102

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

I Le groupe $\mathcal{U}$.

<u>Notation\définition 1</u> on note $\mathcal{U}=\{z\in\mathbb{C} \mid z\bar{z}=1\}$. C'est un sous-groupe de $\mathbb{C}^*$, noyau du morphisme $\mathbb{C}^*\to\mathbb{R}_+^*, z\mapsto z\bar{z}$.

<u>définition 2</u> on appelle exponentielle la fonction $\exp: \mathbb{C}\to\mathbb{C}^*, z\mapsto\sum_{n=0}^{\infty}\frac{z^n}{n!}$.
c'est un morphisme de groupes. On note parfois $\exp(z)=e^z$

<u>remarque 3</u>: $\forall x\in\mathbb{R}$, $\exp(ix)\in\mathcal{U}$. On peut donc considérer
$f: \mathbb{R}\to\mathcal{U}, x\mapsto\exp(ix)$.
f est un morphisme de groupes

<u>définition 4</u>: On appelle cosinus et sinus les fonctions
$\cos=\mathrm{Re}(f)$ $\sin=\mathrm{Im}(f)$.

<u>définition 5</u>: On appelle π le nombre $2\inf\{x>0 \mid \cos(x)=0\}$.
On remarque que $e^{i\pi}+1=0$ (identité d'Euler).

<u>remarque 6</u>: l'exponentielle est surjective, de noyau $2i\pi\mathbb{Z}$.

<u>propriété 7</u>: $\mathcal{U}\simeq\mathbb{R}/2\pi\mathbb{Z}$

<u>proposition 8</u>: Soit $z\in\mathbb{C}^*$. Alors il existe un unique couple (r,u) avec $r\in\mathbb{R}_+^*$, $u\in\mathcal{U}$, vérifiant $z=ru$.

on a $r=|z|$.

<u>proposition 9</u>: on a les identités remarquables

Formule de Moivre: $\forall n\in\mathbb{N}, \forall t\in\mathbb{R}$ $(\cos t+i\sin t)^n=\cos nt+i\sin nt$

Formule d'Euler: $\forall x\in\mathbb{R}$, $\cos x=\frac{1}{2}(\exp(ix)+\exp(-ix))$

$\sin x=\frac{1}{2i}(\exp(ix)-\exp(-ix))$

<u>Application 10</u>: linéarisation de $t\mapsto(\sin t)^n$ et $t\mapsto(\cos t)^n$
$\forall t\in\mathbb{R}$, $(\cos t)^3=\frac{1}{4}(\cos 3t+3\cos t)$

$\forall t\in\mathbb{R}$ $(\sin t)^4=\frac{1}{8}(\cos 3t-4\cos 2t+3)$

<u>Application 11</u>: noyau de ~~Dirichlet~~ convolution.
$\forall x\in\mathbb{R}$, $\forall n\in\mathbb{N}$ $D_n(x)=\sum_{k=-n}^{n}e^{ikx}=\frac{\sin((n+\frac{1}{2})x)}{\sin\frac{x}{2}}$

$\forall f: \mathbb{R}\to\mathbb{R}$ 2π-périodique, intégrable,
$\forall x\in\mathbb{R}$, $S_n(f)(x)=(D_n*f)(x)$

<u>Exercice 12</u> $\forall n\in\mathbb{N}$, $\exists! P_n\in\mathbb{R}[X]$, $\forall t\in\mathbb{R}$, $P_n(\cos t)=\cos(nt)$.

P_n est le n-ième polynôme de Tchebytchev de première espèce.

<u>Application 13</u>: interpolation polynomiale: théorème de Weierstrass
toute fonction continue sur un segment est limite uniforme de fonctions polynomiales.

<u>définition 14</u>: on note $\mathcal{U}_n$ le sous-groupe de $\mathcal{U}$ constitué des racines n-ièmes de l'unité, pour $n\geq 1$:

$$\mathcal{U}_n=\{z\in\mathbb{C}, z^n=1\}.$$

<u>proposition 15</u>: $\forall n\geq 1$, $\mathcal{U}_n=\{\exp(2i\frac{k}{n}\pi), k\in[\![0,n-1]\!]\}$.

<u>exemple 16</u>: $\mathcal{U}_1=\{1\}$
$\mathcal{U}_2=\{1,-1\}$
$\mathcal{U}_3=\{1,j,j^2\}$ où $j=\exp(\frac{2i\pi}{3})=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$.
$\mathcal{U}_4=\{1,-1,i,-i\}$.

<u>proposition 17</u>: $\forall n\in\mathbb{N}\setminus\{0,1\}$, $\sum_{\omega\in\mathcal{U}_n}\omega=0$.

proposition 18 : · les sous-groupes fermés de $\mathcal{U}$ sont $\mathcal{U}$ et les $\mathcal{U}_n$, $n \geq 1$.

· les sous-groupes de $\mathcal{U}$ sont soit fermés, soit denses.

exemple 19 : · le groupe des éléments de $\mathcal{U}$ d'ordre fini $\bigcup_{n \geq 1} \mathcal{U}_n$ est isomorphe à $\mathbb{Q}/\mathbb{Z}$.

· si p est premier, on appelle p-ième groupe de Prüfer $\mathcal{O}_p = \bigcup_{\alpha \in \mathbb{N}^*} \mathcal{U}_{p^\alpha}$

II Sous-groupes des racines de l'unité.

On fixe $n \geq 1$.

Proposition 20 : $\mathcal{U}_n$ est un groupe cyclique d'ordre n, isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

réciproquement, tout sous-groupe fini de $\mathbb{C}^\times$ est l'un des $\mathcal{U}_k$.

exemple 21 : Si $\dim E = n$, le centre de $SL(E)$ est isomorphe à $\mathcal{U}_n$.

définition 22 : On note $\mu_n^\times$ l'ensemble des générateurs de $\mathcal{U}_n$.

proposition 23 : $\mu_n^\times = \{\exp(\frac{2ik\pi}{n}) \mid k \in [\![0, n-1]\!], k \wedge n = 1\}$.

corollaire 24 : $\mathrm{card}(\mu_n^\times) = \varphi(n)$ où φ est l'indicatrice d'Euler.

corollaire 25 : $n = \sum_{d \mid n} \varphi(d)$.

application 26 : Soit $\mathbb{K}$ un corps et G un sous-groupe de $\mathbb{K}^\times$. Si G est fini, alors G est cyclique.

définition 27 : On note $\Phi_n = \prod_{\omega \in \mu_n^\times} (X - \omega)$, que l'on appelle le n-ième cyclotomique

proposition 28 : Φ_n est unitaire, de degré $\varphi(n)$

exemple 29 : $\Phi_1 = X - 1$
$\Phi_2 = X + 1$
$\Phi_3 = X^2 + X + 1$

de manière générale, si p est premier, $\Phi_p = \frac{X^p - 1}{X - 1}$

proposition 30 : $X^n - 1 = \prod_{d \mid n} \Phi_d$.

proposition 31 : $\Phi_n \in \mathbb{Z}[X]$.

théorème 32 : Φ_n est irréductible sur $\mathbb{Q}$.

corollaire 33 : si $\omega \in \mu_n^\times$, alors son polynôme minimal ~~est~~ sur $\mathbb{Q}$ est Φ_n.

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

application 34 (Dirichlet faible) :

par tout entier $n \geq 1$, il existe une infinité de nombres premiers de la forme $1 + dn$ avec $d \in \mathbb{N}$. DVP 1

III Applications à la géométrie plane

dans cette section, E représente le plan euclidien $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$, de base canonique $((1,0),(0,1))$. On note $SO(E)$ les rotations vectorielles de E.

~~définition 35 : On appelle rotation toute application linéaire $r \in \mathcal{L}(E)$ telle que det r = 1, ...~~

définition 35 : Soit $\mathbb{S}^1 = \{v \in E, \|v\| = 1\} \simeq \mathcal{U}$.

On note A l'ensemble des couples de $\mathbb{S}^1 \times \mathbb{S}^1$.

On définit une action de $\mathcal{U}$ sur A par :

$z \cdot (u, v) = (zu, zv)$.

On note $\hat{A}$ l'ensemble des orbites de l'action. Une orbite est appelé angle orienté.

proposition 36 : l'application $\hat{A} \to SO(E)$, $\alpha = (u,v) \mapsto r_\alpha$ où r_α est l'unique rotation telle que $r_\alpha(u) = v$, est une bijection

remarque 37 : $\hat{A}$ peut donc être muni d'une structure de groupes.

exemple 38 : $\mathbb{R} \to SO_2(\mathbb{R})$; $\theta \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ est un morphisme de noyau $2\pi\mathbb{Z}$

corollaire 39 : $\mathbb{U} \simeq SO_2(\mathbb{R}) \simeq \mathbb{R}/2\pi\mathbb{Z}$ et donc $\mathbb{U} \simeq SO(E)$.

définition 40 : la mesure d'un angle orienté $\alpha \in \hat{A}$ est donnée par le choix d'un isomorphisme $SO(E) \simeq SO_2(\mathbb{R})$. C'est un réel θ tel que $\exp(i\theta) \mapsto r_\alpha$.

exercice 41 : si $M = (-1,0)$, alors $\mathbb{R} \to \mathcal{E}$, $t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ est une paramétrisation de $S^1 \setminus \{M\}$.

corollaire 42 : On peut identifier $\mathbb{U}$ et S^1 à la droite projective $\mathbb{RP}^1 = \mathbb{R} \cup \{\infty\}$.

IV Transformée de Fourier discrète.

On note $f := \{f_0, \dots, f_{N-1}\}$ un échantillon de taille $N \in \mathbb{N}^*$, et on pose $\omega_N = \exp(\frac{2i\pi}{N})$.

définition 43 : la transformée de Fourier discrète de f est le vecteur $\hat{f} = (\hat{f}_0, \dots, \hat{f}_N)$ où $\hat{f}_k := \sum_{j=0}^{N-1} f_j \, \omega_N^{-jk}$.

proposition 44 : Soit $\mathcal{F}_d : \mathbb{C}^N \to \mathbb{C}^N$, $f \mapsto \hat{f}$. Alors $\mathcal{F}_d$ est un isomorphisme d'espaces vectoriels.

proposition 45 : la transformée de Fourier ~~discrète~~ inverse est donnée par

$$f_j = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}_k \, \omega_N^{jk}$$

application 46 : Soit $v = (v_0, \dots, v_{N-1}) \in \mathbb{C}^N$. On pose
$M_c = \begin{pmatrix} c_0 & c_{N-1} & \cdots & c_1 \\ c_1 & c_0 & \cdots & c_2 \\ \vdots & \vdots & & \vdots \\ c_{N-1} & c_{N-2} & \cdots & c_0 \end{pmatrix}$. Alors M est diagonalisable et $Sp_{\mathbb{C}}(M_c) = \hat{c}$.

application 47 : transformée de Fourier rapide en ~~[illegible]~~ informatique.

remarque 48 : Il s'agit en fait de la transformée de Fourier de la mesure de comptage : les propriétés liées à la convolution sont donc vérifiées : $\widehat{f*g} = \hat{f} \times \hat{g}$.

V Représentations de groupes finis.

G désigne un groupe fini de cardinal n, V un $\mathbb{C}$-ev de dimension finie

proposition 49 : si (V,ρ) est une représentation de G, alors $\rho(g)^n = \mathbb{I}_d$

corollaire 50 : $Sp(\rho(g)) \subset \mathbb{U}_n$.

On suppose désormais que G est abélien.

proposition 51 : les représentations irréductibles de G sont de dimension 1

corollaire 52 : si $\chi : G \to \mathbb{C}$ est un caractère irréductible, $\chi(g) = \rho(g)$ est un morphisme de G dans $\mathbb{U}_n$.

réciproquement, tout morphisme de G dans $\mathbb{U}_n$ est un caractère irréductible

définition 53 : on note $\hat{G}$ l'ensemble des caractères abélien de G, appelé groupe dual de G.

On suppose que G est cyclique : $G \simeq \mathbb{Z}/n\mathbb{Z}$.

proposition 54 : $\hat{G} \simeq \mathbb{U}_n \simeq G$. (non canonique).

propriété 55 : soit $\omega \in \mathbb{U}_n^*$. La table des caractères de G est

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

VI Théorème de Wedderburn

Soit K un « corps gauche ». (non commutatif)

théorème 56 : K est fini $\Rightarrow$ K est commutatif.

dvp 2