Groupes des nombres complexes de module 1 / Sous-groupes des racines de l'unité / Applications

I - Nombres complexes de module 1

1) Le groupe $\mathbb{U}$

[ARN]

Prop / def 1 : $z \mapsto |z|$ est un morphisme de groupes de $\mathbb{C}^*$ dans $\mathbb{R}_+^*$. Son noyau, noté $\mathbb{U}$, est le sous-groupe de $\mathbb{C}^*$ constitué des $z \in \mathbb{C}^*$ tels que $|z| = 1$.

Pom 13 analyse

def 2 : on définit la fonction exponentielle complexe par
$$\forall z \in \mathbb{C}, \quad \exp z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

thm 3 : i) exp est surjective sur $\mathbb{C}^*$ et c'est un morphisme de $(\mathbb{C}, +)$ sur $(\mathbb{C}^*, \times)$.
ii) $\mathbb{R} \to \mathbb{C}$, $x \mapsto \exp(ix)$ est 2π-périodique, surjective et à valeurs dans $\mathbb{U}$. En particulier on a l'isomorphisme
$$\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$$

ARN

def 4 : Les fonctions $\mathbb{R} \to \mathbb{R}$, $x \mapsto \mathrm{Re}(\exp ix)$ et $x \mapsto \mathrm{Im}(\exp ix)$ sont appelées fonctions cosinus et sinus.
$$\cos x = \frac{e^{ix} + e^{-ix}}{2}, \qquad \sin x = \frac{e^{ix} - e^{-ix}}{2i}$$

Prop 5 (Moivre) $\forall n \in \mathbb{N}$, $(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)$

appl 6 : calcul du noyau de Dirichlet
$$\sum_{k=-n}^{n} e^{ikx} = \frac{\sin\left(\frac{2n+1}{2} x\right)}{\sin\left(\frac{x}{2}\right)} \quad \forall x \in \mathbb{R} \setminus 2\pi\mathbb{Z}$$

2) Considérations géométriques

Prop 7 : $\mathbb{U}$ est le cercle unité du plan complexe et admet le paramétrage rationnel suivant :
$$(\cos x, \sin x) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \quad t = \tan\frac{x}{2} \quad x \neq \pi \ [2\pi]$$

appl 8 : les solutions de l'équation diophantienne dans $\mathbb{N}^3$
$x^2 + y^2 = z^2$ sont les triplet $(x, y, z) \in \mathbb{N}^3$ tels que (x, y, z) ou (y, x, z) soit égal à $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$ où $\gcd(u, v) = 1$ et $d \in \mathbb{N}$.

Gr fini

Ba ab

def 9 : On définit le groupe diédral D_n comme le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Prop 10 : Le groupe des isométries conservant le polygone régulier à n côtés est isomorphe au groupe diédral : on a
$$\mathrm{Isp}_n \simeq \mathrm{Isp}_n^+ \rtimes \langle s \rangle = D_n$$
où s est une symétrie orthogonale et Isp_n^+ le groupe des isométries directes qui préservent P_n (ici constitué des n rotations de centre O et de rayon $k\frac{2\pi}{n}$ où O est le centre de P_n).

Rem : O est l'isobarycentre des sommets de P_n (Cela découle de la propriété de Moivre : $\sum_{k=0}^{n-1} e^{ik\frac{2\pi}{n}} = 0$).

II Sous groupe des racines nièmes de l'unité

1) Le groupe μ_n

Prop/def 11 : $\mathbb{U} \to \mathbb{U}$, $z \mapsto z^n$ est un morphisme de groupe. Son noyau, noté μ_n, est un sous-groupe de $\mathbb{U}$ appelé groupe des racines nièmes de l'unité. De plus μ_n est de cardinal n et cyclique.

def 12 : on appelle racine nième primitive de l'unité tout générateur de l'unité c'est à dire les éléments

$$\exp\left(\frac{2ik\pi}{n}\right), \quad k \in [\![0, n-1]\!], \ \gcd(k,n) = 1$$

on note μ_n' leur ensemble.

applications B : i) Les sous groupes finis de $SO_2(\mathbb{R})$ sont de la forme $\{r_{\frac{2k\pi}{n}}, k = 1..n\}$ pour $n \in \mathbb{N}^*$ où $r_{\frac{2k\pi}{n}}$ désigne la rotation vectorielle d'angle $\frac{2k\pi}{n}$.

ii) thm (Kronecker) Soit $P \in \mathbb{Z}[X]$ unitaire et dont les racines sont de module ≤ 1. Alors les racines de P sont des racines de l'unité.

2) Polynômes cyclotomiques

def 14 : on définit le $n$ième polynôme cyclotomique par

$$\Phi_n(X) = \prod_{\zeta \in \mu_n'} (X - \zeta)$$

Thm 15 : i) les polynômes cyclotomiques sont unitaires à coefficients dans $\mathbb{Z}$

ii) $\deg \Phi_n = \varphi(n)$ où φ désigne l'indicatrice d'Euler

iii) Φ_n est irréductible dans $\mathbb{Z}[X]$

Prop 16 : $\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$ où μ désigne la fonction de Möbius

Applications (suite) i) Un polynôme unitaire irréductible dont une racine de module ≤ 1 est soit égal à X soit égal à un polynôme cyclotomique.

ii) thm (Wedderburn) : Tout corps fini est commutatif

iii) Constructibilité à la règle et au compas :

Rappel : le théorème de Wantzel donne une condition nécessaire de constructibilité à savoir que si $x \in \mathbb{R}$ est constructible alors x est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}[x] : \mathbb{Q}]$ est une puissance de 2.

- On ne peut pas construire à la règle et au compas un heptagone régulier
- On ne peut pas construire à la règle et au compas un polygone régulier à p^2 côtés (où p est un nombre premier impair).
- Un pentagone régulier est constructible à la règle et au compas.
- thm (Gauss, 1796) Le polygone à n côtés est constructible à la règle et au compas si et seulement si n est de la forme

$$n = 2^r p_1 \cdots p_s$$

[ADMIS]

où $(r,s) \in \mathbb{N}^2$ et $p_1, \ldots, p_s$ des nombres premiers distincts de la forme $1 + 2^{2^i}$.

III Représentation des groupes finis [GOU] [PEY]

On considère un groupe fini G d'ordre n et $\rho : G \to GL(V)$ une représentation de G où V est un $\mathbb{C}$-e.v de dimension finie.

Prop 18 : $\forall g \in G$, $\rho_V(g)$ est diagonalisable et son spectre est inclus dans μ_n.

Thm 19 : Si G est abélien, les représentations irréductibles de G sont les caractères linéaires, à savoir les applications $G \to \mathbb{C}^*$ et celles-ci sont à valeur dans μ_n.

Appl 20 : <u>table des caractères d'un groupe cyclique</u> : soit $G = \langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$

	1	g	g^2	...	g^{n-1}
χ_1	1	1	1	...	1
χ_2	1	ω_n	ω_n^2	...	ω_n^{n-1}
⋮	⋮	⋮	⋮		⋮
χ_n	1	ω_n^{n-1}	$\omega_n^{2(n-1)}$	...	$\omega_n^{(n-1)(n-1)}$

où on a noté $\omega_n = e^{\frac{2i\pi}{n}} \in \mu_n$.

Exemples 21 : i) A_4 admet 3 caractères linéaires distincts : $\hat{A}_4$ est de cardinal 3 donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$. On note η un générateur

	id	$H \setminus \{id\}$	$t H$	$t^2 H$
1	1	1	1	1
η	1	1	ω_3	ω_3^2
η^2	1	1	ω_3^2	ω_3

où $H = \{id, (12)(34), (13)(24), (14)(23)\}$ et $t = (123)$.

ii) soit $n \in \mathbb{N}$ pair. On admet $\frac{n}{2}+1$ représentations irréductibles de degré deux définies par les relations

$$k \in [\![1, \tfrac{n}{2}-1]\!], \quad \rho_k(r^k) = \begin{pmatrix} \omega_n^{kk} & 0 \\ 0 & \omega_n^{-kk} \end{pmatrix} \qquad \rho_k(sr^k) = \begin{pmatrix} 0 & \omega_n^{-kk} \\ \omega_n^{kk} & 0 \end{pmatrix}$$

où r est la rotation d'angle $\frac{2\pi}{n}$ et s une des symétries. On peut calculer leur caractère :

	r^k	sr^k
χ_k	$2\cos\left(\frac{2\pi kk}{n}\right)$	0

$k \in [\![0, n-1]\!]$.

ARN - Armand'is Frayssé - Algèbre tome 1

Pea alg - Aviva Szpirglas - Algèbre L3

Perrin - bé le Perrin !

FGN alg 1 - Francinou Gianella Nicolas X ORAUX ENS algèbre 1.

Escoffier - " Théorie de Galois " (2e édition).

Combes - " Algèbre géométrie "

[COL] Colmez

[PEY] Peyré " algèbre discrète de la transformée de Fourier ".

0.1 Théorème de Kronecker

Théorème : (Kronecker) Soit P un polynôme qui vérifie la propriété $\mathscr{K}_n$ suivante :

- $P \in \mathbb{Z}[X]$ et est de degré n.

- $P = X^n + a_1 X^{n-1} + \cdots + a_n$ avec $a_n \neq 0$.

- Les racines de P dans $\mathbb{C}$ sont de module inférieur ou égal à 1.

Alors les racines de P sont des racines de l'unité.

Démonstration. Notons α_i, $1 \leq i \leq n$ les racines de P. **Les relations entre les coefficients a_i et les racines α_i donnent une majoration des coefficients de P.** En effet, comme $\forall i \in \{1, \cdots, n\}, |\alpha_i| \leq 1$ on trouve

$$|a_k| = |\sigma_k(\alpha_1, \cdots, \alpha_n)| \leq \binom{n}{k}.$$

(noter qu'on a changé l'indexation naturelle des coefficients donc on n'a pas $|a_k| = |a_n \sigma_{n-k}|$)

Soit $R(X) = X^n + b_1 X^{n-1} + \cdots + b_n$ un polynôme vérifiant $\mathscr{K}_n$. On a donc pour tout $1 \leq k \leq n$, $|b_k| \leq \binom{n}{k}$. Par suite, b_k prend une des $1 + 2\binom{n}{k}$ valeurs

$$-\binom{n}{k}, \cdots, -1, 0, 1, \cdots, \binom{n}{k}$$

et l'ensemble Ω_n des polynômes vérifiant la propriété $\mathscr{K}_n$ est fini car de cardinal majoré par $\prod_{k=1}^{n}(1 + 2\binom{n}{k})$. Considérons les polynômes :

$$P_k(X) = \prod_{i=1}^{n}(X - \alpha_i^k) \in \mathbb{C}[X] \quad et \quad Q_k^Y(X) = X^k - Y \in \mathbb{Z}[X, Y].$$

pour $k \in \mathbb{N}^*$. On considère le résultant $R_k(Y)$ en la variable X des polynômes $P_1 = P$

et $Q_k^Y(X)$:

$$R_k(Y) = \begin{vmatrix} 1 & & & 1 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & & 1 & 0 & & 1 \\ a_n & & a_1 & -Y & & 0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_n & & & -Y \end{vmatrix}.$$

L'écriture de ce déterminant montre que R_k est un polynôme (en la variable Y) à coefficients entiers. Par ailleurs, les racines de P_1 sont $\alpha_1, \cdots, \alpha_n$ donc par le lien résultant-racines on a

$$R_k(Y) = \prod_{i=1}^{n} Q_k^Y(\alpha_i) = \prod_{i=1}^{n} (\alpha_i^k - Y) = (-1)^n P_k(Y).$$

Ainsi, les polynômes P_k sont unitaires à coefficients entiers donc vérifient la propriété $\mathscr{K}_n$ puisque $0 < |\alpha_i^k| \leq |\alpha_i| \leq 1$. Comme l'ensemble Ω_n est fini, l'ensemble Z_n des racines des polynômes dans Ω_n est lui aussi fini. Soit α_i une racine de P. Par ce qui précède, on a une application

$$\varphi : \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & Z_n \\ k & \longmapsto & \alpha_i^k \end{array}$$

qui est non injective par le principe des tiroirs : il existe deux entiers $1 \leq r < s$ tels que $\alpha_i^r = \alpha_i^s$ de sorte que $\alpha_i^{s-r} = 1$. Par suite les racines de P sont des racines de l'unité. □

Corollaire : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. Si P est **irréductible** et que ses racines dans $\mathbb{C}$ sont de module ≤ 1 alors soit $P = X$ soit P est un polynôme cyclotomique.

Démonstration. Supposons $P \neq X$. 0 n'est donc pas racine de P car celui-ci est irréductible. Ainsi, par le théorème de Kronecker les racines de P sont des racines de l'unité : $\exists N \in \mathbb{N}^*$ tel que $P | X^N - 1$. Or la DFI de $X^N - 1$ dans $\mathbb{Z}[X]$ est

$$\prod_{d|N} \Phi_d(X).$$

par irréductibilité des polynômes cyclotomiques sur $\mathbb{Z}$. Donc $P = \Phi_d(X)$ pour $d|N$. □

Leçon : 143, 144, 152.

Référence : Szpirglas.

0.2 Irréductibilité sur $\mathbb{Z}$ des polynômes cyclotomiques $\Phi_{n,\mathbb{Q}}$

Définitions : On note U_n l'ensemble des racines n-ièmes de l'unité et

$$U_n' = \left\{ exp(\frac{2ik\pi}{n}) \middle| 0 \leq k < n, \quad pgcd(k,n) = 1 \right\}$$

l'ensemble des racines n-ièmes primitives. Le n-ième polynôme cyclotomique est le polynôme défini par

$$\boxed{\Phi_n(X) = \prod_{\zeta \in U_n'} (X - \zeta)}.$$

Théorème : 1) Les polynômes cyclotomiques sont des polynômes **unitaires** à **coefficients entiers**. De plus, on a

$$deg(\Phi_n) = \varphi(n) \quad et \quad X^n - 1 = \prod_{d|n} \Phi_d(X).$$

2) Pour tout entier n, le polynôme cyclotomique Φ_n est **irréductible** dans $\mathbb{Z}[X]$.

Démonstration. 1) Le degré de Φ_n est donné par $deg(\Phi_n) = card(U_n') = \varphi(n)$. De plus, on a

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n \\ \zeta d'ordre\ d}} (X - \zeta) = \prod_{d|n} \underbrace{\prod_{\zeta \in \mu_d} (X - \zeta)}_{= \Phi_d(X)}.$$

Montrons par récurrence sur n que Φ_n est unitaire à coefficients entiers.
Initialisation : On a $\Phi_1(X) = X - 1$ qui vérifie bien ces propriétés.
Hérédité : Supposons démontré le fait que pour tout $m < n$, les Φ_m sont des polynômes unitaires à coefficients entiers. Le polynôme Φ_n est donné par la division euclidienne suivante, dans laquelle, par hypothèse de récurrence, le diviseur est unitaire à coefficients entiers et le reste est nul :

$$X^n - 1 = \left(\prod_{d|n, d<n} \Phi_d(X) \right) \times \Phi_n(X)$$

ce qui permet de conclure car d'une manière générale si $A(X)$ et $B(X)$ sont à coefficients entiers, et si de plus $B(X)$ est unitaire, alors le quotient et le reste de la

division euclidienne de $A(X)$ par $B(X)$ dans $\mathbb{C}[X]$ sont dans $\mathbb{Z}[X]$ (on fait la d.e dans $\mathbb{Z}$ puis on dit qu'elle coïncide avec celle dans $\mathbb{C}$ par unicité).

2) Soit ζ une racine primitive n-ième de l'unité. On considère

$$I(\zeta) = \left\{ g \in \mathbb{Q}[X] \middle| g(\zeta) = 0 \right\}.$$

qui est un idéal de $\mathbb{Q}[X]$, c'est donc un idéal principal. On note f le générateur de cet idéal dont on montre aisément qu'il est irréductible.

Le polynôme $f(X)$ divise $X^n - 1$ (dans $\mathbb{Q}[X]$) puisque $X^n - 1 \in I(\zeta)$. De plus, $f(X)$ est unitaire à coefficients entiers. En effet, les facteurs irréductibles de $X^n - 1$ sont à coefficients entiers par le théorème de Gauss : en effet $\mathbb{Z}$ est factoriel (thm fondamental de l'arithmétique) donc $\mathbb{Z}[X]$ l'est par le théorème de Gauss. Par suite, $X^n - 1$ admet une écriture de la forme $a \times P_1 \cdots P_r$ avec $a \in \mathbb{Z}$ et les $P_i \in \mathbb{Z}[X]$ irréductibles sur $\mathbb{Z}$ et unitaires. En particuliers ils sont primitifs donc irréductibles sur $\mathbb{Q}$ par le théorème de Gauss. Enfin, $a = 1$ car $X^n - 1$ est unitaire et cette DFI dans $\mathbb{Z}[X]$ est donc la DFI de $X^n - 1$ dans $\mathbb{Q}[X]$ par unicité de sorte que $f(X) \in \mathbb{Z}[X]$. Il existe donc un polynôme h tel que $X^n - 1 = f(X)h(X)$ et h est unitaire à coefficients entiers puisqu'il est obtenu comme dans 1) par une division euclidienne dans $\mathbb{Z}[X]$.

Démontrons par l'absurde que si p est un nombre premier qui ne divise pas n, alors ζ^p est aussi une racine de f. On sait que ζ^p est racine de $X^n - 1$. Si ζ^p n'est pas une racine de f, c'est une racine de h donc ζ est une racine de $h(X^p)$. Par suite, $f(X) \Big| h(X^p)$: il existe $g \in \mathbb{Q}[X]$ tel que $h(X^p) = f(X)g(X)$. On a $g \in \mathbb{Z}[X]$ (tjs le même argument). En réduisant modulo p on obtient

$$\overline{h}(X^p) \underset{Frob}{=} \overline{h}(X)^p = \overline{f}(X)\overline{g}(X)$$

Il s'ensuit que $\overline{f}(X)$ et $\overline{h}(X)$ ont un facteur en commun noté $l(X)$ dans $\mathbb{F}_p[X]$ et que $X^n - \overline{1} = \overline{f}(X)\overline{h}(X)$ est divisible par $l(X)^2$: $X^n - \overline{1} = l(X)^2 k(X)$. Vu que p est un nombre premier ne divisant pas n, le polynôme dérivé nX^{n-1} est non nul et est divisible par $l(X)$:

$$nX^{n-1} = l(X)^2 k'(X) + 2l'(X)l(X)k(X).$$

On voit donc que $l(X)$ devrait être une puissance de X ce qui est absurde car 0 n'est pas racine de $l(X)$.

Nous avons donc démontré que si p est un nombre premier ne divisant pas n, alors ζ^p est aussi une racine de f. Mais toutes les racines primitives n-ièmes sont obtenues à partir de ζ en élevant à des puissances p-ièmes, pour des nombres premiers p ne divisant pas n (en effet, ζ^q est une racine primitive n-ième de l'unité s.s.i $pgcd(q,n) = 1$ et si on écrit q sous la forme $q = p_1 \cdots p_r$ la condition équivaut à la condition : pour tout $1 \leq j \leq r$, p_j et n sont premiers entre eux). Par suite, $f(X)$ et $\Phi_n(X)$ sont unitaires et ont les mêmes zéros. De plus, par construction, $\Phi_n(X)$ n'a que des racines simples et $f(X)$ divise $\Phi_n(X)$ donc $f = \Phi_n$. On a vu que f était irréductible donc il en est de même pour Φ_n.

□

Leçon : 120, 141.

Référence : [Szpirglas] Pearson algèbre L3 p 599-601 .