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

102

I- Le groupe des nombres complexes de module 1.

I.1- Définition et premières propriétés.

Déf 1: L'application $|\cdot|: \mathbb{C}^* \longrightarrow \mathbb{R}_+^*, z \longmapsto |z|$ est un morphisme de groupes. son noyau noté U est le groupe des nombres complexes de module 1.

Rmq 2: U est le cercle unité du plan complexe. C'est le plus grand (au sens de l'inclusion) sous-groupe borné de $\mathbb{C}^*$.

Théo 3: (décomposition polaire) L'application $f: U \times \mathbb{R}_+^* \longrightarrow \mathbb{C}^*, (z, r) \longmapsto rz$ est un isomorphisme.

Coro 4: Le groupe U est un compact connexe de $\mathbb{C}$.

I.2 - Exponentiel et trigonométrie.

Prop 5: L'application $\varphi: \mathbb{R} \longrightarrow U, x \longmapsto e^{ix}$ est un épimorphisme de groupes et son noyau est un sous-groupe discret de $\mathbb{R}$.

Notation 6: On note π le réel positif tel que $\ker\varphi = 2\pi\mathbb{Z}$.

Théo 7: (relèvement) Soit I un intervalle de $\mathbb{R}$. Toute application continue $f: I \longrightarrow U$ se relève en une application $\tilde{f}: I \longrightarrow \mathbb{R}$ telle que $e^{i\tilde{f}} = f$.

Coro 8: Tout morphisme continue de $\mathbb{R}$ dans U est de la forme $t \longmapsto e^{iat}$ pour un unique $a \in \mathbb{R}$.

App 9: Le groupe dual de U est isomorphe à $\mathbb{Z}$.

Déf 10: On définit $\cos x = \mathrm{Re}(\varphi(x))$ et $\sin x = \mathrm{Im}(\varphi(x))$.

Prop 11: 1/ Formule d'Euler: $\cos x = \dfrac{e^{ix} + e^{-ix}}{2}$, $\sin x = \dfrac{e^{ix} - e^{-ix}}{2i}$.

2/ Formule de Moivre: $(e^{ix})^n = \cos nx + i\sin nx$.

App 12: 1/ Linéarisation de $(\cos x)^n$ et $(\sin x)^n$ en vue d'une intégration par exemple;

2/ Calcul du noyau de Dirichlet et de Fejer.

I.3- Paramétrisation rationnelle.

Notons $M = (-1, 0)$ et pour tout $t \in \mathbb{R}$, $A_t = (0, t)$. L'intersection de la droite (MA_t) et $U \setminus \{M\}$ a pour coordonnées: $M_t = \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$.

Prop 13: L'application $\mathbb{R} \longrightarrow U \setminus \{M\}, t \longmapsto M_t$ est une bijection. Elle se prolonge à $\mathbb{R} \cup \{\infty\} \longrightarrow U$ en associant à ∞ le point M.

I.4 - Mesure d'un angle orienté.

Soit $\hat{A}$ l'ensemble des couples de vecteurs de $\mathbb{R}^2$. On définit une relation d'équivalence sur $\hat{A}$ par: $(u, v) \mathcal{R} (u', v') \Leftrightarrow \exists r \in SO_2(\mathbb{R})$ telle que $r(u) = u'$ et $r(v) = v'$.

Déf 14: La classe d'équivalence de (u,v) est appelée angle orienté de u et v. On note $\hat{A}$ l'ensemble des angles orientés.

Prop 15: L'application $\hat{A} \longrightarrow SO_2(\mathbb{R}), \alpha = (u,v) \longmapsto r_\alpha$, où r_α est l'unique rotation r telle que $r(u)=v$ est une bijection.

Rmq 16: Cette bijection munit $\hat{A}$ d'une structure de groupe.

Prop 17: L'application $g : \mathbb{R} \longrightarrow U \longrightarrow SO_2(\mathbb{R})$

$$\theta \longmapsto e^{i\theta} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

est surjective et son noyau est $2\pi\mathbb{Z}$.

Rmq 18: U et $SO_2(\mathbb{R})$ sont isomorphes à $\mathbb{R}/2\pi\mathbb{Z}$.

Déf 19: La mesure d'un angle orienté α est un réel θ tel que $e^{i\theta}$ est l'élément de U associé à r_α.

Rmq 20: La mesure d'un angle dépend du choix de l'orientation du plan.

II – Sous-groupes de U et racines de l'unité.

II.1 – Sous-groupes de U.

Prop 21: Un sous-groupe de U est dense ou fini.

Prop 22: Le sous-groupe $\langle e^{i\theta} \rangle = \{ e^{in\theta}, n \in \mathbb{Z} \}$ est dense si $\theta \notin 2\pi\mathbb{Q}$ et fini sinon.

App 23: L'ensemble des valeurs d'adhérence de la suite $(\sin n)_{n \geq 0}$ est le segment $[-1,1]$.

II.2 – Racines de l'unité.

Déf 24: L'application $U \longrightarrow U, z \longmapsto z^n$ est un morphisme de groupes. Son noyau U_n, est le groupe des racines $n^{\text{ièmes}}$ de l'unité.

Prop 25: L'application $\mathbb{Z}/n\mathbb{Z} \longrightarrow U_n$ est un isomorphisme de groupes $\quad k \longmapsto e^{\frac{2i\pi k}{n}}$

Cor 26: U_n est cyclique d'ordre n et engendré par l'ensemble $U_n^* = \{ e^{\frac{2i\pi k}{n}}, k \wedge n = 1 \}$ des racines primitives n-ièmes de l'unité.

Prop 27: $U_d \subseteq U_n \iff d \mid n$.

Prop 28: $U_n = \bigcup_{d \mid n} U_d$ et $|U_n^*| = \varphi(n)$.

App 29: $$n = \sum_{d \mid n} \varphi(d).$$

Prop 30: U_n est le seul sous-groupe d'ordre n de U.

App 31: Les sous-groupes finis de $SO_2(\mathbb{R})$ sont cycliques de la forme $\{ r_{\frac{2k\pi}{n}}, k = 1, \dots, n \}$ pour $n \in \mathbb{N}^*$ et avec r_θ la rotation d'angle θ.

App 32: Soit G un groupe fini de cardinal n.

1.) Soit $\rho : G \longrightarrow GL(V)$ une représentation de G. Pour tout $g \in G$, $\rho(g)$ est diagonalisable et son spectre est inclu dans U_n.

2.) Les éléments du dual de G sont les morphismes de G dans U_n.

III - Polynômes cyclotomiques.

Déf 33: Pour $n \in \mathbb{N}^*$, on définit le n-ième polynôme cyclotomique par : $\Phi_n(X) = \prod_{\xi \in U_n^*} (X - \xi)$.

Exple 34: $\Phi_1(X) = X - 1$; $\Phi_2(X) = X + 1$; $\Phi_3(X) = X^2 + X + 1$.

Prop 35: i) Φ_n est unitaire de degré $\varphi(n)$ à coefficients dans $\mathbb{Z}$.

ii) $X^n - 1 = \prod_{d|n} \Phi_d$.

iii) $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$, où μ désigne la fonction de Möbius.

Théo 36: Φ_n est irréductible sur $\mathbb{Q}$.

Cor 37: Le polynôme minimal d'une racine primitive n-ième de l'unité est Φ_n.

Théo 38: (Kronecker) Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose que $P(0) \neq 0$. Alors les racines de P sont des racines de l'unité. Si P est en plus irréductible, alors P est un polynôme cyclotomique.

App 39: 1.) (Wedderburn) Tout corps fini est commutatif.

2.) (Dirichlet faible) Pour $n \geq 1$ fixé, il existe une infinité de nombres premiers congrus à 1 modulo n.

IV - Transformée de Fourier discrète. [PEY]

Déf 40: Soient $f := \{f_0, \dots, f_{N-1}\}$ un échantillon de taille N et $w_N = e^{\frac{2i\pi}{N}}$. On définit la transformée de Fourier discrète de f comme le vecteur $\hat{f} = \{\hat{f}_0, \dots, \hat{f}_{N-1}\}$ avec $\hat{f}_k := \sum_{n=0}^{N-1} f_n w_N^{-nk}$.

Prop 41: Soit $\mathcal{F} : \mathbb{C}^N \longrightarrow \mathbb{C}^N$, $f \longmapsto \hat{f}$. $\mathcal{F}$ est un isomorphisme d'espace vectoriels.

Prop 42: On a la formule d'inversion suivante :

$$f_n = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}_k w_N^{nk}, \quad \forall n = 0, \dots, N-1.$$

App 43: Soit $c = (c_0, \dots, c_{N-1}) \in \mathbb{C}^N$. On pose $M = \begin{pmatrix} c_0 & c_{N-1} & \cdots & c_1 \\ c_1 & c_0 & \ddots & c_2 \\ \vdots & \ddots & \ddots & \vdots \\ c_{N-1} & c_{N-2} & \cdots & c_0 \end{pmatrix}$. Alors M est diagonalisable et le spectre de M est $\hat{c}$. ∎

Références : 1/ Audin ;

2/ Oraux X-ENS 1 ;

3/ Perrin ;

4/ Gozard ;

5/ Combes.

6/ Peyré.

Théorème (Kronecker): Soit $P = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$, avec $a_n \neq 0$. Supposons que les racines $\alpha_1, \ldots, \alpha_n$ complexes de P comptées avec multiplicité sont telles que :

$$0 < |\alpha_i| \leq 1 \quad , \forall i \in \{1, \ldots, n\}.$$

Alors, α_i est une racine de l'unité pour tout $i \in \{1, \ldots, n\}$ si de plus P est irréductible, alors P est un polynôme cyclotomique.

Preuve:

Soit E_n l'ensemble de tels polynômes de degré n.

Objectif 1: Montrons que E_n est fini.

Soient $Q = X^n + b_1 X^{n-1} + \cdots + b_n \in E$ et $\beta_1, \ldots, \beta_n$ les racines complexes comptées avec multiplicité. Il suffira de démontrer que les b_j appartiennent à un sous-ensemble fini de $\mathbb{Z}$.

Par les relations coefficients-racines, on a :

$$b_j = (-1)^j \sigma_j(\beta_1, \ldots, \beta_n) \quad , j \in \{1, \ldots, n\} \text{ et } \sigma_j$$

désigne le $j^{ième}$ polynôme symétrique élémentaire.

Comme $|\beta_i| \leq 1$, on a :

$$|b_j| = |\sigma_j(\beta_1, \ldots, \beta_n)| = \left| \sum_{1 \leq i_1 < \cdots < i_j \leq n} \beta_{i_1} \cdots \beta_{i_j} \right|$$

$$\leq \sum_{1 \leq i_1 < \cdots < i_j \leq n} |\beta_{i_1} \cdots \beta_{i_j}| \leq C_n^j \quad (1)$$

$b_j \in \mathbb{Z}$, alors d'après (1), $b_j \in H_j = \{-C_n^j, \ldots, 0, \ldots, C_n^j\}$

$\text{card}(H_j) = 2C_n^j + 1$

Conclusion: $\text{Card}(E_n) \leq \prod_{j=1}^{n} (2C_n^j + 1) < +\infty$.

Posons $P_k(X) = (X-\alpha_1^k)\cdots(X-\alpha_n^k)$, $k \in \mathbb{N}^*$.

P_k est un polynôme unitaire de degré n et son coefficient non constant est non nul puisque ce dernier est égal à $(-1)^n \alpha_1^k \cdots \alpha_n^k$ par les relations coefficients - racines.

Objectif 2 : Montrons que $P_k \in E_n$ pour tout $k \in \mathbb{N}^*$.

Sachant que $|\alpha_i^k| \leq 1$, $\forall i \in \{1, \dots, n\}$ et $k \in \mathbb{N}^*$, il reste à montrer que $P_k(X) \in \mathbb{Z}[X]$. Pour ce faire, soient $Q_k(X,Y) = Y - X^k \in \mathbb{Z}[X,Y]$ et $R_k = \mathrm{Res}_X(P, Q_k)$.

Comme $P, Q_k \in \mathbb{Z}[X,Y]$, alors $R_k \in \mathbb{Z}[Y]$ et

$$R_k(Y) = \prod_{i=1}^{n} Q_k(\alpha_i, Y) = \prod_{i=1}^{n} (Y - \alpha_i^k) = P_k(Y).$$ Ainsi P_k est à coefficients dans $\mathbb{Z}$.

Conclusion : $P_k \in E_n$, $\forall k \in \mathbb{N}^*$.

Posons $\phi_i : \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{C}^* \\ k & \longmapsto & \alpha_i^k \end{array}$.

Conséquences de 1 et 2 : En étant fini, il n'existe qu'un nombre fini de P_k distincts et l'ensemble Z_n des racines des P_k est fini. Par conséquent, l'application ϕ_i est non injective. On en déduit qu'il existe $k_1 \neq k_2$ tels que $\alpha_i^{k_1} = \alpha_i^{k_2}$. Supposons que $k_1 > k_2$. Alors on a :

$$\alpha_i^{k_1 - k_2} = 1 \quad \text{donc} \quad \alpha_i \in U_{k_1 - k_2}.$$

Ceci étant vrai pour $i \in \{1, \dots, n\}$, on a le résultat voulu.

- Si P est irréductible.

P est unitaire et irréductible sur $\mathbb{Z}$, alors P est irréductible sur $\mathbb{Q}$. Par conséquent, P est scindé à racines simples sur $\mathbb{C}$. Ainsi, P admet n racines distinctes sur $\mathbb{C}$. Ces dernières étant des racines de l'unité, notons m_i l'ordre de α_i et posons $m = \text{ppcm}(m_1, \dots, m_n)$. On a :

$$\alpha_i^m = 1 \ , \forall i \in \{1, \dots, n\} \Rightarrow X - \alpha_i \mid X^m - 1 \quad (2)$$

P scindé à racines simples, alors $(X - \alpha_i)$ sont deux à deux premiers entre eux et $P = \prod_{i=1}^{n} (X - \alpha_i)$.

D'après (2), P divise $X^m - 1 = \prod_{d \mid m} \Phi_d(X)$.

Comme P est irréductible, il existe $d \mid m$ tel que $P \mid \Phi_d(X)$.

Φ_d étant irréductible sur $\mathbb{Q}$, on a : $P = \Phi_d$.

Références : 1/ Oraux X-ENS, algèbre 1

2/ Szpirglas, Arivia Algèbre L3