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

I. Définitions et premières propriétés.

1) Groupe des nombres complexes de module 1.

Def 1 : Soit $\varphi : \mathbb{C}^* \to \mathbb{R}_+^*$, $z \mapsto |z|$. φ est un morphisme du groupe $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$. $\mathrm{Ker}\varphi = \{z \in \mathbb{C}^* \mid |z| = 1\}$ est un sous-grp de cet ensemble, noté $\mathbb{U}$. On l'appelle aussi cercle unité de $\mathbb{C}$.

Thm 2 : $f : \mathbb{R}_+^* \times \mathbb{U} \to \mathbb{C}^*$, $(r,u) \mapsto ru$ est un isomorphisme de $\mathbb{R}_+^* \times \mathbb{U}$ sur $\mathbb{C}^*$

2) Exponentielle complexe.

Def 3 : On définit $\exp : \mathbb{C} \to \mathbb{C}$, $z \mapsto \sum_{k=0}^{+\infty} \frac{z^k}{k!}$

Thm 4 : $g : \mathbb{R} \to \mathbb{U}$, $x \mapsto \exp(ix) =: e^{ix}$ est un morphisme surjectif.

Def 5 : On définit π comme le double du plus petit réel $\alpha > 0$ tq $\mathrm{Re}(g(\alpha)) = 0$.

Rmq 6 : $\mathrm{Ker}\, g = 2\pi\mathbb{Z} = \{2k\pi, k \in \mathbb{Z}\}$.

App 7 : Soit la suite de terme général $z_n = \prod_{k=1}^{n} (1 + \frac{i}{k})$ l'ensemble des v.a. de $(z_n)_n$ est $\mathbb{U}$ tout entier.

Def 8 : On définit $\cos : x \mapsto \mathrm{Re}(g(x))$ et $\sin : x \mapsto \mathrm{Im}(g(x))$.

Rmq 9 : On a donc $e^{ix} = \cos x + i \sin x$.

Prop 10 : (Formules de Moivre) $\forall x \in \mathbb{R}, \forall n \in \mathbb{Z}$, $e^{inx} = \cos(nx) + i\sin(nx)$

App 11 : linéarisation de $\cos^n x$ et $\sin^n x$.

Prop 12 : (Formules d'Euler) $\cos x = \frac{e^{ix} + e^{-ix}}{2}$; $\sin x = \frac{e^{ix} - e^{-ix}}{2i}$.

App 13 : Calcul du noyau de Dirichlet
$\forall (N,x) \in \mathbb{N} \times \mathbb{R} \setminus 2\pi\mathbb{Z}$, $D_N(x) = \sum_{n=-N}^{N} e^{inx} = \frac{\sin[(N+\frac{1}{2})x]}{\sin(\frac{x}{2})}$

II. Nombres complexes de module 1 et géométrie.

1) Propriétés topologiques et géométriques

Def 14 : Le groupe orthogonal de $\mathbb{R}^n$, noté $O(n)$ est l'ensemble $\{A \in \mathcal{M}_n(\mathbb{R}) \mid {}^tAA = I_n\}$.

Rmq 15 : Dans la suite, on se restreint à la dimension 2.

Rmq 16 : Soit $A \in O(2)$, $\det A = \pm 1$.

Def 17 : On définit $SO(2) = \{A \in O(2) \mid \det A = 1\}$

Prop 18 : Le groupe $SO(2)$ est isomorphe au groupe $\mathbb{U}$.

Prop 19 : $\mathbb{U}$ est compact.

Prop 20 : $\mathbb{U}$ est connexe par arcs.

Def 21 : Grâce à l'exponentielle complexe, on définit

$$\begin{array}{ccccc} \mathbb{R} & \longrightarrow & \mathbb{U} & \longrightarrow & SO(2) \\ \theta & \longmapsto & e^{i\theta} & \longmapsto & \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{array}$$

Cette application est surjective, périodique de période 2π et définit un isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} SO(2)$

L'image du réel θ par cette application s'appelle rotation d'angle θ.

Prop 22 : Étant donnés deux vecteurs unitaires d'un plan vectoriel, il existe une unique rotation qui envoie l'un sur l'autre.

2) Homographies du plan complexe.

Def 23 : Une homographie du plan complexe est une application $h : z \mapsto \frac{az+b}{cz+d}$ où $a,b,c,d \in \mathbb{C}$ et $ad - bc \neq 0$.
$\mathcal{D}_h = \{z \in \mathbb{C} \mid cz + d \neq 0\}$.

Rmq 24 : On s'intéresse à $\overline{\mathbb{C}} = \mathbb{C} \cup \{+\infty\}$. Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_n(\mathbb{C})$, on lui associe l'application

$$h : z \mapsto h(z) = \begin{cases} \frac{az+b}{cz+d} & \text{si } z \in \mathbb{C} \setminus \{-\frac{d}{c}\} \\ \infty & \text{si } z = -\frac{d}{c} \text{ et } c \neq 0 \\ \infty & \text{si } z = \infty \text{ et } c = 0 \\ a/c & \text{sinon} \end{cases}$$

Prop 25 : Soient h et h' deux homographies associées à M et M' dans $GL_n(\mathbb{C})$ alors $h \circ h'$ est associée à MM'.

Prop 26 : Soient h et h' deux homographies qui coïncident en au moins 3 points de $\overline{\mathbb{C}}$, associées respectivement à M et M', alors $h = h'$ et $\exists \lambda \in \mathbb{C}^*$ tel que $M = \lambda M'$.

Prop 27 : Soit $PO(\mathbb{U})$ l'ensemble des homographies qui stabilisent $\mathbb{U}$, ie. $h \in PO(\mathbb{U}) \Leftrightarrow h(\mathbb{U}) \subset \mathbb{U}$.
Alors $h \in PO(\mathbb{U})$ ssi h est de la forme $z \mapsto \frac{\alpha z + \beta}{\bar{\beta} z + \bar{\alpha}}$, $|\alpha| \neq |\beta|$

Def 28: Soit $\mathcal{C}$ un cercle du plan euclidien. Une involution $I_a : \mathcal{C} \to \mathcal{C}$, $m \mapsto m'$, $a \notin \mathcal{C}$ telle que (am) recoupe $\mathcal{C}$ en m' est une involution de Frégier de centre a. (avec $m'=m$ si (am) tangente à $\mathcal{C}$)

Prop 29: Si $\mathcal{C}=\mathbb{U}$, $\{I_a, a \notin \mathcal{C}\} \subset PO(\mathbb{U})$.

Prop 30: "Presque" tous les éléments non-involutifs de $PO(\mathbb{U})$ sont de la forme $I_v \circ I_u$, $u,v \in \mathbb{C}\setminus\mathbb{U}$.

Thm 31: (théorème de Pascal) Si a,b,c,a',b' et c' sont 6 points distincts du cercle $\mathbb{U}$, si les droites (ab') et $(a'b)$, (ac') et $(a'c)$, (bc') et $(b'c)$ se coupent respectivement en p,q et r alors les points p,q et r sont alignés. [cf Annexe].

III. Sous-groupe des racines de l'unité

1) Racines de l'unité

Def 32: On note $\mathbb{U}_n=\{z\in\mathbb{U} \mid z^n=1\}$ l'ensemble des racines n-ième de l'unité.

Ex 33: $\mathbb{U}_2=\{-1,1\}$; $\mathbb{U}_3=\{1,j,j^2\}$.

Prop 34: $\mathbb{U}_n$ est un sous-grp cyclique de $\mathbb{U}$ de cardinal n, et on a $\mathbb{U}_n=\{e^{\frac{2ik\pi}{n}} \mid k\in[\![0,n-1]\!]\}$ $\forall n\in\mathbb{N}^*$.

Prop 35: Les sous-groupes de $\mathbb{U}$ sont :
- soit finis donc sous-grp des racines de l'unité $\mathbb{U}_n$
- soit denses dans $\mathbb{U}$.

App 36: $\mathbb{U}_n$ est l'ensemble des sommets du polygône régulier à n côtés.

Def 37: $z\in\mathbb{U}_n$ est appelée racine primitive n-ième de l'unité si c'est un générateur de $\mathbb{U}_n$. Notons μ_n cet ensemble, on a
$\mu_n=\{e^{\frac{2ik\pi}{n}} \mid k\in[\![0,n-1]\!] \text{ et } k\wedge n=1\}$.

Def 38: On définit l'indicatrice d'Euler $\varphi : \mathbb{N}^* \to \mathbb{N}$, $n \mapsto \#\{k<n \mid k\wedge n=1\}$

Prop 39: Le cardinal de μ_n est $\varphi(n)$.

2) Polynômes cyclotomiques

Def 40: Soit $n\in\mathbb{N}^*$. On définit le polynôme cyclotomique
$$\Phi_n(X)=\prod_{\omega\in\mu_n}(X-\omega).$$

Thm 41: (Propriétés sur les polynômes cyclotomiques)
1. $X^n-1=\prod_{d\mid n}\Phi_d(X)$
2. $\Phi_n\in\mathbb{Z}[X]$, $\deg(\Phi_n)=\varphi(n)$ et Φ_n est unitaire.
3. Si p est premier, $\Phi_p(X)=\sum_{k=0}^{p-1}X^k$.

App 42: (thm de Dirichlet faible) $\forall n\geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo n. DVP 1

Prop 43: $\forall n\in\mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Q}[X]$.

Rmq 44: $\forall n\in\mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Z}[X]$.

Thm 45: (thm de Wedderburn) Tout corps fini est commutatif.

IV. Applications.

1) Aux matrices

Def 46: Pour tout $n\in\mathbb{N}^*$, on note S_n le groupe des permutations de $\{1,\dots,n\}$ muni de la loi de composition.

Rmq 47: $\mathrm{Card}(S_n)=n!$

Def 48: A toute permutation $\sigma\in S_n$, on associe la matrice de passage P_σ dans la base canonique $\mathcal{B}=(e_j)_{1\leq j\leq n}$ de $\mathbb{K}^n$ à la base $\mathcal{B}_\sigma=(e_{\sigma(j)})_{1\leq j\leq n}$. P_σ est la matrice de permutation associée à σ : $P_\sigma=(\delta_{\sigma(i)j})_{1\leq i,j\leq n}$

Rmq 49: $P_\sigma e_j=e_{\sigma(j)}$ $\forall 1\leq j\leq n$.

Thm 50: L'application $P : S_n \to GL_n(\mathbb{C})$, $\sigma \mapsto P_\sigma$ est un morphisme de grp injectif et, pour toute permutation $\sigma\in S_n$, $\det(P_\sigma)=\varepsilon(\sigma)$

Prop 51: P_σ est une matrice orthogonale.

Prop 52: Soit P_σ la matrice de permutation associée à un k-cycle, alors $P_\sigma^k=I_n$ et les vp de P_σ sont dans $\mathbb{U}_k$.

<u>Généralisation</u> : Soit $A \in \mathcal{M}_n(\mathbb{C})$, si $\exists k \in \mathbb{N}^*$, $A^k = I_n$ alors les vp de A sont les racines k-ième de l'unité et A est diagonalisable.

<u>Def 53</u> : Soit $n \in \mathbb{N}^*$, $a_1, \dots, a_n \in \mathbb{C}$. On définit

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & & \ddots & \vdots \\ a_2 & \cdots & & a_1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$$

la matrice circulante associée à $(a_1, \dots, a_n)$.

<u>Prop 54</u> : Soit $P \in \mathbb{C}[X]$ tel que $P(X) = a_1 + \dots + a_n X^{n-1}$ alors, $\det(A) = \prod_{k=0}^{n-1} P(\omega^k)$ avec $\omega = e^{\frac{2ik\pi}{n}}$.

2) <u>Aux polynômes.</u>

<u>Def 55</u> : On note $\mathcal{P}$ l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$ dont les racines sont de module inférieur ou égal à 1.

DVP 2

<u>Thm 56</u> : (Kronecker) Soit $P \in \mathcal{P}$, si z est une racine de P. Soit z est nul, soit z est une racine de l'unité.

<u>Cor 57</u> : Soit $P \in \mathcal{P}$ non constant et irréductible. Alors $P = X$ ou P est un polynôme cyclotomique.

<u>Def 58</u> : Soit $P \in \mathbb{C}[X]$ non constant. L'enveloppe convexe des racines de P est l'intersection de tous les convexes contenant les racines de P.

DVP 3

<u>Thm 59</u> : (thm de Gauss-Lucas). Soit $P \in \mathbb{C}[X]$ non constant. Alors les racines de P' sont dans l'enveloppe convexe de P.

<u>App. 60</u> : Déterminer le plus grand entier $n \geq 2$ tel que les racines non nulles de $(X+1)^n - X^n - 1$ soient de module 1.

3) <u>A la théorie des caractères.</u>

<u>Def 61</u> : Une représentation linéaire de G dans V est un morphisme de groupe $\rho : G \to GL(V)$. On dit que V est une représentation de G.

<u>Def 62</u> : Le degré de la représentation est la dimension de V.

<u>Ex 63</u> : Si ρ est constante égale à Id_V, la rep. est triviale.

<u>Def 64</u> : Si ρ est une représentation de G, son caractère est l'application $\chi_\rho : G \to \mathbb{K}$ définie par, $\forall g \in G$, $\chi_\rho(g) = tr(\rho(g))$.

<u>Ex 65</u> : $\chi_{\rho_{triv}} : g \mapsto 1 \quad \forall g \in G$.

<u>Thm 66</u> : Si $\mathbb{K} = \mathbb{C}$, ρ une représentation de G de caractère $\chi : G \to \mathbb{C}$. Si $g \in G$ est d'ordre r, $\chi(g)$ est alors somme de n racines r-ième de l'unité, avec $n = \dim V$.

<u>Def 67</u> : On dit qu'une rep. V de G est irréductible si les seuls sous-espaces G-invariants de V sont $\{0\}$ et V. Son caractère est irréductible.

<u>Thm 68</u> : Le groupe G est abélien ssi toutes ses représentations irred. sont de degré 1.

<u>Def 69</u> : Si A est un GAF, son dual $\hat{A}$ est l'ensemble des caract. irred. de A.

<u>App. 70</u> : Table de caractères de $\mathbb{Z}/n\mathbb{Z}$. [cf Annexe]

<u>Thm 71</u> : Si $A = \mathbb{Z}/n\mathbb{Z}$, $\hat{A} \simeq \mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

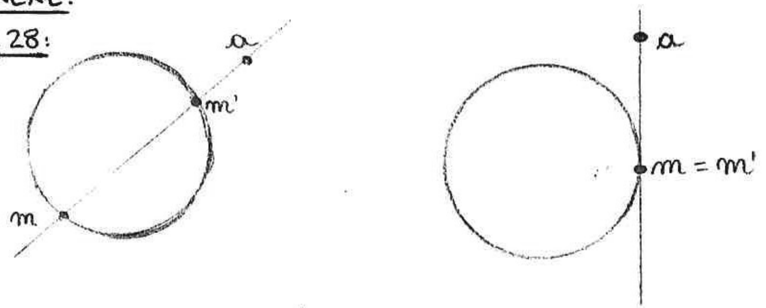
<u>Rmq 72</u> : Si on exclut la 1ère ligne de la table de caract. de $\mathbb{Z}/n\mathbb{Z}$, la matrice est de Vandermonde.

<u>Thm 73</u> : (thm de relèvement des caractères) Soit A un GAF et B un sous-grp de A. Alors le morphisme de restriction de $\hat{A}$ sur $\hat{B}$ est surjectif.

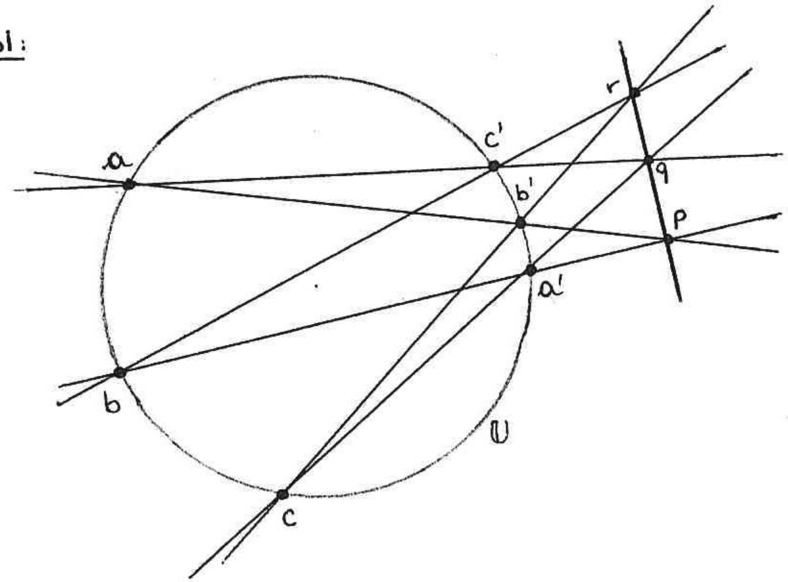
<u>Thm 74</u> : (thm de structure des GAF) Soit A un GAF, $\exists!$ famille d'entiers $a_i \geq 2$, $i \in [\![1, s]\!]$ tq $a_{i+1} | a_i$ $\forall i \in [\![1, s-1]\!]$ et $A \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_s\mathbb{Z}$.

ANNEXE.

Def 28:



Thm 31:



App. 70: Table de caractère de $\mathbb{Z}/n\mathbb{Z}$.

	$\bar{0}$	$\bar{1}$		$\overline{n-1}$
χ_0	1	1	...	1
χ_1	1	ω	...	ω^{n-1}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_{n-1}	1	ω^{n-1}	...	$\omega^{(n-1)^2}$

avec $\omega = e^{\frac{2i\pi}{n}}$

$\chi_k(\bar{a}) = \omega^{ka}$ $\quad 0 \leq k \leq n-1$, $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$.

REFERENCES.

- Cours de mathématiques - Algèbre 1, Arnaudiès - Fraysse (Parties I & III.1))
- Géométrie, Audin (Partie II.1)).
- Géométrie analytique classique, Eiden (Partie II.2))
- Mathématiques pour l'agrégation - Algèbre & Géométrie, Rombaldi (Parties III.2) et IV.1))
- Algèbre, Gourdon (Partie IV.1))
- CVA, Caldero (Partie IV.2))
- Oraux X-ENS - Algèbre 1, FGN (Partie IV.2))
- NH2G2, II, Caldero (Partie IV.3)).