

Leçon 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

1 Nombres complexes de module 1

1.1 Exponentielle et fonctions trigonométriques

Définition 1. Pour tout nombre complexe $z = a + ib$ on définit son module $|z| = \sqrt{a^2 + b^2}$.

Proposition 2. Pour tout $z, z' \in \mathbb{C}$ on a :

1. $|z| \geq 0$ et $|z| = 0 \iff z = 0$;
2. $|zz'| = |z| |z'|$;
3. $|z| = |\bar{z}|$;
4. Si $z' \neq 0$ alors $|\frac{z}{z'}| = \frac{|z|}{|z'|}$;
5. $|z|^2 = z\bar{z}$;
6. $|z + z'| \leq |z| + |z'|$.

Définition 3. On définit la fonction exponentielle complexe par $e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$.

Proposition 4. La fonction exponentielle est de classe $\mathcal{C}^\infty$ et sa dérivée est elle même en tout point de $\mathbb{C}$. De plus pour tout $z, \zeta \in \mathbb{C}$ on a $e^z e^\zeta = e^{z+\zeta}$, $e^z \neq 0$, $(e^z)^{-1} = e^{-z}$, $|e^z| = e^{\operatorname{Re}(z)}$ et $|e^z| = 1 \iff z \in i\mathbb{R}$.

Théorème 5. L'application $\varphi : \mathbb{R}_+^* \times \mathbb{U} \rightarrow \mathbb{C}^*$; $(r, e^{i\theta}) \mapsto re^{i\theta}$ est un isomorphisme.

Définition 6. On appelle cosinus et sinus les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ définies par $\cos(t) = \operatorname{Re}(e^{it})$ et $\sin(t) = \operatorname{Im}(e^{it})$.

Proposition 7. Ainsi pour tout $t \in \mathbb{R}$ on a $e^{it} = \cos(t) + i \sin(t)$ et les propriétés suivantes :

$$\text{— } \cos(t) = \sum_{n=0}^{\infty} \frac{(-1)^n t^{2n}}{(2n)!} ;$$

$$\text{— } \sin(t) = \sum_{n=0}^{\infty} \frac{(-1)^n t^{2n+1}}{(2n+1)!} ;$$

— Les fonctions sont 2π périodiques, de classe $\mathcal{C}^\infty$, $\cos$ est paire et $\sin$ est impaire ;

$$\text{— } (\cos)' = -\sin \text{ et } (\sin)' = \cos ;$$

$$\text{— } \cos(t) = \frac{e^{it} + e^{-it}}{2} \text{ et } \sin(t) = \frac{e^{it} - e^{-it}}{2i} ;$$

$$\text{— } \cos(t)^2 + \sin(t)^2 = 1$$

1.2 Groupe des nombres complexes de module 1

Proposition 8. L'application $|\cdot| : \mathbb{C} \rightarrow \mathbb{R}_+$ est un morphisme de groupe dont on note le noyau $\mathbb{U}$.

Définition 9. On a alors $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ l'ensemble des nombres complexes de module 1.

Théorème 10. L'application $(\mathbb{R}, +) \rightarrow (\mathbb{U}, \times)$; $t \mapsto e^{it}$ est un morphisme de groupe surjectif non injectif, son noyau est $2\pi\mathbb{Z}$.

Théorème 11. Le groupe $SO_2(\mathbb{R})$ est isomorphe au groupe multiplicatif $\mathbb{U}$ par l'application $R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \mapsto e^{i\theta}$

Théorème 12. Le groupe $\mathbb{U}$ est compact et connexe par arc.

2 Racines de l'unité

2.1 Groupe $\mathbb{U}_n$

Définition 13. On définit pour $n \in \mathbb{N}^*$ le groupe $\mathbb{U}_n = \{z \in \mathbb{U} \mid z^n = 1\}$ des racines n -ièmes de l'unité.

Exemple 14. On a $\mathbb{U}_2 = \{-1, 1\}$, $\mathbb{U}_3 = \{1, j, j^2\}$ et $\mathbb{U}_4 = \{-1, -i, 1, i\}$.

Proposition 15. On a $\mathbb{U} = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$.

Théorème 16. Tout sous groupe fini du groupe multiplicatif d'un corps $(\mathbb{K}^*, \times)$ est cyclique.

Corollaire 17. $\mathbb{U}_n$ est un sous groupe cyclique d'ordre n de $(\mathbb{C}^*, \times)$.

Proposition 18. $\mathbb{U}_d \subset \mathbb{U}_n \iff d|n$ et $n = \sum_{d|n} \varphi(d)$.

Théorème 19. Soit H un sous groupe de $\mathbb{U}$, si H est d'ordre fini n alors $H = \mathbb{U}_n$, sinon H est dense dans $\mathbb{U}$.

Applications 20. On a $\overline{\{\cos(n) \mid n \in \mathbb{N}\}} = \overline{\{\sin(n) \mid n \in \mathbb{N}\}} = [-1, 1]$

2.2 Polynômes cyclotomiques

Définition 21. Une racine n -ième primitive de l'unité de $\mathbb{C}$ est un élément $\zeta \in \mathbb{U}_n$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. C'est un générateur de $\mathbb{U}_n$ de sorte qu'il y ait $\varphi(n)$ racines primitives de l'unité, leur ensemble est noté $\mathbb{U}_n^*$.

Définition 22. Le n -ième polynôme cyclotomique de $\mathbb{C}$ est $\Phi_n(X) \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta)$.

Exemple 23. Sur $\mathbb{Q}$ on a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Remarque 24. Si $\zeta \in \mu_n^*(\mathbb{K})$ alors les ζ^d avec $\text{pgcd}(d, n) = 1$. Le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 25. On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proposition 26. Dans $\mathbb{Q}$ on a $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 27. Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Théorème 28. Soit $\zeta \in \mathbb{U}_n^*$, alors Φ_n est le polynôme minimal de ζ sur $\mathbb{Q}$.

Corollaire 29. Soit $\zeta \in \mathbb{U}_n^*$, alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Corollaire 30. Soient α resp α' , une racine n -ième de l'unité resp m -ième de l'unité telles que $\text{pgcd}(n, m) = 1$. Alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\alpha') = \mathbb{Q}$ et $\mathbb{Q}(\alpha\alpha') = \mathbb{Q}(\mathbb{U}_{nm})$.

3 Applications

3.1 Une application géométrique

Exemple 31. (Déterminant Circulant) Soient $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, $\omega = e^{2i\pi/n}$ et $P = \alpha_n X^{n-1} + \dots + \alpha_2 X + \alpha_1$ on a alors

$$\det \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_n & \alpha_1 & \dots & \alpha_{n-1} \\ \vdots & \dots & \dots & \vdots \\ \alpha_2 & \alpha_3 & \dots & \alpha_1 \end{pmatrix} = \prod_{i=0}^{n-1} P(\omega^i)$$

Applications 32. Soient $\mathcal{P} = (z_1, \dots, z_n)$ un polynôme à n sommets et $a, b \in]0, 1[$ tels que $a + b = 1$. La suite vectorielle définie par $\mathcal{P}_0 = \mathcal{P}$ et $\mathcal{P}_{k+1} = (ap_{k,1} + bp_{k,2}, \dots, ap_{k,n} + bp_{k,1})$ où $\mathcal{P}_k = (p_{k,1}, \dots, p_{k,n})$ converge vers l'isobarycentre de $\mathcal{P}$.

3.2 Groupe unitaire [GOU21]

Définition 33. Une matrice $U \in \mathcal{M}_n(\mathbb{C})$ est dite unitaire lorsque ${}^t \overline{U} U = I_n$. L'ensemble des matrices unitaires constitue un groupe noté $\mathcal{U}_n(\mathbb{C})$.

Remarque 34. Si $U \in \mathcal{U}_n(\mathbb{C})$ alors $\det(U) \in \mathbb{U}$.

Exemple 35. La matrice $A = \text{diag}(e^{i\varphi_1}, \dots, e^{i\varphi_n})$ avec $\varphi_k \in \mathbb{R}$ pour $k \in \llbracket 1, n \rrbracket$ est unitaire et $\det(A) = e^{i(\varphi_1 + \dots + \varphi_n)}$.

Théorème 36. Soit $U \in \mathcal{U}_n(\mathbb{C})$, alors il existe une matrice unitaire $P \in \mathcal{U}_n(\mathbb{C})$ telle que $P^{-1}UP = P^*UP = \text{diag}(e^{i\theta_1}, \dots, e^{i\theta_n})$ où les θ_i sont des réels.

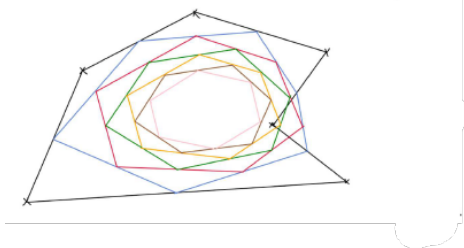
Corollaire 37. Toutes les valeurs propres d'une matrice unitaire sont des éléments de $\mathbb{U}$.

Théorème 38. L'ensemble $\mathcal{U}_n(\mathbb{C})$ est connexe par arc et compact.

Théorème 39. (Décomposition polaire) Soit $A \in \mathcal{M}_n(\mathbb{C})$, alors il existe $U \in \mathcal{U}_n(\mathbb{C})$ et $H \in \mathcal{H}_n^+(\mathbb{C})$ telles que $A = UH$. Si de plus A est inversible alors cette décomposition est unique.

4 Annexe

FIGURE 2: Suite de polygones



Suite de polygones

Dev 1 : Polynômes cyclotomiques irréductibles 26 et 27
Dev 2 : Suites de polygones 31 et 32

Références

- [CAL22] Philippe CALDERO : Carnet de voyage en algèbre. Calvage et Mounet, 2022.
- [GOU21] Xavier GOURDON : Les maths en tête. Algèbre et probabilités. Editions Ellipses, 2021.
- [PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.
- [Tau20] Patrice TAUVEL : Analyse complexe pour la licence 3. Dunod, 2020.
- [17] Jean Étienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Supérieur, 2017.

RAPPORT DU JURY :

Les notions élémentaires concernant les nombres complexes de module 1 (définitions, exponentielle complexe, trigonométrie, etc.) doivent être présentés, avant d'aborder l'aspect "groupe" de S_1 en considérant son lien avec $(\mathbb{R}, +)$ et en examinant ses sous-groupes (en particulier finis). Il est souhaitable de présenter des applications en géométrie plane, par exemple la constructibilité des polygones réguliers. Plus généralement, la leçon invite à expliquer où et comment les nombres complexes de module 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques : spectres de

matrices remarquables, polynômes cyclotomiques, et éventuellement les représentations de groupes, etc. On peut également s'intéresser aux sous-groupes compacts de $\mathbb{C}^*$.

Pour aller plus loin, on peut s'intéresser aux nombres de module 1 et aux racines de l'unité dans $\mathbb{Q}[i]$, ou à la dualité des groupes abéliens finis ou encore aux transformées de Fourier discrètes et rapides. Des aspects analytiques du sujet peuvent être évoqués (théorème de relèvement, logarithme complexe, analyse de Fourier sur $\mathbb{R}^n$) mais ne doivent occuper ni le coeur de l'exposé, ni l'essentiel d'un développement.