113 Groupe des nombres complexes de module un. Sous groupes des racines de l'unité. Applications

I] Groupe des nombres complexes de module un

Def: On appelle groupe des nombres complexes de module un
$$\mathbb{U} = \{ z \in \mathbb{C} \,,\, |z| = 1 \}$$

C'est un groupe topologique commutatif compact. C'est le noyau du morphisme
$$\begin{aligned} (\mathbb{C}^\times, \cdot) &\longrightarrow (\mathbb{R}^\times_+, \cdot) \\ z &\longmapsto |z| \end{aligned}$$

I.1] L'exponentielle [Rud]

On note $\exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}$ la série entière de rayon de convergence infini (noté aussi e^z)

Prop: (i) $\exp$ est holomorphe sur $\mathbb{C}$, $\exp' = \exp$

(ii) $f : (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times)$, $t \longmapsto e^{it}$ morphisme continue, surjectif non injectif

Donc $\mathrm{Ker}(f)$ est un sous groupe strict de $\mathbb{R}$ fermé, donc discret.

Def: On note π l'unique élément positif tq $\mathrm{Ker}(f) = 2\pi\mathbb{Z}$

I.2] Cosinus/sinus

Def: On définit pour $x \in \mathbb{R}$, $\cos x = \mathrm{Re}(f(x))$ et $\sin x = \mathrm{Im}(f(x))$

Prop: (i) (Euler) $\cos x = \frac{e^{ix} + e^{-ix}}{2}$ et $\sin x = \frac{e^{ix} - e^{-ix}}{2i}$

(ii) (Moivre) $e^{inx} = \cos(nx) + i\sin(nx)$

Application: formule de linéarisation de $\cos^n(x)$ et $\sin^n(x)$

I.3] Théorème du relèvement [CL1] [CL3]

On identifie $\mathbb{C}$ à $\mathbb{R}^2$ et $\mathbb{U}$ au cercle S^1

Thm: (i) Soit $\varphi : [a,b] \longrightarrow S^1$ $\mathcal{C}^k$ $(k \geq 0)$ alors il existe $\tilde{\varphi} : [a,b] \longrightarrow \mathbb{R}$ tq $e^{i\tilde{\varphi}(t)} = \varphi(t)$, $\forall t \in [a,b]$

$\tilde{\varphi}$ est appelé un relèvement de φ

(ii) $\tilde{\varphi}$ est unique modulo 2π

Applications: Soit $\gamma : [0,1] \longrightarrow \mathbb{C}^\times$ lacet $\mathcal{C}^0$ alors $\theta : [0,1] \to \mathbb{R}$, $\theta = \gamma/|\gamma|$ est un relèvement

la quantité $\mathrm{Ind}_0(\gamma) = \frac{\theta(1) - \theta(0)}{2\pi}$ est un entier indépendant de θ (indice de γ par rapport à 0)

I.4] Sous groupes de $\mathbb{U}$

Thm: Un sous-groupe de $\mathbb{U}$ est soit dense, soit un groupe des racines $n$ième de l'unité

Application : (au système dynamique)

On identifie $\mathbb{U}$ au tore $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ et pour $\alpha \in \mathbb{T}$, on note $R_\alpha = \begin{array}{l} \mathbb{T} \longrightarrow \mathbb{T} \\ x \longmapsto x+\alpha \end{array}$ la rotation d'angle α

alors (i) si $\alpha = p/q \in \mathbb{Q}$, tout orbite de R_α est périodique de période q

(ii) si $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, toute orbite de R_α est dense

on dit que R_α est minimale

II| Angles et géométrie

II.1| Argument

Par I.1|, on a la suite exacte

$$0 \longrightarrow 2\pi\mathbb{Z} \longrightarrow \mathbb{R} \xrightarrow{f} \mathbb{U} \longrightarrow 0$$
$$[t] \longmapsto t \longmapsto e^{it}$$

Prop : (i) Il n'existe pas de scindage continue de f ($\nexists\, \varphi\ \mathcal{C}^0$ tq $f \circ \varphi = \mathrm{Id}_{\mathbb{U}}$)

(ii) $\tilde{f} : \mathbb{R}/2\pi\mathbb{Z} \longrightarrow \mathbb{U}$ isomorphisme, homéomorphisme

Rq : (i) est dû au problème de relèvement I.3|

Déf : On note Arg la fonction argument définit pour $z \in \mathbb{C}^*$ par $\mathrm{Arg}(z) = \tilde{f}^{-1}\left(\frac{z}{|z|}\right)$

II.2| $\mathbb{U} \simeq SO(2)$ [T]

On a le morphisme naturel $\Psi : (\mathbb{C}^\times, \times) \longrightarrow (GL_2(\mathbb{R}), \times)$
$$a+ib \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Prop : $\Psi(\mathbb{U})$ est isomorphe et homéomorphe à $SO(2)$

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

Applications : 1| $SO(2)$ groupe commutatif

2| On a un isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \longrightarrow SO(2)$
$$\theta \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

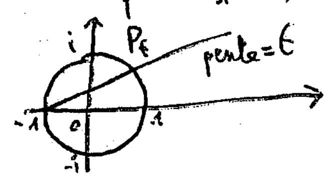
3) On peut définir sur tout plan euclidien orienté une mesure des angles orientés de vecteurs

II.3| Paramétrisation rationnelle de $\mathbb{U}$ [C]

On identifie $\mathbb{C}$ à $\mathbb{R}^2$

Une paramétrisation rationnelle du cercle unité par $\mathbb{P}_1(\mathbb{R})$ est donnée par

$$\begin{array}{lcl} \mathbb{P}_1(\mathbb{R}) & \longrightarrow & \mathbb{U} \\ t & \longmapsto & P_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \\ \infty & \longmapsto & (-1, 0) \end{array}$$



Application : permet de trouver les solutions entières du théorème de Pythagore $a^2+b^2=c^2$, $(a,b,c) \in \mathbb{Z}^3$

III] sous-groupe fini de $\mathbb{U}$

On note $\mu_n = \{ z \in \mathbb{C},\ z^n = 1 \}$ le sous groupe de $\mathbb{U}$ des racines $n^{\text{ième}}$ de l'unité. On a $\mu_n = \{ e^{2i\pi k/n},\ k \in [\![0, n-1]\!] \}$

Prop : μ_n est cyclique (isomorphe à $\mathbb{Z}/n\mathbb{Z}$). On note μ_n^* ses générateurs (ce sont les racines primitives de l'unité définies par $e^{2i\pi k/n}$ avec $k \wedge n = 1$)

III.1] Polynomes cyclotomiques [GOU]

Def : On définit le $n^{\text{ième}}$ polynome cyclotomique par

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Thm : (i) $\Phi_n \in \mathbb{Z}[X]$ et il est irréductible sur $\mathbb{Q}$

(ii) (Kronecker) Soit $P \in \mathbb{Z}[X]$ unitaire, irréductible sur $\mathbb{Q}$ n'ayant que ces racines de module ≤ 1 alors $P = X$ ou $P = \Phi_m$, $m \geq 1$

Applications : 1) (Dirichlet faible) pour $n \geq 2$, il existe une infinité de nb 1er congru à 1 mod n [FGN 1]

2) (Wedderburn) Tout corps fini est commutatif [P]

III.2] Polygones de Gauss [Car]

En identifiant $\mathbb{C}$ à $\mathbb{R}^2$, on peut voir μ_n comme un n-gône régulier (noté P_n)

Def : On se donne les points d'affixe 0 et 1 de $\mathbb{C}$, $z \in \mathbb{C}$ est constructible si z est constructible à la règle et au compas en un nombre fini d'étapes à partir de 0 et 1.

Thm : (Wantzel) z est constructible $\iff$ $z \in L/\mathbb{Q}$ tel que $\exists!$ une tour d'extensions $\mathbb{Q} = L_0 \subseteq L_1 \subseteq \dots \subseteq L_n = L$ avec $[L_i : L_{i-1}] = 2$, $\forall i$

Application : (Gauss) Le polygone à n-côtés P_n est constructible si et seulement si $n = 2^\alpha$, $\alpha \geq 2$
ou $n = 2^\beta p_1 \dots p_r$ avec p_i nombres premiers de Fermat distincts et $\beta \geq 1$

Exemple : $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$

P_5 est constructible car $\left[\mathbb{Q}[e^{2i\pi/5}] : \mathbb{Q}\right] = 2$
→ 5 est un nombre premier de Fermat

III.3] Quelques utilisations

1) Transformée de Fourier rapide

* multiplication de 2 polynomes en $O(n \log n)$

2) Calcul du déterminant d'une matrice circulante

$C = (c_0, \dots, c_{n-1}) \in M_n(\mathbb{R})$ matrice circulante alors

$\det C = \prod_{k=0}^{n-1} P_c(w^k)$ avec $P_c(J) = C = \sum_{j=0}^{n-1} c_j J^j$

$J = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 1 & & & 0 \end{pmatrix}$ et $w = e^{2i\pi/n}$

[C] Combes ~~ (Mneimné)

[Car] Carrega "Théorie des corps ...

[CL1] Chambert Loir Analyse 1

[CL3) Chambert Loir Analyse 3

[GOU] Gourdon "Algèbre"

[RUD] Rudin "Analyse complexe ..

[T] Tauvel Géométrie

[W] Warusfel Structures algébriques finies

Developpements possibles

- Gauss
- Kronecker
- Irreductibilité de Φ_n
- Wedderburn
- solution entières de Pythagore
- Construction des angles orientés
- Relevement
- determinant circulant