbb{Z}/n\mathbb{Z}\right)^2} \zeta^{uv}$. Or on a vu que si $\zeta^u \neq 1$ la somme $\sum_{v\in\mathbb{Z}/n\mathbb{Z}} \left(\zeta^u\right)^v$ est nulle. Donc $|\tau_n|^2 = n$ et $|\tau_n| = \sqrt{n}$. [Q]

5.4. La trace de φ est la somme de ses valeurs propres répétées avec leur multiplicité. Donc $\tau_n = \sqrt{n}\big(a-b+i(c-d)\big)$ 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 φ^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 $\dfrac{n-1}{2}$. On en conclut que $c+d = \dfrac{n-1}{2}$ et $a+b = n-(c+d) = \dfrac{n+1}{2}$. [Q]

5.5. La matrice de φ relativement à la base canonique de V est $M = \left(\zeta^{pq}\right)_{(p,q)\in[\![0\,,n-1]\!]^2}$. Le déterminant de φ est donc le déterminant de Van der Monde associé à la famille $(1\,,\zeta\,,\cdots,\zeta^{n-1})$. Ainsi $\operatorname{Dét}\varphi = \prod_{0\leqslant p<q<n} (\zeta^q-\zeta^p)$. Il y a C_n^2 facteurs dans ce produit chaque facteur ayant pour argument $\dfrac{\pi}{2}+\dfrac{(p+q)\pi}{n}$. Un calcul simple donne

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

et comme $(n-1)^2$ est multiple de 4, $\dfrac{\pi}{n}\sum_{0\leqslant p<q<n}(p+q) \equiv 0 \quad [2\pi]$. Il en résulte que $\operatorname{Dét}\varphi = i^{\frac{n(n-1)}{2}}n^{\frac{n}{2}}$. [Q]

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

- $a = b = \dfrac{n+1}{4}$ et $c-d = \pm 1$, auquel cas $n \equiv -1 \quad [4]$. 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 $c+d = \dfrac{n-1}{2}$ il vient $a = b = c = \dfrac{n+1}{4}$ et $d = \dfrac{n-3}{4}$. Dans ce cas $\tau_n = \sqrt{n}\big(a-b+i(c-d)\big) = i\sqrt{n}$.
- $c = d = \dfrac{n-1}{4}$ et $a-b = \pm 1$, auquel cas $n \equiv 1 \quad [4]$. 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 $a+b = \dfrac{n+1}{2}$ donne

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

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

6. Réciprocité quadratique

6.1. Soit $x\in\mathcal{O}_L\cap K$. L'endomorphisme $m_{x,L}=x\,\mathrm{Id}_L$ 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 $m_{x,K}=x\,\mathrm{Id}_K$ de $m_{x,L}$ à K donc $x\in\mathcal{O}_K$.
Réciproquement soit $x\in\mathcal{O}_K$. Le polynôme unitaire $P_x=X^2-\big(x+\sigma(x)\big)X+x\sigma(x)$ est à coefficients entiers d'après 3.5 et comme $\widetilde{P}_x(m_{x,L})=\widetilde{P}_x(x)\,\mathrm{Id}_L$, la relation $\widetilde{P}(x)=0$ 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 $\zeta=\mathrm{e}^{\frac{2i\pi}{p}}$. On a $\tau_p=\sum_{k=1}^{p}\zeta^{k^2}$ donc $\tau_p^q=\sum_{n_1+\cdots+n_p=q}\dfrac{q!}{n_1!\cdots n_p!}\prod_{k=1}^{p}\zeta^{k^2n_k}$. Dans cette somme tous les coefficients $\dfrac{q!}{n_1!\cdots n_p!}$ 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 ζ sont éléments de l'anneau $\mathcal{O}_L$, on en déduit que $\tau_p^q-\sum_{k=1}^{p}\zeta^{k^2q}\in q\mathcal{O}_L$. Par ailleurs l'application $x\longmapsto x^2q$ de $\mathbb{Z}/p\mathbb{Z}$ dans lui même induit une permutation de l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ si $\left(\dfrac{q}{p}\right)=1$ et induit une bijection de l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ sur son complémentaire si $\left(\dfrac{q}{p}\right)=-1$. Comme la somme des racines p^{e} de l'unité est nulle, il vient $\sum_{k=1}^{p}\zeta^{k^2q}=\left(\dfrac{q}{p}\right)\sum_{k=1}^{p}\zeta^{k^2}=\left(\dfrac{q}{p}\right)\tau_p$. On en conclut que $\tau_p^q-\left(\dfrac{q}{p}\right)\tau_p\in q\mathcal{O}_L\cap K=q\mathcal{O}_K$. [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 $\omega\in\left\{\tau_p\,,\,\dfrac{1+\tau_p}{2}\right\}$ (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, $\tau_p^q-\left(\dfrac{q}{p}\right)\tau_p=n\tau_p$ avec $n=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}-\left(\dfrac{q}{p}\right)$. Or par 6.2 et 6.3, $n\equiv 0\ \ [q]$ et par 1.2, $p^{\frac{q-1}{2}}\equiv\left(\dfrac{p}{q}\right)\ \ [q]$, donc $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\dfrac{p}{q}\right)\equiv\left(\dfrac{q}{p}\right)\ \ [q]$. Il s'agit là d'une congruence modulo q entre entiers relatifs égaux à ±1 et $q>2$: on a donc une égalité, que l'on peut écrire sous la forme $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. [Q]

©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

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 $\Phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \longmapsto \mathbb{Z}/pq\mathbb{Z}$ 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 Φ est donc surjective, et comme la source et le but de Φ ont le même cardinal pq, Φ est bijective. [Q]

6.6. Grâce à la bijection Φ précédente on a

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

On a déjà vu en 6.2 pourquoi $\displaystyle\sum_{X\in\mathbb{Z}/p\mathbb{Z}} \mathrm{e}^{\frac{2i\pi qX^2}{p}} = \left(\frac{q}{p}\right)\tau_p$ si bien que $\tau_{pq} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\tau_p\tau_q$.

[Q]

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

– Ou bien p et $q \equiv 1 \quad [4]$: alors $\tau_{pq} = \sqrt{pq} = \tau_p\tau_q$ (cf 5.6) et $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ (cf 6.6).

– Ou bien p et $q \equiv 3 \quad [4]$: alors $\tau_{pq} = \sqrt{pq} = -\tau_p\tau_q$ (cf 5.6) et $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ (cf 6.6).

• Supposons $\dfrac{p-1}{2}$ et $\dfrac{q-1}{2}$ de parité contraire : alors $pq \equiv 3 \quad [4]$ et $\tau_{pq} = i\sqrt{pq} = i\tau_p\tau_q$ (cf 5.6) donc $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ (cf 6.6).

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

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

• Si $q \equiv 1 \quad [4]$, 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 $2^{\frac{q-1}{2}}(-1)^{\frac{q-1}{4}} \equiv 1 \quad [q]$, et comme $2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \quad [q]$, on a $\left(\frac{2}{q}\right) = (-1)^{\frac{q-1}{4}}$ avec $\dfrac{q+1}{2}$ impair. Donc $\left(\frac{2}{q}\right) = (-1)^{\frac{q-1}{4}\,\frac{q+1}{2}} = (-1)^{\frac{q^2-1}{8}}$.

• Si $q \equiv -1 \quad [4]$, 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 $\left(\frac{2}{q}\right) = (-1)^{\frac{q+1}{4}}$ avec $\dfrac{q-1}{2}$ impair. Donc $\left(\frac{2}{q}\right) = (-1)^{\frac{q+1}{4}\,\frac{q-1}{2}} = (-1)^{\frac{q^2-1}{8}}$.

 ©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021

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

♦ ♦
♦

 ©EduKlub S.A.
Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Fichier généré pour Visiteur (), le 31/05/2021