Leçon 102 : Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. App°s.

Rombaldi
Berhuy (dev 1)
Isenmann (dev 2)

I. Le groupe $\mathbb{U}$ et la trigonométrie

1. Définitions et premières propriétés

Définition 1.1 On note $\mathbb{U}$ l'ensemble des nombres complexes z de module 1.
On appelle $\mathbb{U}$ l'ensemble des racines de l'unité.

Définition 1.2 Pour tout $n \in \mathbb{N}^*$, on note $\mathbb{U}_n$ l'ensemble des nombres complexes z tels que $z^n = 1$. Les éléments de $\mathbb{U}_n$ sont appelés racines n-ièmes de l'unité.

Proposition 1.3 Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est de cardinal n.

Proposition 1.4 $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \cdot)$ et pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Proposition 1.5 Soit H un sous-groupe borné de $(\mathbb{C}^*, \cdot)$ alors H est un sous-groupe de $\mathbb{U}$.
Si H est un sous-groupe fini alors H est cyclique.

Conséquence 1.6 Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un groupe cyclique.

2. $\mathbb{U}$ et l'exponentielle complexe

Définition 1.7 On appelle exponentielle la fonction somme de la série entière, de rayon de convergence infini, $\sum_{n=0}^{+\infty} \frac{z^n}{n!}$.

Proposition 1.8 La fonction exp est holomorphe sur $\mathbb{C}$ et est sa propre dérivée.

Proposition 1.9 La fonction $\exp : (\mathbb{C}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ réalise un morphisme de groupes surjectif, non injectif.

Théorème 1.10 La fonction $\phi : \mathbb{R} \longrightarrow \mathbb{C}$, $t \longmapsto \exp(it)$ réalise un morphisme de groupes de $(\mathbb{R}, +)$ sur $(\mathbb{U}, \cdot)$ surjectif non injectif.

Proposition - Définition 1.11 Le sous-groupe $\operatorname{Ker} \phi$ de $(\mathbb{R}, +)$ est de la forme $b\mathbb{Z}$ où $b = \inf \{x > 0 \mid \phi(x) = 0\}$.
On définit 2π le nombre b.

Corollaire 1.12 Le groupe $\mathbb{U}$ est isomorphe à $\mathbb{R}/2\pi\mathbb{Z}$.

Application 1.13 Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{\exp(\frac{2ik\pi}{n}) \mid k \in [\![0, n-1]\!]\}$.

3. Liens avec la géométrie plane

On identifie $\mathbb{C}$ à $\mathbb{R}^2$, alors $\mathbb{U}$ s'identifie à la sphère unité $\mathbb{S}^1$.

Théorème 1.14 SO_2 agit transitivement sur $\mathbb{U}$.

Définition 1.15 Pour $\theta \in \mathbb{R}$, on définit $\sin\theta := \operatorname{Im}(\phi(\theta))$ et $\cos\theta := \operatorname{Re}(\phi(\theta))$.

Proposition 1.16 L'application $\rho : \mathbb{U} \longrightarrow SO_2(\mathbb{R})$, $\exp(i\theta) \longmapsto R(\theta)$, où $R(\theta)$ désigne la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, est un isomorphisme de groupes.

Proposition 1.17 L'isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq SO_2(\mathbb{R})$ permet de définir une mesure des angles orientés de vecteurs.

II. Applications diverses

1. Polynômes cyclotomiques

Définition 2.1 Pour tout $n \in \mathbb{N}^*$, on appelle racine n-ième primitive de l'unité tout générateur de $\mathbb{U}_n$, il s'agit alors des $\exp \frac{2i\pi k}{n}$ avec $k \wedge n = 1$.

On note $\mathbb{U}_n'$ l'ensemble des racines n-ièmes primitives de l'unité.

Proposition 2.2 Pour tout $n \geqslant 1$, $\mathbb{U}_n = \bigcup_{d \mid n} \mathbb{U}_d'$.

Définition 2.3 On appelle polynôme cyclotomique le polynôme $\Phi_n(X) = \prod_{z \in \mathbb{U}_n'} (X-z)$.

Théorème 2.4 Pour tout $n \geqslant 1$, $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Corollaire 2.5 Soient p un nombre premier et $r \in \mathbb{N}^*$. Alors $\Phi_{p^r}(X) = \sum_{k=0}^{p-1} X^{kp^{r-1}}$ $= \Phi_p(X^{p^{r-1}})$.

Théorème 2.6 Pour tout $n \in \mathbb{N}^*$, Φ_n est unitaire dans $\mathbb{Z}[X]$.

Théorème 2.7 Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Q}[X]$.

Lemme 2.8 Soient $q, d, n \in \mathbb{N}^*$ avec $q \geqslant 2$. Alors $q^d - 1 \mid q^n - 1$ si et seulement si $d \mid n$. Le cas échéant, $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$ pour d diviseur strict.

Théorème 2.9 (Wedderburn) Soit A un anneau (unitaire) vérifiant $A^* = A \setminus \{0\}$ fini. Alors A est commutatif.

développement 1

2. En algèbre linéaire

Définition 2.10 Soient $c_0, \dots, c_n \in \mathbb{C}$. On définit la matrice circulante C associée par :

$$C = \begin{pmatrix} c_0 & c_{n-1} & \cdots & c_1 \\ \vdots & & \ddots & \vdots \\ & & & c_{n-1} \\ c_n & \cdots & & c_0 \end{pmatrix}$$

Proposition 2.11 La famille de vecteurs $v_k = \frac{1}{\sqrt{n}} \omega_k$ forme une base orthonormale de vecteurs propres.

Proposition 2.12 On a : $\det C = \prod_{k=0}^{n} P_c(\omega_k)$ où $P_c = \sum_{k=0}^{n} c_k X^k$.

Application 2.13 Soit P_0 un polygone à n sommets. On construit par récurrence $(P_k)_k$ où les sommets de P_{k+1} sont les milieux des arêtes de P_k. Alors $(P_k)_k$ converge vers l'isobarycentre de P_0.

3. Dual d'un groupe abélien fini

Dans ce paragraphe, G désigne un groupe abélien fini d'ordre n.

Définition 2.14 On appelle caractère de G une application $\chi : G \longrightarrow \mathbb{C}^*$, morphisme de groupes.

On note $\widehat{G}$, et on appelle dual de G, l'ensemble des caractères de G.

Théorème 2.15 $(\widehat{G}, \cdot)$ est un groupe abélien.

Proposition 2.16 Soit $\chi \in \widehat{G}$, alors χ est à valeurs dans $\mathbb{U}_n$.

Lemme 2.17 Soit H un sous-groupe de G. Tout caractère χ de H se prolonge en un caractère sur G.

Théorème 2.18 (classification des groupes abéliens finis) Soit G un groupe abélien fini non trivial. Alors, il existe $r \in \mathbb{N}^*$, $n_1, \dots, n_r \geqslant 2$ vérifiant pour tout $i \in [\![1, r-1]\!]$ $n_i \mid n_{i+1}$, tels que $G \simeq \mathbb{U}_{n_1} \times \dots \times \mathbb{U}_{n_r}$.

développement 2