

Leçon N° 102 Groupe des complexes de module 1

I) Préambules

Notations

Définition 1: Soit $z = a + ib \in \mathbb{C}$. On définit le module de z comme étant $|z| = \sqrt{a^2 + b^2} \in \mathbb{R}^+$.

Proposition 2: $\forall z \in \mathbb{C}$, $|z| = \sqrt{z \bar{z}}$.

Remarque 3: 1) Soit $z \in \mathbb{R}$, le module de z n'est autre que sa valeur absolue.

2) $z = 1$ ou $z = -1$ ont le même module.

3) $z = 0$ ou $z = 1$ ont le même module.

4) $\forall z \in \mathbb{C}$, z et $\bar{z}$ ont le même module.

Proposition 4: $|z|$ est une norme sur $\mathbb{C}$.

Proposition 5: $\forall z \in \mathbb{C}$, $|\operatorname{Re}(z)| \leq |z|$ et $|\operatorname{Im}(z)| \leq |z|$.

Proposition 6: $\forall z, z' \in \mathbb{C}$, $|zz'| = |z||z'|$.

Si $z \neq 0$, $\left| \frac{1}{z} \right| = \frac{1}{|z|}$.

Corollaire 7: $\forall z \in \mathbb{C}$ et $\forall n \in \mathbb{N}$, $|z^n| = |z|^n$.

2) Le groupe $(\mathbb{C}^*, \times)$

Proposition 8: $\mathbb{C}^*$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Étant entendu que $\mathbb{C}^* = \{z \in \mathbb{C} \mid |z| \neq 0\}$.

Proposition 9: $\forall z \in \mathbb{C}^*$, $\exists \theta \in \mathbb{R}$ tq $z = |z|e^{i\theta} = |z|(\cos \theta + i \sin \theta)$.

(cf Annexe A2, on a obtenu $\cos \theta = \operatorname{Re}(z)$ et $\sin \theta = \frac{\operatorname{Im}(z)}{|z|}$).

Définition 10: $\forall z \in \mathbb{C}^*$, $\exp(z) = \sum_{k=0}^{+\infty} \frac{z^k}{k!}$.

Donc $\exp(i\theta) = \cos(\theta) + i \sin(\theta)$.

Exemples 11: $e^{i\pi} = -1$, $e^{i\frac{\pi}{2}} = i$, $e^{i\frac{3\pi}{2}} = -i$, $e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$.

Proposition 12: $\forall (\theta, \theta') \in \mathbb{R}^2$, $e^{i\theta} = e^{i\theta'}$ si et seulement si $\theta - \theta' = 2k\pi$.

Proposition 13: $\forall (\theta, \theta') \in \mathbb{R}^2$, $e^{i\theta} e^{i\theta'} = e^{i(\theta + \theta')}$.

Exemple 14: $e^{i\pi} + 1 = 0$.

Proposition 15: (Formule de Moivre) $\forall \theta \in \mathbb{R}$ et $\forall n \in \mathbb{N}$, $(e^{i\theta})^n = e^{in\theta}$.

Proposition 16: $\forall z \in \mathbb{C}^*$, $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$.

Corollaire 17: $\forall z \in \mathbb{C}^*$, $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$ (pour l'écriture complexe de z).

Définition 18: $\forall z \in \mathbb{C}^*$ tq $z = |z|e^{i\theta}$, on appelle $\operatorname{Arg}(z)$ le réel θ , $\operatorname{Arg}(z) \in \mathbb{R}/2\pi\mathbb{Z}$.

Proposition 19: (Formule d'Euler) $\forall \theta \in \mathbb{R}$, $\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}$ et $\sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}$.

Application 20: $\cos(3\pi) = \cos(3\pi) = -1$ et $\sin(3\pi) = 0$.

Théorème 21: $\forall z \in \mathbb{C}^*$, il y a exactement n racines n -ièmes de z .

Notation 22: On note $\mathbb{U}_n$ l'ensemble des racines n -ièmes de 1.

Proposition 23: $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal n .

Exemple 24: $\mathbb{U}_4 = \{1, i, -1, -i\}$, $\mathbb{U}_3 = \{1, \omega, \omega^2\}$ où $\omega = e^{i\frac{2\pi}{3}}$.

Corollaire 25: $\sum_{k=0}^{n-1} \omega^k = 0$.

Exemple 26: $\mathbb{U}_4 = \{1, i, -1, -i\}$.

$\mathbb{U}_3 = \{1, \omega, \omega^2\}$ avec $\omega = e^{i\frac{2\pi}{3}}$.

$\mathbb{U}_2 = \{1, -1\}$.

$\mathbb{U}_1 = \{1\}$.

$\mathbb{U}_0 = \{1\}$.

$\mathbb{U}_n = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ avec $\omega = e^{i\frac{2\pi}{n}}$.

$\mathbb{U}_2 = \{1, -1\}$ avec $-1 = e^{i\pi}$.

$\mathbb{U}_1 = \{1\}$.

$\mathbb{U}_0 = \{1\}$.

II) Cyclotomie.

1) Polynômes cyclotomiques.

Définition 26: Soit $n \in \mathbb{N}^*$. Une racine n -ième primitive de 1 est un élément $\zeta \in \mathbb{C} \setminus \{0\}$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1 \quad \forall d < n$.

Proposition 27: Si on note $\mu_n(\mathbb{C})$ et $\mu_n^*(\mathbb{C})$ les racines et les racines primitives n -ième de l'unité alors $\zeta \in \mu_n^*(\mathbb{C})$ ssi $\langle \zeta \rangle = \mu_n(\mathbb{C})$.

Corollaire 28: $|\mu_n^*(\mathbb{C})| = \varphi(n)$ où φ est l'indicateur d'Euler.

Définition 29: Le n -ième polynôme cyclotomique est

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*(\mathbb{C})} (X - \zeta).$$

Remarque 30: Si $\zeta \in \mu_n^*(\mathbb{C})$, les autres sont ζ^p avec $\text{m.p.c.} = 1$.

2) Φ_n est unitaire de degré $\varphi(n)$.

Proposition 31: $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Corollaire 32: $n = \sum_{d|n} \varphi(d)$.

Exemples 33: $\Phi_1(X) = X - 1$.

$$\Phi_2(X) = X + 1$$

$$\Phi_3(X) = X^2 + X + 1$$

$$\Phi_4(X) = X^2 + 1$$

$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$$

$$\Phi_6(X) = X^2 - X + 1$$

$$\Phi_8(X) = X^4 + 1$$

Proposition 34: Si p est premier, $\Phi_p(X) = X^{p-1} + \dots + 1$.

2) Indéductibilité des polynômes cyclotomiques.

Proposition 35: On a $\Phi_n \in \mathbb{Z}[X]$.

Théorème 36: Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$. Dev 1.

Corollaire 37: Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$.

Corollaire 38: Si $\zeta \in \mu_n^*(\mathbb{C})$, son polynôme minimal sur $\mathbb{Q}$ est Φ_n .

Corollaire 39: Si $\zeta \in \mu_n^*(\mathbb{C})$, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

3) Applications.

Proposition 40: Soient α, α' des racines n -ième et m -ième de 1 primitives. Si $\text{m.p.c.} = 1$, alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\alpha') = \mathbb{Q}$.

Lemme 40-1: Soit $\mathbb{Q} \subset \Gamma$ une extension, $\mathbb{Q}$ et $\mathbb{Z}$ deux

corps intérieurement, $\mathbb{Q} \subset \Gamma$ le sous-corps de l'engendré par $\mathbb{Q}$ et $\mathbb{Z}$. Alors $[\mathbb{Q} : \mathbb{Z}] \leq [\Gamma : \mathbb{Q}]$.

Application 41 (Wedderburn): Tout corps fini est commutatif. Dev 2.

Proposition 42: Soit $\mathbb{Q}$ un corps et $\sigma : \mathbb{Q} \rightarrow \mathbb{Q}$

l'isomorphisme canonique.

On a alors $\Phi_{n,\sigma}(X) = \sigma(\Phi_n(X))$

ou $\Phi_{n,\sigma}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{Q})} (X - \sigma(\zeta))$.

En particulier Φ_n, Γ_p s'obtiennent à partir de Φ_n, α par réduction modulo p .

Application 4.3: Soit $n \in \mathbb{N}^*$, et γ - équivalence entre :

- i) $\exists p \in \mathbb{D}$ avec $p \mid n = 1$ et Φ_n, Γ_p soit irréductible sur $\mathbb{F}_p$
- ii) $(n/p) \neq 1$ est cyclotomique
- iii) On a $n = 1, 2, 4, q^2$ ou q^2 avec q premier impair.

III) Polygones réguliers

Lemme 4.4: On considère la matrice circulante

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_n & a_1 & \dots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & a_1 \end{pmatrix} \in M_n(\mathbb{C})$$

$$\text{et } J = \begin{pmatrix} 1 & \omega & \dots & \omega^{n-1} \\ \omega & 1 & \dots & \omega^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{n-1} & \omega^{n-2} & \dots & 1 \end{pmatrix} \in M_n(\mathbb{C})$$

Alors $A = P(J)$ où $P = \sum_{i=0}^{n-1} a_i X^{i-1}$

$$\text{et } A \sim \begin{pmatrix} P(\omega^0) & & \\ & \ddots & \\ & & P(\omega^{n-1}) \end{pmatrix} \text{ où } \omega = e^{\frac{2\pi i}{n}}$$

Application 4.5: Soit $P_0 \in \mathbb{C}$ l'axe un polygone à n sommets.

On définit la suite de polygones (P_i) par $P_{i+1}, i = \frac{P_{i-1} + P_{i+1}}{2}$

Soit $g = \frac{1}{n} \sum_{i=1}^n P_{0,i}$ l'isobarycentre de P_0 .

La suite P_i converge géométriquement vers le polygone circonscrit Q . (cf annexe 3)