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

I Nombres complexes de module 1

1) Le groupe $\mathbb{U}$

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

Exemple 2. $\pm 1, \pm i \in \mathbb{U}$.

Remarque 3. *En identifiant $\mathbb{C}$ et $\mathbb{R}^2$, $\mathbb{U}$ est identifié à $\mathbb{S}^1$.*

Théorème 4. *L'application $\mathbb{R}^{+\star} \times \mathbb{U} \to \mathbb{C}^\star$ envoyant (r, u) sur ru est un isomorphisme.*

Proposition 5. *Les groupes $\mathbb{U}$, $\mathbb{R}/2\pi\mathbb{Z}$ et $\mathcal{SO}_2(\mathbb{R})$ sont isomorphes.*

Proposition 6. *Le groupe $\mathbb{U}$ est compact et connexe.*

2) Fonctions trigonométriques

Définition 7. On définit les séries entières suivantes :

$$\exp(z) = e^z = \sum_{n\in\mathbb{N}} \frac{z^n}{n!} \quad \cos(z) = \sum_{n\in\mathbb{N}} \frac{(-1)^n z^{2n}}{(2n)!} \quad \sin(z) = \sum_{n\in\mathbb{N}} \frac{(-1)^n z^{2n+1}}{(2n+1)!}$$

Proposition 8.
- *(i) Pour tout $z \in \mathbb{C}$, on a $\exp(iz) = \cos(z) + i\sin(z)$.*
- *(ii) Pour tout $z_1, z_2 \in \mathbb{C}$, on a $e^{z_1+z_2} = e^{z_1}e^{z_2}$.*
- *(iii) Pour tout $z \in \mathbb{C}$, on a $e^z \neq 0$, $\frac{1}{e^z} = e^{-z}$, $\overline{e^z} = e^{\overline{z}}$ et $|e^z| = e^{\mathrm{Re}\, z}$.*
- *(iv) Pour tout $z \in \mathbb{C}$, $|\exp(z)| = 1 \Leftrightarrow z \in i\mathbb{R}$.*
- *(v)* exp *est un morphisme de groupe surjectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^\star, \times)$.*
- *(vi)* exp, sin *et* cos *sont des séries entières de rayon de convergence infini, et sont donc définies et holomorphes sur $\mathbb{C}$. De plus,* exp *est sa propre dérivée.*
- *(vii) Pour $\theta \in \mathbb{R}$, $\cos\theta$ et $\sin\theta$ sont réels.*

Corollaire 9 (Moivre)**.** *Pour $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$, on a :*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Corollaire 10 (Euler)**.** *Pour $\theta \in \mathbb{R}$, on a :*

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad \text{et} \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Application 11. *On peut exprimer $\cos(n\theta)$ comme un polynôme en $\cos\theta$: ce sont les polynômes de Tchebychev.*

3) Paramétrisation du cercle unité

Proposition 12. *Dans $\mathbb{C}$, $\mathbb{U}$ est le cercle de centre 0 et de rayon 1. Il peut être paramétré, à l'exception de $(-1, 0)$ par l'application :*

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^2 \\ t & \longmapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{array}$$

Corollaire 13. *L'ensemble des points de $\mathbb{U}$ à coordonnées rationnelles sont denses dans $\mathbb{U}$.*

Application 14 (Triplets pythagoriciens)**.** *Soient $x, y, z \in \mathbb{N}$. Alors (x, y, z) est solution de l'équation diophantienne $x^2 + y^2 = z^2$ si, et seulement si, il existe $d \in \mathbb{Z}$ et u, v premiers entre eux tels que, à permutation près, on a $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$.*

4) Argument, rotations et angles orientés

On identifie ici $\mathbb{R}^2$ au plan complexe $\mathbb{C}$.

Définition 15. Pour $z \in \mathbb{C}^\star$, on appelle argument de z, noté $\arg z$, tout réel θ tel que $\frac{z}{|z|} = e^{i\theta}$. L'argument est donc bien défini dans $\mathbb{R}/2\pi\mathbb{Z}$.

Exemple 16. $\arg i = \frac{\pi}{2}$, $\arg x = 0$ *ou* 2π *pour* $x \in \mathbb{R}^{+\star}$.

Définition 17. La rotation autour de $a \in \mathbb{C}$ d'angle θ est l'application $r_{\theta,a}\mathbb{C} \to \mathbb{C}$ définie pour $z \in \mathbb{C}$ par $r_{\theta,a}(z) = a + (z - a)e^{i\theta}$.

Proposition 18. *Les rotations sont des isométries. En particulier, $\mathbb{U}$ est stable par toute rotation autour de 0.*

Application 19. *Les rotations du plan préservant un polygone régulier à n côtés de centre 0 est un groupe constitué des n rotations de centre 0 et d'angle $\frac{2k\pi}{n}$ pour $k \in [\![0, n-1]\!]$.*

Remarque 20. *Si on rajoute les symétries, on obtient le groupe des isométries du plan préservant le polygone régulier : le groupe diédral D_{2n}.*

Proposition 21. *Il existe une unique rotation envoyant $u \in \mathbb{U}$ sur $v \in \mathbb{U}$.*

Définition 22. On appelle angle orienté l'orbite de l'action de $\mathbb{U}$ sur $\mathbb{U} \times \mathbb{U}$ définie par $z \cdot (u, v) = (zu, zv)$.

Proposition 23. *L'application qui à un angle orienté $\overline{(u, v)}$ associe l'unique rotation envoyant u sur v est une bijection, notée Φ.*

Corollaire 24. *L'ensemble des angles orientés est un groupe s'il est muni de l'opération : $\overline{(u, v)} + \overline{(u', v')} = \Phi^{-1}\left(\Phi\left(\overline{(u, v)}\right) \circ \Phi\left(\overline{(u', v')}\right)\right)$.*

II Racines de l'unité

1) Sous-groupes des racines de l'unité

Définition 25. Soit $n \in \mathbb{N}^\star$. On appelle racine n-ième de l'unité dans $\mathbb{C}$ tout nombre complexe z tel que $z^n = 1$. On note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité.

Définition 26. Soit $n \in \mathbb{N}^\star$. Une racine n-ième de l'unité est dite primitive si elle est d'ordre n dans $\mathbb{C}^\star$. On note μ_n l'ensemble des racines primitives n-ièmes de l'unité.

Proposition 27. *Pour $n \in \mathbb{N}^\star$, $\mathbb{U}_n$ est un groupe cyclique d'ordre n engendré par $e^{\frac{2i\pi}{n}}$. Les racines primitives sont les générateurs de $\mathbb{U}_n$.*

Corollaire 28. *Pour $n \in \mathbb{N}^\star$, on a $|\mu_n| = \varphi(n)$.*

Proposition 29. *Un sous-groupe de $\mathbb{U}$ est fini ou dense.*

Proposition 30. *On a $\mathbb{U}_d \subset \mathbb{U}_n \Leftrightarrow d \mid n$, et $\mathbb{U}_n = \bigcup_{d|n} \mu_d$.*

Application 31. *On a $n = \sum_{d|n} \varphi(d)$.*

2) Polynômes cyclotomiques

Définition 32. On définit le n-ième polynôme cyclotomique par :

$$\Phi_n(X) = \prod_{\zeta \in \mu_n} (X - \zeta) \in \mathbb{C}[X]$$

Proposition 33. *Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 34. $\forall n \in \mathbb{N}^\star, X^n - 1 = \prod_{d|n} \Phi_d(X)$

Exemple 35. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 36. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 37. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Z}[X]$.*

Lemme 38. *Soit $a \in \mathbb{Z}$ et p premier tel que $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Théorème 39 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

III Application aux représentations

Soit G un groupe d'ordre n et V un $\mathbb{C}$-espace vectoriel de dimension d.

Définition 40. Une représentation linéaire de G est un morphisme $\rho : G \to \mathcal{GL}(V)$. On appelle caractère de ρ la fonction $g \mapsto \mathrm{tr}(\rho(g))$.

Remarque 41. *Se donner une représentation de G dans V revient à se donner une action de groupes de G sur V en posant $\rho(g)(x) = g \cdot x$.*

Exemple 42. *$\rho : g \mapsto Id_V$ est une représentation de G sur V.*

Exemple 43. *On suppose que G agit sur un ensemble X de cardinal d. Soit $(e_x)_{x \in X}$ une base de V. La représentation suivante est appelée représentation de permutation associée à X :*

$$\rho : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(V) \\ s & \longmapsto & (e_x \mapsto e_{s \cdot x}) \end{array} \right.$$

Proposition 44. *Soient $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G et $g \in G$. Alors $\rho(g)$ est diagonalisable de valeurs propres dans $\mathbb{U}_n$.*

Corollaire 45. *Soient χ un caractère de G et $g \in G$. Alors $\chi(g)$ s'écrit comme somme de racines n-ièmes de l'unité.*

Théorème 46. *G est abélien si et seulement si toute représentation irréductible est de degré 1.*

Exemple 47. *La table de caractères de $\mathbb{Z}/n\mathbb{Z}$ est :*

$\mathbb{Z}/n\mathbb{Z}$	0	1	2	$\cdots$	$n-1$
χ_1	1	1	1	$\cdots$	1
χ_2	1	ω	ω^2	$\cdots$	ω^{n-1}
χ_3	1	ω^2	ω^4	$\cdots$	ω^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_n	1	ω^{n-1}	ω^{n-2}	$\cdots$	ω

où $\omega = e^{\frac{2i\pi}{n}}$.

Proposition 48. *L'application $\iota : G \to \widehat{\widehat{G}}$ définie pour $g \in G$ par $\iota(g) : \chi \mapsto \chi(g)$ est un isomorphisme.*

Proposition 49. *G et $\widehat{G}$ ont même exposant.*

Théorème 50. *Il existe un unique entier ℓ et une unique suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Développements

— Étude des polynômes cyclotomiques (36,37) [Per96]
— Structure des groupes abéliens finis (48,49,50) [Col09]
— Forme faible de la progression arithmétique de Dirichlet (38,39) [FGN13a]

Références

[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions*. Ellipses
[Aud06] M. Audin. *Géométrie*. EDP Sciences
[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses
[Col09] P. Colmez. *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1*. Cassini