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

1 Groupe des complexes de module 1

1.1 Définitions et premières propriétés

Proposition 1. L'application $\varphi : \mathbb{C}^* \to \mathbb{R}_+^*$ définie par $\varphi(z) = |z|$ définit un morphisme de groupes.

Définition 2. Son noyau est appelé groupe des nombres complexes de module 1, et noté $\mathbb{U}$.

Théorème 3. $\mathbb{C}^*$ est alors isomorphe à $\mathbb{R}_+^* \times \mathbb{U}$.

1.2 L'exponentielle complexe

Définition 4. L'exponentielle est définie, pour $z \in \mathbb{C}$, par $\exp(z) = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$.

Proposition 5. La restriction de exp à $i\mathbb{R}$ prend ses valeurs dans $\mathbb{U}$, et $\mathcal{E} : \mathbb{R} \to \mathbb{C}$ définie par $\mathcal{E}(t) = \exp(it)$ définit un morphisme surjectif de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$.

Définition 6. On définit alors les fonctions $\cos = \Re(\mathcal{E})$ et $\sin = \Im(\mathcal{E})$.

Définition 7. On note π le double du plus petit zéro strictement positif de cos.

Proposition 8. Alors $\mathcal{E}$ est 2π-périodique et $\ker(\mathcal{E}) = 2\pi\mathbb{Z}$.

Proposition 9 (De Moivre)**.** On a, pour tout $\theta \in \mathbb{R}, (e^{i\theta})^n = e^{in\theta}$.

Proposition 10. On a, pour tout $\theta \in \mathbb{R}, \cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}, \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}$.

***Application* 11.** *Pour $\theta \in \mathbb{R}, \cos^3(\theta) = \frac{1}{4}\cos(3\theta) + \frac{3}{4}\cos(\theta)$.*

***Application* 12** (Polynômes de Tchebychev)**.** *Pour $n \in \mathbb{N}, x \in \mathbb{R}$, on pose $T_n(x) = \cos(n\arccos x)$. T_n définit une fonction polynomiale de degré n. Ses racines sont appelées points de Tchebychev, et sont utiles en interpolation numérique.*

1.3 Le cercle unité en géométrie

Définition 13. Soit $z \in \mathbb{C}^*$. On appelle argument de z tout réel θ tel que $e^{i\theta} = \frac{z}{|z|}$.

Si $z \in \mathbb{C}^*$, on appelle argument principal, et on note $\arg(z)$, son unique argument situé sur $]-\pi, \pi]$.

Proposition 14. Les arguments de z définissent une mesure de l'angle orienté $(1, z/|z|)$.

***Exemple* 15.** $\arg(1+i) = \frac{\pi}{4}$.

Proposition 16. L'application $\begin{cases} \mathbb{U} & \to SO_2(\mathbb{R}) \\ e^{i\theta} & \mapsto \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \end{cases}$ est un isomorphisme.

Remarque 17. En effet, $z \mapsto e^{i\theta}z$ effectue une rotation de centre O et d'angle θ.

2 Racines de l'unité et cyclotomie

2.1 Sous-groupes des racines de l'unité

Soit $n \in \mathbb{N}^*$.

Définition 18. On définit l'ensemble des racines n-èmes de l'unité par $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$.

Proposition 19. $\mathbb{U}_n = \{e^{2ik\pi/n}, k \in [\![0, n-1]\!]$.

Remarque 20. Les racines n-èmes de l'unité forment dans le plan complexe un polygone régulier à n côtés, inscrit dans le cercle unité.

Proposition 21. $\mathbb{U}_n$ est un groupe cyclique, engendré par $e^{2i\pi/n}$. C'est même le seul sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal n. Il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Définition 22. $\omega \in \mathbb{U}_n$ est dite racine primitive n-ème de l'unité si elle engendre $\mathbb{U}_n$. On note Π_n l'ensemble des racines primitives n-èmes.

Proposition 23. $e^{2ik\pi/n} \in \Pi_n$, si et seulement si, $k \wedge n = 1$.

Corollaire 24. $|\Pi_n| = \varphi(n)$ où φ est l'indicatrice d'Euler.

Définition 25. $\mathbb{Q}(\mathbb{U}_n)$ est appelé corps cyclotomique d'indice n.

Proposition 26. Pour tout $\omega \in \Pi_n$, $\mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(\omega)$.

2.2 Polynômes cyclotomiques

Définition 27. On appelle polynôme cyclotomique d'indice n le polynôme $\Phi_n = \prod_{\omega \in \Pi_n} (X - \omega)$.

Proposition 28. On a $X^n - 1 = \prod_{d|n} \Phi_d$, et $\Phi_n \in \mathbb{Z}[X]$.

Théorème 29. $\deg(\Phi_n) = \varphi(n)$ et Φ_n est irréductible dans $\mathbb{Q}[X]$.

Corollaire 30. Φ_n est le polynôme minimal de $e^{2i\pi/n}$ sur $\mathbb{Q}$, et $[\mathbb{Q}(\omega_n) : \mathbb{Q}] = \varphi(n)$.

2.3 Application : polygones réguliers constructibles

On note $\mathcal{P}$ le plan affine euclidien orienté.

Définition 31. Soit X partie de $\mathcal{P}$ avec $|X| \geq 2$, soit $M \in \mathcal{P}$. On dit que M est constructible en un pas à partir de X si M est point d'intersection de deux droites, une droite et un cercle, ou deux cercles déterminés à partir des points de X. On dit que M est constructible s'il existe une suite d'ensembles $\mathcal{B}_0, \cdots, \mathcal{B}_n$ tels que $\mathcal{B}_0 = \{O, I\}$ et pour tout $n, \mathcal{B}_{n+1} = \mathcal{B}_n \cup \{A_n\}$ où A_n constructible en un pas à partir de $\mathcal{B}_{n-1}$, et tels que $M \in \mathcal{B}_n$.

Théorème 32 (Wantzel)**.** Soit $x \in \mathbb{R}$. x est constructible si et seulement si il existe une suite finie $L_0, \cdots, L_q$ de sous-corps de $\mathbb{R}$ tels que $L_0 = \mathbb{Q}, x \in L_q$ et $\forall k \leq q-1, [L_{k+1} : L_k] = 2$.

Théorème 33 (Gauss-Wantzel)**.** Soit p premier, soit $\alpha \in \mathbb{N}^*$. L'angle $\dfrac{2\pi}{p^\alpha}$ est constructible ssi $p = 2$ ou ($\alpha = 1$ et p est un nombre de Fermat, soit $p = 1 + 2^{(2^\beta)}$).

Corollaire 34. Si un polygone régulier est constructible, son nombre de côtés est de la forme $2^\alpha p_1 \cdots p_r$ où les p_i sont des nombres premiers de la forme ci-dessus.

***Exemple* 35.** *Les polygones réguliers à 5 et 17 côtés sont constructibles.*

3 Représentations et caractères

3.1 Dual d'un groupe abélien fini

Définition 36. Soit G un groupe abélien fini. Un caractère de G est un morphisme de groupes $\chi : G \to \mathbb{C}^*$. L'ensemble des caractères de G est appelé dual de G, et noté $\widehat{G}$.

***Exemple* 37.** *La signature ε est un caractère du groupe symétrique $\mathcal{S}_n$.*

Proposition 38. $(\widehat{G}, \times)$ est un groupe abélien.

Proposition 39. Si $n = |G|$, alors tout caractère de G prend ses valeurs dans $\mathbb{U}_n$, l'ensemble des racines n-èmes de l'unité. En particulier, $\widehat{G}$ est un groupe fini.

Théorème 40. Supposons G cyclique, soit g générateur de G, soit ω une racine primitive n-ème de l'unité. Alors $\widehat{G} = \{\chi_0, \cdots, \chi_{n-1}\}$ où pour $j \in [\![0, n-1]\!]$, $\chi_j : g^k \mapsto \omega^{jk}$. En particulier, G et $\widehat{G}$ sont isomorphes.

Lemme 41. Soit H sous-groupe de G, soit χ caractère de H. Alors χ se prolonge en un caractère de G.

Théorème 42. Il existe une suite d'entiers $d_1, \cdots, d_k$ tels que pour tout j, $d_j | d_{j+1}$ et que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$.

Corollaire 43. Si G abélien fini, G est toujours isomorphe à $\widehat{G}$.

3.2 Représentations linéaires de groupes finis

Soit G groupe fini d'ordre N.

Proposition 44. Soit $N = |G|$, soit ρ une représentation de G Alors, pour tout $g \in G$, $\rho(g)$ est diagonalisable à valeurs propres dans $\mathbb{U}_N$.

Proposition 45. Si χ caractère de ρ, on a pour tout $g \in G, \chi(g^{-1}) = \overline{\chi(g)}$.

***Application* 46.** *Pour tout $n \in \mathbb{N}$, la table de caractères de $\mathcal{S}_n$ ne contient que des réels.*

Théorème 47. Soit G groupe fini, soit $X = \{\chi_1, \cdots, \chi_r\}$ l'ensemble de ses caractères irréductibles. Pour $1 \leq i \leq r$, on note $K_i = \ker(\chi_i) = \{x \in G, \chi_i(x) = \chi_i(e_G)\}$. Alors, si H sous-groupe de G, H est distingué dans G, si et seulement si, il existe $I \subseteq [\![1, r]\!], H = \bigcap_{i \in I} K_i$.

Remarque 48. La connaissance des caractères des caractères des groupes abéliens permet de construire, par passage au quotient, des tables de caractères de groupes non abéliens.

***Exemple* 49.** *Si on note V_4 le sous-groupe de $\mathcal{A}_4$ engendré par les bi-transpositions, $\mathcal{A}_4/V_4$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, et on déduit de la table de $\mathbb{Z}/3\mathbb{Z}$ celle de $\mathcal{A}_4$.*

Développements

— Irréductibilité des polynômes cyclotomiques.
— Théorème de Gauss-Wantzel.
— Théorème de structure des groupes abéliens finis.

Références

[1] J.-M. Arnaudiès, H. Fraysse, Cours de mathématiques - Tomes 1 et 2, Dunod.

[2] I. Gozard, Théorie de Galois, Ellipses.

[3] G. Peyré, L'algèbre discrète de la transformée de Fourier, Ellipses.

[4] G. Rauch, Les groupes finis et leurs représentations, Ellipses.