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 S^1

Déf ① On appelle groupe des nombres complexes de module 1, le noyau du morphisme de groupe suivant : $\begin{pmatrix} \mathbb{C}^\times \to \mathbb{R}_+^\times \\ z \mapsto |z| \end{pmatrix}$

on le note $\mathbb{U} = \{z \in \mathbb{C}^\times, |z| = 1\} \triangleleft (\mathbb{C}^\times, \times)$

Rmq ② $\mathbb{U}$ n'est autre que le cercle unité S^1 de $\mathbb{C}$.

Théo ③ L'application $\rho : \begin{pmatrix} \mathbb{R}_+^\times \times \mathbb{U} \to \mathbb{C}^\times \\ (r, u) \mapsto ru \end{pmatrix}$ définit un isomorphisme.

Théo ④ L'application $e : \begin{pmatrix} (\mathbb{R},+) \to (\mathbb{U}, \times) \\ x \mapsto e^{ix} \end{pmatrix}$ est un morphisme surjectif, 2π-périodique, de noyau $\mathrm{Ker}(e) = 2\pi\mathbb{Z}$.

On en déduit, l'isomorphisme suivant : $\boxed{\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}}$

2°) Applications trigonométriques.

Déf ⑤ Les fonctions $\begin{pmatrix} \mathbb{R} \to \mathbb{R} \\ x \mapsto Re(e^{ix}) \end{pmatrix}$ et $\begin{pmatrix} \mathbb{R} \to \mathbb{R} \\ x \mapsto Im(e^{ix}) \end{pmatrix}$ sont appelés fonctions cosinus et sinus.

Prop ⑥ • Formule de Moivre : $\forall n \in \mathbb{N}, \ e^{inx} = \cos(nx) + i\sin(nx)$

• Formule d'Euler : $\cos(x) = \dfrac{e^{ix} + e^{-ix}}{2}$, $\sin(x) = \dfrac{e^{ix} - e^{-ix}}{2i}$

Ex ⑦ $e^{2i\pi/3} = j$, $e^{-2i\pi/3} = j^2$, $e^{i\pi/2} = i$, $e^{i\pi} = -1$

App ⑧ $\displaystyle\sum_{k=0}^{n} \cos(k\theta) = \cos\left(\frac{n\theta}{2}\right) \frac{\sin\left(\frac{n+1}{2}\theta\right)}{\sin\left(\frac{\theta}{2}\right)} \quad \forall \theta \in \mathbb{R}\backslash 2\pi\mathbb{Z}$.

App ⑨ Linéarisation $\cos^n x$: $\cos^n(x) = \dfrac{1}{2^n} \cdot \displaystyle\sum_{k=0}^{n} \binom{n}{k} e^{i(2k-n)x}$

App ⑩ Expression de $\cos(nx)$ comme un polynôme en $\cos(x)$:

$\cos(nx) = T_n(\cos x)$ où $T_n(y) = \displaystyle\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} y^{n-2k} \cdot (1-y^2)^k \cdot (-1)^k$ le polynôme de Tchebychev.

3°) Paramétrisation sur le cercle unité.

Déf ⑪ On appelle équation de Diophante, l'équation :

$\forall (x,y,z) \in \mathbb{N}^3, \quad x^2 + y^2 = z^2$.

Prop ⑫ $(x,y,z) \in \mathbb{N}^3$ solution de $x^2 + y^2 = z^2$ $\iff$ $\left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{Q}^2$ avec $z \neq 0$, solution de l'équation : $X^2 + Y^2 = 1$

Théo ⑬ Paramétrisation du cercle S^1 :

L'application $\begin{pmatrix} \mathbb{R} \to \mathbb{U}\backslash\{M\} \\ t \mapsto M_t \end{pmatrix}$ est une bijection où $M = (-1, 0)$

et $M_t = \left(-\dfrac{(t^2-1)}{t^2+1}, \dfrac{2t}{t^2+1}\right)$.

Elle se prolonge en : $\begin{pmatrix} \mathbb{R} \cup \{\infty\} \to \mathbb{U} \\ t \mapsto M_t \end{pmatrix}$ en associant à ∞ le point M.

4°) Angles et Rotations :

Déf ⑭ Les isométries positives d'un plan euclidien, notée $O^+(2)$, sont les rotations du plan.

Prop ⑮ $O^+(2) = \left\{ M \in \mathcal{M}_2(\mathbb{R}) \ / \ M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a^2 + b^2 = 1 \right\}$

Prop : $O^+(2)$ est isomorphe et homéomorphe au groupe $\mathbb{U}$, par l'application $\rho : \begin{pmatrix} \mathbb{U} \to O^+(2) \\ a+ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{pmatrix}$

Cor ⑯ $O^+(2)$ commutatif.

Prop ⑰ Étant donnés deux vecteurs unitaires $(u, v) \in \mathbb{R}^2$,

$\exists! \, r \in O^+(2) \ / \ r(u) = v$

Déf ⑱ On appelle par $\hat{\mathcal{A}}$, l'ensemble des couples de vecteurs unitaires de $\mathbb{R}^2$

on définit une relation d'équivalence sur $\hat{\mathcal{A}}$ par :

$(u, v) \sim (u', v') \iff \exists f \in O^+(2) \ / \ f(u) = u', f(v) = v'$

on appelle angle orienté de (u, v), la classe d'équivalence de (u,v) par la RE $\sim$.

on note $\mathcal{A} := \hat{\mathcal{A}}/\sim$ l'ensemble des angles orientés de vecteurs

Prop (19) L'application ϕ de $\hat{A}/\sim$ dans $O^+(2)$, qui a un représentant (u, v) associe l'unique $f \in O^+(2)$ tel que $f(u) = v$, est bien défini et est une bijection.

cor (20) L'application $\begin{pmatrix} \mathbb{R} \longrightarrow O^+(2) \\ \theta \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{pmatrix}$ est surjective, 2π-périodique, de noyau $2\pi\mathbb{Z}$.

Elle induit l'isomorphisme : $\begin{pmatrix} \mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\simeq} O^+(2) \\ \theta \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{pmatrix}$

qui permet de définir une mesure des angles orientés de vecteurs

II - Racines de l'unité et Applications :

1°) Définition - Propriétés - Racines de l'unité.

Def (21) Le morphisme de groupe $\pi : \begin{pmatrix} \mathbb{U} \longrightarrow \mathbb{U} \\ z \longmapsto z^n \end{pmatrix}$ a pour noyau,

$\operatorname{Ker} \pi = \{ z \in \mathbb{U},\ z^n = 1 \}$. on le note μ_n.

Un élément de μ_n est appelé racine n-ième de l'unité.

Prop (22) L'application $\begin{pmatrix} \mathbb{Z}/n\mathbb{Z} \longrightarrow \mu_n \\ k \longmapsto e^{2ik\pi/n} \end{pmatrix}$ est un isomorphisme de groupe.

cor (23) μ_n est un groupe cyclique d'ordre n : $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$.

App (24) Le seul sous groupe fini de $(\mathbb{C}^*, \times)$ de cardinal n est μ_n.

App (25) Théorème de Kronecker : $\boxed{\text{DVLP n°1}}$

soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes sont toutes de module inférieur ou égal à 1. on suppose $P(0) \neq 0$.

Alors toutes les racines de P sont des racines de l'unité.

Rmq (26) Les racines n-ième de l'unité sont les sommets d'un polygone régulier à n côtés.

Def (27) on appelle racine nieme primitive de l'unité dans $\mathbb{C}$, tout générateur du groupe μ_n.

on note μ_n^* l'ensemble de ces racines.

Prop (28) • $\mu_n^* = \{ e^{2ik\pi/n},\ k \in [\![0, n-1]\!],\ k \wedge n = 1 \}$

• $|\mu_n^*| = \varphi(n)$

Ex (29) $\mu_2^* = \{-1\}$, $\mu_3^* = \{j, j^2\}$, $\mu_5^* = \mu_5 \setminus \{1\}$, $\mu_{12}^* = \{ e^{i\pi/6}, e^{-i\pi/6}, e^{5i\pi/6}, e^{-5i\pi/6} \}$

Prop (30) $\mu_d \subseteq \mu_n \iff d \mid n$

Prop (31) $\mu_n = \bigsqcup_{d \mid n} \mu_d^*$

App (32) $n = \sum_{d \mid n} \varphi(d)$

2°) Polynomes cyclotomiques.

Def (33) on appelle n-ième polynome cyclotomique sur $\mathbb{Q}$, le polynome :

$$\phi_n = \prod_{\omega \in \mu_n^*} (X - \omega) = \prod_{\omega \in \{ e^{2ik\pi/n},\ k \wedge n = 1 \}} (X - \omega)$$

Ex (34) $\phi_1 = X - 1$, $\phi_2 = X + 1$, $\phi_3 = X^2 + X + 1$

Prop (35) i) $X^n - 1 = \prod_{d \mid n} \phi_d$ (permet de calculer les ϕ_i par récurrence)

ii) ϕ_n est unitaire, de degré $\varphi(n)$

iii) $\phi_n \in \mathbb{Z}[X]$, irreductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$. $\boxed{\text{DVLP n°2}}$

App (36) $\forall p$ premier, $\phi_{p^n} = \sum_{0}^{p-1} (X^{p^{n-1}})^k$

App (37) Corollaire du théorème de Kronecker. $\boxed{\text{DVLP n°1}}$

(si) $P \in \mathbb{Z}[X]$ unitaire, irreductible, à racines de module ≤ 1

alors $P = X$ ou P est un polynome cyclotomique

Théo (38) (si) $\omega \in \mu_n^*$ alors ϕ_n est le polynome minimal de ω,

et $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.

on appelle $\mathbb{Q}(\omega)$ extension cyclotomique.

3°) polygones réguliers.

Def (39) soit $n \in \mathbb{N}$ avec $n \geq 3$. Dans le plan $\mathbb{R}^2$, considérons le polygone régulier convexe P_n à n sommets formé par les affixes des racines n-ième de l'unité $\omega_k = e^{2ik\pi/n}$, avec $k \in \{0, \dots, n-1\}$.

Le groupe Diedral D_n est le sous groupe des isometries du plan affine qui laissent P_n invariant.

Prop (40) soit $n \geq 3$. Le groupe diédral D_n est d'ordre $2n$ et il est engendré par la symétrie axiale s et la rotat° r d'angle $\theta = \frac{2\pi}{n}$ définis par : $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ avec $\theta = \frac{2\pi}{n}$

$D_n = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle$.

Déf (41) on se place dans un plan affine euclidien $\mathbb{R}^2$, muni d'un repère oxy. On dit qu'un point M du plan est constructible en une étape à partir de P_0 (partie de $\mathbb{R}^2$ / $\# P_0 \geq 2$) par la règle et le compas ssi M est le point d'intersection de :

- 2 cercles distincts (cercle de centre un point A de P_0, de rayon $\|AB\|$ avec $B \in P_0$)
- ou 1 droite et 1 cercle
- ou 2 droites distinctes (droite passant par 2 points de P_0)

Prop/Déf (42) soit $x \in \mathbb{R}$. $[(x,0)$ constructible $\Leftrightarrow (0,x)$ constructible$]$. Ainsi, "x" constructible

Prop (43) $M(x,y)$ est un point constructible $\Leftrightarrow$ x, y sont des nombres constructibles.

Thm (44) Wantzel soit $t \in \mathbb{R}$.

$[t$ est constructible $\Leftrightarrow \exists$ une suite finie $(K_0, K_1, \dots, K_p)$ de sous corps de $\mathbb{R}$ / $t \in L^p$, $\forall i \in [\![0, p-1]\!]$, L_{i+1}/L_i extension quadratique, $L_0 = \mathbb{Q}]$

Cor (45) ssi $x \in \mathbb{R}$ est constructible alors $\exists e \in \mathbb{N}$ / $[\mathbb{Q}(x) : \mathbb{Q}] = 2^e$

Déf (46) soit $n \in \mathbb{N}^*$. on dit que le polygone régulier à n côtés est constructible ssi l'angle $\frac{2\pi}{n}$ est constructible.

Déf (47) Les nombres de Fermat, sont les nombres de la forme :

$$\forall n \in \mathbb{N}, \quad F_n = 2^{2^n} + 1$$

Thm (48) Gauss - Wantzel :

soit $p \geq 3$ nombre premier. soit $\alpha \in \mathbb{N}^*$.

le polygone régulier à p^α côtés est constructible $\Leftrightarrow$ $\alpha = 1$ et p un nombre premier de Fermat.

Ex (49).
- Les polygones réguliers à 5 côtés, 17 côtés sont constructibles.
- les polygones réguliers à 7 côtés, p^2 côtés ne sont pas constructibles.

III - Représentations des groupes finis.

Déf (50) soit V un $\mathbb{C}$-ev de dimension finie n. soit G un groupe fini. Une représentation linéaire de G est la donnée d'un ev V et d'un morphisme de groupe $\rho : (G \to GL(V))$. on la note (ρ, V)

Prop (51) soit G un groupe fini d'ordre n. soit (ρ, V) représentation de G. Alors $\forall g \in G$, $\rho(g)$ est diagonalisable et son spectre est inclu dans μ_n.

Prop (52) soit G un groupe fini.

ssi G est abélien alors toutes les représentations (resp caractères) irréductibles sont de degré un, à valeurs dans μ_n.

App (53) Table de Caractère d'un groupe cyclique : $G = \langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$

	1	g	g^2	$\dots$	g^{n-1}
χ_1	1	1	1	$\dots$	1
χ_2	1	ω_n	ω_n^2	$\dots$	ω_n^{n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$		
χ_n	1	ω_n^{n-1}	$\omega_n^{2(n-1)}$	$\dots$	$\omega_n^{(n-1)(n-1)}$

avec $\omega_n = e^{2i\pi/n}$

App (54) Table de caractère du groupe Diédral : D_n

soit n pair. Alors D_n admet $\frac{n}{2} - 1$ représentations irréductibles de degré deux définies par :

$$\forall h \in [\![1, \tfrac{n}{2} - 1]\!], \quad \rho_h(r^k) = \begin{pmatrix} \omega_n^{hk} & 0 \\ 0 & \omega_n^{-hk} \end{pmatrix}, \quad \rho_h(sr^k) = \begin{pmatrix} 0 & \omega_n^{-hk} \\ \omega_n^{hk} & 0 \end{pmatrix}$$

Référence : Audin / Combes / Gozard /