Leçon 012 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

1. Nombre complexe de module et exponentielle. —

1. *Fonctions trigonométriques.* —

- L'exponentielle est une fonction entière définie par exp : $\mathbb{C} \to \mathbb{C}^*$, $z \mapsto \sum_{k=0}^{\infty} \frac{z^k}{k!}$.
- On définit les fonctions cosinus et sinus définies de $\mathbb{R}$ dans $\mathbb{R}$ par $cos(x) = Re(e^{ix})$ et $sin(x) = Im(e^{ix})$.
- Prop : Formule de Moivre : $e^{inx} = cos(nx) + isin(nx)$.
- Prop : Formule d'Euler : $cos(x) = \frac{e^{ix}+e^{-ix}}{2}$, $sin(x) = \frac{e^{ix}-e^{-ix}}{2i}$.
- Prop : $cos^2(x) + sin^2(x) = 1$ pour tout $x \in \mathbb{R}$.
- App : $\sum_{k=0}^{n} e^{ik\theta} = e^{in\frac{\theta}{2}} \frac{sin(\frac{(n+1)\theta}{2})}{sin(\frac{\theta}{2})}$.

2. *Le groupe des nombres complexes de module 1 et topologie.* —

- On appelle groupe des nombres complexes de module 1 le noyau du morphisme de groupes $\mathbb{C}^* \to \mathbb{R}_+^*$, $z \mapsto |z|$. On le note $\mathbb{U}$.
- Ex : 1, -1, i, $-i$ et $\frac{1+i\sqrt{3}}{2}$ appartiennent à $\mathbb{U}$.
- Rem : Lorsqu'on identifie le plan complexe à $\mathbb{R}^2$, $\mathbb{U}$ s'apparente au cercle unité $\mathbb{S}^1$.
- Thm : L'application $\mathbb{R}_+^* \to \mathbb{C}^*$, $(r, u) \mapsto ru$ est un isomorphisme de groupes.
- Thm : L'application $\mathbb{R} \to \mathbb{U}$, $x \mapsto e^{2i\pi x}$ est un morphisme de groupe surjectif de noyau $\mathbb{Z}$.
- Cor : $\mathbb{U} \simeq \mathbb{R}/\mathbb{Z}$.
- Rem : C'est isomorphisme de groupes topologiques.
- Cor : $\mathbb{U}$ est un compact connexe de $\mathbb{C}$.
- Cor : $\pi_1(\mathbb{S}^1) \simeq \mathbb{Z}$.
- DEV 1 :Les morphimes continus ϕ de $(\mathbb{S}^1, \times)$ vers $(GL_n(\mathbb{R}), \times)$ sont de la forme :

$$\phi \ : \ e^{it} \mapsto Q \begin{pmatrix} R_{tk_1} & & & & & \\ & \ddots & & & & \\ & & R_{tk_r} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} Q^{-1}$$

avec $Q \in GL_n(\mathbb{R})$, $r \in \mathbb{N}$, $k_1, ..., k_r \in \mathbb{Z}^*$ et $\forall \theta \in \mathbb{R}$, $\mathbb{R}_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

3. *Un peu de géométrie.* —

- Prop : Pour u, v vecteurs unitaires de $\mathbb{R}^2$, il existe une unique rotation envoyant u sur v. Autrement dit $SO_2(\mathbb{R})$ agit simplement transitivement sur $\mathbb{S}^{\nVdash}$.
- On munit A l'ensemble des couples de vecteurs unitaires de $\mathbb{R}^2$ de la relation d'équivalence : $(u, v)R(u', v')$ si la même rotation envoie u sur v et u' sur v'.
- La classe d'équivalence de (u, v) est appelée angle orienté. On note $\bar{A}$ l'ensemble des angles orientés.
- Rem : Il s'agit de l'ensemble des d'orbites de l'action de $SO_2(\mathbb{R})$ sur les couples distincts de $\mathbb{S}^1$.
- Prop : L'application qui à $\overline{(u, v)} \in \bar{A}$ envoie l'unique rotation $r \in SO_2(\mathbb{R})$ telle que $r(u) = v$ est une bijection. C'est la relation orbite stabilisateur.
- Cela munit $\bar{A}$ d'une structure de groupe.
- L'isomorphisme entre $S0_2(\mathbb{R})$ et $\mathbb{R}/\mathbb{Z}$ permet de définir une mesure des angles orientés de vecteurs.

2. Groupe des racines de l'unité et applications. —

1. *Définitions et premières propriétés.* —

- On note μ_n l'ensemble des nombres complexes z tel que $z^n = 1$.
- Prop : μ_n est un sous-groupe de $\mathbb{C}^*$ cyclique de cardinal n.
- Rem : L'isomorphisme avec $\mathbb{Z}/n\mathbb{Z}$ est donné par $\mathbb{Z}/n\mathbb{Z} \to \mu_n$, $\bar{k} \mapsto e^{\frac{2i\pi k}{n}}$.
- Def : Une racine n^{ième} primitive de l'unité est un élément ξ de $\mathbb{C}$ tel que $\xi^n = 1$ mais $\xi^d \neq 1$, pour tout $d < n$. Autrement dit, ξ est un générateur du groupe μ_n. Il y a $\phi(n)$ racine primitive n^{ième}. On note leur ensemble μ_n^*.

2. *Cyclotomie.* —

- Def : Le n^{ième} polynôme cyclotomique est défini par : $\Phi_n(X) = \prod_{\xi \in \mu_n^*}(X - \xi)$.
- Rem : Si ξ est une racine primitive de l'unité, les autres sont les ξ^m avec pgcd$(n, m) = 1$. Le polynôme Φ_n est unitaire de degré $\phi(n)$.
- Prop : On a la formule : $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
- Rem : On comparant les degrés, on trouve la formule : $n = \sum_{d|n} \phi(d)$.
- Ex : $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$.
- Prop : On a $\Phi_n(X) \in \mathbb{Z}[X]$.
- Application : Thm de Wedderburn : Tout corps fini est commutatif.
- Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.

3. *Représentation des groupes finis.* — Dans ce qui suit G sera un groupe fini et V un $\mathbb{C}$-ev de dimension finie.

- Def : Une représentation linéaire de G est un morphisme de $\rho : G \to GL(V)$. Le caractère associé à ρ est l'application $\chi_\rho : g \in G \mapsto \mathrm{tr}(\rho(g)) \in \mathbb{C}$.
- Def : Une représentation ρ est dite irréductible si il n'existe pas de sous-espace vectoriel non trivial qui soit stable par $\rho(g)$ pour tout $g \in G$. Un caractère irréductible est un caractère associé à une représentation irréductible.
- Soit ρ une représentation de G alors pour tout $g \in G$, $\rho(g)$ est diagonalisable et Sp$(\rho(g)) \subset \mathbb{U}_n$.
- Table de caractère des groupes cycliques (cf Annexe)
- Def : Un nombre complexe x est dit entier algébrique s'il existe un polynôme $P \in \mathbb{Z}[X]$, unitaire tel que $P(x) = 0$.

- Ex : Les entiers naturels, les racines n^{ième} de l'unité, le nombre d'or sont des entiers algébriques.
- Prop : Un rationnel est un entier algébrique si et seulement si il est entier.
- Prop : Les entiers algébriques forment un sous-anneau de $\bar{\mathbb{Q}}$.
- Cor : Soit χ caractère de G, alors pour tout $g \in G$, $\chi(g)$ est un entier algébrique.
- Prop : Soit C une classe de conjugaison de G et χ un caractère irréductible. Alors pour tout $g \in C$, le nombre complexe $|C|\chi(g)/\chi(1)$ est un entier algébrique.
- Cor : Si de plus $\mathrm{pgcd}(|C|, \chi(1)) = 1$. Alors pour tout $g \in C$, $\chi(g)/\chi(1)$ est un entier algébrique et si $\chi(g) \neq 0$ alors $\rho(g)$ est une homothétie.
- DEV 2 : Thm de Burnside : Soient p et q dux nombres premiers distincts et α, β deux entiers positifs. Tout groupe fini d'ordre $p^\alpha q^\beta$ est résoluble.
- Cor : Si G est un groupe fini comme dans le théorème précédent avec $\alpha + \beta \geq 2$, alors G n'est pas simple.
- Cor : Le premier groupe simple non abélien est d'ordre 60, il s'agit de A_5.

Références Livre 1, Auteur(s) 1 : Sous-partie 1, Sous-partie 3.
Live 2, Auteur(s) 2 : Dev 1(Dev), Partie 2.
Livre 3 : Partie 3, Dev 2(Dev).

December 18, 2023

Toury Lucas, ENS Rennes