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

102

[ARN]

I. Nombres complexes de module 1

1) Définitions, trigonométrie

déf: on note $\mathbb{U} := \ker \begin{pmatrix} \mathbb{C}^* \to \mathbb{R}_+^* \\ z \mapsto |z| \end{pmatrix}$ le sous-groupe de $\mathbb{C}^*$ des nombres complexes de module 1.

Rq: $\mathbb{U} \cap \mathbb{R} = \{-1, 1\}$.

déf: on définit $\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!}$ pour $z \in \mathbb{C}$

on note aussi $e^z = \exp(z)$

prop: $f : \mathbb{R} \to \mathbb{U}$, $x \mapsto e^{ix}$ est un morphisme surjectif de noyau $2\pi\mathbb{Z}$, où $\pi := 2\min\{x>0 / \mathrm{Re}(f(x)) = 0\}$

cor: $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z}$

déf: on définit $\cos x := \mathrm{Re}(f(x))$, $\sin x := \mathrm{Im}(f(x))$

prop:
- formule de Moivre: $(e^{ix})^n = \cos nx + i \sin nx$
- formules d'Euler: $\cos x = \frac{e^{ix} + e^{-ix}}{2}$, $\sin x = \frac{e^{ix} - e^{-ix}}{2i}$

App: linéarisation de $\cos^n x$, $\sin^n x$

2) Considérations géométriques

prop: dans le plan complexe, $\mathbb{U}$ est le cercle de centre 0 et de rayon 1.
une paramétrisation rationnelle en est donnée par:

$$t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \quad \text{(le point } (-1,0) \text{ est exclu)}$$

App: triplets pythagoriciens:
soit $(x,y,z) \in \mathbb{N}^3$,

$x^2+y^2=z^2 \iff \exists d \in \mathbb{N}, u, v \in \mathbb{N}^*, u \wedge v = 1$ tq.

(x,y,z) ou $(y,x,z) = (d(u^2-v^2), 2duv, d(u^2+v^2))$

prop: $\mathbb{U} \to SO(2,\mathbb{R})$, $e^{ix} \mapsto \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$ est un isomorphisme de groupes

cor: $\mathbb{R}/2\pi\mathbb{Z} \simeq SO(2,\mathbb{R})$

Application aux angles orientés de vecteurs

on note $\mathcal{A}$ l'ensemble des couples de vecteurs unitaires de $\mathbb{R}^2$ et on définit la relation d'équivalence suivante:
$(u,v) \sim (u',v') \iff \exists f \in SO(2,\mathbb{R})$ tq. $f(u)=u'$ et $f(v)=v'$

$\mathcal{A}/\sim$ est l'ensemble des angles orientés de vecteurs.

prop: l'application de $\mathcal{A}/\sim$ dans $SO(2,\mathbb{R})$ qui à un représentant (u,v) associe l'unique $f \in SO(2,\mathbb{R})$ tq. $f(u)=v$ est bien définie et est une bijection

cor: l'isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \to SO(2,\mathbb{R})$, $\theta \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$

permet de définir une mesure des angles orientés de vecteurs

3) Sous-groupe des racines de l'unité

déf: on définit $\mu_n := \ker \begin{pmatrix} \mathbb{U} \to \mathbb{U} \\ z \mapsto z^n \end{pmatrix} = \{z \in \mathbb{C} / z^n = 1\}$ $_{n \in \mathbb{N}^*}$

le sous-groupe de $\mathbb{U}$ des racines n-ièmes de l'unité

Rq: si $\omega \in \mu_n \setminus \{1\}$, $\sum_{i=0}^{n-1} \omega^i = 0$

App: $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$, on en déduit une construction effective du pentagone régulier à la règle et au compas voir annexe

[AUD]

prop: $\mathbb{Z}/n\mathbb{Z} \to \mu_n$, $k \mapsto e^{\frac{2i\pi k}{n}}$ est un isomorphisme de groupes

cor: μ_n est cyclique, de cardinal n, de générateurs l'ensemble $\mu_n^\times := \{e^{\frac{2i\pi k}{n}} / k \wedge n = 1\}$ des racines n-ièmes primitives de l'unité.

prop: les sous-groupes de $\mathbb{U}$ sont soit denses, soit finis.

prop: μ_n est le seul sous-groupe de cardinal n de $\mathbb{C}^\times$

App: • les sous-groupes finis de $SO(2,\mathbb{R})$ sont cycliques
• les sous-groupes finis de $O(2,\mathbb{R})$ sont cycliques ou diédraux

prop: $\mu_d \subseteq \mu_n \iff d \mid n$

prop: $|\mu_n^\times| = \varphi(n)$

ex: $e^{\frac{i\pi}{3}}$ et $e^{-\frac{i\pi}{3}}$ sont les seules racines 6-ièmes primitives de 1

[PER] **prop:** $\mu_n = \bigsqcup_{d \mid n} \mu_d^\times$

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

[PER] ## II. Polynômes cyclotomiques et applications

def: on définit le n-ième polynôme cyclotomique Φ_n de $\mathbb{C}[X]$ par :

$$\Phi_n(X) := \prod_{\zeta \in \mu_n^\times} (X - \zeta) = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} (X - e^{\frac{2i\pi k}{n}})$$

prop: $\deg \Phi_n = \varphi(n)$

prop: $X^n - 1 = \prod_{d \mid n} \Phi_d$ / **cor:** $\Phi_n \in \mathbb{Z}[X]$

cor: on peut calculer Φ_n par récurrence : $\Phi_n = \frac{X^n - 1}{\prod_{d \mid n, d < n} \Phi_d}$

[GOZ] **ex:** si p premier, $\Phi_p = \sum_{i=0}^{p-1} X^i$, $\Phi_{p^n} = \sum_{i=0}^{p-1} (X^{p^{n-1}})^i$

[CAL] ### Calcul plus rapide des polynômes cyclotomiques

prop:
• $\Phi_n(X) = \prod_{d \mid n} (X^d - 1)^{\mu(n/d)}$

où μ est la fonction de Möbius : $\mu(n) = \begin{cases} (-1)^k \text{ si } n = p_1 \cdots p_k \text{ avec les } p_i \text{ distincts} \\ 0 \text{ si } n \text{ n'est pas sans facteur carré.} \end{cases}$

• $\Phi_{nq}(X) = \frac{\Phi_n(X^q)}{\Phi_n(X)}$ si q est premier et $q \nmid n$

• $\Phi_n(X) = \Phi_m(X^{n/m})$ où $n = \prod_{\alpha_i \geq 0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $m = p_1 \cdots p_k$

[PER] **thm:** Φ_n est irréductible dans $\mathbb{Z}[X]$

cor: le polynôme minimal d'une racine n-ième primitive de l'unité est Φ_n

cor: si $\zeta \in \mu_n^\times$, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$

[X-ENS] **thm (Kronecker):** soit $P \in \mathbb{Z}[X]$ unitaire dont les racines sont non nulles et de module ≤ 1, alors ses racines sont des racines de l'unité.

cor: soit $P \in \mathbb{Z}[X]$ unitaire dont les racines sont de module ≤ 1, alors P est le produit de puissances de X et de polynômes cyclotomiques

DEV 1

Rq: le théorème peut aussi s'énoncer ainsi : tout entier algébrique dont les conjugués sont de module ≤ 1 est une racine de 1.

Applications des polynômes cyclotomiques

[PER] **thm (Wedderburn):** tout corps fini est commutatif

[COT] **thm (Dirichlet):** pour $n \geq 1$, il existe une infinité de nombres premiers congrus à 1 modulo n

thm (Wantzel): $\omega \in \mathbb{C}$ est constructible ssi $\exists \mathbb{L}_0, \dots, \mathbb{L}_n$ des corps tq : $\mathbb{Q} = \mathbb{L}_0$, $\omega \in \mathbb{L}_n$ et $\forall i$, $\mathbb{L}_i \subseteq \mathbb{L}_{i+1}$ et $[\mathbb{L}_{i+1} : \mathbb{L}_i] = 2$

DEV 2 [CAR]

Thm (Gauss-Wantzel): le polygone régulier à n côtés est constructible ssi $n = 2^a p_1 \cdots p_r$, $a, r \in \mathbb{N}$, où les p_i sont des nombres premiers de Fermat distincts

Rq: on ne sait pas s'il existe plus de 38 polygones réguliers constructibles avec un nombre impair de côtés, celui qui en possède le plus parmi ceux connus en possède 4 294 967 295 voir annexe

III. Vers d'autres horizons

1) Représentations de groupes finis

G désigne un groupe fini de cardinal n, V un ev de dim $<\infty$

prop: si $\rho : G \to GL(V)$ est une représentation, alors $\rho(g)^n = 1$

cor: $Sp\,\rho(g) \subseteq \mu_n$

on suppose désormais que G est abélien.

prop: les représentations irréductibles de G sont de degré 1.

cor: si $\chi : G \to \mathbb{C}$, $g \mapsto \mathrm{tr}\,\rho(g)$ est un caractère irréductible, alors $\chi(g) = \rho(g)$ et χ est un morphisme de G dans μ_n.

réciproquement, un morphisme $\chi : G \to \mu_n$ est un caractère irréductible

[PEY] **def**: on note $\hat{G}$ le groupe des morphismes de G dans $\mathbb{C}^\times$, appelé dual de G

Cas des groupes cycliques

on suppose que $G = \mathbb{Z}/n\mathbb{Z}$

prop: $\hat{G} = \mu_n \simeq G$

Rq: l'isomorphisme n'est pas canonique

	0	1	2	⋯	$n-1$
χ_1	1	1	1	⋯	1
χ_2	1	ω	ω^2	⋯	ω^{n-1}
⋮	⋮	⋮	⋮		⋮
χ_n	1	ω^{n-1}	$\omega^{2(n-1)}$	⋯	$\omega^{(n-1)(n-1)}$

est la table de caractères de G, où $\omega \in \mu_n^\times$

Cas des groupes abéliens finis : G groupe abélien fini

Thm (structure des groupes abéliens finis): $\exists!\,(n_1, \dots, n_r)$ tq. $n_i \mid n_{i+1}$ et $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$

lemme: $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$

cor: $G \simeq \hat{G}$

2) Transformée de Fourier discrète [PEY]

def: soit $f = (f_0, \dots, f_{N-1}) \in \mathbb{C}^N$, on définit la TFD de f par : $\hat{f} := (\hat{f}_0, \dots, \hat{f}_{N-1})$ avec $\hat{f}_k := \sum_{n=0}^{N-1} f_n \omega_N^{-nk}$ avec $\omega_N = e^{\frac{2i\pi}{N}}$

def: on note $\mathcal{F} : \mathbb{C}^N \to \mathbb{C}^N$, $f \mapsto \hat{f}$; sa matrice dans la base canonique de $\mathbb{C}^N$ est donnée par :

$$\Omega_N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N^{-1} & \omega_N^{-2} & \cdots & \omega_N^{-(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega_N^{-(N-1)} & \omega_N^{-2(N-1)} & \cdots & \omega_N^{-(N-1)(N-1)} \end{pmatrix}$$

prop: on a la formule d'inversion : $f_n = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}_k \omega_N^{nk}$, $n = 0, \dots, N-1$

Rq: cela se traduit par $\Omega_N^{-1} = \frac{1}{N} \Omega_N^*$

def: soit $f, g \in \mathbb{C}^N$, on définit le produit de convolution de f avec g par : $(f * g)_n = \sum_{k=0}^{N-1} f_k g_{n-k}$, $n = 0, \dots, N-1$ avec $n-k$ pris modulo N

prop: soit $f, g \in \mathbb{C}^N$, alors $\forall n \in \{0, \dots, N-1\}$, $\widehat{(f*g)}_n = \hat{f}_n \hat{g}_n$

Application: matrices circulantes

Soit $c = (c_0, \dots, c_{N-1}) \in \mathbb{C}^N$, $C \in \mathcal{M}_N(\mathbb{C})$ est dite circulante si elle est de la forme

$$C = \begin{pmatrix} c_0 & c_{N-1} & \cdots & c_1 \\ c_1 & c_0 & \cdots & c_2 \\ \vdots & \ddots & \ddots & \vdots \\ c_{N-1} & c_{N-2} & \cdots & c_0 \end{pmatrix}$$

alors C est diagonalisable, $Sp(C) = \hat{c}$ et Ω_N est une matrice de passage de la base canonique à la base propre.

T.S.V.P. →

pour $x \in \mathbb{C}^N$, on a $Cx = c * x$ et donc :

$$Cx = b \Leftrightarrow c*x = b \Leftrightarrow x = \mathcal{F}^{-1}\left(\left(\frac{\hat{b}_n}{\hat{c}_n}\right)_{n=0,\dots,N-1}\right) \quad \left(\begin{matrix}\hat{c}_n \neq 0 \\ \text{si } C \in GL_N(\mathbb{C})\end{matrix}\right.$$

Rq : la transformée de Fourier rapide fournit un algo pour calculer la TFD en $O(N \ln N)$

[PER] 3) Quaternions

def : dans la $\mathbb{R}$-algèbre des quaternions $\mathbb{H}$, on définit le conjugué $\bar{q}$ de $q := a + bi + cj + dk$ par :
$\bar{q} := a - bi - cj - dk$

prop : $q \mapsto \bar{q}$ est un antiautomorphisme involutif de $\mathbb{H}$

def : on définit la norme $N(q)$ de $q := a + bi + cj + dk$ par :
$N(q) = q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2$

prop : $N : \mathbb{H}^* \to \mathbb{R}_+^*$ est un morphisme de groupes surjectif de noyau le groupe G des quaternions de norme 1

Rq : si $q \in G$, $q^{-1} = \bar{q}$

prop : G est homéomorphe à la sphère S^3

thm : $G/\{-1,1\}$ est isomorphe à $SO(3,\mathbb{R})$

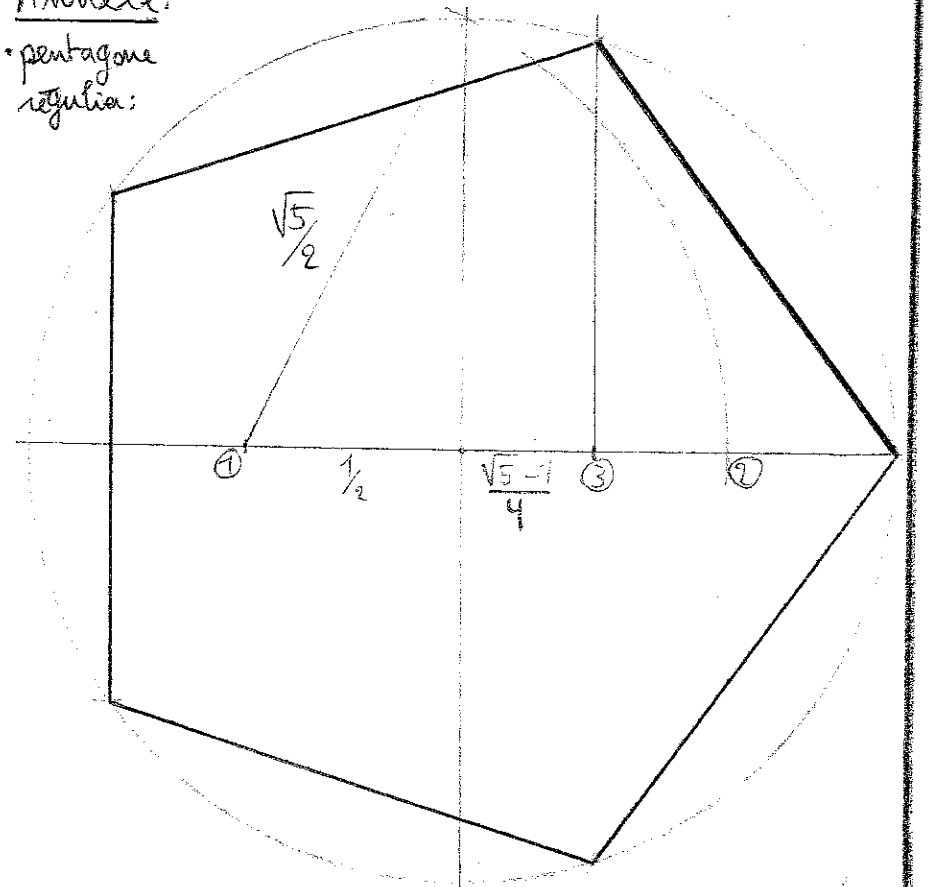
Références : [ARN] : Annaucliès - Fraysse, Algèbre
[AUD] : Audin, Géométrie
[PER] : Perrin, Cours d'algèbre
[GOZ] : Gozard, Théorie de Galois
[CAL] : Calais, Extensions de corps - Théorie de Galois
[X-ENS] : FGN, Oraux X-ENS Algèbre 1
[COM] : Combes, Algèbre et géométrie

[CAR] : Carrega, Théorie des corps : la règle et le compas
[PEY] : Peyré, L'algèbre discrète de la transformée de Fourier

---

Annexe :

- pentagone régulier :



- polygone régulier à 4 294 967 295 côtés :