

I. De l'exponentielle complexe au groupe $\mathbb{U}$

I. A. Autour de l'exponentielle

[Rud98, Prologue, p1-4] [AF93, §VI.7, p226]

DÉFINITION 1. [EXPONENTIELLE, COSINUS ET SINUS]

On définit les séries entières suivantes :

$$\exp(z) = e^z = \sum_{n \in \mathbb{N}} \frac{z^n}{n!} \quad \cos(z) = \sum_{n \in \mathbb{N}} \frac{(-1)^n z^{2n}}{(2n)!} \quad \sin(z) = \sum_{n \in \mathbb{N}} \frac{(-1)^n z^{2n+1}}{(2n+1)!}$$

PROPOSITION 2.

- (i) $\exp, \sin, \cos$ sont des séries entières de rayon de convergence infini et sont donc définies et holomorphes sur $\mathbb{C}$. De plus $\exp$ est sa propre dérivée,
- (ii) Pour tout $z \in \mathbb{C}$, on a $\exp(iz) = \cos(z) + i \sin(z)$,
- (iii) Pour $\theta \in \mathbb{R}$, $\cos(\theta)$ et $\sin(\theta)$ sont réels et $|e^{i\theta}| = 1$.
- (iv) $\exp$ est un morphisme surjectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$ de noyau $i a \mathbb{Z}$ pour un $a \in \mathbb{R}_+$.
- (v) Pour $z_1, z_2 \in \mathbb{C}$, $\exp(z_1 + z_2) = \exp(z_1) \exp(z_2)$,

REMARQUE 3. On note alors $\mathcal{E} : \mathbb{R} \rightarrow \mathbb{C}^*, t \mapsto e^{it}$ et $\pi = a/2$ (ainsi $e^{i\pi} + 1 = 0$). Cette application associe à un angle t l'unique point u de module 1 dont l'angle entre $[Ox)$ et $[Ou)$ est t . On le précisera dans la partie II. A. .

COROLLAIRE 4. [FORMULE DE MOIVRE ET D'EULER]

- Pour $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$, on a $(\cos(\theta) + i \sin(\theta))^n = \cos(n\theta) + i \sin(n\theta)$.
- Pour $\theta \in \mathbb{R}$, on a $\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}$ et $\sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}$.

APPLICATION 5. Développement de $\cos(n\theta)$ et $\sin(n\theta)$ par la formule de MOIVRE. Linéarisation de $\cos^n(\theta)$ et $\sin^n(\theta)$ par les formules d'EULER. Exemples de $\cos^5(\theta)$ et $\sin^5(\theta)$.

APPLICATION 6. Polynôme de TCHEBYCHEV.

APPLICATION 7. Calcul des noyaux de DIRICHLET et FEJÉR :

$$D_N = \sum_{n=-N}^N e^{in \cdot} = \frac{\sin\left(\frac{2N+1}{2} \cdot\right)}{\sin(\cdot/2)} \quad \text{et} \quad K_N = \frac{1}{N} \sum_{n=0}^{N-1} D_n = \sum_{n=-N}^N \left(1 - \frac{|n|}{N}\right) e_n = \frac{\sin^2(N \cdot / 2)}{\sin^2(\cdot / 2)}$$

I. B. Le groupe des nombres complexes de module 1

[AF93, §VI.7/8, p226]

On notera $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ le groupe des racines de l'unité, $\mathbb{U}_{\mathbb{Q}} = \{e^{2ip\pi} \mid p \in \mathbb{Q}\}$. Pour $n \in \mathbb{N}^*$, on pose $\mathbb{U}_n = \{e^{2ik\pi/n} \mid k \in \mathbb{N}^*\}$ le sous-groupe des racines n -ièmes de l'unité.

EXEMPLE 8. $\mathbb{U}_1, \mathbb{U}_2, \mathbb{U}_3, \mathbb{U}_4$ et représentation sur le plan.

[VOIR ANNEXE]

PROPOSITION 9.

- Pour $n \in \mathbb{N}^*$, $\mathbb{U}_n \subset \mathbb{U}_{\mathbb{Q}} \subset \mathbb{U}$ sont des sous-groupes de $(\mathbb{C}^*, \times)$ et $\mathbb{U}_n$ est fini d'ordre n .
- $\mathcal{E} : \mathbb{R} \rightarrow \mathbb{U}$ est un morphisme surjectif et induit un isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.
- $\mathbb{R}_+^* \times \mathbb{U} : \mathbb{C}^* \rightarrow \mathbb{C}^*, (r, u) \mapsto r\mathcal{E}(u)$ est un isomorphisme de groupes.

APPLICATION 10. Pour $n \geq 2$, on a $\sum_{\omega \in \mathbb{U}_n} \omega = 0$.

APPLICATION 11. Résolution de $z^n = z_0$ pour un $z_0 \in \mathbb{C}$.

PROPOSITION 12.

- (i) Tout sous-groupe de $\mathbb{U}$ est soit discret, soit dense dans $\mathbb{U}$. De plus les seuls sous-groupes discrets sont les $(\mathbb{U}_n)_{n \in \mathbb{N}}$.
- (ii) $\mathbb{U}_{\mathbb{Q}}$ est dense et $\mathcal{E}_{|\mathbb{Q}|}$ induit un isomorphisme $\mathbb{Q}/\mathbb{Z} \simeq \mathbb{U}_{\mathbb{Q}}$.
- (iii) Les sous-groupes compacts de $(\mathbb{C}^*, \times)$ sont $\mathbb{U}$ et les $(\mathbb{U}_n)_{n \in \mathbb{N}}$.
- (iv) Chaque $\mathbb{U}_n$ est cyclique et isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Les générateurs de $\mathbb{U}_n$ sont les racines n -ièmes primitives de l'unité : $\mathbb{U}_n^\times = \{e^{2ik\pi/n} \mid k \in \mathbb{Z} \text{ et } k \wedge n = 1\}$.
- (v) $\phi_n : \mathbb{U} \rightarrow \mathbb{U}, z \mapsto z^n$ est un morphisme de groupe continu pour $n \in \mathbb{Z}^*$, de noyau $\mathbb{U}_{|n|}$.

EXEMPLE 13. Racines primitives 2, 3, 4, 8-èmes de l'unité.

PROPOSITION 14. On note $\varphi(n)$ le cardinal de $\mathbb{U}_n^\times$.

- $\mathbb{U}_d \subset \mathbb{U}_n$ si et seulement si $d \mid n$,
- $\mathbb{U}_n = \cup_{d \mid n} \mathbb{U}_d^\times$,
- $n = \sum_{d \mid n} \varphi(d)$.

REMARQUE 15. $u \in \mathbb{U}_n$ est d'ordre n si et seulement si $u^d \neq 1$ pour tout $d < n$ tel que $d \mid n$.

II. Angles orientés et argument

II. A. Angles orientés et rotations du plan [Aud06, §III.1, p73] [Rom17, §4.6, p112]

Notion d'angles orientés, lien avec l'argument d'un nombre complexe

DÉFINITION 16. [ROTATION]

La rotation autour de 0 d'angle θ est l'application $r_\theta : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto z\mathcal{E}(\theta)$.

La rotation autour de $a \in \mathbb{C}$ d'angle θ est l'application $r_{\theta, a} : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto a + r_\theta(z - a)$.

PROPOSITION 17. Les rotations sont des isométries. En particulier $\mathbb{U}$ est stable par toute rotation autour de 0.

APPLICATION 18. [ROTATIONS PRÉSERVANT UN POLYGONE À n CÔTÉS]

Les rotations du plan préservant un polygone régulier à n côtés de centre O est un groupe constitué des n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in \llbracket 0, n-1 \rrbracket$. Autrement dit c'est $\{z \mapsto z\omega \mid \omega \in \mathbb{U}_n\}$.

REMARQUE 19. Si l'on rajoute les n symétries d'axe 2 sommets ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair, on obtient le groupe des isométries du plan préservant le polygone régulier à n côtés : c'est le groupe diédral D_{2n} .

II. B. Argument continu et logarithme continu sur les ouverts de $\mathbb{C}^*$ [Tau06, §5.3, p62]

DÉFINITION 20. Soit Ω un ouvert de $\mathbb{C}^*$.

- Un argument continu sur Ω est une application continue $\Theta : \Omega \rightarrow \mathbb{R}$ telle que pour tout $z \in \Omega$, $\frac{z}{|z|} = \mathcal{E} \circ \Theta(z)$.
- Un logarithme continu sur Ω est une application continue $\ell : \Omega \rightarrow \mathbb{C}$ telle que pour tout $z \in \Omega$, $z = \exp \circ \ell(z)$.

PROPOSITION 21. Soit $\Omega = \mathbb{C} \setminus \mathbb{R}_-$.

- Il existe un argument continu Θ sur Ω . Si on suppose de plus Θ à valeurs dans $] -\pi, \pi[$, on a alors unicité et on appelle Θ la détermination principale de l'argument,
- Il existe un logarithme continu sur Ω .

PROPOSITION 22. Soit Ω un ouvert connexe de $\mathbb{C}$ et $\ell : \Omega \rightarrow \mathbb{C}$. Alors on a équivalence :

- Il existe $C \in \mathbb{C}$ tel que $C + \ell$ est un logarithme continu sur Ω ,
- ℓ est une primitive de $z \mapsto 1/z$ sur Ω .

En particulier, tout logarithme continu sur Ω est holomorphe.

III. Polynômes cyclotomiques

III. A. Définitions et propriétés

[Per96, §3.4, p80]

Soit $n \in \mathbb{N}^*$.

DÉFINITION 23. [POLYNÔMES CYCLOTOMIQUES]

On définit le n -ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Exemples, ...

PROPOSITION 24.

- Φ_n est unitaire de degré $\varphi(n) = \text{card}(\{k \in [1, n] \mid k \wedge n = 1\})$.
- $X^n - 1 = \prod_{d \mid n} \Phi_d$. En particulier, si n est premier : $\Phi_n = X^n - 1$.

PROPOSITION 25. $\Phi_n \in \mathbb{Z}[X]$.

THÉORÈME 26. Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

COROLLAIRE 27. On a $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.

III. B. Applications

[Gou09, p89/93] [FGN07, p213]

THÉORÈME 28. [THÉORÈME DE WEDDERBURN]

Toute algèbre à division finie est un corps.

THÉORÈME 29. [THÉORÈME DE KRONECKER]

Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes les racines de P sont de module inférieur ou égal à 1 et $P(0) \neq 0$, alors toutes les racines de P sont des racines primitives de l'unité.

COROLLAIRE 30. [THÉORÈME DE KRONECKER]

Soit $P \in \mathbb{Z}[X]$ unitaire de degré n et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P = X$ ou $P = \Phi_n$.

IV. Autres applications

IV. A. Représentations linéaires complexes / caractères d'un groupe abélien fini ? [Rom17, Ch6, p179] [Ser98, Ch2, p23]

Soit G un groupe et E un $\mathbb{C}$ -espace vectoriel de dimension finie.

DÉFINITION 31. [REPRÉSENTATION]

Une représentation (linéaire) de G dans E est un morphisme de groupes $\rho : G \longrightarrow \mathrm{GL}(E)$.

REMARQUE 32. Se donner une représentation de G dans E revient à se donner une action de groupes de G sur E en posant $\rho(g)(x) = g.x$.

PROPOSITION 33. Lorsque $\dim(E) = 1$ et G est fini, $E \simeq \mathbb{C}$ et on a $\rho(g)|_{\mathbb{C}} : \mathbb{C} \longrightarrow \mathbb{C}$ pour tout $g \in G$.

EXEMPLE 34. [REPRÉSENTATION TRIVIALE] $\rho : g \longmapsto \mathrm{Id}_E$ est une représentation de G sur E .

EXEMPLE 35. Si E est de dimension 1 :

- les représentations de $\mathfrak{S}_n$ dans E sont $\rho : \sigma \longrightarrow \mathrm{Id}_E$ et $\rho : \sigma \longrightarrow \varepsilon(\sigma) \mathrm{Id}_E$.
- les représentations de $\mathbb{Z}/2\mathbb{Z}$ dans E sont $\rho : \bar{x} \longrightarrow \mathrm{Id}_E$ et ρ définie par $\rho(\bar{1}) = -\mathrm{Id}_E$.

EXEMPLE 36. [REPRÉSENTATIONS DE PERMUTATIONS]

$\mathfrak{S}_n \longrightarrow \mathrm{GL}_n(\mathbb{C}), \sigma \longmapsto P_\sigma$ est une représentation de $\mathfrak{S}_n$ sur $\mathbb{C}^n$.

Plus généralement, si G est fini de cardinal n et E est de dimension n , soit $(e_g)_{g \in G}$ une base de E . Alors l'application linéaire $\rho(g)$ définie par $\rho(g)(e_h) = e_{gh}$ pour $h \in G$ définit une représentation de G dans E .

Caractères : propriétés des caractères : somme de racines de l'unité, etc

Table des caractères irréductibles de $\mathbb{Z}/n\mathbb{Z}$: on retrouve des racines n -ièmes de l'unité ...

IV. B. Transformée de FOURIER discrète et interpolation polynomiale [Pey04, §III.2, p65]

Soit $N \in \mathbb{N}^*$ et $\omega = \exp(2i\pi/N)$.

DÉFINITION 37. [TRANSFORMÉE DE FOURIER DISCRÈTE]

Soit $f = (f_0, \dots, f_{N-1}) \in \mathbb{C}^{N+1}$. On définit la transformée de FOURIER discrète de f par le vecteur $\hat{f}$ tel que :

$$\forall k \in \llbracket 0, N-1 \rrbracket, \quad \hat{f}_k = \frac{1}{N} \sum_{j=0}^{N-1} f_j \omega^{-kj}$$

PROPOSITION 38. L'application $f \longmapsto \hat{f}$ est un isomorphisme d'espaces vectoriels de $\mathbb{C}^n$ dans lui-même.

REMARQUE 39. Autrement dit, pour tout $(c_0, \dots, c_{N-1}) \in \mathbb{C}^n$, il existe un unique polynôme $P = \frac{1}{N} \sum_{i=0}^{N-1} a_i X^i \in \mathbb{C}_{N-1}[X]$ tel que pour tout $k \in \llbracket 0, N-1 \rrbracket$, on a $P(\omega^k) = c_k$.

COROLLAIRE 40. La transformée de FOURIER inverse discrète de $\hat{f}$ est le vecteur de j -ième coordonnée $\sum_{k=0}^{N-1} \hat{f}_k \omega^{kj}$.

APPLICATION 41. [TRANSFORMÉE DE FOURIER RAPIDE]

On peut calculer la transformée de FOURIER discrète d'un N -échantillon en $\mathcal{O}(N \log(N))$ (alors que la formule initiale donne un $\mathcal{O}(N^2)$).

ANNEXE

Dessin du cercle unité et racines primitives, polygones réguliers.
Table de caractères

SPEECH

Les nombres complexes sont un outil puissant, en géométrie comme en algèbre. Leur richesse est en grande partie déterminée par la sphère unité et les propriétés de ses éléments, notamment de ses sous-groupes, interviennent donc fréquemment.

Dans une première partie, on reconstruit $\mathbb{C}$ à partir de l'exponentielle complexe, cela mène aux propriétés de linéarisation et aux propriétés de $\mathbb{U}$.

Dans un second temps, on s'intéresse aux déterminations continues d'argument et de logarithme.

Ensuite, on regarde les applications en algèbre avec les polynômes cyclotomiques et leurs propriétés.

Enfin, il y a de nombreuses autres applications du groupe des racines de l'unité, nous regardons leur rôle dans les représentations linéaires complexes, puis dans les questions autour de la transformée de FOURIER discrète, qui permet des multiplications rapides.

QUESTIONS

Q Pourquoi sait-on qu'il n'y a pas d'argument continu sur $\mathbb{C}^*$?

R Pour le logarithme, on sait que c'est une primitive de $z \mapsto 1/z$, et en intégrant sur un chemin fermé on ne trouve pas 0.

Q Donner des applications des polynômes cyclotomiques ?

Q Soit $\alpha \in [0, \pi/2[$. Partant de $x_0 = 1$, on génère x_1 comme le point d'intersection distinct de x_0 du cercle trigonométrique avec la droite passant par x_0 et d'angle α avec la droite (Ox_1) . Puis les points $x_2, x_3, \dots$ sont générés itérativement de manière similaire : x_{i+1} est obtenu comme le point d'intersection distinct de x_i du cercle trigonométrique avec la droite passant par x_i et telle que (Ox_i) est la bissectrice de $\widehat{x_{i-1}x_ix_{i+1}}$. Calculer $x_1, x_2, \dots$. Montrer que $\{x_i\}_{i \in \mathbb{N}}$ est fini ou dense dans $\mathbb{U}$.

R Distinguer selon que α/π soit commensurable ou non.

Q Peut-on trouver deux dés de lois indépendantes μ et ν telle que la somme des deux dés suive une loi uniforme sur $\llbracket 2, 12 \rrbracket$.

R Supposons que ce soit le cas. On calcule la fonction génératrice de la somme des deux dés et on obtient $g_{1+2}(s) = \frac{1}{11} s^2 \frac{1-s^{11}}{1-s} = g_1(s)g_2(s)$. Ainsi g_{1+2} a 0 pour racine double et les 10 autres racines sont $\mathbb{U}_{11} \setminus \{1\}$, g_1 a 0 pour racine simple et des éléments de $\mathbb{U}_{11} \setminus \{1\}$ conjugués, tout comme g_2 . C'est absurde puisqu'alors soit g_1 a 7 racines et g_2 en a 5, mais elles ne peuvent pas avoir chacune 6 racines.

BIBLIOGRAPHIE

[AF93] J.M. ARNAUDIÈS et H. FRAYSSE : *Cours de mathématiques, Tome 1, Algèbre*. Dunod, 1993.

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[FGN07] S. FRANCINO, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2^{ème} édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. PEYRÉ : *L'algèbre discrète de la transformée de FOURIER*. Ellipses, 2004.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rud98] W. RUDIN : *Analyse réelle et complexe*. Dunod, 2^{ème} édition, 1998.

[Ser98] J.-P. SERRE : *Représentations linéaires des groupes finis*. Hermann, 1998.

[Tau06] P. TAUVEL : *Analyse complexe pour la Licence 3*. Dunod, 2006.