

2 Leçon 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications

I. De l'exponentielle au cercle unité

1. L'exponentielle complexe [TAU] [ELA]

Fonction exponentielle, prop, morphisme de groupes, cosinus et sinus, formule de De Moivre

2. Le groupe des nombres complexes de module 1 [TAU]

Cercle unité, morphisme de $\mathbb{R}$ dans $\mathbb{U}$, d'ef de π , unicité de l'écriture exponentielle

II. Les racines de l'unité [TL1] [PER] [IP]

Racine n -ème, exemples, racine de l'unité, prop, racine primitive n -ième, indicatrice d'Euler
DEV 1 : Théorème de Kronecker

III. Applications

1. Polynômes cyclotomiques [PER]

n -ème polynôme cyclotomique, formule $X^n - 1$, exemples, unitaire et dans $\mathbb{Z}[X]$

DEV 1 : Irréductibilité de $\Phi_n(X)$ + polynôme minimal d'une racine primitive n -ième de l'unité

Intersection d'extensions, théorème de Dirichlet faible

2. Le groupe unitaire [GRI] [GOU]

Endomorphisme unitaire, groupe unitaire, d'et et valeurs propres, théorème diagonalisation, $U_n(\mathbb{C})$ est CPA, décomposition polaire, rayon spectral

Présentation :

- Les nombres complexes sont un outil puissant en algèbre et géométrie, et lorsque l'on considère la boule unité, on observe de nombreuses propriétés sur ses éléments et ses sous-groupes.
- La fonction exponentielle nous permet surtout d'avoir une notation plus compacte et très maniable des nombres complexes : l'écriture exponentielle.
C'est aussi un moyen de définir le nombre π .
- Le terme « décomposition polaire » vient sûrement de l'analogie avec l'écriture d'un nombre complexe non nul sous la forme $z = re^{i\theta}$ avec $r > 0$. En effet, si $n = 1$, $\mathcal{H}_1(\mathbb{C}) = \mathbb{R}_+^*$ et $U_1(\mathbb{C}) = \{z \in \mathbb{C}; |z| = 1\} = e^{i\theta}$.

Développements :

- Théorème de Kronecker
 - L'oral à l'agrégation de mathématiques - Une sélection de développements, Isenmann-Pecatte, p277
 - Carnet de voyage en Algèbre, Caldero-Peronnier, p30
- Irréductibilité des polynômes cyclotomiques + degré d'une extension cyclotomique
 - Théorie de Galois, Gozard, p69
 - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p384
 - Cours d'algèbre, Perrin, p80

Références :

- [TAU] Analyse complexe pour la Licence 3, Tauvel
- [ELA] Suites et séries numériques, suites et séries de fonctions, El Amrani
- [TL1] Tout en un pour la licence 1
- [PER] Cours d'algèbre, Perrin
- [IP] L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte
- [GRI] Algèbre linéaire, Grifone
- [GOU] Algèbre-Probabilités, Gourdon

Def 102: Groupe des nombres complexes de module 1.
Racines de l'unité. Applications.

Id l'exponentielle au cercle unité

1) L'exponentielle complexe [TAU] [ELA]

Def 1: On définit la fonction exponentielle sur $\mathbb{C}$
par: $e^z = \exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \quad \forall z \in \mathbb{C}$

Remarque 2: Cette série entière a un rayon de convergence infini.

Prop 3: La fonction exponentielle est infiniment dérivable sur $\mathbb{C}$ et admet pour dérivée e^z en tout point $z \in \mathbb{C}$.

Prop 4: $\forall z_1, z_2 \in \mathbb{C}: e^{z_1+z_2} = e^{z_1} \cdot e^{z_2}$

Prop 5: $\forall z \in \mathbb{C}$, on a: $e^z \neq 0$; $\frac{1}{e^z} = e^{-z}$;
 $\overline{e^z} = e^{\overline{z}}$; $|e^z| = e^{\operatorname{Re}(z)}$

Corollaire 6: $\forall z \in \mathbb{C}, |e^z| = 1 \Leftrightarrow z \in i\mathbb{R}$.

Théorème 7: L'application $z \mapsto e^z$ est un morphisme de groupes de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$. Il est continu, surjectif, mais non injectif.

Def 8: On appelle fonctions cosinus et sinus (complexes), notées $\cos$ et $\sin$, les applications de $\mathbb{C}$ dans $\mathbb{C}$

définies par:

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2} \quad \text{et} \quad \sin(z) = \frac{e^{iz} - e^{-iz}}{2i}$$

Corollaire 9: $\forall z \in \mathbb{C}, \cos(z) = \sum_{n=0}^{+\infty} (-1)^n \frac{z^{2n}}{(2n)!}$
et $\sin(z) = \sum_{n=0}^{+\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!}$

Prop 10: Soit $z \in \mathbb{C}$. Alors: $e^{iz} = \cos(z) + i\sin(z)$
et $\cos^2(z) + \sin^2(z) = 1$.

Prop 11 (formule de De Moivre): Soit $n \in \mathbb{N}$ et $x \in \mathbb{R}$. Alors:
 $(\cos(x) + i\sin(x))^n = \cos(nx) + i\sin(nx)$.

2) Le groupe des nombres complexes de module 1 [TAU]

Def 12: On appelle cercle unité de $\mathbb{C}$ l'ensemble des nombres complexes de module 1:

$$U = \{z \in \mathbb{C}; |z| = 1\}.$$

C'est un sous-groupe de $(\mathbb{C}^*, \times)$.

Exemple 13: $1, -1, i, -i$ sont des éléments de U .

Prop 14: On a: $e^{iz} \in U \Leftrightarrow z \in \mathbb{R}$.

Théorème 15: L'application $\ell: x \mapsto e^{ix}$ est un morphisme continu du groupe $(\mathbb{R}, +)$ dans le groupe $(U, \times)$. Il est surjectif et son noyau est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}_+^*$.

Def 16: On note le nombre $\pi := \frac{a}{2}$. Ainsi: $\mathbb{R}/\pi\mathbb{Z} \simeq U$.

Corollaire 17: Le noyau du morphisme $(\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \times)$ est $2i\pi\mathbb{Z}$.

La fonction exponentielle complexe est périodique, et l'ensemble de ses périodes est $2i\pi\mathbb{Z}$.

Théorème 18: L'application $f: \mathbb{R}_+^* \times U \rightarrow \mathbb{C}^*$
 $(a, u) \mapsto au$
est un isomorphisme de groupes.

III Les racines de l'unité [L11] [PER] [IP]

Def 19: Soit $n \in \mathbb{N}^*$. Une racine n -ème de l'unité est un complexe z tel que $z^n = 1$.

Notation 20: On note U_n l'ensemble des racines n -ièmes de l'unité.

Prop 21: n est un multiple de m , $U_n \subset U_m$. $\square$

Exemple 22: $\psi_1 = \{1\}$; $\psi_2 = \{-1, 1\}$; $\psi_3 = \{1, -1, i, -i\}$
 $\psi_4 = \{1, i, j, j^3\}$ en résolvant $z^4 = 1$.

Déf 23: Une racine de l'unité est une racine n -ième de l'unité pour un $n \in \mathbb{N}^*$.

Notation 24: On note ψ_n l'ensemble des racines de l'unité.

Prop 25: $\psi_n = \bigcup_{m \in \mathbb{N}^*} \psi_m$.

Prop 26: ψ_n est un sous-groupe cyclique de ψ . Ses éléments sont les $e^{2ik\pi/n}$ où k parcourt les entiers modulo n : $\psi_n = \{e^{2ik\pi/n}; k \in \{0, 1, \dots, n-1\}\}$.

Corollaire 27: Les seuls sous-groupes finis de $\mathbb{C}^*$ sont ψ_n .

Exemple 28: ψ_6 est engendré par $e^{2i\pi/6} = e^{i\pi/3}$.

Déf 29: On appelle racine primitive n -ième de l'unité tout générateur de ψ_n .

Remarque 30: Ce sont en fait les $e^{2ik\pi/n}$ où k est premier avec n .

Notation 31: On note ψ_n^* leur ensemble. On a $|\psi_n^*| = \varphi(n)$ où φ est l'indicatrice d'Euler.

Prop 32: On a $\psi_n = \bigcup_{d|n} \psi_d^*$.

Application 33: On a: $m = \sum_{d|m} \varphi(d)$.

Déf 34: Soit A un anneau. Soit $n \in \mathbb{N}$ et $h \in \mathbb{O}; m \in \mathbb{N}$. On définit le h -ième polynôme symétrique élémentaire e_h de $A[x_1, \dots, x_m]$ par: $e_h = \sum_{1 \leq i_1 < i_2 < \dots < i_h \leq m} x_{i_1} x_{i_2} \dots x_{i_h}$.

Théorème 35: Soit $P \in A[x]$ un polynôme scindé unitaire, tel que $P(x) = \sum_{i=0}^m a_i x^i$ avec $a_m = 1$. On note $z_1, \dots, z_m$ ses racines. Alors pour tout $h \in \mathbb{O}; m \in \mathbb{N}$, on a:

$$e_k(z_1, \dots, z_m) = (-1)^k a_{m-k}.$$

Théorème 36 (de Kronecker): Soit $P \in \mathbb{Z}[x]$ un polynôme unitaire dont les racines complexes sont de module inférieur ou égal à 1. On suppose que 0 n'est pas racine. Alors toutes les racines de P sont des racines de l'unité.

Corollaire 37: Soit $P \in \mathbb{Z}[x]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = x^n$ ou P est un polynôme cyclotomique.

DEV 1

Corollaire 38: Soit $m \in \mathbb{N}^*$, ζ un sous-groupe fini de $\mathbb{C}_m^*(\mathbb{Z})$ et $m \geq 3$. Alors la projection de ζ dans $\mathbb{C}_m^*(\mathbb{Z}/m\mathbb{Z})$ est injective et ζ est isomorphe à un sous-groupe de $\mathbb{C}_m^*(\mathbb{Z}/m\mathbb{Z})$.

III Applications

1) Polynômes cyclotomiques [PER]

Déf 39: On appelle n -ième polynôme cyclotomique le polynôme: $\Phi_n(x) = \prod_{z \in \psi_n^*} (x - z)$.

Remarque 40: Φ_n est unitaire de degré $\varphi(n)$.

Prop 41: On a: $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Remarque 42: par récurrence, on peut calculer Φ_n :

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}.$$

Exemple 43: $\Phi_1(x) = x - 1$; $\Phi_2(x) = x + 1$; $\Phi_3(x) = x^2 + x + 1$
 $\Phi_4(x) = x^2 + 1$

Prop 44: $\forall m \in \mathbb{N}^*, \Phi_m(x) \in \mathbb{Z}[x]$.

Lemme 45: Soit $P, Q \in \mathbb{Q}[x]$ non nuls. On suppose que $P \in \mathbb{Z}[x]$, et que P et Q sont unitaires. Alors P et Q sont dans $\mathbb{Z}[x]$.

Théorème 46: Le polynôme cyclotomique $\Phi_n(x)$ est irréductible dans $\mathbb{Q}[x]$.

DEV 2

Corollaire 47: Si $v \in V_n^*$, alors son polynôme minimal sur $\mathbb{Q}$ est Φ_n , et alors $[\mathbb{Q}(v) : \mathbb{Q}] = \phi(n)$.

Corollaire 48: Soit $\alpha \in V_n^*$ et $\alpha' \in V_m^*$, on suppose que $\text{pgcd}(m, n) = 1$. Alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\alpha') = \mathbb{Q}$.

Application 49 (théorème de Dirichlet faible): Soit $m \geq 1$.

Alors il existe une infinité de nombres premiers p vérifiant $p \equiv 1 \pmod{m}$.

2) Le groupe unitaire $U(n)$ [600]

Prop 50: Soit $(E, \langle \cdot, \cdot \rangle)$ un espace hermitien et $n \in \mathbb{Z}(E)$. On a équivalence entre:

- $\|u\| = \|v\| \quad \forall u, v \in E$
- $\langle u, v \rangle = \langle v, u \rangle \quad \forall u, v \in E$
- Si $(e_i)_{i=1}^n$ est une base de E , $A = M_{e_i}(u)_{i=1}^n$ alors

$$A^T \cdot A = I_n.$$

On dit alors que u est unitaire.

Def 51: Une matrice $A \in M_n(\mathbb{C})$ vérifiant $A^T \cdot A = I_n$ est dite unitaire. L'ensemble des matrices unitaires est un groupe appelé groupe unitaire, noté $U(n)$.

Prop 52: Soit $A \in U(n)$. Alors $|\det A| = 1$ et les valeurs propres de A sont toutes de module 1.

Théorème 53: Soit E un espace hermitien et $n \in \mathbb{Z}(E)$ un endomorphisme unitaire. Alors il existe une base orthonormale qui diagonalise n .

Corollaire 54: Soit $u \in U_n(\mathbb{C})$. Alors il existe $P \in U_n(\mathbb{C})$ tel que: $P^{-1} u P = P^T \cdot u \cdot P = \begin{pmatrix} e^{i\theta_1} & & 0 \\ & e^{i\theta_2} & \\ 0 & & e^{i\theta_m} \end{pmatrix}$

où les θ_i sont des nombres réels.

Application 55: $U_n(\mathbb{C})$ est connexe par arcs en continu. Soit $\gamma: [0, 1] \rightarrow U_n(\mathbb{C})$ une courbe continue. On a $\gamma(0) = I_n$ et $\gamma(1) = u$.

Théorème 56 (décomposition polaire): Soit $A \in GL_n(\mathbb{C})$. Alors il existe un unique couple (U, H) où $U \in U_n(\mathbb{C})$ et H est hermitienne définie positive, tel que $A = U \cdot H$.

Corollaire 57: Soit $A \in GL_n(\mathbb{C})$. Alors:

$$\|A\| = \sqrt{p(A^T A)}$$

où p est le rayon spectral donné par:

$$p(M) = \max_{1 \leq i \leq n} |\lambda_i|; \lambda_i \in \text{Sp}(M)$$

et $\| \cdot \|$ est la norme matricielle induite par la norme euclidienne $\|x\|_2 = \left(\sum_{i=1}^n |x_i|^2 \right)^{1/2}$ pour $x \in \mathbb{R}^n$.