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

Cadre : $n \in \mathbb{N}^*$, $\mathcal{P}$ est l'ensemble des nombres premiers

I - Structure du groupe des nombres complexes de module 1

1 - Exponentielle complexe et trigonométrie

Def 1 : On note $\mathbb{U}$ le noyau du morphisme de groupes (multiplicatifs)

$$|\cdot| : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$$
$$z \longmapsto |z|$$

C'est le groupe des nombres complexes de module 1.

Prop 2 : $\exp(i\cdot) : (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times)$ est un morphisme de groupes surjectif, de noyau $2\pi\mathbb{Z}$
$$t \longmapsto e^{it}$$

Cor 3 : On a même $\mathbb{U} \simeq \frac{\mathbb{R}}{2\pi\mathbb{Z}} \simeq \frac{\mathbb{R}}{\mathbb{Z}}$ et $[t] \in [0, 2\pi[$ est appelé argument de e^{it}

Def 4 : On pose $\cos : \mathbb{R} \to \mathbb{R}$, $x \mapsto \mathrm{Re}[e^{ix}]$; $\sin : \mathbb{R} \to \mathbb{R}$, $x \mapsto \mathrm{Im}[e^{ix}]$

Prop 5 : (i) cos et sin sont 2π-périodiques

(ii) $\forall x, y \in \mathbb{R}$ $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$

$\sin(x+y) = \cos(x)\sin(y) + \sin(x)\cos(y)$

(iii) $\forall x \in \mathbb{R}$, $\sin\left(x + \frac{\pi}{2}\right) = \cos(x)$, $\cos\left(x + \frac{\pi}{2}\right) = -\sin(x)$

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

(v) Formule de De Moivre : $\forall x \in \mathbb{R}$, $\forall n \in \mathbb{N}$: $(\cos(x) + i\sin(x))^n = \cos(nx) + i\sin(nx)$

Applic 6 : Linéarisation de fonctions trigonométriques, utiles pour le calcul de primitives et d'intégrales

Ex 7 : $\forall x \in \mathbb{R}$, $\cos^2(x) = \left(\frac{e^{ix} + e^{-ix}}{2}\right)^2 = \frac{1}{4}\left[2\cos(2x) + 2\right] = \frac{1 + \cos(2x)}{2}$

Donc $\displaystyle\int_0^{\pi} \cos^2(x)\,dx = \frac{1}{2}\int_0^{\pi}\left[1 + \cos(2x)\right]dx = \frac{\pi}{2}$

Applic 8 : Calcul des noyaux de Dirichlet et de Fejér

$\forall t \in \mathbb{R}$, $\forall N \in \mathbb{N}$, $D_N(t) = \displaystyle\sum_{k=-N}^{N} e^{ikt} = \frac{\sin\left(\frac{2N+1}{2}t\right)}{\sin\left(\frac{t}{2}\right)}$, $F_N(t) = \displaystyle\frac{1}{N}\sum_{k=0}^{N-1} D_k(t) = \frac{\sin^2\left(\frac{Nt}{2}\right)}{\sin^2\left(\frac{t}{2}\right)}$

Applic 9 : $P_\theta(X) = \displaystyle\sum_{k=0}^{n} \binom{n}{k}\sin(k\theta)X^k = \mathrm{Im}\left[\left(1 + e^{i\theta}X\right)^n\right]$

2 - Rotations et angles orientés du plan

Prop 10 : On a un isomorphisme de groupes

$$\Psi : \frac{\mathbb{R}}{2\pi\mathbb{Z}} \longrightarrow SO_2(\mathbb{R})$$
$$\theta \longmapsto \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} =: R_\theta$$

donc $\mathbb{U} \simeq SO_2(\mathbb{R})$

Rq 11 : On a donc une action de $\mathbb{U}$ sur lui-même par multiplication à gauche.

Def 12 : On appelle angle orienté du couple de vecteurs $(u, v) \in (\mathbb{R}^2 \setminus \{0\})^2$ l'unique $\theta \in \frac{\mathbb{R}}{2\pi\mathbb{Z}}$ tel que $\frac{v}{\|v\|_2} = R_\theta \cdot \frac{u}{\|u\|_2}$ (cf Fig 1). On note $\theta = \overline{(u,v)}$

Rq 13 : On a donc $\overline{(u,v)} = -\overline{(v,u)}$

Def 14 : On appelle mesure de l'angle orienté $\overline{(u,v)}$ l'image de $\overline{(u,v)}$ dans $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$

Ex 15 : $\overline{(e_1, e_2)}$ est de mesure $\frac{\pi}{2}$

$\overline{(\vec{OA}, \vec{OB})}$ est de mesure l'argument de $\frac{z_B}{z_A} \in \mathbb{C}$

3 - Sous-groupes de $\mathbb{U}$

Prop 16 : Tout sous-groupe de $\mathbb{R}$ est de la forme $a\mathbb{Z}$ où $a \in \mathbb{R}$, ou est dense (pour la topologie donnée par la valeur absolue)

Cor 17 : Tout sous-groupe de $\mathbb{U}$ est dense ou cyclique

Ex 18 : (i) $\left(e^{\frac{2ik\pi}{n}}\right)_{k \in [\![0, n-1]\!]}$ est cyclique $\left(\simeq \frac{\mathbb{Z}}{n\mathbb{Z}}\right)$

(ii) $\left(e^{in}\right)_{n \in \mathbb{Z}}$ est dense dans $\mathbb{U}$

Cor 19 : $\{\cos(n), n \in \mathbb{Z}\}$ et $\{\sin(n), n \in \mathbb{Z}\}$ sont denses dans $[-1, 1]$

II - Racines de l'unité

1 - Étude des sous-groupes finis de $\mathbb{U}$

Prop 20 : $\forall n \in \mathbb{N}^*$, $\mathbb{U}$ admet un unique sous-groupe d'ordre n. On le note μ_n, c'est l'ensemble des racines (complexes) de $X^n - 1 \in \mathbb{C}[X]$

On a $\mu_n = \left\{e^{\frac{2ik\pi}{n}}, k \in [\![0, n-1]\!]\right\}$

Prop 21 :

(i) $\forall z \in \mu_n$, $\bar{z} \in \mu_n$ et $\bar{z} = z^{-1}$ (valable pour tout $z \in \mathbb{U}$)

(ii) Si $n \geq 2$, $\displaystyle\sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = 0$

Ex 22 : $\mu_1 = \{1\}$, $\mu_2 = \{-1, 1\}$, $\mu_3 = \{j, \bar{j}, 1\}$ où $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ ($\bar{j} = j^2$)

$\mu_4 = \{i, -1, -i, 1\}$

Prop 25 : On a un isomorphisme de groupe

$$\varphi : \left(\mathbb{Z}/n\mathbb{Z}, +\right) \xrightarrow{\sim} (\mu_n, \times)$$
$$k \longmapsto e^{\frac{2ik\pi}{n}}$$

Prop 26 : Les générateurs de μ_n sont les $e^{\frac{2ik\pi}{n}}$ où $k \wedge n = 1$. Ces générateurs sont au nombre de $\varphi(n)$ (φ désigne l'indicatrice d'Euler)

Ex 27 : $\mu_1 = \{1\}$, $\varphi(1) = 1$; $\mu_2 = \langle -1 \rangle$; $\varphi(2) = 1$; $\mu_3 = \langle j \rangle = \langle j^2 \rangle$, $\varphi(3) = 2$; $\mu_4 = \langle i \rangle = \langle -i \rangle$, $\varphi(4) = 2$

Prop 28 : Soit $a \in \mathbb{C}$, l'équation $z^n = a$ admet pour solution l'ensemble
$$\left\{ \sqrt[n]{|a|}\, e^{\frac{i(\arg(a) + 2k\pi)}{n}},\ k \in [\![0, n-1]\!] \right\}$$

Appli 27 : (Formule de Cardan)
Soient $p, q \in \mathbb{R}$. Les racines du polynôme $X^3 + pX + q$ sont calculables explicitement.
Soit $\Delta = -(4p^3 + 27q^2)$ le discriminant du polynôme. On a trois cas possibles :
(i) Si $\Delta > 0$, alors P admet trois racines réelles distinctes.
(ii) Si $\Delta = 0$, alors P admet des racines réelles, dont une multiple.
(iii) Si $\Delta < 0$, alors P admet une racine réelle et deux racines complexes conjuguées (cf Fig 1)

DVPT 1

2 - Matrices d'ordre fini

Def 28 : Soit $A \in \mathcal{M}_p(\mathbb{K})$. On dit que A est d'ordre fini si $\exists m \in \mathbb{N}^*$: $A^m = I_p$

Prop 29 : Les valeurs propres d'une matrice d'ordre fini m sont des racines de l'unité dans μ_m

Prop 30 : On a un morphisme de groupes $(S_n, \circ) \longrightarrow (GL_n(\mathbb{C}), \times)$, où $\forall (i,j) \in [\![1,n]\!]^2$, $[P_\sigma]_{ij} = \delta_{i,\sigma(j)}$
$$\sigma \longmapsto P_\sigma$$
Donc $Sp(P_\sigma) \subset \mu_m$.

Ex 30-bis : Si $\sigma = (2\,3) \in S_3$, alors $P_\sigma = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ et $Sp(P_\sigma) = \{1, 1, j^2\}$ où $j = e^{\frac{2i\pi}{3}}$

Appli 31 : Soit $Z^{[0]} = [z_1^{[0]}, \dots, z_n^{[0]}]^T \in \mathbb{C}^n$. Soit $(Z^{[k]})_{k \in \mathbb{N}}$ la suite définie par $Z^{[k+1]} = \frac{1}{2}\left[z_1^{[k]} + z_2^{[k]}, \dots, z_n^{[k]} + z_1^{[k]}\right]^T$, alors $(Z^{[k]})$ converge vers $\frac{1}{n}[g, \dots, g]^T$, où $g = \frac{1}{n}\sum_{i=1}^{n} z_i^{[0]}$. Géométriquement, on a convergence vers l'isobarycentre du polygone dont les sommets ont pour affixe les $z_i^{[0]}$ (cf Fig 2)

3 - Cyclotomie

Def 32 : On définit $\mu_n^* = \left\{ e^{\frac{2ik\pi}{n}},\ k \wedge n = 1,\ k \in [\![0, n-1]\!] \right\}$; c'est l'ensemble des racines primitives n-ième de l'unité (éléments d'ordre n)

Rq 33 : On a $|\mu_n^*| = \varphi(n)$ (indicatrice d'Euler)

Ex 33-bis : $\mu_4^* = \{i, -i\}$

Def 34 : On définit le n-ième polynôme cyclotomique par
$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi) \in \mathbb{C}[X]$$

Rq 35 : Φ_n est unitaire de degré $\varphi(n)$

Prop 36 : $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Prop 37 : $\Phi_n \in \mathbb{Z}[X]$

Ex 38 : On peut calculer « récursivement » les polynômes cyclotomiques :
$\Phi_1 = X - 1$, $\Phi_2 = \frac{X^2 - 1}{X - 1} = X + 1$, $\Phi_3 = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$, $\Phi_4 = \frac{X^4 - 1}{(X-1)(X+1)} = X^2 + 1$

Rq 39 : Si n est premier, alors $\Phi_n = X^{n-1} + X^{n-2} + \dots + X + 1$

Th 40 : Φ_n est irréductible sur $\mathbb{Z}[X]$ et même sur $\mathbb{Q}[X]$

Rq 41 : Ce résultat est faux sur un corps fini

C-Ex 42 : Si $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, alors $\Phi_4 = X^2 + 1$ est réductible sur $\mathbb{F}_p[X]$ ($p \neq 2$)

Def 43 : (Corps cyclotomique)
On pose $\mathbb{Q}(\xi) = \{P(\xi),\ P \in \mathbb{Q}[X]\}$, où $\xi \in \mu_n^*$, $n \in \mathbb{N}^*$

Rq 43-bis : On a $\mathbb{Q}(\xi) \simeq \frac{\mathbb{Q}[X]}{\langle \Phi_n \rangle}$

Th 43-ter : $\{x \in \mathbb{Q}(\xi) : \forall \sigma \in \mathrm{Aut}_{\text{corps}}\mathbb{Q}(\xi),\ \sigma(x) = x\} = \mathbb{Q}$

DVPT 2

III - Applications diverses en algèbre

1 - Transformée de Fourier rapide

Dans toute cette partie, $\omega \in \mu_n^*$ désigne une racine primitive n-ième de l'unité fixée.

Prop 44 : $DFT_\omega : \frac{\mathbb{C}[X]}{\langle X^n - 1 \rangle} \longrightarrow \mathbb{C}^n$ est un morphisme de $\mathbb{C}$-algèbres (multiplication coordonnée par coordonnée)
$$P \longmapsto (P(1), \dots, P(\omega^{n-1}))$$

Prop 45 : Dans les bases $\{1, X, \dots, X^{n-1}\}$ de $\frac{\mathbb{C}[X]}{\langle X^n - 1 \rangle}$ et $\{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$ de $\mathbb{C}^n$, on a
$$Mat(DFT_\omega) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & & & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{bmatrix} = V_\omega \text{ (Vandermonde)}$$

L'inverse de V_ω est donnée par $V_\omega^{-1} = \frac{1}{n} V_{\omega^{-1}}$

Méthode 47 : (Algorithme FFT) Si $n = 2^d$, $A = \sum_{i=0}^{n-1} a_i X^i$, $B = \sum_{j=0}^{n-1} b_j X^j \in \mathbb{C}[X]$, $\omega \in \mu_n^*$
On écrit $A(\omega) = A_1(\omega^2) + \omega A_2(\omega^2)$ où $A_1 = \sum_{j=0}^{\frac{n}{2}-1} a_{2j} X^j$, $A_2 = \sum_{j=0}^{\frac{n}{2}-1} a_{2j+1} X^j$
De même $B(\omega) = B_1(\omega^2) + \omega B_2(\omega^2)$
donc $(AB)(\omega) = (A_1B_1 + XA_2B_2)(\omega^2) + \omega(A_1B_2 + A_2B_1)(\omega^2)$.
Les polynômes $A_1B_1 + XA_2B_2$ et $A_1B_2 + A_2B_1$ sont de degré $\leq n - 1$, et plus $\leq 2^{d-1}$. On a abaissé le degré. Puis on procède récursivement, jusqu'à atteindre le degré 1. Enfin, on utilise DFT_ω pour obtenir AB.

Prop 48 La multiplication des polynômes s'effectue en $O(n\log_2(n))$ opérations.

Ex 49 : Soit $P = X^2+X+1$ et $Q = X-1$.

Prenons $n=4$, $\mu_4^* = \{i,-i\}$ $DFT_i(P) = (3, i, 1, -i)$

$DFT_i(Q) = (0, -1+i, -2, -1-i)$

DFT_i est un morphisme de $\mathbb{C}$-algèbre donc $DFT_i(PQ) = DFT_i(P)\,DFT_i(Q)$

Donc $DFT_i(PQ) = (0, -1-i, -2, -1+i)$

Puis $\frac{1}{4} DFT_{-i}(DFT_i(PQ)) = \frac{1}{4}(-4, 0, 0, 4) = (-1, 0, 0, 1)$

Donc $(PQ)(X) = X^3-1$

2 - Applications géométriques

Déf 50 Un nombre complexe z est dit constructible (à la règle et au compas) si et seulement s'il existe une suite $A_0 \subset \dots \subset A_n$ de parties de $\mathbb{C}$ avec

(i) $A_0 = \{0, 1\}$ (ii) $z \in A_n$

(iii) $A_i = A_{i-1} \cup \{z_i\}$ où z_i est ... deux droites ou cercles dont z_i est point d'intersection

Ex 51 cf fig 3

Ex 52 $\sqrt{2}$ est constructible

- $\cos\left(\frac{2\pi}{3}\right)$ est constructible
- $\sqrt[3]{2}$ est constructible

Déf 53 Un polygone est dit constructible si ses sommets le sont

Prop 54 Le polygone régulier à n côtés est constructible si et seulement si $e^{\frac{2i\pi}{n}}$ est un nombre constructible

Th 55 (Théorème de Gauss-Wantzel)

Le polygone régulier à n côtés est constructible si et seulement si $n = 2^\alpha p$, où $\alpha \in \mathbb{N}$ et p est un produit de nombres premiers de la forme $1+2^{2^\beta}$, $\beta \in \mathbb{N}$

Ex 56 Le polygone à $17 = 1+2^{2^2}$ côtés est constructible

Rem 57 : Si $\vec{OP} = (-1, 0)$, $A, B \in S^1$ alors $\overline{(\vec{OA}, \vec{OB})} = 2\,\overline{(\vec{PA}, \vec{PB})}$ (cf fig 4)

Prop 57-bis $\cos\left(\frac{2\pi}{5}\right) = \sqrt{\frac{-1+\sqrt{5}}{4}}$

3 - Représentation de groupe

Lemme 58 (Lemme de prolongement des caractères)

Soit G un groupe abélien fini, soit $H \leq G$ (sous-groupe). Soit χ un caractère de H (morphisme de H dans $(\mathbb{C}^*, \times)$). Il existe un autre caractère $\tilde{\chi} : G \to \mathbb{C}^*$ tel que $\tilde{\chi}|_H = \chi$

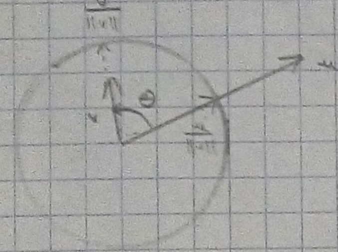
Th 58-bis (Théorème de structure des groupes abéliens finis)

Soit G un groupe abélien fini. Il existe $d_1 | \dots | d_r \in \mathbb{Z}$ uniques à ... près, tels que $G \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{d_r\mathbb{Z}}$

Ex 59 : Si $|G| = 180 = 2^2 \times 3^2 \times 5$, $G \simeq \frac{\mathbb{Z}}{180\mathbb{Z}}$, $G \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{90\mathbb{Z}}$ ou $G \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{60\mathbb{Z}}$

Prop 60 Soit G un groupe fini et soit $\rho : G \to GL(V)$ une représentation de G (linéaire) dans V un $\mathbb{C}$-espace vectoriel de dimension finie. Pour tout $g \in G$, les valeurs propres de $\rho(g)$ sont dans $\mu_{|G|}$

Annexe :



$\theta = (u, v)$

Fig. 1

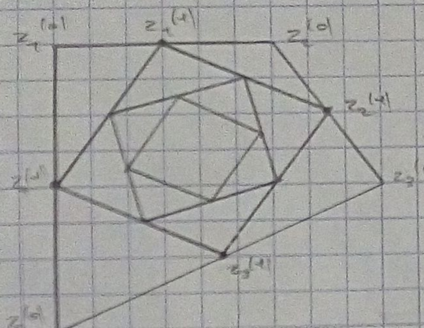


Fig. 2

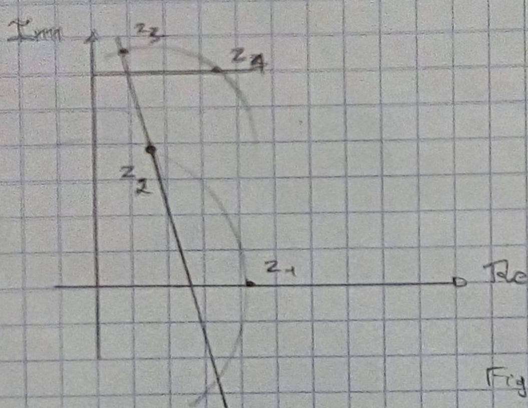


Fig. 3

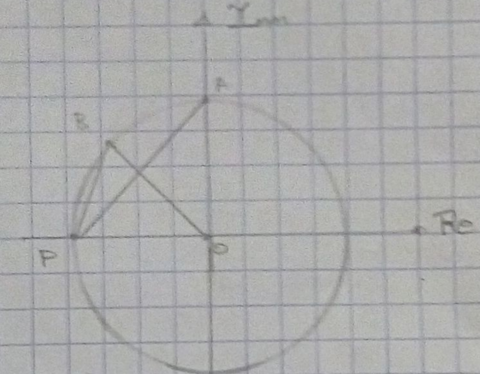


Fig. 4

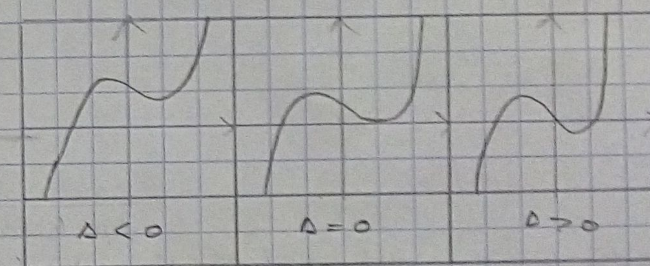


Fig. 5

Références

P. Tauvel, Géométrie

D. Perrin, Cours d'algèbre

A. Caldero, J. Germoni, Nouvelles Histoires Hédonistes de Groupes et Géométries

Peyré, L'algèbre discrète de la Transformée de Fourier