102

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

I] Nombres complexes de module 1

A] Le groupe $\mathbb{U}$

Def 1: On définit $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ l'ensemble des complexes de module 1.

Ex 2: $\pm 1, \pm i \in \mathbb{U}$.

Prop 3: Soit $\mathbb{S}^1$ la sphère unité de $\mathbb{R}^2$. Alors $\mathbb{U} \to \mathbb{S}^1$, $a+ib \mapsto (a,b)$ est un homéomorphisme.

Cor 4: $\mathbb{U}$ est compact.

Prop 5: $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

B] Fonction exponentielle, fonctions trigonométriques

Def 6: On définit l'exponentielle de $z \in \mathbb{C}$ par :
$e^z = \exp(z) := \sum_{n=0}^{+\infty} \frac{z^n}{n!}$

Prop 7: $\exp|_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}_+^*$ est une bijection croissante.

Cor 8: $\forall z \in \mathbb{U}$, $e^z \in \mathbb{U} \Leftrightarrow z \in i\mathbb{R}$.

Thm 9: $\exp : \mathbb{C} \to \mathbb{C}^*$ est surjective.

Cor 10: L'application $\mathbb{R} \to \mathbb{U}$, $t \mapsto e^{it}$ est un morphisme de groupes surjectif non injectif.

Def 11: Le noyau de ce morphisme étant de la forme $\alpha\mathbb{Z}$, $\alpha > 0$, on définit $\pi = \frac{\alpha}{2}$.

Rem 12: Cor 10 permet ainsi d'avoir un paramétrage de $\mathbb{U}$.

Def 13: On définit les fonctions cosinus et sinus par : $\forall t \in \mathbb{R}$, $\cos(t) = \mathrm{Re}(e^{it})$, $\sin(t) = \mathrm{Im}(e^{it})$

Rem 14: On a alors $\forall t \in \mathbb{R}$, $\cos(t) = \frac{e^{it}+e^{-it}}{2}$, $\sin(t) = \frac{e^{it}-e^{-it}}{2i}$ et $e^{it} = \cos(t) + i\sin(t)$

Ex 15: $e^{i\pi} = -1$, $\cos(\pi) = -1$, $\sin(\pi) = 0$.

Thm 16: $\forall t \in \mathbb{R}$, $\cos(t)^2 + \sin(t)^2 = 1$ et cos et sin sont 2π-périodiques.

Prop 17: On peut ainsi donner une autre paramétrisation de $\mathbb{U} \setminus \{-1\}$: $t \in \mathbb{R} \mapsto \frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2} \in \mathbb{U} \setminus \{-1\}$

App 18: Les solutions dans $\mathbb{Z}^3$ de $x^2+y^2=z^2$ sont données par : $(d(u^2-v^2) ; 2duv ; d(u^2+v^2))$ où $u \wedge v = 1$ et $d \in \mathbb{N}$.

C] Argument d'un nombre complexe

Thm 19: $\forall z \in \mathbb{C}^*$, $\exists! r \in \mathbb{R}_+^*$, $\exists! \omega \in \mathbb{U}$ / $z = r\omega$.
De plus, $|z| = r$

Def 20: Soit $z \in \mathbb{C}^*$. On appelle argument de z tout réel $t \in \mathbb{R}$ tel que $e^{it} = \frac{z}{|z|}$. Si V est un ouvert de $\mathbb{C}^*$, une détermination continue de l'argument sur V est une application $\theta : V \to \mathbb{R}$ continue telle que $\theta(z)$ soit un argument de z pour tout $z \in V$.

Ex 21: π et 3π sont des arguments de -1.

Thm 22: Il n'existe pas de détermination continue de l'argument sur $\mathbb{C}^*$.

Prop-def 23: On appelle détermination principale de l'argument la fonction $\mathrm{Arg} : \mathbb{C} \setminus \mathbb{R}_- \to]-\pi ; \pi[$ qui à $z \in \mathbb{C} \setminus \mathbb{R}_-$ associe son unique argument entre $-\pi$ et π. Arg est une détermination continue de l'argument.
Une application de ces résultats est la recherche de détermination continue du logarithme :

Prop 24 : $f : U \to \mathbb{C}$ est une détermination continue du log si et seulement si il existe une détermination continue de l'argument θ telle que $\forall z \in U$, $f(z) = |z| + i\theta(z)$

Cor 25 : Il n'existe pas de détermination continue du log sur $\mathbb{C}^*$.

Cor 26 : $\text{Log} : \mathbb{C} \setminus \mathbb{R}_- \to \mathbb{C}$, $z \mapsto |z| + i\text{Arg}(z)$ est une détermination continue du logarithme appelée détermination principale du logarithme.

II) Racines complexes de l'unité

A] Les groupes $\mathbb{U}_n$

Def 27 : Soit $n \in \mathbb{N}^*$. On définie $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$

Ex 28 : $\mathbb{U}_1 = \{1\}$, $\mathbb{U}_2 = \{\pm 1\}$, $\mathbb{U}_4 = \{\pm 1, \pm i\}$

Rem 29 : En particulier, $\forall n \in \mathbb{N}^*$, $\mathbb{U}_n \subset \mathbb{U}$.

Prop 30 : Soit $n \in \mathbb{N}^*$. Alors pour tout $z \in \mathbb{C}$, $z \in \mathbb{U}_n$ si et seulement si $\exists k \in [\![0, n-1]\!] / z = e^{\frac{2ik\pi}{n}}$

Cor 31 : $X^n - 1 = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}})$

Thm 32 : Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un groupe multiplicatif isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, il est cyclique et $e^{\frac{2i\pi}{n}}$ est un générateur.

Cor 33 : Les sous-groupes de $\mathbb{U}_n$ sont les $\mathbb{U}_d$ pour $d | n$.

B] Polynômes cyclotomiques

Def 34 : Une racine $z \in \mathbb{U}_n$ est dite primitive si elle est génératrice de $\mathbb{U}_n$.

Ex 35 : Le théorème 32 donne un exemple de racines primitives.

Prop 36 : Soient $k \in [\![0, n-1]\!]$ et $z = e^{\frac{2ik\pi}{n}} \in \mathbb{U}_n$. z est primitive si et seulement si $k \wedge n = 1$.

Cor 37 : Si φ est l'indicatrice d'Euler donnée par : $\varphi(n) = \text{Card}(\mathbb{Z}/n\mathbb{Z})^*$, alors il y a $\varphi(n)$ racines primitives dans $\mathbb{U}_n$.

App 38 : $n = \sum_{d | n} \varphi(d)$

Def 39 : On définie le n-ième polynôme cyclotomique par : $\Phi_n(X) = \prod_{\substack{\omega \in \mathbb{U}_n \\ \omega \text{ primitive}}} (X - \omega)$

Ex 40 : Si $p \in \mathbb{N}^*$ est premier, $\Phi_p(X) = 1 + X^2 + \dots + X^{p-1}$

Rem 41 : $\deg \Phi_n = \varphi(n)$.

Thm 42 : (DEV 1) $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d | n} \Phi_d(X)$

Cor 43 : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$

App 44 : (Théorème de Dirichlet faible) Il existe une infinité de nombres premiers p tels que $p \equiv 1 [n]$

Rem 45 : La version forte établie le même résultat pour $p \equiv m [n]$ dès que $m \wedge n = 1$.

App 46 : (Théorème de Wedderburn) Tout corps fini est commutatif.

Thm 47 : Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}[X]$

App 48 : Soit $\omega = e^{\frac{2i\pi}{n}}$ et $\mathbb{K} = \mathbb{Q}(\omega)$. Alors $[\mathbb{K} : \mathbb{Q}] = \varphi(n)$.

III) Diverses applications en algèbre

A] Constructibilité à la règle et au compas

Def 49 : Soit $\mathcal{B} \subset \mathbb{R}^2$ et soit $M \in \mathbb{R}^2$. M est dit constructible à partir de $\mathcal{B}$ si on a l'une des scénarios suivants :
① M est intersection de deux droites données par deux éléments de $\mathcal{B}$
② M est à l'intersection de deux cercles centrés en un point de $\mathcal{B}$ et de rayon la distance entre deux points de $\mathcal{B}$.
③ M est à l'intersection d'une droite et un cercle comme précédemment.
On pose $\mathcal{B} = \{(0,0), (1,0)\}$. M est dit constructible s'il existe des points $M_1, \dots, M_p = M$ tels que $\forall i \in [\![1;p]\!]$, M_i est constructible par rapport à $\mathcal{B} \cup \{M_1; \dots; M_{i-1}\}$.

Thm 50 : (de Wantzel) Un point $M \in \mathbb{R}^2$ d'affixe z est constructible si et seulement si il existe $L_1 = \mathbb{Q}, L_2, \dots, L_p$ des sous-corps de $\mathbb{C}$ tels que $\forall i \in [\![1;p-1]\!]$, $L_i \subset L_{i+1}$ et $[L_{i+1} : L_i] = 2$ et $z \in L_p$.

Cor 51 : Si z est constructible, il est algébrique sur $\mathbb{Q}$ de degré une puissance de 2.

Rem 52 : La réciproque est fausse.

Def 53 : Un angle $\theta \in \mathbb{R}$ est constructible si $e^{i\theta}$ l'est. Le polygône régulier à n côtés est constructible si l'angle $\frac{2\pi}{n}$ est constructible.

Thm 54 : $(\mathcal{D} \in \mathcal{V}_2)$ (de Gauss-Wantzel) Soit $p \geq 3$ premier et $\alpha \in \mathbb{N}^*$. Le polygône à p^α côtés est constructible si et seulement si $\alpha = 1$ et $\exists n \in \mathbb{N}^*$, $p = 2^n + 1$

Cor 55 : Les polygônes réguliers à n côtés constructibles sont ceux tels que $n = 2^\alpha p_1 \dots p_k$ où les p_i sont des nombres premiers de Fermat 2 à 2 distincts.

B] Déterminant circulant

Def 56 : Une matrice circulante est une matrice de la forme $\begin{pmatrix} a_1 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & & & \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$.

Prop 57 : Soit $P(X) = \sum_{k=0}^{n-1} a_{k+1} X^k$. Le déterminant de cette matrice est alors $\prod_{k=0}^{n-1} P(\omega^k)$ où $\omega = e^{\frac{2i\pi}{n}}$.

App 58 : Si $\mathcal{P}_0$ est un polygone et que $\mathcal{P}_{i+1}$ est celui obtenu via $\mathcal{P}_i$ en prenant le milieu des arrêtes, alors les sommets de $\mathcal{P}_n$ convergent vers l'isobarycentre des sommets de $\mathcal{P}_0$.

C] Représentations linéaires

Soit G un groupe fini d'ordre $n \in \mathbb{N}^*$.

Def 59 : Une représentation de G est un couple (ρ, V) où V est un $\mathbb{C}$-espace vectoriel de dimension finie et $\rho : G \to GL(V)$ un morphisme de groupes.
$\chi : G \to \mathbb{C}$, $g \mapsto \mathrm{tr}(\rho(g))$ est le caractère de (ρ, V).

Prop 60 : Les valeurs propres de $\rho(g)$, $g \in G$, sont des racines de l'unité.

Cor 61 : $\forall g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$

Thm 62 : $\ker \rho = \{g \in G \mid \chi(g) = \chi(1)\}$

App 63 : Soient $\chi_1, \dots, \chi_r$ les caractères irréductibles de G. Les sous-groupes distingués de G sont exactement les $\bigcap_{i \in I} H_i$ où $I \subset [\![1;r]\!]$ et $\forall i \in [\![1;r]\!]$, $H_i = \{g \in G \mid \chi_i(g) = \chi_i(1)\}$.

Rem 64 : Ceci permet de lire les sous-groupes distingués de G dans sa table de caractère.

References :

- Analyse complexe pour la licence, Tauvel [1]
- Algèbre et géométrie, Rombaldi [2]
- Algèbre, Gourdon [3]
- Cours d'algèbre, Perrin [4]
- Algèbre de la transformée de Fourier discrète, Peyré [5]
- Algèbre et géométrie, Combes [6]
- Théorie des corps, Carrega [7]