113. Groupe des nombres complexes de module 1. Applications

(I) Groupe des nombres complexes de module 1

Def: On note $\mathbb{U}$ le noyau du morphisme de gpes $f : (\mathbb{C}^*, \cdot) \longrightarrow (\mathbb{R}_+^*, \cdot)$, $z \longmapsto |z|$. C'est un sous-gpe du gpe multiplicatif $\mathbb{C}^*$, que l'on appelle gpe des nbres complexes de module 1.

Rq: $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ est le cercle unité de $\mathbb{C}$.

1) L'exponentielle complexe et fonct° trigonométriques réelles

Def: On note $\exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}$ la série entière de rayon de convergence $R = +\infty$ (notée aussi e^z).

Thm: - L'applicat° $\exp : (\mathbb{C}, +) \longrightarrow (\mathbb{C}^*, \cdot)$, $z \longmapsto e^z$ est un morphisme de gpes continu, surjectif et non injectif.

- L'applicat° $f : (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \cdot)$, $t \longmapsto e^{it}$ est un morphisme de gpes continu, surjectif et non injectif, de noyau $2\pi\mathbb{Z}$ où 2π est le plus petit réel strictement positif a tq $e^{ia} = 1$.

Coroll IR: L'application f induit un isomorphisme $\tilde{f} : t \longmapsto e^{it}$ de $(\mathbb{R}/2\pi\mathbb{Z}, +)$ sur $(\mathbb{U}, \cdot)$.

Def: Si $z \in \mathbb{C}^*$, l'argument de z, noté $\arg(z)$, est défini par : $\arg(z) = \tilde{f}^{-1}\left(\frac{z}{|z|}\right)$. Tout représentant θ de $\arg(z)$ dans $\mathbb{R}$ est appelé un argument de z et on a donc $z = |z| e^{i\theta}$.

Def: On définit les fonctions trigonométriques réelles cosinus et sinus par : $\forall x \in \mathbb{R}$, $\cos(x) = \mathrm{Re}(f(x))$ et $\sin(x) = \mathrm{Im}(f(x))$, ce qui conduit à l'égalité : $e^{x+iy} = e^x(\cos(y) + i\sin(y))$; $(x, y) \in \mathbb{R}^2$.

Prop: [Formules d'Euler] $\forall x \in \mathbb{R}$, $\cos(x) = \frac{e^{ix} + e^{-ix}}{2}$ et $\sin(x) = \frac{e^{ix} - e^{-ix}}{2i}$

Prop: [Formule de Moivre] $\forall m \in \mathbb{Z}$, $(\cos(x) + i\sin(x))^m = \cos(mx) + i\sin(mx)$; $x \in \mathbb{R}$

Applicat°: - Formules de linéarisation de $\cos^m(x)$ et $\sin^m(x)$

- Calcul de sommes :

exple : $\forall m \in \mathbb{N}$, $S_m = \sum_{k=0}^{m} e^{ik\theta} = \begin{cases} e^{i\frac{m\theta}{2}} \dfrac{\sin\left(\left(\frac{m+1}{2}\right)\theta\right)}{\sin\left(\frac{\theta}{2}\right)} & \text{si } \theta \not\equiv 2\pi\mathbb{Z} \\ m+1 & \text{sinon} \end{cases}$

2) Sous-gpes de $\mathbb{U}$

a) Racines de l'unité

Notat°: On note $\mu_m = \{z \in \mathbb{C} \mid z^m = 1\}$ le ss-gpe de $\mathbb{U}$ des racines m-ièmes de l'unité. On a $\mu_m = \{e^{2ik\pi/m} ;\ 0 \leq k \leq m-1\}$

Prop: μ_m est cyclique d'ordre m.

Cocyc: μ_m est isomorphe au gpe additif $\mathbb{Z}/m\mathbb{Z}$

Thm: Si $\mathbb{K}$ est un corps commutatif, tout ss-gpe fini du gpe multiplicatif $\mathbb{K}^*$ est cyclique.

Coroll IR: le seul sous-gpe fini d'ordre m du gpe $\mathbb{U}$ est μ_m.

Def: Les générateurs de μ_m sont appelés les racines m-ièmes primitives de l'unité. Leur ensemble est noté μ_m^*.

Cocyc: $\mu_m^* = \{e^{\frac{2ik\pi}{m}} : 0 \leq k \leq m-1,\ k \wedge m = 1\}$ et est de cardinal $\varphi(m)$.

Prop: $\mu_m = \bigsqcup_{d|m} \mu_d^*$

b) Autres sous-gpes de $\mathbb{U}$

Prop: Soit H un sous-gpe fermé de $\mathbb{U}$. Alors soit $H = \mathbb{U}$, soit H est fini et égal à μ_m où m est son ordre.

Applicat°: Thm de Kronecker :

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $m \geq 1$ et irréductible de $\mathbb{Q}[X]$. On suppose que toutes les racines de P sont de module ≤ 1.
Alors $P = X$ ou bien il existe $k \in \mathbb{N}^*$ tq $P \mid (X^k - 1)$.

← (DVPT)

(II) Applications en algèbre

1) Cyclotomie

Def: Soit m un entier > 0. On appelle m-ième polynôme cyclotomique et on note $\Phi_m(X)$, le pdt $\prod_{\zeta} (X - \zeta)$, où ζ parcourt les racines primitives m-ièmes de l'unité de $\mathbb{C}$. On a donc $\Phi_m(X) = \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^*} \left(X - e^{\frac{2ik\pi}{m}}\right)$.

Prop: a) Φ_m est un polynôme unitaire à coefficients entiers, de degré $\varphi(m)$.

b) le polynôme $X^m - 1$ est le pdt des $\Phi_d(X)$ pour tous les diviseurs d de m.

Thm: Pour chaque entier $m > 0$, le polynôme $\Phi_m(X)$ est irréductible de $\mathbb{Q}[X]$

Applicat°: i) Dans le 2° cas du thm de Kronecker, P est un polynôme irréductible de $\mathbb{Q}[X]$ divisant $X^k - 1$. C'est donc un polynôme cyclotomique.

← (DVPT)

ii) Version faible du thm de la progression arithmétique de Dirichlet :

Pour $m \geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo m

iii) Thm de Wedderburn :

Tout corps fini est commutatif.

2) Caractère d'un gpe abélien

Def : Soit G un gpe abélien fini. On appelle caractère de G tout morphisme de G dans le ss-gpe multiplicatif $\mathbb{C}^*$.

On note $\hat{G}$ l'ensemble des caractères de G.

Exple : Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est un caractère de $\mathbb{F}_p$ (p premier)

Prop : Soit G un gpe abélien fini d'ordre n. Soit $\chi \in \hat{G}$.
On a $\mathrm{Im}(\chi) \subset \mu_n \subset \mathbb{U}$.

Def : On définit une loi interne $\cdot$ sur $\hat{G}$ en posant, pour $\chi, \psi \in \hat{G}$ et $g \in G$,

$$(\chi \cdot \psi)(g) = \chi(g)\,\psi(g)$$

On munit ainsi $\hat{G}$ d'une structure de gpe abélien.

Def : $\hat{G}$ est appelé le dual de G.

Prop : Soient H, K des ss-gpes abéliens finis et $G = H \times K$. Alors les gpes $\hat{G}$ et $\hat{H} \times \hat{K}$ sont isomorphes.

Thm : Tout gpe abélien fini est isomorphe à son dual.

III Applications en géométrie

1) Théorème du relèvement

Def : Soient I un intervalle de $\mathbb{R}$ et f une application continue de I dans $\mathbb{C}$ vérifiant $|f(t)| = 1 \ \forall t \in I$. On appelle relèvement de f toute application continue θ de I dans $\mathbb{R}$ tq $e^{i\theta(t)} = f(t) \ \forall t \in I$.

Thm : Soient I un intervalle de $\mathbb{R}$ et $f : I \longrightarrow \mathbb{C}$ une application de classe $\mathcal{C}^k$, $k \geq 1$, vérifiant $|f(t)| = 1 \ \forall t \in I$. Alors :

i) L'applicat° f possède des relèvements, et si θ_1, θ_2 sont 2 tels relèvements, il existe $k \in \mathbb{Z}$ tq $\theta_2(t) - \theta_1(t) = 2k\pi$ pour tout $t \in I$.

ii) Tout relèvement de f est de classe $\mathcal{C}^k$. ← (DVPT)

Applicat° : Soit $\gamma : [0,1] \longrightarrow \mathbb{C}^*$ une applicat° continue vérifiant $\gamma(0) = \gamma(1)$.
Soit θ un relèvement $\gamma/|\gamma|$.

Le nombre $\mathrm{Ind}_0(\gamma) = \frac{\theta(1) - \theta(0)}{2\pi}$ est un entier indépendant de θ.

De plus, si γ est $\mathcal{C}^1$, alors $\mathrm{Ind}_0(\gamma) = \frac{1}{2i\pi} \int_0^1 \frac{\gamma'(t)}{\gamma(t)}\,dt$.

2) $\mathbb{U} \simeq O^+(2)$ et notion d'angle

On se place dans le plan euclidien $\mathbb{R}^2$.

Rappel : $O^+(2)$ est le ss-gpe des isométries positives de $\mathbb{R}^2$.

Prop : Le gpe $O^+(2)$ est isomorphe et homéomorphe au gpe $\mathbb{U}$, via l'applicat°

$$\varphi : O^+(2) \longrightarrow \mathbb{U}, \quad \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \longmapsto a + ib$$

Coro IR : Le gpe $O^+(2)$ est commutatif.

Prop : L'application $\Psi : \mathbb{R} \longrightarrow \mathbb{U} \longrightarrow O^+(2)$, $\theta \longmapsto e^{i\theta} \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ est surjective et périodique, de période 2π.

Coque : Ψ induit un isomorphisme de gpes $\tilde{\Psi} : \mathbb{R}/2\pi\mathbb{Z} \longrightarrow O^+(2)$
On a donc $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.

Def : L'image du réel θ s'appelle rotation d'angle θ.

Notat° : On note $\mathcal{A}$ l'ensemble des couples de vecteurs unitaires de $\mathbb{R}^2$.

Def : On définit une relation d'équivalence sur $\mathcal{A}$ par $(u,v) \mathcal{R} (u',v')$ ssi il existe une rotat° f de $\mathbb{R}^2$ tq $f(u) = u'$ et $f(v) = v'$.
La classe d'équivalence de (u,v) est appelée l'angle orienté de u et v, notée abusivement (u,v). On note $\hat{\mathcal{A}}$ l'ensemble des angles orientés de vecteurs.

Prop : L'applicat° $\tilde{\Phi} : \mathcal{A} \longrightarrow O^+(2)$ qui, au couple de vecteurs unitaires (u,v), associe l'unique rotation r qui envoie u sur v, définit une applicat° bijective $\Phi : \hat{\mathcal{A}} \longrightarrow O^+(2)$.

Coque : Comme $O^+(2)$ est un gpe (commutatif), on en déduit une structure de gpe (commutatif) sur $\hat{\mathcal{A}}$.

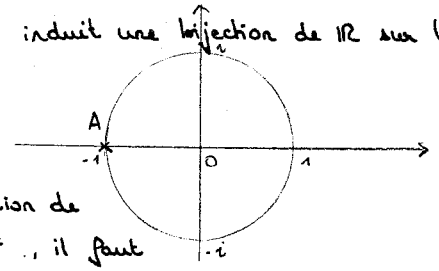
On se donne désormais une orientation de $\mathbb{R}^2$.

Prop : L'isomorphisme $\tilde{\Psi} : \mathbb{R}/2\pi\mathbb{Z} \longrightarrow O^+(2)$, $\theta \longmapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ permet de définir une mesure de l'angle orienté (u,v) : le réel θ, défini modulo 2π, est une mesure de l'angle orienté (u,v).

3) Paramétrisation rationnelle de $\mathcal{U}$

On se place dans le plan affine euclidien $\mathcal{E}$.

Prop : L'application $\mathbb{R} \longrightarrow \mathcal{E}$, $t \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ induit une bijection de $\mathbb{R}$ sur le cercle unité privé du point $A(-1,0)$.



Applicat : Pour que $(x,y,z) \in \mathbb{N}^3$ soit solution de l'équation diophantienne : $x^2 + y^2 = z^2$, il faut et il suffit qu'il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux, tels que (x,y,z) ou (y,x,z) soit égal à $(d(u^2-v^2),\ 2duv,\ d(u^2+v^2))$

4) Polygones de Gauss

Def : Soit $\mathcal{P}$ un plan euclidien et $\mathcal{B}$ un sous-ensemble fini de $\mathcal{P}$ ayant au moins 2 éléments. Les éléments de $\mathcal{B}$ sont appelés points de base.
Un point M de $\mathcal{P}$ est dit constructible à la règle et au compas à partir de $\mathcal{B}$ s'il existe une suite finie de points de $\mathcal{P}$ se terminant par M :
$M_1, M_2, \dots, M_m = M$ tq pour tout $1 \leq i \leq m$, M_i est un point d'intersection :

- soit de 2 dtes
- soit d'une dte et d'un cercle
- soit de 2 cercles

(ces dtes et ces cercles étant obtenus à l'aide de l'ensemble $E_i = \mathcal{B} \cup \{M_1, \dots, M_{i-1}\}$)

Thm : L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

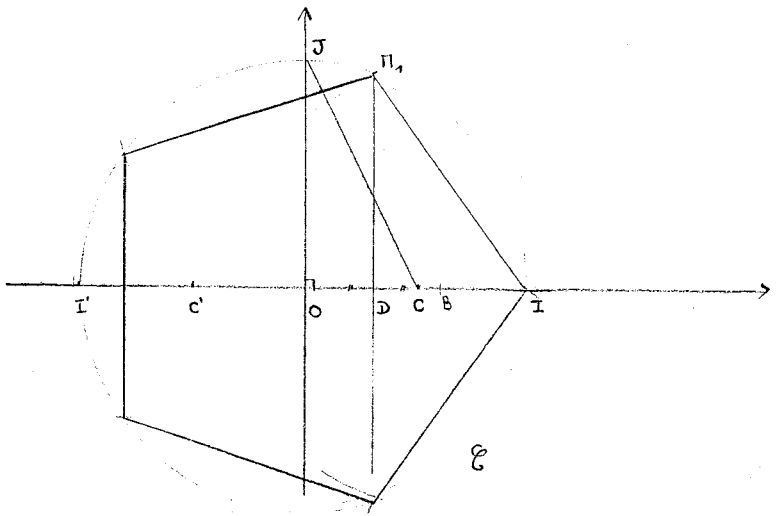
Thm : Soit $t \in \mathbb{R}$. t est un nombre constructible ssi il existe un entier $p \geq 1$ et une suite de sous-corps de $\mathbb{R}$, $L_1, L_2, \dots, L_p$, tq :

- $L_1 = \mathbb{Q}$
- $\forall\, 1 \leq j \leq p-1$, $L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$
- $t \in L_p$

Thm : [Wantzel] Tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2.

Thm : [Gauss] Les polygônes réguliers constructibles (à la règle et au compas) sont ceux dont le nombre de côtés n est de la forme 2^α avec $\alpha \geq 2$ ou de la forme $2^\alpha p_1 p_2 \cdots p_r$ avec $\alpha \in \mathbb{N}$ et où les p_i sont des nombres premiers distincts qui sont des nombres de Fermat.

Applicat : $5 = 2^{2^1} + 1$ est un nombre premier de Fermat donc le pentagone régulier est constructible.



Références :

- Arnaudiès - Fraysse
- Audin
- Carrega
- Chambert-Loir 1
- Combes
- Demazure
- Gourdon Algèbre
- Lelong-Ferrand
- Perrin
- Tauvel (algèbre et géométrie)