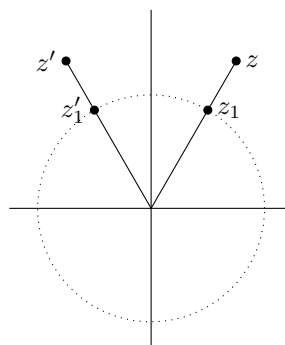


# Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

Mohamed NASSIRI

Les nombres complexes sont un outil puissant en géométrie et en algèbre. De plus, l'ensemble des nombres complexes,  $\mathbb{C}$ , est entièrement déterminée à partir de l'ensemble des nombres complexes de module 1,  $\mathbb{U}$ .

Illustrons ceci rapidement sur un exemple. Pour étudier la rotation qui à  $z$  associe  $z'$  comme sur la figure ci-contre, on applique une homothétie de rapport  $\frac{1}{|z|}$  au point d'affixe  $z$ . On obtient donc un point d'affixe  $z_1$  qui appartient donc au cercle unité. On applique ensuite la rotation au point d'affixe  $z_1$ , on obtient un point d'affixe  $z'_1$  qui appartient encore au cercle unité. Enfin, à ce dernier point, on lui applique l'homothétie de rapport  $|z|$  et on obtient le point d'affixe  $z'$ .



La fonction exponentielle joue un rôle important. C'est un morphisme du groupe  $(\mathbb{C}, +)$  sur le groupe  $(\mathbb{C}^*, \cdot)$ . On peut également définir  $\pi$  comme le nombre qui vérifie  $e^{i\pi} + 1 = 0$ . La fonction exponentielle nous permet surtout d'avoir une notation plus compacte et très maniable des nombres complexes : le nombre complexe non nul  $z$ , de module  $\rho$  et d'argument  $\theta$ , s'écrit alors  $\rho e^{i\theta}$ . C'est l'écriture dite exponentielle de  $z$ .

Une des applications importantes des nombres complexes de module 1 sont les polynômes cyclotomiques. Pour  $m \in \mathbb{N}^*$ , on considère l'ensemble  $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$  des racines  $m$ -ièmes de l'unité dans  $\mathbb{C}$ , et on appelle racine primitive  $m$ -ièmes de l'unité tout générateur de  $\mathbb{U}_m$ . On note  $\mathcal{P}_m(\mathbb{C})$  l'ensemble des racines primitives  $m$ -ièmes de l'unité. On appelle  $m$ -ième polynôme cyclotomique le polynôme

$$\Phi_{m,\mathbb{Q}}(X) = \prod_{\xi \in \mathcal{P}_m(\mathbb{C})} (X - \xi)$$

Les polynômes cyclotomiques ont des applications variées : théorème de Wedderburn, théorème de Dirichlet (version faible), etc.

On a une interprétation géométrique sympathique des racines  $n$ -ièmes de l'unité : l'ensemble des points ayant pour affixe les racines  $n$ -ièmes de l'unité est l'ensemble des  $n$  sommets d'un polygone régulier de centre  $O$  et inclus dans le cercle trigonométrique. De plus, avec la notion de *racines primitives*, on a l'interprétation suivante :

### Théorème

Soient  $m \in \mathbb{N}^*$  et  $\xi$  une racine primitive  $n$ -ièmes de l'unité dans  $\mathbb{C}$ . Alors les (autres) racines primitives  $m$ -ièmes de l'unité sont les  $\xi^k$ , où  $1 \leq k \leq n$   $\text{pgcd}(k, n) = 1$ .

En particulier, si  $n$  est premier, toutes les racines  $n$ -ièmes de l'unité dans  $\mathbb{C}$  sont primitives.

### Interprétation géométrique

Les polygones réguliers étoilés à  $n$  sommets d'un seul tenant s'obtiennent en joignant de  $k$  en  $k$ , avec  $\text{pgcd}(k, n) = 1$ , les sommets d'un polygone régulier à  $n$  sommets.

En particulier, si  $n$  est premier, tous les polygones réguliers étoilés à  $n$  sommets sont d'un seul tenant.

Les représentations linéaires de groupes offrent également aux nombres complexes de module 1 une place importante. En effet, en considérant un groupe fini  $G$  d'ordre  $n$  et une représentation linéaire de  $G$  dans un  $\mathbb{C}$ -espace vectoriel de dimension finie  $V$   $\rho : G \rightarrow \text{GL}(V)$ , alors on en déduit que

$$\forall g \in G, g^n = e \Rightarrow \rho(g)^n = \rho(g^n) = \rho(e) = Id_V$$

Ce qui se traduit par le fait que pour tout  $g \in G$ ,  $\rho(g)$  est diagonalisable dans  $\mathbb{C}$  et ses valeurs propres sont de module 1. Une des applications intéressantes est la caractérisation des sous-groupes distingués de  $G$  et des noyaux de caractères irréductibles de  $G$ . Cette caractérisation permet de lire très rapidement les sous-groupes distingués d'un groupe sur sa table de caractères.

En algèbre linéaire, on peut montrer que le déterminant de la matrice, de taille  $n \times n$ , dite circulante fait apparaître les racines  $n$ -ième de l'unité. Une application géométrique amusante est le résultat suivant : Soit  $Z = (z_1, \dots, z_n) \in \mathbb{C}^n$  une suite d'affixes du plan complexe. En notant,  $Z_k = (z_{k,1}, \dots, z_{k,n})$ , on définit par récurrence

$$Z_0 = Z \text{ et } Z_{k+1} = \left( \frac{z_{k,1} + z_{k,2}}{2}, \dots, \frac{z_{k,n-1} + z_{k,n}}{2}, \frac{z_{k,n} + z_{k,1}}{2} \right)$$

Alors la suite  $(Z_k)_{k \in \mathbb{N}}$  converge vers l'isobarycentre des affixes  $z_1, \dots, z_n$ .

Ce théorème a une interprétation géométrique très intéressante ! En partant d'un polygone à  $n$  côtés, le polygone des milieux "converge" vers l'isobarycentre du polygone de départ. Attention cependant à l'emploi du mot "convergence" ... Même si, intuitivement, on comprend ce que ça veut dire, ce n'est pas mathématique correcte s'il n'y a pas de définition d'une topologie sur l'ensemble des polygones qui permettrait à une suite de polygones de tendre vers un point.

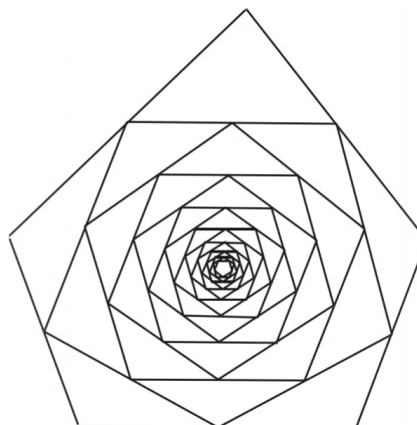


Illustration de la "convergence" des polygones

Le plus intrigant est que cette affirmation reste encore vraie si le polygone est non convexe (on dit aussi *polygone concave*). En effet, dans la démonstration, la suite de points est quelconque !

On sait que  $\mathbb{C}$  est algébriquement clos d'après le théorème de D'Alembert-Gauss, donc il est inutile de vouloir chercher un sur-corps de  $\mathbb{C}$ . Cependant, si l'on sacrifie la commutativité, on peut créer un sur-corps de  $\mathbb{C}$  : le corps des quaternions  $\mathbb{H}$ . Le lien entre quaternions et transformations géométriques est donné par l'isomorphisme :

$$G/\{-1, 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

où  $G$  est le groupe des quaternions de norme 1. Ce qui permet de faire explicitement le lien entre les quaternions et les rotations dans l'espace sont les *formules de rotation d'Olinde Rodrigues*.

### Références

- [GOUal] Les maths en tête : Algèbre, Xavier Gourdon
- [PER] Cours d'algèbre, Daniel Perrin ♠
- [GOZ] Théorie de Galois, Ivan Gozard
- [PEY] L'algèbre discrète de la transformée de Fourier, Gabriel Peyré ♠
- [BIA] Mathématiques pour le CAPES et l'Agrégation Interne, Jean de Biasi
- [ML3an] Mathématiques L3 Analyse, Jean-Pierre Marco

### Développements

- $SO_3(\mathbb{R})$  et les quaternions
- Théorème de Wedderburn
- Table des caractères de  $\mathfrak{S}_4$  et les isométries du tétraèdre
- Noyaux de caractères et sous-groupes distingués

# 1 Groupes des nombres complexes de module 1 [BIA] p.74 → 76

## 1.1 Définitions et premières propriétés

**Théorème 1** L'ensemble des nombres complexes de module 1 est un groupe multiplicatif  $\mathbb{U}$ , sous-groupe multiplicatif de  $(\mathbb{C}^*, \cdot)$ . C'est le noyau du morphisme

$$(\mathbb{C}^*, \cdot) \rightarrow (\mathbb{R}_+^*, \cdot) \\ z \mapsto |z|$$

**Proposition-Définition 2** Soit  $z = x + iy$  l'affixe d'un point  $M$  du plan. Alors  $\frac{z}{|z|}$  est l'affixe d'un point  $m$  qui appartient au cercle trigonométrique. Si  $\theta = (\bar{u}, \overline{Om}) \pmod{2\pi}$ , alors on a

$$\frac{z}{|z|} = \cos\theta + i\sin\theta$$

avec  $\cos\theta = \frac{x}{\sqrt{x^2+y^2}}$  et  $\sin\theta = \frac{y}{\sqrt{x^2+y^2}}$   
 $\theta$  est appelé argument de  $z$  et est noté  $\arg z = \theta$ .  
 La valeur de  $\theta \in ]-\pi, \pi[$  est appelé argument principal de  $z$  et est noté  $\text{Arg} z = \theta$ .  
 $z = |z|(\cos\theta + i\sin\theta)$  est appelé forme trigonométrique de  $z$ .

**Proposition 3** (i)  $\arg(-z) = \pi + \arg z \pmod{2\pi}$   
 (ii)  $\arg(\bar{z}) = -\arg z \pmod{2\pi}$   
 (iii)  $\forall z_1, z_2 \in \mathbb{C}^*, \arg(z_1 z_2) = \arg(z_1) + \arg(z_2) \pmod{2\pi}$

**Proposition 4** Formule de Moivre  
 $\forall n \in \mathbb{N}$ , on a

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

**Proposition-Définition 5** On pose  $e^{i\theta} = \cos\theta + i\sin\theta$ . Alors, on a  
 (i) Formules d'Euler

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2}$$

(ii) Formule de Moivre exponentielle

$$(e^{i\theta})^n = e^{in\theta}$$

(iii) Pour la beauté

$$e^{i\pi} = -1$$

Le nombre complexe non nul  $z$ , de module  $\rho$  et d'argument  $\theta$ , s'écrit alors  $\rho e^{i\theta}$ . C'est l'écriture exponentielle de  $z$ .

# 1.2 Autour de l'exponentielle complexe [ML3an] p.404 → 406

**Proposition-Définition 6** La fonction exponentielle complexe coïncide pour  $z \in \mathbb{C}$  avec la série convergente

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

**Proposition 7** (i) La fonction exponentielle complexe est un morphisme du groupe  $(\mathbb{C}, +)$  sur le groupe  $(\mathbb{C}^*, \cdot)$ .

(ii) La fonction  $\exp$  est holomorphe sur  $\mathbb{C}$  et égale à sa fonction dérivée.

(iii) La fonction  $\exp$  est surjective sur  $\mathbb{C}^*$ .

**Proposition 8** (i) La restriction  $\exp|_{\mathbb{R}}$  est une bijection dérivable strictement croissante et convexe de  $\mathbb{R}$  sur  $\mathbb{R}_+^*$ .

(ii) De plus, on a

$$\lim_{x \rightarrow -\infty} \exp(x) = 0 \quad \text{et} \quad \lim_{x \rightarrow +\infty} \exp(x) = +\infty$$

**Proposition 9** La fonction

$$\Phi : \mathbb{R} \rightarrow \mathbb{C} \\ x \mapsto \exp(ix)$$

est périodique, à valeurs dans le cercle unité, et elle est surjective. Sa période est notée  $2\pi$ .  
 La fonction exponentielle est donc  $2i\pi$ -périodique.

## 2 Racines de l'unité et cyclotomie

### 2.1 Racines de l'unité et cyclotomie [GOZ] p.67 → 69

**Proposition-Définition 10** Soit  $m \in \mathbb{N}^*$ . L'ensemble  $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$  des racines  $m$ -ièmes de l'unité dans  $\mathbb{C}$ .

$\mathbb{U}_m$  est un groupe cyclique d'ordre  $m$ .

On appelle racine primitive  $m$ -ièmes de l'unité tout générateur de  $\mathbb{U}_m$ . On notera  $\mathcal{P}_m(\mathbb{C})$  l'ensemble des racines primitives  $m$ -ièmes de l'unité.

**Proposition 11**  $\mathcal{P}_m(\mathbb{C}) = \{\exp(2ik\pi/m), 1 \leq k \leq m, \text{pgcd}(k, m) = 1\}$  a pour cardinal  $\varphi(m)$ .

**Proposition 12** Soient  $m \in \mathbb{N}^*$  et  $\xi$  une racine primitive  $m$ -ièmes de l'unité dans  $\mathbb{C}$ . Alors les (autres) racines primitives  $m$ -ièmes de l'unité sont les  $\xi^k$ , où  $1 \leq k \leq m, \text{pgcd}(k, m) = 1$ .

**Définition 13** Le sous-corps  $\mathbb{Q}(\mathbb{U}_m)$  de  $\mathbb{C}$  engendré par les racines  $m$ -ièmes de l'unité, qui est  $\mathbb{Q}(\xi)$  où  $\xi$  une racine primitive  $m$ -ièmes de l'unité quelconque, est appelé corps cyclotomique d'indice  $m$ .

**Définition 14** Soit  $m \in \mathbb{N}^*$ . On appelle  $m$ -ième polynôme cyclotomique le polynôme

$$\Phi_{m,\mathbb{Q}}(X) = \prod_{\xi \in \mathcal{P}_m(\mathbb{C})} (X - \xi)$$

$\Phi_{m,\mathbb{Q}}(X)$  est un polynôme unitaire de degré  $\varphi(m)$  et à coefficients dans  $\mathbb{C}$ .

**Proposition 15** (i)

$$X^m - 1 = \prod_{d|m} \Phi_{d,\mathbb{Q}}(X)$$

(ii)  $\forall n \in \mathbb{N}^*$ ,  $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$

(iii)  $\forall n \in \mathbb{N}^*$ ,  $\Phi_{n,\mathbb{Q}}(X)$  est irréductible dans  $\mathbb{Q}[X]$

**Application 16** ♠ Théorème de Wedderburn ♠  
Tout corps fini est commutatif. [PER] p.82

**Corollaire 17** Soit  $n \in \mathbb{N}^*$ , le polynôme minimal sur  $\mathbb{Q}$  de toute racine primitive  $n$ -ième de l'unité est  $\Phi_{n,\mathbb{Q}}(X)$ . Donc  $[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$

## 2.2 Racines $n$ -ième de l'unité et polygones réguliers [BIA] p.79-80

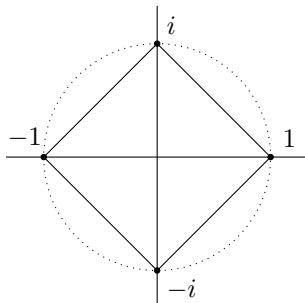
**Définition 18** Soit  $n \in \mathbb{N}^*$ . On note l'ensemble  $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$  des racines  $n$ -ièmes de l'unité dans  $\mathbb{C}$ .

On appelle racine primitive  $n$ -ièmes de l'unité tout générateur de  $\mathbb{U}_n$ .

On note  $\mathcal{U}_n(\mathbb{C})$  l'ensemble des racines primitives  $n$ -ièmes de l'unité et  $\mathcal{P}_n$  l'ensemble des points ayant pour affixe les racines  $n$ -ièmes de l'unité.

**Proposition 19**  $\mathcal{P}_n$  est l'ensemble des  $n$  sommets d'un polygone régulier de centre  $O$  et inclus dans le cercle trigonométrique.

**Exemple 20**  $\mathcal{U}_4(\mathbb{C}) = \{1, -1, i, -i\}$ .



**Proposition 21** Soient  $m \in \mathbb{N}^*$  et  $\xi$  une racine primitive  $n$ -ièmes de l'unité dans  $\mathbb{C}$ . Alors les (autres) racines primitives  $m$ -ièmes de l'unité sont les  $\xi^k$ , où  $1 \leq k \leq n$  et  $\text{pgcd}(k, n) = 1$ .

En particulier, si  $n$  est premier, toutes les racines  $n$ -ièmes de l'unité dans  $\mathbb{C}$  sont primitives.

**Remarque 22** Interprétation géométrique

Les polygones réguliers étoilés à  $n$  sommets d'un seul tenant s'obtiennent en joignant de  $k$  en  $k$ , avec  $\text{pgcd}(k, n) = 1$ , les sommets d'un polygone régulier à  $n$  sommets.

En particulier, si  $n$  est premier, tous les polygones réguliers étoilés à  $n$  sommets sont d'un seul tenant.

Voir Figure 1, Figure 2 et Figure 3.

## 3 Représentations linéaires de groupes

### 3.1 Définitions et premières propriétés [PEY] p.194 → 205

**Définition 23** Soit  $V$  un  $\mathbb{C}$ -espace vectoriel de dimension finie  $n$ . Une représentation linéaire d'un groupe  $G$  dans  $V$  est la donnée d'un morphisme  $\rho : G \rightarrow \text{GL}(V)$ . Ceci correspond à la donnée d'une action linéaire du groupe  $G$  sur  $V$  :

$$\begin{aligned} G \times V &\rightarrow V \\ (g, v) &\mapsto g.v = \rho(g)(v) \end{aligned}$$

Une représentation  $\rho$  est dite fidèle si  $G$  agit fidèlement sur  $V$ .

**Exemple 24** Fort de l'isomorphisme  $\text{Is}(\Delta_4) \approx \mathfrak{S}_4$ , on peut établir une représentation du groupe  $\mathfrak{S}_4$  sur l'espace vectoriel  $\mathbb{R}^3$  comme un groupe de transformations orthogonales.

**Définition 25** • Soient  $\rho$  et  $\rho'$  deux représentations d'un même groupe  $G$  respectivement sur deux  $\mathbb{C}$ -espace vectoriel  $V$  et  $V'$ . Un opérateur d'entrelacement est une application linéaire  $\tau : V \rightarrow V'$  tel que pour tout  $g \in G$ ,  $\tau \circ \rho(g) = \rho'(g) \circ \tau$

$$\begin{array}{ccc} V & \xrightarrow{\tau} & V' \\ \rho(g) \downarrow & & \downarrow \rho'(g) \\ V & \xrightarrow{\tau} & V' \end{array}$$

• Deux représentations  $\rho$  et  $\rho'$  d'un même groupe  $G$  respectivement sur deux  $\mathbb{C}$ -espace vectoriel  $V$  et  $V'$  sont dites isomorphes si  $\tau$  est bijective.

**Définition 26** • Si une représentation  $\rho$  de  $G$  sur  $V$  admet un sous-espace vectoriel  $W \subset V$  stable pour tous les  $\rho(g) \in \text{GL}(V)$ , elle induit une représentation  $\rho_W$  sur  $W$  appelée sous-représentation.

• Une représentation sur un espace  $V$  est dite irréductible si elle admet exactement deux sous-représentations :  $\{0\}$  et  $V$  tout entier.

**Proposition 27** Toute représentation peut s'écrire comme somme de représentations irréductibles.

**Proposition 28** Lemme de Schur :

Soient  $\rho$  et  $\rho'$  deux représentations irréductibles d'un groupe  $G$  respectivement sur deux  $\mathbb{C}$ -espace vectoriel  $V$  et  $V'$  et  $f \in \mathcal{L}(V, V')$  un opérateur d'entrelacement. Alors

(i) si  $\rho$  et  $\rho'$  ne sont pas isomorphes,  $f = 0$ .

(ii) Si  $f \neq 0$ , alors  $f$  est un isomorphisme.

Si on suppose  $V = V'$ , alors  $f$  est une homothétie.

**3.2 Caractères [PEY] p.207 → 226**

**Définition 29** Soit  $\rho$  une représentation d'un groupe  $G$  sur un  $\mathbb{C}$ -espace vectoriel  $V$  de dimension  $n$ .

On lui associe son caractère  $\chi_\rho$  défini par  $\chi_\rho(g) = \text{tr}(\rho(g))$ , où  $\text{tr}$  désigne la trace.

C'est une fonction de  $G$  dans  $\mathbb{C}$ , (i.e.)  $\chi_\rho \in \mathbb{C}[G]$ .

**Proposition 30** Soient  $\chi_\rho$  et  $\chi_{\rho'}$  deux caractères de représentations irréductibles. Alors

(i)  $\chi_\rho$  est le caractère d'une représentation irréductible si et seulement si

$$\langle \chi_\rho, \chi_\rho \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_\rho(g)} = 1$$

(ii) Si  $\chi_\rho$  et  $\chi_{\rho'}$  deux caractères de représentations irréductibles non isomorphes, alors  $\langle \chi_\rho, \chi_{\rho'} \rangle = 0$

**Proposition 31** En notant  $(\chi_i)_{i=1}^p$  les caractères irréductibles de  $G$  et  $(C_i)_{i=1}^p$  les classes de conjugaison de  $G$ , on a :

(i) Formule de Burnside :  $\sum_{i=1}^p \chi_i(1)^2 = |G|$

(ii) Orthogonalité des caractères :

$$\sum_{i=1}^p \chi_i(C_k) \overline{\chi_i(C_l)} = 0 \text{ pour } k \neq l.$$

**Définition 32** Une table des caractères est un tableau constitué des éléments de la matrice  $(\chi_i(C_j))_{1 \leq i, j \leq p}$ .

	1	$ C_1 $	...	$ C_p $
	1	$C_1$	...	$C_p$
$\chi_1 = \mathbb{1}$	1	1	...	1
$\chi_2$	$\chi_2(1)$	$\chi_2(C_2)$	...	$\chi_2(C_p)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\chi_p$	$\chi_p(1)$	$\chi_p(C_2)$	...	$\chi_p(C_p)$

**3.3 Noyau de caractères [PEY] p.230 → 232**

**Proposition 33** Soit  $G$  un groupe fini et  $\rho : G \rightarrow \text{GL}(V)$  une représentation, de caractère  $\chi_V$  sur un espace  $V$  de dimension  $d$ . On note  $g \in G$  un élément d'ordre  $k$ . Alors :

(i)  $\rho(g)$  est diagonalisable.

(ii)  $\chi_V$  est somme de  $\chi_V(1) = \dim V = d$  racines  $k^{\text{ième}}$  de l'unité.

(iii)  $|\chi_V(g)| \leq \chi_V(1) = d$ .

(iv)  $K_{\chi_V} := \{g \in G \mid \chi_V(g) = \chi_V(1)\}$  est

un sous-groupe distingué de  $G$ . On le nomme le noyau de la représentation.

**Proposition 34**  $\spadesuit$  Noyaux de caractères et sous-groupes distingués  $\spadesuit$

Soient  $G$  un groupe fini, et  $\widehat{G} = \{\rho_1, \dots, \rho_r\}$  son dual, formé de représentants des représentations irréductibles non isomorphes. Les sous-groupes distingués d'un groupe fini  $G$  sont exactement du type

$$\bigcap_{i \in I} \{g \in G \mid \chi_i(g) = \chi_i(e)\} \text{ où } I \subset \{1, \dots, r\}$$

**Corollaire 35**  $\spadesuit$   $G$  est simple si et seulement si pour tout  $i \neq 1$ , pour tout  $g \in G \setminus \{e\}$ ,  $\chi_i(g) = \chi_i(e)$ .

**4 Application à l'algèbre linéaire**

**Proposition 36** Déterminant circulant :

Soit  $(a_i)_{i=1 \dots n} \in \mathbb{C}^n$

$$\begin{vmatrix} a_1 & a_2 & \dots & a_n \\ a_n & a_1 & \dots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & a_1 \end{vmatrix} = \prod_{k=0}^{n-1} P(\omega^k)$$

où  $P = \sum_{k=1}^n a_k X^{k-1}$  et  $\omega$  une racine primitive  $n$ -ième de l'unité. [GOUal] p.180

**Application 37**  $\spadesuit$  Suite de polygones  $\spadesuit$

Soit  $Z = (z_1, \dots, z_n) \in \mathbb{C}^n$  une suite d'affixes du plan complexe.

En notant,  $Z_k = (z_{k,1}, \dots, z_{k,n})$ , on définit par récurrence

$$Z_0 = Z \text{ et}$$

$$Z_{k+1} = \left( \frac{z_{k,1} + z_{k,2}}{2}, \dots, \frac{z_{k,n-1} + z_{k,n}}{2}, \frac{z_{k,n} + z_{k,1}}{2} \right)$$

Alors la suite  $(Z_k)_{k \in \mathbb{N}}$  converge vers l'isobarycentre des affixes  $z_1, \dots, z_n$ .

**5 Quaternions [PER] p.160 → 164**

**Proposition-Définition 38** Il existe une algèbre  $\mathbb{H}$  de dimension 4 sur  $\mathbb{R}$ , appelé algèbre des quaternions, muni d'une base  $1, i, j, k$  telle que :

(i) 1 est élément neutre pour la multiplication,

(ii) on a les formules +ùù

$$jk = -kj = i, \quad ki = -ik = j, \quad ij = -ji = k$$

$$i^2 = j^2 = k^2 = -1$$

Un quaternions s'écrit alors

$$q = a + bi + cj + dk, \text{ avec } a, b, c, d \in \mathbb{R}$$

**Définition 39**  $\mathbb{H}$  est muni de la norme algébrique  $N$  suivante :  $\forall q = a + bi + cj + dk \in \mathbb{H}$  Ce groupe est d'ordre 8 et non abélien.

$$N(q) = a^2 + b^2 + c^2 + d^2$$

**Proposition 40** Le groupe  $G$  des quaternions de norme 1 est le groupe

$$\{\pm 1, \pm i, \pm j, \pm k\}$$

**Théorème 41**  $\spadesuit$   $SO_3(\mathbb{R})$  et les quaternions  $\spadesuit$   
Soit  $G$  le groupe des quaternions de norme 1. On a l'isomorphisme suivant :

$$G/\{-1, 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

## Illustrations

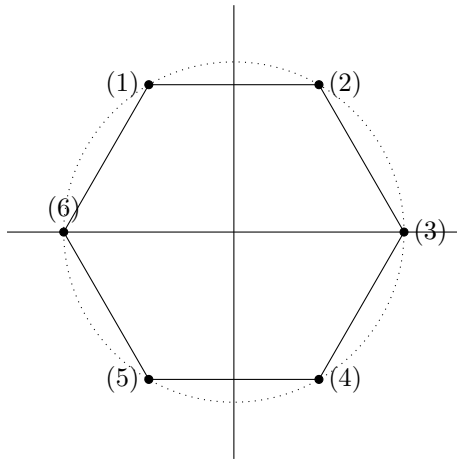


Figure 1 : Polygone régulier étoilé d'un seul tenant avec  $n = 6$  et  $k = 5$ .

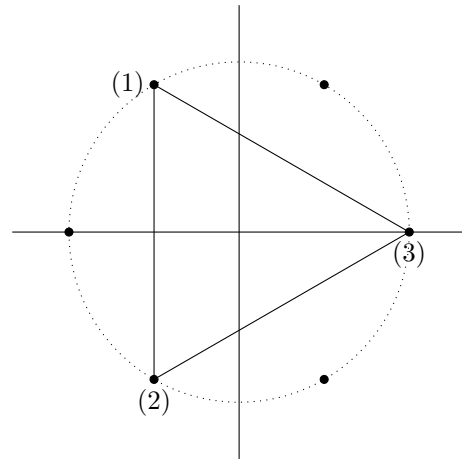


Figure 2 : Echec du polygone régulier étoilé d'un seul tenant avec  $n = 6$  et  $k = 2$ .

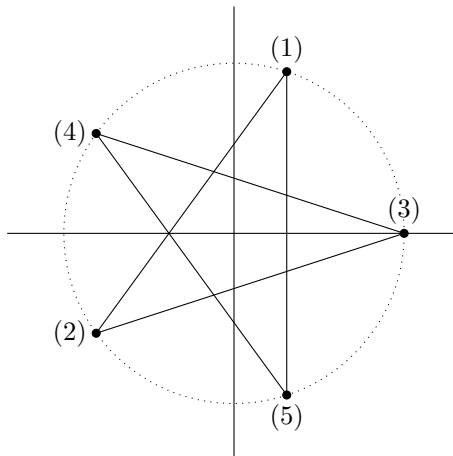


Figure 3 : Polygone régulier étoilé d'un seul tenant avec  $n = 5$  et  $k = 2$ .

## Questions

---

### Exercice : Groupes de Prüfer

Soit  $p$  un nombre premier. On rappelle que l'on note  $\mathbb{U}_n$  l'ensemble des racines  $n$ -ièmes de l'unité (dans le corps des nombres complexes  $\mathbb{C}$ ). On appelle  $p$ -groupe de Prüfer l'ensemble

$$\mathbb{U}_{p^\infty} = \bigcup_{k=0}^{\infty} \mathbb{U}_{p^k}$$

- 1) Montrer que c'est un groupe et que les  $\mathbb{U}_{p^k}$  forment une suite croissante de sous-groupes.
  - 2) Soit  $H$  un sous-groupe strict de  $\mathbb{U}_{p^\infty}$ . Montrer que l'ensemble des ordres des éléments de  $H$  est fini. En déduire que  $H$  est l'un des  $\mathbb{U}_{p^n}$ .
  - 3) Montrer que le quotient de  $\mathbb{U}_{p^\infty}$  par  $\mathbb{U}_{p^k}$  est isomorphe à  $\mathbb{U}_{p^\infty}$ .
- 

*Solution* : 1) Soient  $z$  et  $z'$  deux éléments de  $\mathbb{U}_{p^\infty}$ . Alors

$$z^{p^n} = z'^{p^{n'}} = 1$$

pour un certain  $n$  et un certain  $n'$  et donc

$$(zz')^{p^{\sup(n, n')}} = 1$$

De plus, comme  $z^{p^{n+1}} = 1$ , on a donc

$$\mathbb{U}_{p^n} < \mathbb{U}_{p^{n+1}}$$

A titre d'illustration, on peut donner les premiers éléments de  $\mathbb{U}_{2^\infty}$  :

$$\mathbb{U}_{2^\infty} = \{1, -1, i, -i, e^{i\pi/4}, e^{3i\pi/4}, e^{-i\pi/4}, e^{-3i\pi/4}, \dots\}$$

De plus,  $\mathbb{U}_{p^\infty}$  est un sous-groupe multiplicatif du groupe des nombres complexes de module 1.

2) On rappelle qu'un élément d'ordre  $p^k$  est une racine primitive  $p^k$ -ième de l'unité et donc engendre  $\mathbb{U}_{p^k}$ .

Raisonnons par l'absurde. Si la suite des ordres des éléments de  $H$  était infinie, alors pour tout  $z \in \mathbb{U}_{p^\infty}$  d'ordre  $p^k$ , il existerait un élément  $h \in H$  d'ordre supérieur  $p^{k'}$  et  $H$  contiendrait  $\mathbb{U}_{p^{k'}}$  et donc  $z$ . Par suite,  $\mathbb{U}_{p^\infty}$  serait inclus dans  $H$ , donc égal à  $H$ .

Soit maintenant, un élément de  $H$  d'ordre maximum  $p^{k_0}$ , alors  $H$  est égal à  $\mathbb{U}_{p^{k_0}}$  par le même argument.

3) Considérons l'application

$$\begin{aligned} \varphi : \mathbb{U}_{p^\infty} &\rightarrow \mathbb{U}_{p^\infty} \\ z &\mapsto z^{p^n} \end{aligned}$$

Manifestement,  $\varphi$  est un morphisme de groupe. Son noyau est  $\mathbb{U}_{p^n}$  et elle est surjective. En effet, tout élément de  $\mathbb{U}_{p^\infty}$  est de la forme  $e^{2li\pi/p^k}$  et est l'image de  $e^{2li\pi/p^{k+n}}$ . Donc par le premier théorème d'isomorphisme, on a

$$\mathbb{U}_{p^\infty} / \mathbb{U}_{p^n} \xrightarrow{\sim} \mathbb{U}_{p^\infty}$$

---

**Exercice** : Calculer l'expression

$$A = \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) ; \quad n \in \mathbb{N}^*$$

---



*Solution* : D'après la formule d'Euler, on a

$$\sin\left(\frac{k\pi}{n}\right) = \frac{e^{ik\pi/n} - e^{-ik\pi/n}}{2i} = e^{-ik\pi/n} \frac{e^{2ik\pi/n} - 1}{2i}$$

Ainsi, on a donc

$$A = \underbrace{\frac{e^{-i\pi/n} e^{-2i\pi/n} \dots e^{-i(n-1)\pi/n}}{2^{n-1} i^{n-1}}}_{:=B} \underbrace{(e^{-2i\pi/n} - 1)(e^{-4i\pi/n} - 1) \dots (e^{-2(n-1)i\pi/n} - 1)}_{:=C}$$

D'une part, le calcul de  $B$  donne

$$\begin{aligned} B &= \frac{e^{-i\pi/n} e^{-2i\pi/n} \dots e^{-i(n-1)\pi/n}}{2^{n-1} i^{n-1}} = \frac{e^{-i\pi/n[1+2+\dots+n-1]}}{2^{n-1} i^{n-1}} = \frac{e^{-\frac{i\pi}{n} \frac{n(n-1)}{2}}}{2^{n-1} i^{n-1}} \\ &= \frac{e^{-i\pi \frac{(n-1)}{2}}}{2^{n-1} i^{n-1}} \\ &= \frac{(e^{-\frac{i\pi}{2}})^{n-1}}{2^{n-1} i^{n-1}} \\ &= \frac{(-i)^{n-1}}{2^{n-1} i^{n-1}} \\ &= \frac{(-1)^{n-1}}{2^{n-1}} \end{aligned}$$

D'autre part, pour le calcul de  $C$ , on aura besoin des racines  $n$ -ièmes de l'unité! En effet,

$$C = (e^{-2i\pi/n} - 1)(e^{-4i\pi/n} - 1) \dots (e^{-2(n-1)i\pi/n} - 1)$$

On voit apparaître les racines  $n$ -ièmes de l'unité sauf 1.

Considérons le polynôme  $Q(X) = X^n - 1$  dont les racines sont les racines  $n$ -ièmes de l'unité (avec 1) et le polynôme

$$P(X) = \frac{Q(X)}{X-1} = 1 + X + X^2 + \dots + X^{n-1}$$

dont les racines sont les racines  $n$ -ièmes de l'unité sauf 1. Par conséquent,

$$P(X) = 1 + X + X^2 + \dots + X^{n-1} = (X - e^{-2i\pi/n})(X - e^{-4i\pi/n}) \dots (X - e^{-2(n-1)i\pi/n})$$

Ainsi, on remarque que

$$C = (-1)^{n-1} P(1) = (-1)^{n-1} n$$

Finalement,

$$A = B.C = \frac{(-1)^{n-1}}{2^{n-1}} \cdot (-1)^{n-1} n = \frac{n}{2^{n-1}}$$