102 : Exemple des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications

I L'exponentielle complexe, le groupe $\mathbb{U}$ et les racines de l'unité

Def : $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$

1) Construction de l'exponentielle, des fonctions trigonométriques et propriétés.

On définit pour tout nombre complexe z

$$\exp z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$$

$$\cos z = \frac{\exp(iz) + \exp(-iz)}{2} \; ; \; \sin z = \frac{\exp(iz) - \exp(-iz)}{2i}$$

Théorème :

(i) exp, cos et sin sont analytiques sur $\mathbb{C}$ et $\exp' = \exp$; $\sin' = \cos$; $\cos' = -\sin$.

(ii) $\exp(z_1 + z_2) = \exp(z_1)\exp(z_2)$ $\forall z_1, z_2 \in \mathbb{C}$

$\forall z \in \mathbb{C}$, $\exp z \neq 0$ et $(\exp z)^{-1} = \exp(-z)$.

(iii) $\cos^2 z + \sin^2 z = 1$ et $\cos z + i \sin z = \exp(iz)$, $\forall z \in \mathbb{C}$

(iv) $|\exp z| = \exp(\mathrm{Re}\, z)$ et $\exp z \in \mathbb{U} \Leftrightarrow z \in i\mathbb{R}$

(v) $\exp \bar{z} = \overline{\exp z}$ $\forall z \in \mathbb{C}$, et $z \in \mathbb{R}$

$\Rightarrow \sin z$ et $\cos z \in \mathbb{R}$.

Le nombre π : proposition et définition :

La fonction $\cos : \mathbb{R} \to \mathbb{R}$ possède un plus petit zéro > 0. π est par définition le double de ce zéro.

Théorème :

(i) $\cos \frac{\pi}{2} = 0$; $\sin \frac{\pi}{2} = 1$; $\exp(i\pi) + 1 = 0$

(ii) exp est $2i\pi$ périodique ; cos et sin sont 2π périodiques.

(iii) $\forall z \in \mathbb{U}$, $\exists ! \, t \in [0, 2\pi[$ tel que $\exp(it) = z$

(iv) $\exp : \mathbb{C} \to \mathbb{C}^*$ est surjective.

- $\varphi : \mathbb{R} \to \mathbb{U}$, $t \mapsto \exp(it)$ est donc injective non surjective, $\ker \varphi = 2\pi\mathbb{Z}$,

donc $\mathbb{U} \cong \mathbb{R}/2\pi\mathbb{Z}$.

- Enfin, on note $\gamma_r : [0,1] \to \mathbb{C}$, $t \mapsto re^{2i\pi t}$, $L(\gamma_r) = 2\pi r$.

2) Les racines $n^{\text{ièmes}}$ de l'unité

Théorème : Soit $n \geq 1$. L'équation $z^n = 1$ possède n racines distinctes. L'ensemble $\mathbb{U}_n$ de ces racines est un sous groupe de $\mathbb{U}$ d'ordre n, cyclique.

Corollaire : $\mathbb{C}$ est algébriquement clos.

Définition: On appelle racine primitive $n^{ième}$ de l'unité tout générateur de U_n. Elles sont en nombre $\varphi(n)$.

Proposition : Soit G un sg fini d'ordre n de $\mathbb{C}^*$. Alors $G = U_n$

Corollaire : les sous groupes finis de $O_2(\mathbb{R})$ sont les $\mathbb{Z}/n\mathbb{Z}$ et D_n

Proposition: $U_d \subset U_n \iff d \mid n$. Autrement dit, U_n admet un unique sous groupe d'ordre d $\forall d \mid n$, c'est U_d.

Proposition: Un sous groupe de U est soit un U_n, soit dense dans U.

II Polynomes cyclotomiques.

1) Définitions.

Soit K un corps, $n \in \mathbb{N}^*$, $P_n = X^n - 1 \in K[X]$, K_n le corps de décomposition de de $X^n - 1$ et $U_n(K)$ l'ensemble des racines $n^{ièmes}$ de l'unité dans K_n. $U_n^*(K)$ l'ensemble des racines $n^{ièmes}$ primitives. On pose:

$$\Phi_{n,K}(X) = \prod_{\omega \in U_n^*(K)} (X - \omega) \quad \text{si } p \nmid n \quad (p = \operatorname{car} K).$$

Théorème:

(i) $\prod_{d \mid n} \Phi_{n,K} = X^n - 1$ (ii) $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$

(iii) Si $\sigma : \mathbb{Z} \to K$ est le morphisme canonique, $\Phi_{n,K} = \sigma(\Phi_{n,\mathbb{Q}})$

Corollaire 1: on peut étendre la définition de Φ_n au cas où $\operatorname{car} K \mid n$.

Corollaire 2: Théorème de Wedderburn.

2) Calcul des polynomes cyclotomiques.

Soit K un corps et $n \in \mathbb{N}^*$ / $\operatorname{car} K \nmid n$.

En notant $\Phi_n = \Phi_{n,K}$, on a :

$$\Phi_n(X) = \prod_{d \mid n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}$$ où μ est la fonction de Moebius

$$\Phi_{nq}(X) = \frac{\Phi_n(X^q)}{\Phi_n(X)}$$ où q est premier, $q \nmid n$.

Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $m = p_1 \cdots p_k$, $\Phi_n(X) = \Phi_m\left(X^{\frac{n}{m}}\right)$

$$\Phi_{2n}(X) = \begin{cases} \Phi_n(-X) & \text{si } n \text{ est impair} \\ \Phi_n(X^2) & \text{si } n \text{ est pair.} \end{cases}$$

3) Irreductibilité des polynomes cyclotomiques.

a) Sur $\mathbb{F}_p$

Proposition : Φ_n mod p est sans facteur carré et tous ses facteurs irréductibles sont de même degré

Réduction totale (p+n). Proposition :

$X^n - 1$ scindé sur $\mathbb{F}_p \iff \Phi_n$ scindé sur $\mathbb{F}_p \iff \Phi_n$ a une racine dans $\mathbb{F}_p \iff p \equiv 1 \mod n \iff \exists k \in \mathbb{Z} / p \mid \Phi_n(k)$ dans $\mathbb{Z}$.

Conséquence : Soit $n \in \mathbb{N}^*$. Il existe une infinité de nombres premiers de la forme $an+1$.

Théorème : $\exists p$ premier tel que Φ_n est irréductible sur $\mathbb{F}_p \iff (\mathbb{Z}/n\mathbb{Z})^*$ cyclique $\iff n = 1, 2, 4$ ou $q^\alpha, 2q^\alpha$ (q premier impair).

b) Sur $\mathbb{Z}$.

Théorème : Φ_n est irréductible dans $\mathbb{Z}[X]$.
autrement dit, les Φ_n sont les polynomes minimaux des racines primitives $n^{ième}$ de l'unité.

Corollaire : Le polygone régulier à n côtés est constructible ssi $n = 2^\alpha F_1 \cdots F_p$ où les F_i sont des nombres de Fermat premier.

III Caractères d'un groupe Abelien fini. (Gaf).

Définition : un caractère d'un gaf G est un morphisme $\chi : G \to (\mathbb{C}^*, \cdot)$. $\hat{G}$ l'ensemble des caractères est muni d'une structure de groupes. On a $\chi^{-1} = \overline{\chi}$.
Un caractère d'un gaf d'ordre n est à valeurs dans U_n.

Proposition : si G est cyclique, $G \cong \hat{G}$.

Lemme : Soit G un gaf, H un sous groupe de G, $\chi \in \hat{H}$. $\exists \hat{\chi} \in \hat{G}$ tel que $\hat{\chi}_{|H} = \chi$.

Conséquence : (i) $\sum_{x \in G} \chi(x) = \begin{cases} |G| \text{ si } \chi \text{ est trivial} \\ 0 \text{ sinon.} \end{cases}$

(ii) $\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} |\hat{G}| \text{ si } x = 1 \\ 0 \text{ sinon} \end{cases}$

(iii) $|G| = |\hat{G}|$.

Corollaire 1 : Notons $\mathbb{C}[G]$ l'ensemble des fonctions de G dans $\mathbb{C}$. Muni du produit scalaire $\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$, $\mathbb{C}[G]$ est un espace hermitien.
Alors $\hat{G}$ est une bon de $\mathbb{C}[G]$.

Corollaire 2 : $\varphi : \begin{cases} G \to \hat{\hat{G}} \\ x \mapsto ev(x) \end{cases}$ est un isomorphisme.

Corollaire 3 : Théorème de décomposition des groupes abeliens finis.

Références :

Partie I 1) Rudin Principes d'analyse mathématique

Partie II Perrin, cours d'algèbre
Goblot, algèbre commutative
Carrega, théorie des corps