Devoir sur table n^o 4

8/11/2023, 13h45–17h45

Avertissement. Le candidat peut utiliser les résultats énoncés dans les questions ou parties précédentes. Chaque partie est d'ailleurs largement indépendante des précédentes, une fois admis les résultats qui y sont démontrés. La partie Préliminaires n'est utilisée que dans la partie iv.

Définitions et notations. Soient $\zeta \in \mathbb{C}$ et $\mathcal{F}_\zeta = \{\zeta^n \mid n \in \mathbb{N}\}$.

— On note : $\mathbb{Q}[\zeta] = \{P(\zeta) \mid P \in \mathbb{Q}[X]\}$ le $\mathbb{Q}$-espace vectoriel engendré par $\mathcal{F}_\zeta$: c'est une $\mathbb{Q}$-algèbre.

— On note : $\mathbb{Z}[\zeta] = \{P(\zeta) \mid P \in \mathbb{Z}[X]\}$ le sous-groupe additif de $\mathbb{Q}[\zeta]$ engendré par $\mathcal{F}_\zeta$.

— Un sous-corps de $\mathbb{C}$ de dimension finie (vu comme $\mathbb{Q}$-espace vectoriel) est appelé un *corps de nombres*.

— Soit K un corps de nombres, muni de sa structure de $\mathbb{Q}$-espace vectoriel de dimension finie. On rappelle que si $f \in \mathrm{L}(K)$ alors, pour tout $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Q}[X]$, on a : $P(f) = \sum_{i=0}^{d} a_i f^i$, où $f^0 = \mathrm{Id}_K$ et f^i désigne $f \circ \cdots \circ f$ (composée i fois) pour tout $i \in \mathbb{N}\backslash\{0\}$. On dit que P *annule* f si : $P(f) = 0_{\mathrm{L}(K)}$.

— Si $v_1, \ldots, v_n$ sont des éléments de K, on note $\sum_{i=1}^{n} \mathbb{Z}v_i$ le sous-groupe additif de K engendré par les v_i.

— On dit que $x \in K$ est un *entier algébrique* s'il existe un polynôme $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$.

— On note $\mathcal{O}_K$ l'ensemble des éléments de K qui sont des entiers algébriques.

— Pour tout $x \in K$, on note $m_x : \begin{cases} K & \to & K \\ y & \mapsto & xy \end{cases}$ l'endomorphisme de multiplication par x.

— Soient n et k deux entiers. On suppose n non nul. 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 : $\zeta = \zeta_n = \exp\left(\frac{2i\pi}{n}\right)$, on notera τ_n la somme : $\tau_n = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} (\zeta_n)^{x^2}$.

Préliminaires

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

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

   Indication : regrouper deux à deux dans le produit les termes de la forme x et yx^{-1}, pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

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

Première partie – Généralités

3. Soit $\zeta \in \mathbb{C}$. Montrer que les deux propositions suivantes sont équivalentes :
   (i) Il existe un polynôme P unitaire à coefficients rationnels ayant ζ pour racine ;
   (ii) La $\mathbb{Q}$-algèbre $\mathbb{Q}[\zeta]$ est un corps de nombres.

4. Soient K un corps de nombres et $x \in K$. Montrer que les propositions suivantes sont équivalentes :
   (i) L'élément x est un entier algébrique ;
   (ii) Il existe un polynôme P unitaire à coefficients entiers annulant m_x ;
   (iii) Il existe un entier naturel n et une famille $\mathbb{Q}$-génératrice de K, notée $(v_1, \ldots, v_n)$, tels que :

$$m_x\left(\sum_{i=1}^{n} \mathbb{Z}v_i\right) \subseteq \sum_{i=1}^{n} \mathbb{Z}v_i.$$

   Indication pour (iii) $\Rightarrow$ (i) : on pourra introduire des coefficients $a_{i,j}$ tels que : $\forall j \in [\![1, n]\!]$, $xv_j = \sum_{i=1}^{n} a_{i,j} v_i$, et considérer le déterminant du système obtenu.

5. Montrer que si x et y sont des entiers algébriques, alors $x+y$ et xy sont des entiers algébriques.
Indication : on pourra montrer qu'on peut choisir un entier n, et des vecteurs $v_1, \dots, v_n$ comme dans la question précédente, qui conviennent à la fois pour m_x et m_y.

Ainsi $\mathcal{O}_K$ est un sous-anneau de K, appelé *l'anneau des entiers algébriques de K*.

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

Deuxième partie – Entiers des corps quadratiques

Soit $D \in \mathbb{Q}$ qui n'est pas le carré d'un rationnel. Si D est négatif, on notera $\sqrt{D}$ le complexe $i\sqrt{-D}$. Un corps de la forme $\mathbb{Q}[\sqrt{D}]$ (avec D non carré) est dit *corps quadratique*. On remarque que $(1, \sqrt{D})$ est une $\mathbb{Q}$-base de $\mathbb{Q}[\sqrt{D}]$.

On note σ l'isomorphisme de corps $\sigma : \begin{cases} \mathbb{Q}[\sqrt{D}] & \to & \mathbb{Q}[\sqrt{D}] \\ a+b\sqrt{D} & \mapsto & a-b\sqrt{D} \end{cases}$ (dans cette définition : $(a,b) \in \mathbb{Q}^2$).

7. Montrer que les seuls isomorphismes de corps de $\mathbb{Q}[\sqrt{D}]$ dans lui-même sont l'identité et σ.
8. Soit $D' \in \mathbb{Q}^*$. Montrer :

$$\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}] \iff \exists r \in \mathbb{Q}^*,\ D = r^2 D'.$$

9. Montrer qu'il existe un unique $d \in \mathbb{Z}$ *sans facteur carré* (c'est-à-dire, si n^2 divise d avec $n \in \mathbb{N} \setminus \{0\}$, alors : $n = 1$) tel que : $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{d}]$.
10. Soit K un sous-corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$. Montrer que K est un corps quadratique.

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

11. Soit $x \in K$. Montrer que $x \in \mathcal{O}_K$ si et seulement si :

$$\begin{cases} x + \sigma(x) \in \mathbb{Z}, \\ x\sigma(x) \in \mathbb{Z}. \end{cases}$$

12. Soit $\omega \in K$ défini par :

$$\omega = \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4, \\ \sqrt{d} & \text{sinon.} \end{cases}$$

Montrer :

$$\mathcal{O}_K = \left\{ x + y\omega \mid (x,y) \in \mathbb{Z}^2 \right\} = \mathbb{Z}[\omega].$$

Troisième partie – Calcul de τ_n

Soient $n \in \mathbb{N} \setminus \{0,1\}$ un entier impair et ζ_n le nombre complexe défini par : $\zeta_n = \exp\left(\frac{2i\pi}{n}\right)$.

13. Montrer : $|\tau_n|^2 = n$.

On cherche à calculer τ_n. Soit V le $\mathbb{C}$-espace vectoriel des fonctions de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$. Soit φ l'endomorphisme de V qui à la fonction f associe la fonction $\varphi(f)$ définie par :

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

14. Montrer que V est de dimension n et en expliciter une base simple. L'utiliser pour en déduire que τ_n est la trace de φ.
15. Montrer :

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

16. En déduire :
$$V = \ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right) \oplus \ker\left(\frac{1}{n}\varphi^2 + \mathrm{Id}_V\right).$$

17. Montrer qu'il existe une base $\mathcal{B}$ de V telle que la matrice représentative de φ dans la base $\mathcal{B}$ soit diagonale, de coefficients diagonaux $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$ et $-i\sqrt{n}$.
Indication : étudier la nature de la restriction de $\frac{1}{\sqrt{n}}\varphi$ à $\ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)$.

Soient a, b, c, d les fréquences d'apparition, respectivement, de $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$ et $-i\sqrt{n}$ sur la diagonale de la matrice trouvée à la question 17.

18. Montrer les égalités :
$$a+b = \frac{n+1}{2}, \qquad c+d = \frac{n-1}{2}, \qquad \text{et :} \qquad (a-b)^2 + (c-d)^2 = 1.$$

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

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

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

Quatrième partie – Réciprocité quadratique

On considère deux nombres premiers impairs distincts p et q.

On note $\left(\frac{q}{p}\right)$ l'entier qui vaut 1 si la classe q modulo p est un carré et -1 sinon. On se propose de montrer la formule :
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \qquad (*)$$

22. Montrer :
$$\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{qx^2} = \left(\frac{q}{p}\right)\tau_p.$$

23. Montrer que l'application :
$$\phi : \begin{cases} \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/pq\mathbb{Z} \\ (x \bmod q, y \bmod p) & \mapsto & (xp+yq) \bmod pq \end{cases}$$
est correctement définie et est bijective.

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

25. Montrer l'égalité $(*)$. *Utiliser la question 20.*

L'objectif des deux prochaines questions est de traiter le cas $p = 2$. On pose désormais : $K = \mathbb{Q}[i]$.

26. Montrer qu'il existe $x \in \mathcal{O}_K$ tel que :
$$(1+i)^q = 1 + i^q + qx.$$

27. Exprimer $(1+i)^q$ en fonction de $2^{\frac{q-1}{2}}$ et en déduire : $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$.

Nous donnons deux applications de ces résultats.

28. Déterminer si 101 est un carré dans $(\mathbb{Z}/691\mathbb{Z})^\times$ (on admet que 101 et 691 sont des nombres premiers).

On admet le résultat difficile suivant :

Théorème de la progression arithmétique. Étant donnés des entiers a et b non nuls premiers entre eux, l'ensemble $\{ak+b \mid k \in \mathbb{Z}\}$ contient une infinité de nombres premiers.

29. Soit $n \in \mathbb{Z}$. Soit S un ensemble fini de nombres premiers. On suppose que pour tout nombre premier $\ell \notin S$, la classe de n modulo ℓ est un carré dans $\mathbb{Z}/\ell\mathbb{Z}$. Montrer que n est le carré d'un entier.