Concours Agrégation, Mathématiques générales

Leçon 02- Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications

Commentaires du jury 2015 :

Cette leçon est encore abordée de façon élémentaire sans réellement expliquer où et comment les nombres complexes de modules 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques (polynômes cyclotomiques, spectre de matrices remarquables, théorie des représentations). Il ne faut pas non plus oublier la partie "groupe" de la leçon : on pourra s'intéresser au relèvement du groupe unité au groupe additif des réels et aux propriétés qui en résultent (par exemple l'alternative " sous-groupes denses versus sous-groupes monogènes "). On pourra aussi s'intéresser aux groupes des nombres complexes de $\mathbb{Q}(i)$, et les racines de l'unité qui y appartiennent.

Commentaires du jury 2016 :

Il ne faut pas uniquement aborder cette leçon de façon élémentaire sans réellement expliquer où et comment les nombres complexes de modules 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques (exponentielle complexe et ses applications, polynômes cyclotomiques, spectre de matrices remarquables, théorie des représentations). Il ne faut pas non plus oublier la partie « groupe » de la leçon : on pourra s'intéresser au relèvement du groupe unité au groupe additif des réels et aux propriétés qui en résultent. De même les sous-groupes finis de S^1 sont intéressants à considérer dans cette leçon. On pourra aussi s'intéresser aux groupes des nombres complexes de $\mathbb{Q}(i)$, et les racines de l'unité qui y appartiennent ; tout comme aux sous-groupes compacts de $\mathbb{C}^\star$.

Remarque : Notez le lien avec la nouvelle leçon 10 « Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications » ref. [F. M. 1] p. 230 à 238

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2'] Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A.] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. B.C.D.] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)
[Fr. E.] Fresnel J. *Groupes* (Hermann 2001)
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)

Développements conseillés :

(1) Caractères d'un groupe abélien fini, [Fr. A.] p 61 à 65 et [F. M. 1] n° 82 paragraphe 14 p. 230) et applications aux sommes de Gauss [F. M. 1] n° 104 par. 6.1. p 286

(2) Les homomorphismes continus de $(\mathbb{R}, +)$ dans U. Les sous-groupes de U. Les endomorphismes continus de U, [Fr. B.C.D.] p. 78-79 , 84-88

(3) Irréductibilité du polynôme cyclotomique, [Fr. F.] p. 280

(4) Groupe des automorphismes de l'extension $\mathbb{Q}(e^{\frac{2i\pi}{n}})/\mathbb{Q}$, et construction à la règle et au compas du polygone régulier à n côtés [F. M. 1] n° 104 (théorème de Gauss) et [F. M. 1] errata p.282

(5) Le groupe $U(K) := \{z \in K \mid |z| = 1\}$ pour K un sous-corps de $\mathbb{C}$, [F. M. 2] IV.8.1 p.246 à 248 et exercices ci-dessous.

Exercice 0 Sur les angles d'un triangle [F. M. 1] n° 121 paragraphe B p. 351

Exercice 1 L'inégalité triangulaire et une application.

L'inégalité triangulaire. Soient $z, z' \in \mathbb{C}$.

(1) Montrer que $||z| - |z'|| \leq |z + z'| \leq |z| + |z'|$

Preuve. On peut supposer que $z \neq 0$, alors $\frac{z'}{z} = \rho e^{it}$ avec $\rho > 0$ et $0 \leq t < 2\pi$. Alors $|1 + \rho e^{it}|^2 = 1 + 2\rho cost + \rho^2$ et les inégalité sont conséquences de $-1 \leq cost \leq 1$.///

(2) Montrer que z et z' sont $\mathbb{R}$ linéairement dépendants si et seulement si $|z+z'| = |z|+|z'|$ ou $|z+z'| = ||z| - |z'||$.

Preuve. On peut encore supposer que $z \neq 0$ et que $\frac{z'}{z} = \rho e^{it}$ avec $\rho > 0$ et $0 \leq t < 2\pi$. Alors z et z' sont $\mathbb{R}$ linéairement dépendants si et seulement $t = 0$ ou π i.e. $cost = 1$ ou -1.///

(3) Soient $(z_i)_{1 \leq i \leq n} \in \mathbb{C}^n$ avec $|z_i| = 1$. A quelle condition a-t-on $\sum_{1 \leq i \leq n} z_i = n$?

Preuve. Si $n = 1$ la condition est $z_1 = 1$. On examine ensuite le cas $n = 2$ on est alors en présence d'un cas d'égalité dans l'inégalité triangulaire ainsi la CNS est que $z_2 = z_1$ (on a $\rho = 1$ puisque $|z_1| = |z_2|$) et donc que $z_2 = z_1 = 1$. On montre alors le résultat général par récurrence sur n. Supposons donc que $\sum_{1 \leq i \leq n+1} z_i = n + 1$ avec $|z_i| = 1$. Soit $z' = \sum_{1 \leq i \leq n} z_i$ et $z = z_{n+1}$ alors $|z'| \leq n$, ainsi $n + 1 = |z + z'| \leq |z| + |z'| \leq n + 1$ et donc z et z' sont colinéaires et $z' = nz$ et donc z_{n+1} et $\sum_{1 \leq i \leq n} z_i = n$. On conclut avec l'hypothèse de récurrence.///

(4) *Application 1.*

Sous-groupes distingués et représentations linéaires, [F. M. 2] p.166 lemme 2.2.

(5) *Application 2.*

Rappel. Un élément $z \in \mathbb{C}$ est un entier algébrique si il existe $P \in \mathbb{Z}[X]$ unitaire avec $P(z) = 0$. Par le lemme de Gauss on peut alors supposer que P est irréductible. Un élément $z' \in \mathbb{C}$ est dit conjugué de z si il existe un $\mathbb{Q}$-endomorphisme injectif σ de $\mathbb{C}$ dans $\mathbb{C}$ avec $\sigma(z) = z'$. Les conjugués de z sont aussi les racines du polynôme minimal de z dans $\mathbb{Q}[z]$.

Soient $\lambda_1, ..., \lambda_n \in \mathbb{C}$ des racines de l'unité. On suppose que $(\lambda_1 + ... + \lambda_n)/n$ est un entier algébrique, alors, soit $\lambda_1 + ... + \lambda_n = 0$, soit tous les λ_i sont égaux.

Preuve. Si λ est une racine de l'unité, c'est un zéro d'un polynôme de la forme $x^m - 1 = 0$ il suit que les conjugués de λ sont des racines de l'unité. Soit $z := (\lambda_1 + ... + \lambda_n)/n$; alors z est un entier algébrique par hypothèse et donc un conjugué z' de z s'écrit $(\lambda'_1 + ... + \lambda'_n)/n$ où les λ'_i sont des racines de l'unité. Donc $|z'| \leq 1$. Notons Z le produit de tous les conjugués de z. Alors $|Z| \leq 1$. D'autre part Z est rationnel (c'est le terme constant, au signe près, du polynôme minimal de z). Enfin Z est entier algébrique (comme produit d'entiers algébriques) donc $Z \in \mathbb{Z}$. Si $Z = 0$, l'un des conjugués de z est nul donc $z = 0$; si $|Z| = 1$, tous les conjugués de z ont 1 comme module, donc $|z| = 1$ et tous les λ_i sont égaux, puisque leur somme est de module n par la question (3).

Exercice 2 Polynômes caractéristiques des endomorphismes orthogonaux, unitaires, [Fr. B.C.D.] p. 89 et 255.

Application 1. Deux matrices de $O_n(\mathbb{R})$ sont orthogonalement semblables si et seulement si elles ont le même polynôme caractéristique.

Application 2. Un sous-groupe d'exposant fini de $O_n(\mathbb{R})$ est fini, [Fr. B.C.D.] p. 182.

Format exercice corrigé.

On munit $\mathbb{R}^n$ de la structure euclidienne canonique. On note $\|.\|$ la norme euclidienne et on munit $M_n(\mathbb{R})$ de la norme fonctionnelle $\|A\| = \max_{\|x\|=1} \|Ax\|$.

Soit G un sous-groupe de $O_n(\mathbb{R})$ et $N \geq 1$ un entier. On suppose que $U^N = Id$ pour tout $U \in G$.

(1) Rappeler le theorème de réduction des éléments de $O_n(\mathbb{R})$.

Preuve. Soit $O \in O_n(\mathbb{R})$, il existe $P \in O_n(\mathbb{R})$ avec POP^{-1} qui est un tableau diagonal de 1 et de -1 et de matrices de rotations planes de mesure d'angle θ_i avec $0 < \theta_i < \pi$.///

(2) En déduire que $O_n(\mathbb{R})$ a deux composantes connexes (par arcs).

Preuve. Puisque l'application det : $O_n(\mathbb{R}) \to \pm 1$ est continue et surjective il suit que $O_n(\mathbb{R})$ a au moins deux composantes connexes. Montrons que $SO_n(\mathbb{R})$ est connexe par arcs. Soit $O \in SO_n(\mathbb{R})$, puisque $\det O = 1$ il suit qu'il existe $P \in O_n(\mathbb{R})$ avec POP^{-1} un tableau diagonal de 1 et de matrices de rotations planes de mesure d'angle θ_i avec $0 < \theta_i \leq \pi$. Il suffit de considérer alors le même tableau en modifiant les θ_i en $t\theta_i$ avec $0 \leq t \leq 1$ pour obtenir un chemin continu dans $O_n(\mathbb{R})$ de Id à O. Il suit que $SO_n(\mathbb{R})$ et $D(-1)SO_n(\mathbb{R})$ sont les composantes connexes de $O_n(\mathbb{R})$.///

(3) Montrer que $O_n(\mathbb{R})$ est compact.

Preuve. Puisque $M \in M_n(\mathbb{R}) \to M^t M \in M_n(\mathbb{R})$ est continue (les coeff de $M^t M$ sont polynomiaux en ceux de M), il suit que $O_n(\mathbb{R})$ est fermé dans $M_n(\mathbb{R})$. Puisque les colonnes de $O \in O_n(\mathbb{R})$ sont de norme 1 il suit que les coefficients sont en valeur absolue bornés par 1. Ainsi $O_n(\mathbb{R})$ est un fermé borné de l'espace vectoriel normé complet $M_n(\mathbb{R})$ qui est de dimension finie, il est donc compact.///

(4) Montrer que $\|OA\| = \|A\|$ si $A \in M_n(\mathbb{R})$ et $O \in O_n(\mathbb{R})$.

Preuve. Immédiat puisque O est une isométrie (et donc bijective).///

(5) Montrer qu'il existe $\epsilon > 0$ tel que pour tout $U \in G - Id$, on a $\|U - Id\| \geq \epsilon$. En déduire que pour tout $U, U' \in G$ avec $U \neq U'$ on a $\|U - U'\| \geq \epsilon$.

Preuve. Il existe $O \in O_n(\mathbb{R})$ avec OUO^{-1} qui est un tableau diagonal de 1 et de -1 et de matrices de rotations planes d'angle θ_i avec $0 < \theta_i < \pi$. De plus puisque $U^N = Id$ il suit que pour $U \neq Id$ on a même $\frac{2\pi}{N} < \theta_i$. Ainsi puisque $U \in G - Id$, il existe un vecteur colonne X avec $\|X\| = 1$ et $OUO^{-1}X = -2X$ ou $(OUO^{-1} - Id)X = (0, .., 0, -1 + cos\theta_i, -sin\theta_i, 0, .., 0)$. Dans le premier cas on a $\|U - Id\| = \|O(U - Id)O^{-1}\| \geq 2$ et dans le second cas $\|U - Id\| = \|O(U - Id)O^{-1}\| \geq [(-1 + cos\theta_i)^2 + (sin\theta_i)^2]^{1/2} = (2 + 2cos\theta_i) \geq (2 - 2cos\frac{2\pi}{N})^{1/2} =: \epsilon$. On conclut en notant que pour tout $U, U' \in G$ avec $U \neq U'$ on a $\|U - U'\| = \|UU'^{-1} - Id\|$ et $UU'^{-1} \in G - Id$.///

(6) Conclure que G est fini.

Preuve. On recouvre $O_n(\mathbb{R})$ par les boules ouvertes $B(O, \frac{1}{4}\epsilon)$. Par ce qui précède chaque boule contient au plus un élément de G. On conclut avec la compacité de $O_n(\mathbb{R})$.///

Exercice 3 Somme des racines primitives n-ièmes de l'unité, [F. M. 2] question 2. du théorème p.249

Montrer que $S(n) := \sum_{1 \leq k \leq n,\ (n,k)=1} e^{2i\pi\frac{k}{n}} = \mu(n)$ où $\mu(.)$ est la fonction de Mobius. En déduire que $\Phi_n(X) = X^{\varphi(n)} - \mu(n)X^{\varphi(n-1)} + ...$

Preuve : Une propriété caractéristique de la fonction de Möbius est que $\sum_{d|n} \mu(d) = 0$ pour $n > 1$ et $\mu(1) = 1$. D'autre part puisque la somme des racine n-ièmes de l'unité pour $n > 1$ est nulle, il suit que pour $n > 1$ on a $\sum_{d|n} S(d) = 0$ et puisque $S(1) = 1$, l'égalité suit par récurrence sur n.

Exercice 4 Un complément à l'exercice précédent. Sommes de Newton relatives aux racines du polynôme cyclotomique, [F. M. 2'] complément à la page 249.

Soit $n > 0$ un entier. On note U_n le sous-groupe de $\mathbb{C}^\times$ des racines n-ièmes de l'unité et U'_n le sous-ensemble des racines primitives n-ièmes de l'unité. Par définition le n-ième polynôme cyclotomique est $\Phi_n := \prod_{z \in U'_n}(X - z)$.

Soit $h \in \mathbb{N}$, la h-ième somme de Newton relative à Φ_n est $p_h(n) := \sum_{z \in U'_n} z^h$. Dans la littérature on les appelle sommes de Ramanujan.

(1) Montrer que si $(n, m) = 1$, alors l'application $f : (z, z') \in U_n \times U_m \to zz' \in U_{nm}$ est un isomorphisme de groupes. Il suit que f induit une bijection entre $U'_n \times U'_m$ et U'_{nm}.

Preuve. L'application f est clairement un homomorphisme de groupes. Si $f((z, z')) = 1$ avec $(z, z') \in U_n \times U_m$, alors $z = z'^{-1}$ et si $un + vm = 1$ est une relation de Bézout on a donc $z = z^{un+vm} = 1$. Ensuite on remarque que $|U'_n| = \varphi(n)$ et donc $|U'_n \times U'_m| = |U'_{nm}|$.

(2) En déduire que pour h fixé, la fonction $n \in \mathbb{N}^\star \to p_h(n)$ est une fonction arithmétique multiplicative i.e. si $(n,m)=1$, alors $p_h(nm) = p_h(n)p_h(m)$.

Preuve. On a $p_h(n)p_h(m) = (\sum_{z\in U'_n} z^h)(\sum_{z'\in U'_m} z'^h) = \sum_{(z,z')\in U'_n\times U'_m} z^h z'^h = p_h(nm)$.

(3) Plus généralement montrer que $p_h(n) = \sum_{d|(n,h)} d\mu(n/d)$.

Preuve. On remarque que $\sum_{d|n}\sum_{z\in U'_d} z^h = \sum_{z\in U_n} z^h = 0$ si $n \nmid h$ et n si $n \mid h$. Ainsi la formule est conséquence de la formule d'inversion de Möbius.

(4) Une autre formule.

Déduire de 2) et 3) que $p_h(n) = \frac{\mu(\frac{n}{(n,h)})\varphi(n)}{\varphi(\frac{n}{(n,h)})}$.

Preuve. Puisque $n \to p_h(n)$ et $n \to \frac{\mu(\frac{n}{(n,h)})\varphi(n)}{\varphi(\frac{n}{(n,h)})}$ sont des fonctions arithmétiques multiplicatives (à priori à valeurs dans $\mathbb{Q}$), il suffit de vérifier l'égalité pour $n = p^k$ où p est un nombre premier et $k \in \mathbb{N}$. On a $p_h(p^k) = \sum_{z\in U_{p^k}} z^h - \sum_{z\in U_{p^{k-1}}} = 0$ si $p^{k-1} \nmid h$, $-p^{k-1}$ si $p^{k-1} \| h$ et $p^k - p^{k-1}$ si $p^k | h$. On vérifie facilement que ces formules sont aussi vérifiées par la fonction arithmétique multiplicative $n \to \frac{\mu(\frac{n}{(n,h)})\varphi(n)}{\varphi(\frac{n}{(n,h)})}$.

Exercice 5 Sous-groupe de torsion du groupe multiplicatif d'un corps commutatif, [F. M. 2'] complément à la page 121 "Les sous-groupes de $\frac{\mathbb{Q}}{\mathbb{Z}}$" par. 3

Exercice 6 Topologie du groupe des nombres complexes de module 1, [F. M. 2] IV.8.1 p.246

Soit $n \geq 1$, on note μ_n le sous-groupe de $\mathbb{C}^\times$ des racines n-ièmes de l'unité, $\zeta_n \in \mathbb{C}$ une racine primitive n-ième de l'unité et $\mu_\infty := \cup_{n>0}\mu_n$. On note σ l'automorphisme de conjugaison Si $A \subset \mathbb{C}$, on note $U(A) := \{z \in A \mid |z|^2 = z\sigma(z) = 1\}$. On se propose de montrer que :

- Si n est pair, alors $\mu_\infty \cap \mathbb{Q}(\zeta_n) = \mu_n$ et si n est impair, alors $\mu_\infty \cap \mathbb{Q}(\zeta_n) = \mu_{2n} = \mu_n \cup -\mu_n$.
  - Soit $d|n$, montrer que μ_d est l'unique sous-groupe de $\mathbb{C}^\times$ d'ordre d.
  - Soit $\xi \in \mu_\infty \cap \mathbb{Q}(\zeta_n)$ et G le sous-groupe de $\mathbb{Q}(\zeta_n)^\times$ engendré par ζ_n et ξ. Montrer que $G = \mu_m$ avec $m = dn$ et que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$.
  - En déduire que $\varphi(n) = \varphi(nd)$.
  - Conclure.
- Soit K un sous-corps de $\mathbb{C}$. Alors
  - Si $K \cap \sigma(K) \subset \mathbb{R}$, alors $U(K) = \{-1, 1\}$.
  - Si $K \cap \sigma(K) \subsetneq \mathbb{R}$, alors $U(K)$ est infini et par conséquent dense dans $U(\mathbb{C})$. De plus il existe $z \in U(K)$ avec $z \notin \mu_\infty$.
    - On suppose que $K \cap \sigma(K) \subset \mathbb{R}$. Montrer que $U(K) = \{-1, 1\}$.
    - On suppose que $K \cap \sigma(K) \subsetneq \mathbb{R}$.
      - Soit $x \in K \cap \sigma(K)$ avec $x \notin \mathbb{R}$. Soit $a \in \mathbb{Q}$ et $y(a) := \frac{a+x}{a+\sigma(x)}$, montrer que $y(a) \in U(K)$.
      - Montrer que $U(K)$ est infini.
      - En déduire que $U(K)$ dense dans $U(\mathbb{C})$.
      - On suppose que $U(K)$ est de torsion. Montrer qu'il existe $a \in \mathbb{Q}$ avec $o(y(a)) = n > 2$.
      - Soient $b \in \mathbb{Q}$ et $z(b) := \frac{b+y(a)}{b+y(a)^{-1}}$. Montrer que $z(b) \in U(K)$.
      - Conclure à l'aide de la première partie de l'exercice à une absurdité.
  - Exemples.
    - Le groupe $U(K)$ avec $K := \mathbb{Q}(j2^{1/3})$.
      Montrer que $[K : \mathbb{Q}] = 3$ et que $K \neq \sigma(K)$, en déduire que $K \cap \sigma(K) = \mathbb{Q}$ et donc que $U(K) = \{-1, 1\}$.
    - Le groupe $U(\mathbb{Q}(i))$.

Montrer que le groupe $U(\mathbb{Q}[i])$ est isomorphe au groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang i.e. la somme de copies de $\mathbb{Z}$ indexées par $\mathbb{N}$.
Preuve. On rappelle que $\mathbb{Z}[i]$ est un anneau principal, que le groupe des inversibles est le groupe cyclique engendré par i et donc isomorphe au groupe additif $\frac{\mathbb{Z}}{4\mathbb{Z}}$. Un système d'éléments irréductibles de $\mathbb{Z}[i]$ est indexé sur les premiers $\mathcal{P}$ de $\mathbb{N}$. Précisément si $p = 2$, on note $\pi_2 := 1 + i$, c'est l'unique irréductible à associés près avec $2\mathbb{Z} = \pi_2\mathbb{Z}[i] \cap \mathbb{Z}$. Si $p = 1 \mod 4$ alors $p = a^2 + b^2$ avec $0 < a < b$, on note $\pi_p := a + ib$ et $\overline{\pi}_p$ le conjugué, ce sont à associés près les seuls irréductibles π de $\mathbb{Z}[i]$ avec $p\mathbb{Z} = \pi\mathbb{Z}[i] \cap \mathbb{Z}$. Si $p = 3 \mod 4$, alors p est irréductible dans $\mathbb{Z}[i]$. Ainsi $\pi_2 \cup \{\pi_p,\ \overline{\pi}_p \mid p = 1 \mod 4\} \cup \{\pi_p \mid p = 3 \mod 4\}$ est un système Π de représentants à associé près des irréductibles de $\mathbb{Z}[i]$ (voir [F. M. 1] n° 94 p. 260). Si $z \in \mathbb{Q}[i]^\times$, alors $z = i^\epsilon \pi_2^{n_2} \prod_{p=1 \mod 4} \pi_p^{n_p} \overline{\pi}_p^{m_p} \prod_{p=3 \mod 4} p^{n_p}$ où $\epsilon \in \mathbb{Z}$ et $z \in U(\mathbb{Q}[i])$ si et seulement si $n_2 = 0$, $n_p + m_p = 0$ pour $p = 1 \mod 4$ et $n_p = 0$ pour $p = 3 \mod 4$. Soit donc $\mathcal{P}'$ l'ensemble des entiers premiers congrus à $1 \mod 4$, alors l'application $g : U(\mathbb{Q}[i]) \to \frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{\mathcal{P}'}$ définie par $g(z) = (\epsilon \mod 4, (n_p)_{p\in\mathcal{P}'})$ pour $z = (i)^\epsilon \prod_{p\in\mathcal{P}'} (\frac{\pi}{\overline{\pi}})^{n_p}$ induit un isomorphisme du groupe $U(\mathbb{Q}[i])$ avec le groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathcal{P}')}$ qui est isomorphe au groupe $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \mathbb{Z}^{(\mathbb{N})}$ où $\mathbb{Z}^{(\mathbb{N})}$ est le sous-groupe des suites nulles à partir d'un certain rang. ///

— Une application d'une version faible du théorème 90 de Hilbert, [F. M. 2] prop. p. 248.
On suppose que $\sigma(K) = K$ et que $K \subsetneq \mathbb{R}$. On note ρ l'homomorphisme de $\mathbb{C}^\times$ dans lui-même défini par $\sigma(y) = \frac{y}{\sigma(y)}$. Alors ρ induit un homomorphisme surjectif de $K^\times$ dans $U(K)$ dont le noyau est $(K \cap \mathbb{R})^\times$. Montrons cela.
  — Soit $x \in K$ avec $x \notin \mathbb{R}$ et $y := x - \sigma(x)$. Montrer que $-1 = \rho(y)$.
  — Soit $z \in U(K)$ avec $z \neq -1$. Soit $y := 1 + z$, calculer $\rho(y)$ et conclure.
  — Remarque. Si $K = \mathbb{Q}(i)$, alors $U(\mathbb{Q}(i)) \backsimeq \frac{\mathbb{Q}(i)^\times}{\mathbb{Q}^\times}$. On peut retrouver cela en utilisant la décomposition en irréductibles comme au-dessus. On notera que $\rho(\pi_2) = i$ est d'ordre 4.

Exercice 7 Un théorème de Kronecker et une application aux matrices $\in \mathrm{GL}_n(\mathbb{Z})$: les polynômes unitaires de $\mathbb{Z}[X]$ dont les racines complexes vérifient $0 < |z| \leq 1$ sont les produits de polynômes cyclotomiques,
[Fr. F] p. 201.

Soit $P(X) \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers, de degré $n \geq 1$. On suppose que les racines complexes de $P(X)$ sont de module ≤ 1.

(1) Notons $s_1, ..., s_n \in \mathbb{Z}[X_1, ..., X_n]$ les polynémes symétriques élémentaires. Soit $r \geq 1$, on note $\rho : \mathbb{Z}[X_1, ..., X_n] \to \mathbb{Z}[X_1, ..., X_n]$ l'unique homomorphisme tel que $\rho(a) = a$ pour $a \in \mathbb{Z}$ et $\rho(X_i) = X_i^r$ pour tout $1 \leq i \leq n$ (c'est la propriété universelle des anneaux de polynômes). Montrer en utilisant ρ que $\forall \sigma \in S_n$ on a $s_k(X_{\sigma(1)}^r, ..., X_{\sigma(n)}^r) = s_k(X_1^r, ..., X_n^r)$, en déduire que pour tout $k \leq n$, il existe $P_{r,k}(S_1, ..., S_n) \in \mathbb{Z}[S_1, ..., S_n]$ tel que $s_k(X_1^r, ..., X_n^r) = P_{r,k}(s_1, ..., s_n)$.

(2) Calculer $s_k(1, ..., 1)$.

(3) Notons $\theta_1, ..., \theta_n$ les racines complexes (éventuellement répétées) de $F(X)$. Montrer que pour tout $r \geq 1$ et tout $k \leq n$, on a

$$s_k(\theta_1^r, ..., \theta_n^r) \in \mathbb{Z}, \quad |s_k(\theta_1^r, ..., \theta_n^r)| \leq \binom{n}{k}.$$

(4) Montrer que l'ensemble $\{\theta_i^r \mid 1 \leq i \leq n, r \geq 1\}$ est fini.

(5) En déduire que pour toute racine θ de $P(X)$, il existe $r \geq 2$ tel que $\theta^r = \theta$. Conclure.

(6) En déduire la décomposition en irréductible de P dans $\mathbb{Z}[X]$.

(7) Une application du théorème de Kronecker.
Soit $M \in \mathrm{GL}_n(\mathbb{Z})$, on suppose que la suite $M^k, k \in \mathbb{N}$ est bornée. Montrer que M est d'ordre fini.

Preuve. Si $\lambda \in \mathbb{C}$ est racine de χ_M alors la suite λ^k est bornée ainsi $|\lambda| \leq 1$. Le théorème de Kronecker, [Fr. F] exercice 4.4.2 p. 201, appliqué au polynôme χ_M implique que les racines de χ_M sont des racines de l'unité; ainsi il existe $m > 0$ avec $\chi_{M^m} = (X-1)^n$ alors $M^m = Id + N$ où N est nilpotente. Montrons que $N = 0$. Pour cela nous allons montrer que si $m_N(X) = X^d$ avec $d \geq 2$ alors la suite M^{mk} est non bornée pour $k \to \infty$. La somme $\mathbb{C}N^0 + \mathbb{C}N + ... + \mathbb{C}N^{d-1} \subset M_n(\mathbb{C})$ est directe ainsi par l'équivalence des normes en dimension finie il existe $c > 0$ avec $\| \sum_{0 \leq i \leq d-1} a_i N^i \| \geq c \max_{0 \leq i \leq d-1} |a_i|$. Puisque $M^{mk} = (Id+N)^k = Id + \binom{k}{1} N + ... + \binom{k}{d-1} N^{d-1}$ et que $d \geq 2$, le résultat suit. ///

A propos des ordres des éléments de $\mathrm{GL}_n(\mathbb{Z})$ voir [F. M. 1] $n°26$ p. 46.

Exercice 8 Groupe des automorphismes de l'extension $\mathbb{Q}(exp(2i\pi/n)/\mathbb{Q}$, [F. M. 1] $n°$ 104 et [F. M. 1] Errata p.284

Exercice 9 Une application du théorème de Kronecker.

Si $z \in U(\mathbb{Q}(\zeta_n))$ et si z est un entier algébrique i.e. z annule un polynôme unitaire dans $\mathbb{Z}[X]$ ce qui équivaut au fait que le polynôme irréductible de z sur $\mathbb{Q}$ est dans $\mathbb{Z}[X]$ (cf. Le lemme de Gauss [F. M. 1] $n°$ 88). Alors z est une racine de l'unité.

Preuve. Soit $P(X) := \prod_{\sigma \in G}(X - \sigma(z))$ où $G = Aut\mathbb{Q}(\zeta_n)$. Les coefficients de P sont invariants par les éléments de G, ils sont donc dans $\mathbb{Q}$ (c'est le lemme d'Artin dans les extensions cyclotomiques, [F. M. 1] $n°$ 104 question 4) et par suite le polynôme irréductible de z sur $\mathbb{Q}$ divise P. Il suit que $\{\sigma(z),\ \sigma \in G\}$ est égal à l'ensemble des conjugués de z éventuellement avec des répétitions. Puisque la conjugaison complexe est dans G et que G est un groupe abélien il suit que $\sigma(\overline{z}) = \overline{\sigma(z)}$ pour $\sigma \in G$ et donc $|\sigma(z)| = 1$. Ainsi le polynôme irréductible de z est à coefficients entiers et ses racines sont de module 1. Le théorème de Kronecker permet de conclure.

Exercice 10 Sommes de Gauss, une variante de [F. M. 1] question 6.1 $n°$ 104 p. 282.

Soit $p > 2$ premier et ζ une racine primitive p-ième de l'unité dans $\mathbb{C}$.

Si $x \in \mathbb{F}_p - \{0\}$ on note $(\frac{x}{p})$ le symbole de Legendre. On rappelle que $(\frac{x}{p}) = 1 \in \mathbb{Z}$ si x est un carré dans $\mathbb{F}_p$ et -1 sinon.

Si $x = a + p\mathbb{Z}$ on remarque que si $b \in x$ alors $\zeta^b = \zeta^a$ que l'on peut donc noter ζ^x.

On définit (somme de Gauss) $S_p := \sum_{x \in \mathbb{F}_p - \{0\}} (\frac{x}{p}) \zeta^x$.

On va montrer que $(*) S_p^2 = (\frac{-1}{p}) p$.

On a $S_p^2 = \sum_{x,y \in \mathbb{F}_p - \{0\}} (\frac{x}{p})(\frac{y}{p}) \zeta^x \zeta^y = \sum_{x,y \in \mathbb{F}_p - \{0\}} (\frac{xy}{p}) \zeta^{x+y}$.

L'idée est de remarquer que pour $x \in \mathbb{F}_p - \{0\}$ les couples $\{(x,y) \mid y \in \mathbb{F}_p - \{0\}\}$ décrivent le même ensemble que les couples $\{(x,xy) \mid y \in \mathbb{F}_p - \{0\}\}$; ainsi dans l'expression précédente on peut remplacer y par xy et donc $S_p^2 = \sum_{x,y \in \mathbb{F}_p - \{0\}} (\frac{x^2 y}{p}) \zeta^{x+xy}$ et puisque $(\frac{x^2 y}{p}) = (\frac{y}{p})$, il suit que $S_p^2 = \sum_{y \in \mathbb{F}_p - \{0\}} (\frac{y}{p}) \sum_{x \in \mathbb{F}_p - \{0\}} \zeta^{(1+y)x}$. Il suit du lemme qui suit que pour $\zeta^{(1+y)} = 1$ (i.e. $y = -1$) alors $\sum_{x \in \mathbb{F}_p - \{0\}} \zeta^{(1+y)x} = p - 1$ et pour $\zeta^{(1+y)} \neq 1$ alors $\sum_{x \in \mathbb{F}_p - \{0\}} \zeta^{(1+y)x} = -1$ et donc $S_p^2 = (\frac{-1}{p})(p-1) - \sum_{y \in \mathbb{F}_p - \{0,-1\}} (\frac{y}{p}) = (\frac{-1}{p}) p$ puisque $\sum_{y \in \mathbb{F}_p - \{0\}} (\frac{y}{p}) = 0$ (il y autant de carrés que non carrés dans $\mathbb{F}_p - \{0\}$).

Lemme. Soit $\theta \in C$ avec $\theta^p = 1$, si $\theta = 1$ alors $\sum_{x \in \mathbb{F}_p - \{0\}} \theta^x = p - 1$ et si $\theta \neq 1$ alors $\sum_{x \in \mathbb{F}_p - \{0\}} \theta^x = -1$.

Preuve. Seul le cas $\theta \neq 1$ mérite une justification. Remarquer que $\sum_{x \in \mathbb{F}_p} \theta^x$ est égal à la somme des racines p-ièmes de l'unité.

Remarques.

A. Notez que S_p dépend du choix de ζ racine primitive p-ième de l'unité. En effet si ζ' est une autre racine primitive p-ième de l'unité alors $\zeta' = \zeta^a$ pour $a \in \mathbb{F}_p - \{0\}$. Alors $S_p = \sum_{x\in\mathbb{F}_p-\{0\}}(\frac{x}{p})\zeta^x = \sum_{x\in\mathbb{F}_p-\{0\}}(\frac{ax}{p})\zeta^{ax} = (\frac{a}{p})\sum_{x\in\mathbb{F}_p-\{0\}}(\frac{x}{p})\zeta'^x$. Ainsi si a est un carré dans $\mathbb{F}_p - \{0\}$ on retrouve S_p et sinon on trouve l'opposé et au carré on trouve bien un nombre complexe qui est indépendant du choix de ζ.

B. On notera une autre expression. On calcule $\sum_{x\in\mathbb{F}_p-\{0\}}((\frac{x}{p})+1)\zeta^x = \sum_{y\in\mathbb{F}_p-\{0\}}\zeta^{y^2}$ (remarquer que l'équation $y \in \mathbb{F}_p - \{0\} \mid y^2 = x$ a deux solutions y et $-y$) Et puisque $\sum_{x\in\mathbb{F}_p-\{0\}}\zeta^x = \sum_{1\le a\le p-1}\zeta^a = -1$ il suit que $S_p = 1 + \sum_{y\in\mathbb{F}_p-\{0\}}\zeta^{y^2} = \sum_{y\in\mathbb{F}_p}\zeta^{y^2}$.

Corollaire. Soit K un corps avec $Q \subset K \subset C$ et $[K : Q] = 2$ (on dit que K est une extension quadratique de Q alors il existe ζ_n une racine primitive n-ième de l'unité avec $K \subset Q(\zeta_n)$.

Preuve. Soit $\theta \in K - Q$, alors $Q \subset Q(\theta) \subset K$. Ainsi $1 < [Q(\theta) : Q] \mid [K : Q] = 2$ et donc $K = Q(\theta)$. Soit $P \in Q[X]$ le polynôme irréductible de θ sur Q. On a $degP = [Q(\theta) : Q]$, ainsi $P = X^2 + bX + c$. On remarque que $P(X - b/2) = X^2 + d$ et $Q(\theta) = Q(\theta - b/2)$; ainsi quitte à changer θ en $\theta - b/2$, on peut supposer que $P(X) = X^2 + d$. On écrit la décomposition en irréductible de $d \in \mathbb{Q}$. On a $d = \epsilon\prod_{p\in\mathcal{P}} p^{v_p(d)}$ où $\mathcal{P}$ désigne l'ensemble des nombres premiers de $\mathbb{N}$ et $v_p(d) \in \mathbb{Z}$ sont nuls sauf au plus un nombre fini et $\epsilon \in \{1, -1\}$ est le signe de d. Notons $r_p(d) \in \{0, 1\}$ le reste de la division euclidienne de $v_p(d)$ par 2. Alors si $d' := \epsilon\prod_{p\in\mathcal{P}} p^{r_p(d)}$ on peut écrire $d = d'\delta^2$ avec $\delta \in Q - \{0\}$. Ainsi $K = Q(\theta')$ avec $\theta' = \theta/\delta$ et $\theta'^2 = d'$. Soit $\zeta_8 := e^{i\frac{2\pi}{8}}$ et $S_2 := (1 - i)\zeta_8$, alors $S_2^2 = 2$. Il suit alors du calcul des sommes de Gauss que $(\prod_{p\in\mathcal{P},\ r_p(d)=1} S_p)^2 = \epsilon' d'$, avec $\epsilon' \in \{1, -1\}$. Puisque $Q(i),\ Q(S_2) \subset Q(\zeta_8)$ et que pour $p > 2$ on a $Q(S_p) \subset Q(\zeta_p)$ on conclut avec le lemme suivant :

Lemme. Soit $k > 1$, on note $\zeta_k := e^{i\frac{2\pi}{k}}$. Soient $n, m \in N$ et > 1 et $(n, m) = 1$, alors $Q(\zeta_n, \zeta_m) = Q(\zeta_{nm})$.

Preuve. Seule l'inclusion $Q(\zeta_{nm}) \subset Q(\zeta_n, \zeta_m)$ mérite une justification. Il suffit pour cela de considérer une relation de Bezout $1 = um + vn$ ainsi $\frac{1}{mn} = u\frac{1}{n} + v\frac{1}{m}$ et donc $\zeta_{nm} = \zeta_n^u\zeta_m^v$.

Références. On s'est inspiré de la preuve de S. Lang (Algebra). On utilise le symbole de Legendre sur $\mathbb{F}_p - \{0\}$ et on ne l'étend pas à 0. Dans [F. M. 1] question 6.1 n° 104 p. 282, on raisonne sur des représentants de Z/pZ et pour $0 < i < p$ on introduit l'entier i' avec $0 < i' < p$ et $ii' = 1 \bmod p$. A vous de voir quelle rédaction vous convient le mieux. Enfin on ne trouve pas de preuve dans Samuel puisque les sommes de Gauss qu'il considère sont à valeurs dans des corps finis ....