Leçon 102 - Groupe des nombres complexes de module 1. Sous-groupe des racines de l'unité. Applications.

1. Nombres complexes de module 1. —

1. Le groupe $\mathbb{U}$. —

- Def : On appelle groupe des nombres complexes de module 1 le noyau du morphisme de groupes $z \in \mathbb{C}^* \mapsto |z| \in \mathbb{R}_+^*$. On le note $\mathbb{U}$.
- Rem : En identifiant le plan complexe à $\mathbb{R}^2$, $\mathbb{U}$ n'est autre que le cercle unité S^1.
- Thm : L'application $(r,u) \in \mathbb{R}_+^* \times \mathbb{U} \mapsto r.u \in \mathbb{C}^*$ est un isomorphisme de groupes.
- Thm : L'application $x \in \mathbb{R} \mapsto exp(ix) \in \mathbb{U}$ est un morphisme surjectif de groupes, 2π-périodique, de noyau $2\pi\mathbb{Z}$.
  On en déduit $\mathbb{R}/(2\pi\mathbb{Z}) \simeq \mathbb{U}$.
- Cor : $\mathbb{U}$ est un compact connexe de $\mathbb{C}$.

2. Applications trigonométriques. —

- Def : On définit les fonctions cosinus et sinus par $cos(x) = Re(exp(ix))$ et $sin(x) = Im(exp(ix))$.
- Pro : Formule de Moivre : $exp(inx) = cos(nx) + isin(nx)$
  Formules d'Euler : $cos(x) = \frac{exp(ix)+exp(-ix)}{2}$, $sin(x) = \frac{exp(ix)-exp(-ix)}{2i}$
- Ex : $exp(\frac{2i\pi}{3}) = \frac{1+i\sqrt{3}}{2}$, $exp(\frac{i\pi}{2}) = i$.
- App : $\sum_{k=0}^{n} cos(kt) = cos(\frac{nt}{2})\frac{sin((n+1)t/2)}{sin(t/2)}$ pour tous $t \in \mathbb{R} - 2\pi\mathbb{Z}$.
- App : Linéarisation de $cos(x)^n$: $cos(x)^n = \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}exp(ix(2k-n))$.
- App : Expression de $cos(nx)$ comme polynôme en $cos(x)$: $cos(nx) = T_n(cos(x))$ où T_n est le n-ième polynôme de Tchebychev.
- App : Calcul du noyau de Dirichlet et du noyau de Féjer.

3. Paramétrisation sur le cercle unité. —

- Pro : Chercher les $(x,y,z) \in \mathbb{Z}^3$ tels que $x^2+y^2 = z^2$ revient à chercher les $(x',y') \in \mathbb{Q}^2$ tels que $x'^2 + y'^2 = 1$.
- Thm : Paramétrisation rationnelle de $\mathbb{U}$: L'application $t \in \mathbb{R} \mapsto (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \in \mathbb{U} - \{(-1,0)\}$ est une bijection.
  Elle se prolonge à $\mathbb{R} \cup \{\infty\}$ en associant $(-1,0)$ au point ∞.
- App : Les points de $\mathbb{U} - \{(-1,0)\}$ à coordonnées rationnelles sont de la forme $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ pour un $t \in \mathbb{Q}$.
- App : Les solutions entières de $x^2+y^2 = z^2$ sont de la forme $(u^2-v^2, 2uv, u^2+v^2)$ avec $u,v \in \mathbb{Z}$.

4. Mesure d'un angle orienté. —

- Pro : Pour u,v vecteurs unitaires de $\mathbb{R}^2$, il existe une unique rotation envoyant u sur v.
- Def+Pro : On munit A l'ensemble des couples de vecteurs unitaires de $\mathbb{R}^2$ de la relation d'équivalence : $(u,v)R(u',v')$ ssi la même rotation envoie u sur u' et v sur v'.
- Def : La classe d'équivalence de (u,v) pour R est appelée angle orienté.
  On appelle $\overline{A}$ l'ensemble des angles orientés.
- Pro : L'application qui à $\overline{(u,v)} \in \overline{A}$ envoie l'unique rotation $r \in SO_2(\mathbb{R})$ telle que $r(u) = v$ est une bijection.
- Rem : Cette bijection munit $\overline{A}$ d'une structure de groupe.
- Cor : L'application $t \in \mathbb{R} \mapsto \begin{pmatrix} cos(t) & -sin(t) \\ sin(t) & cos(t) \end{pmatrix} \in SO_2(\mathbb{R})$ est un morphisme surjectif, 2π-périodique, de noyau $2\pi\mathbb{Z}$.
  L'isomorphisme induit entre $\mathbb{R}/(2\pi\mathbb{Z})$ et $SO_2(\mathbb{R})$ permet de définir une mesure des angles orientés de vecteurs.

2. Racines de l'unité et cyclotomie. —

1. Sous-groupes des racines de l'unité. —

- Pro : Un sous-groupe de $\mathbb{U}$ est dense ou fini.
  Le sous-groupe $< exp(it) >$ est dense si $t \notin \pi\mathbb{Q}$ et fini sinon.
- App : L'adhérence de la suite $(sin(n))_n$ est le segment $[-1,1]$.
- Def : Pour $n \geq 1$, on définit $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité : les $z \in \mathbb{U}$ tels que $z^n = 1$.
- Pro : $\mathbb{U}_n$ est un groupe cyclique d'ordre n.
  L'application $\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mapsto exp(\frac{2i\pi k}{n}) \in \mathbb{U}_n$ est un isomorphisme de groupes.
- Def+Pro : On appelle racine n-ième primitive de l'unité un générateur de $\mathbb{U}_n$.
  Elles sont de la forme $exp(\frac{2i\pi k}{n})$ pour $pgcd(k,n) = 1$, on note μ_n^* leur ensemble, et il y en a $\phi(n)$.
- Ex : Racines primitives 2ièmes : -1. Racines primitives 3ièmes : j, j^2. Racines primitives 4ièmes : $i, -i$. Racines primitives 8ièmes : $\pm\frac{1 \pm i}{\sqrt{2}}$.
- Pro : $\mathbb{U}_d \subset \mathbb{U}_n$ ssi $d|n$.
- Pro : $\mathbb{U}_n = \sum_{d|n} \mu_d^*$
- App : $n = \sum_{d|n} \phi(d)$.
- Pro : Dans un corps fini de cardinal p^r pour p premier, un élément x non-nul est d'ordre n ssi x est racine de $X^n - 1$ mais pas de $X^d - 1$ $\forall d|n$, $d < n$.
  On en a $\phi(n)$ si $n|p^r - 1$ et 0 sinon.
- App : Le groupe des inversibles d'un corps fini est cyclique d'ordre $p^r - 1$.
- App : Théorème de Wedderburn : Tout anneau A intègre fini (non supposé unitaire ni commutatif) est un corps.

2. Polynômes cyclotomiques. —

- Def : Pour tout $n \geq 1$, on définit $\Phi_n(X) := \Pi_{k \wedge n = 1,\ k \leq n}(X - e^{2i\pi\frac{k}{n}}) \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique.

- **Dev** : Φ_n est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbb{Z}[X]$, de degré $\phi(n) = Card(\mathbb{Z}/n\mathbb{Z}^*)$ et tel que $\Pi_{d|n}\Phi_d = X^n - 1$.
- Ex : $\Phi_1 = X - 1$. $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\phi_8 = X^4 + 1$.
- Pro : Pour p premier, $\Phi_p(X) = X^{p-1} + .. + X + 1$, $\Phi_{p^2}(X) = X^{p(p-1)} + .. + X + 1$.
- Théorème de Kronecker : Soit $P \in \mathbb{Z}[X]$ dont les racines dans $\mathbb{C}$ sont non-nulles et de module ≤ 1. Alors les racines de P sont des racines de l'unité.
- Cor : Si de plus P est irréductible, alors P est un polynôme cyclotomique.

3. Applications en théorie des représentations. —

- Def : Soit G un groupe fini. Une représentation linéaire sur G est un morphisme $\rho : G \to GL(V)$ où V est un $\mathbb{C}$-ev de dimension finie.
  Le caractère χ_ρ est l'application $g \in G \mapsto Tr(\rho(g)) \in \mathbb{C}$.
- Def : Une représentation est dite irréductible ssi aucun sous-espace strict de V n'est stable par tous les $\rho(g)$. Un caractère irréductible est le caractère d'une représentation irréductible.
- Pro : Soit G un groupe fini d'ordre n. Soit ρ une représentation de G.
  $\forall g \in G$, $\rho(g)$ est diagonalisable et son spectre est inclus dans $\mathbb{U}_n$.
- Pro : Si G est abélien, alors toutes ses représentations irréductibles sont de degré 1 et à valeurs dans $\mathbb{U}_n$.
- App : Table de caractères d'un groupe cyclique.
- Pro : Soit G un groupe abélien fini et H un sous-groupe de G. Pour tout caractère $\chi \in \widehat{H}$, il existe un caractère $\widetilde{\chi} \in \widehat{G}$ tel que $\widetilde{\chi}|_H = \chi$.
- **Dev** : Théorème de structure des groupes abéliens finis : Soit G un groupe abélien non trivial. Il existe $r \geq 1$ et des entiers $d_1|..|d_r$ tels que $G \simeq \mathbb{U}_{d_1} \times .. \times \mathbb{U}_{d_r}$.
  Les d_i sont uniques et sont appelés facteurs invariants de G.

Références

Arnaudiès, Fraysse : $\mathbb{U}$, l'isomorphisme $\mathbb{C}^*/\mathbb{R}_+^*$, morphisme surjectif $exp(ix)$, noyau, cos et sin, formule d'Euler, formule de Moivre, linéarisation du cos^n, polynômes de Tchebychev. Détermination de l'argument.
Audin : Relation d'équi pour angle orienté, mesure d'un angle orienté.
Combes : Paramétrisation du cercle unité, triplets pyrhagoriciens. $\phi(n)$, exemples.
Perrin : Etude des polynômes cyclotomiques.(Dev)
Peyré : Représentations, Table des caractères d'un groupe cyclique, Théorème de structure des groupes abéliens finis.(Dev)
Gozard : $\mathbb{U}_n$, groupe cyclique, exemples. Polynômes cyclotomiques.
FGN (Algèbre 1) : Théorème de Kronecker, corollaire.

June 7, 2017

Vidal Agniel, École normale supérieure de Rennes