# Leçon 102 : Groupe des nombres complexes de module 1
# Racines de l'unité. Applications

Références : Arnaudiès-Fraysse 1 ; Combes (algèbre et géométrie) ; Perrin ; Gourdon ; Francinou 1 (pour Kronecker) ; [Audin (géométrie)] Bof ; Goblot ; Audin (géométrie) ; Gozard, Carrega, Berhuy (constructibilité)

## I - Groupe des nombres complexes de module 1

1) Définitions et premières propriétés
2) Exponentielle complexe
3) Argument

## II - Sous-groupes de $(\mathbb{U}, \times)$ - Racines de l'unité

## III - Cyclotomie

1) Polynômes cyclotomiques
2) Applications
3) Extensions cyclotomiques

## IV - Aspects géométriques

1) Rotations vectorielles
2) Angles orientés

## V - Applications

1) Polynômes constructibles à la règle et au compas
2) Réduction des endomorphismes unitaires

DEV 1 : Wedderburn (Gourdon)

DEV 2 : Irréductibilité de $\phi_n$ (Gozard)

# Leçon 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications

## I - Groupe des nombres complexes de module 1 [ARN] [FRAY]

### 1) Définitions et premières propriétés

**DEF 1** : On définit l'ensemble $\mathbb{U} = \{z \in \mathbb{C} \,/\, |z| = 1\}$. C'est le noyau du morphisme : $\mathbb{C}^* \longrightarrow \mathbb{R}_+^*$, $z \longmapsto |z|$

**PROP 2** : $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$ (multiplicatif). On l'appelle groupe des nombres complexes de module 1.

**REM 3** : Dans le plan d'Argand-Cauchy, $\mathbb{U}$ n'est autre que le cercle unité de $\mathbb{C}$, de centre 0 et de rayon 1, d'équation $x^2+y^2=1$.

**EX 4** : Les nombres $-1, 1, i, -i$ sont dans $\mathbb{U}$.

**THM 5** : L'application $f : \mathbb{R}_+^* \times \mathbb{U} \longrightarrow \mathbb{C}^*$, $(r, u) \longmapsto ru$ définit un isomorphisme du groupe $\mathbb{R}_+^* \times \mathbb{U}$ sur $\mathbb{C}^*$.

**PROP 6** : $\mathbb{U}$ est compact et connexe par arcs

### 2) Exponentielle complexe

**DEF 7** : La série $\sum \frac{z^n}{n!}$ converge pour tout $z \in \mathbb{C}$. La fonction somme $z \in \mathbb{C} \longmapsto \sum_{n=0}^{\infty} \frac{z^n}{n!}$ est appelée fonction exponentielle notée exp.

**THM 8** : L'application exp est un morphisme surjectif du groupe $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$. $\forall z, z' \in \mathbb{C}, \exp(z+z') = \exp(z)\exp(z')$

**PROP 9** : L'application exp est holomorphe sur $\mathbb{C}$.

**REM 10** : exp n'est cependant pas injective.

**PROP 11** : L'application $x \in \mathbb{R} \mapsto \exp(ix)$ est à valeurs dans $\mathbb{U}$. On la note $\mathcal{E}$ et c'est un morphisme surjectif de noyau $2\pi\mathbb{Z}$.

**COR 12** : On a donc $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z}$.

**DEF 13** : Les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ : $x \mapsto \mathrm{Re}(\mathcal{E}(x))$ et $x \mapsto \mathrm{Im}(\mathcal{E}(x))$ se nomment respectivement cosinus et sinus et se notent cos et sin. On a donc $\forall x \in \mathbb{R}$, $e^{ix} = \cos(x) + i\sin(x)$.

**PROP 14** : $\forall x \in \mathbb{R}$,
$\forall n \in \mathbb{Z}, \exp(inx) = \cos(nx) + i\sin(nx) = (e^{ix})^n$ (Moivre)
$\cos(x) = \frac{e^{ix}+e^{-ix}}{2}$, $\sin(x) = \frac{e^{ix}-e^{-ix}}{2i}$ (Euler)

### 3) Argument

**DEF 15** : Soit $z \in \mathbb{C}^*$. On appelle argument de $z$ tout réel $\theta$ tel que $e^{i\theta} = \frac{z}{|z|}$. L'ensemble des arguments de $z$ est noté $\arg(z)$.

**THM 16** : L'ensemble $\arg(z)$ est non vide et : $\forall \theta_0 \in \arg(z)$, $\arg(z) = \{\theta_0 + 2k\pi \,/\, k \in \mathbb{Z}\}$

**DEF 17** : On appelle argument principal de $z \in \mathbb{C} \setminus \mathbb{R}^-$ et on note $\mathrm{Arg}(z)$ l'unique réel de $\arg(z) \cap ]-\pi; \pi[$. Ainsi, $\forall z \in \mathbb{C} \setminus \mathbb{R}^-$, $\exists! (r, \theta) \in \mathbb{R}_+^* \times ]-\pi; \pi[$, $z = re^{i\theta}$.

**THM 18 (Relèvement)** : Soit $u : I \subset \mathbb{R} \longrightarrow \mathbb{U}$ de classe $\mathcal{C}^k$, $k \geq 1$. Alors $\exists \alpha : I \longrightarrow \mathbb{R}$ de classe $\mathcal{C}^k$ telle que $\forall t \in I$, $u(t) = e^{i\alpha(t)}$. De plus, si on fixe $\alpha(x_0) = t_0 \in \mathbb{R}$ avec $u(x_0) = e^{it_0}$ alors $\alpha$ est unique. Ref?

**REM 19** : La fonction $z \in \mathbb{C}^* \mapsto \mathrm{Arg}(z)$ possède des règles de calcul similaires à celles du logarithme népérien

## II - Sous-groupes de $(\mathbb{U}, \times)$ - Racines de l'unité

**PROP 20** : Les sous-groupes de $\mathbb{U}$ sont soit cycliques d'ordre $n$ engendré par $e^{2i\pi n\theta}$, $\theta \in \mathbb{Q}$, soit denses dans $\mathbb{U}$ [COMBES]

**THM 21** : Soit $n \in \mathbb{N}$, $n \geq 2$ et $a \in \mathbb{C}$, $a \neq 0$. L'ensemble $R_n(a)$ des racines $n$-ièmes de $a$ i.e $\{z \in \mathbb{C} \,/\, z^n = a\}$ est de cardinal $n$. Pour tout $\theta \in \arg(a)$, on a

$$R_n(a) = \{|a|^{\frac{1}{n}} \exp(i(\tfrac{\theta}{n} + \tfrac{2k\pi}{n})) \,/\, k \in [\![0; n-1]\!]\}.$$

**THM 22** : Soit $n \geq 2$. L'application $f_n : \mathbb{U} \longrightarrow \mathbb{U}$, $z \longmapsto z^n$ est un morphisme de groupes surjectif. Son noyau, noté $\mu_n$, est cyclique. Ses générateurs sont les nombres

$$\zeta_k = \exp(\tfrac{2ik\pi}{n}),\ k \wedge n = 1,\ k \in [\![0, n-1]\!].$$

**DEF 23** : On a $\mu_n = \{z \in \mathbb{C} \,/\, z^n = 1\}$. Ce groupe s'appelle groupe des racines $n$-ièmes de l'unité dans $\mathbb{C}$.

**DEF 24** : On appelle racine $n$-ième primitive de l'unité dans $\mathbb{C}$ tout générateur du groupe $\mu_n$, c'est-à-dire tout nombre $\zeta_k$. On note $\mu_n^*$ leur ensemble

**REM 25** : Il y a donc $\varphi(n)$ générateurs où $\varphi$ est l'indicatrice d'Euler. De plus, $\mu_n = \bigsqcup_{d|n} \mu_d^*$ [ARN] [FRAY]

**EX 26** : $\mu_3 = \{1; j; j^2\}$, $\mu_3^* = \{j; j^2\}$ où $j = e^{\frac{2i\pi}{3}}$.

[GOU] [DET]

**APPLI 27** : Soit $A$ une matrice circulante :
$A=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & & & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$ Alors $\det(A)=P(1)P(\omega)\cdots P(\omega^{n-1})$ avec $\omega=e^{\frac{2i\pi}{n}}$ et $P(X)=a_1+a_2X+\cdots+a_nX^{n-1}$

[FRA 1] **THM 28 (Kronecker)** : Soit $P$ un polynôme de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur à 1. Si $P(0)\neq 0$, alors les racines de $P$ sont des racines de l'unité.

## III - Cyclotomie

### 1) Polynômes cyclotomiques [PER]

On reste dans le contexte des nombres complexes, même si ces notions peuvent s'étendre à des corps quelconques (en faisant attention à la caractéristique).

**DEF 29** : Soit $n\in\mathbb{N}^*$. Le $n$-ième polynôme cyclotomique $\Phi_n(X)\in\mathbb{C}[X]$ est donné par la formule :
$$\Phi_n(X)=\prod_{\zeta\in\mu_n^*}(X-\zeta)$$

**PROP 30** : $\Phi_n$ est un polynôme unitaire de degré $\varphi(n)$

**PROP 31** : On a la formule suivante :
$$X^n-1=\prod_{d\mid n}\Phi_d(X) \text{ et donc } n=\sum_{d\mid n}\varphi(d)$$

**PROP 32** : $\forall n\in\mathbb{N}$, $\Phi_n\in\mathbb{Z}[X]$ et $\Phi_n(0)=1$.
De plus, si $p$ est premier, $\Phi_p(X)=\sum_{k=0}^{p-1}X^k$.

### 2) Applications

**PROP 33** : Soient $n,m\in\mathbb{N}$. $\mathrm{PGCD}(X^n-1,X^m-1)=X^{\mathrm{PGCD}(n,m)}-1$

[PER] **THM 34 (Wedderburn)** : Tout corps fini est commutatif. DEV 1

[GOU 99] **THM 35 (Dirichlet faible)** : Il existe une infinité de nombres premiers tels que $p\equiv 1 \bmod n$ $(n\geq 2)$.

### 3) Extensions cyclotomiques [PER]

DEV 2

**THM 36** : Le polynôme cyclotomique $\Phi_n$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

**COR 37** : Si $\zeta$ est une racine primitive $n$-ième de l'unité dans $\mathbb{C}$ (de caractéristique nulle), son polynôme minimal est $\Phi_n$ et on a donc $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(n)$.

**COR 38** : Soient $\alpha$, $\beta$ deux racines primitives respectivement $n$-ième et $m$-ième de l'unité dans $\mathbb{C}$. Si $m\wedge n=1$, alors $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$.

## IV - Aspects géométriques

### 1) Rotations vectorielles [AVEZ géom. p-153]

On se place dans un espace euclidien $E$ de dimension 2.

**DEF 39** : On appelle automorphisme orthogonal (ou isométrie vectorielle) de $E$ toute application $f$ linéaire de $E$ dans $E$ telle que : $\forall x\in E$, $\|f(x)\|=\|x\|$.

**DEF 40** : On appelle matrice orthogonale toute matrice $M\in\mathcal{M}_2(K)$ telle que $M^{-1}={}^tM$.

**PROP 41** : La matrice d'une isométrie vectorielle dans une base orthonormée est orthogonale.

**NOT 42** : On note $O(E)$ le groupe des isométries vectorielles et $O_2(\mathbb{R})$ le groupe des matrices orthogonales.

**PROP 42** : $\forall f\in O(E)$, $\det(f)\in\{-1;1\}$, de même pour $M\in O_2(\mathbb{R})$.

**DEF 43** : On définit le groupe spécial orthogonal : $SO(E)=\{f\in O(E) ;\ \det(f)=1\}$. Les éléments de $SO(E)$ sont appelés rotations de $E$. De même, on définit $SO_2(\mathbb{R})=\{M\in O_2(\mathbb{R}) ;\ \det(M)=1\}$.

**THM 44** : Une fois $E$ orienté, il existe un isomorphisme de $\mathbb{U}$ sur $SO_2(\mathbb{R})$ défini par $a+ib\mapsto\begin{pmatrix} a & -b \\ b & a\end{pmatrix}$

**COR 45** : Puisque $SO_2(\mathbb{R})\simeq\mathbb{R}/2\pi\mathbb{Z}$, on a $SO_2(\mathbb{R})$ commutatif. De même pour $SO(E)$ (une fois $E$ orienté).

### 2) Angles orientés [GOBLOT] [AUDIN]

**THM 46** : Le groupe $SO(E)$ des rotations vectorielles agit simplement transitivement sur l'ensemble $\mathcal{U}$ des vecteurs unitaires : $\forall(u,u')\in\mathcal{U}$, $\exists!\,\varphi\in SO(E)$, $\varphi(u)=u'$.

**PROP 47** : La relation sur $\mathcal{U}\times\mathcal{U}$ définie par $(u,u')\sim(v,v')$ ssi $\exists\varphi\in SO(E)$, $\varphi(u)=u'$ et $\varphi(v)=v'$ est une relation d'équivalence appelée relation d'équipollence.

**DEF 48** : Le quotient $\mathcal{A}=\mathcal{U}\times\mathcal{U}/\sim$ est appelé ensemble des angles orientés. Une classe $(u,u')\in\mathcal{A}$ est l'angle orienté de vecteurs $(\widehat{u,u'})$.

**PROP 49** : On a une bijection $\theta : SO(E)\to\mathcal{A}$, $\varphi\mapsto(\widehat{u,\varphi(u)})$
$\mathcal{A}$ devient alors un groupe additif.

**PROP 50 (Relation de Chasles et règle du parallélogramme)**
$\forall(u_1,u_2,u_3)\in\mathcal{U}^3$, $(\widehat{u_1,u_2})+(\widehat{u_2,u_3})=(\widehat{u_1,u_3})$
$\forall(u,u',v,v')\in\mathcal{U}^4$, $\left((\widehat{u,u'})=(\widehat{v,v'})\right)\Leftrightarrow\left((\widehat{u,v})=(\widehat{u',v'})\right)$

**DEF 51**: Soient $v_1, v_2$ deux vecteurs non nuls, $u_1, u_2$ les vecteurs unitaires colinéaires et de même sens de sorte que $\forall i \in \{1;2\}$, $u_i = \frac{1}{\|v_i\|} v_i$. On définit l'angle orienté de $v_1$ et $v_2$ par : $(\widehat{v_1, v_2}) = (\widehat{u_1, u_2})$.

**PROP 52 (Mesure des angles)** : En composant les morphismes $\mathcal{E} : x \in \mathbb{R} \mapsto e^{ix}$ ① et $a+ib \in \mathbb{U} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in SO_2(K)$, on obtient un morphisme de $\mathbb{R}$ dans $\mathcal{A}$ qui à $t$ associe $\begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$
$\forall t \in \mathbb{R}, \exists ! \theta \in \mathcal{A}, \cos(t) = \cos(\theta)$ et $\sin(t) = \sin(\theta)$.
Ce morphisme a pour noyau $2\pi\mathbb{Z}$ d'où $\frac{\mathbb{R}}{2\pi\mathbb{Z}} \simeq \mathcal{A}$

## V - Applications [GOZ] [CAR] [BER]

### 1) Polynômes constructibles à la règle et au compas

P désigne un plan affine euclidien orienté, $R = (O, \vec{i}, \vec{j})$ un repère orthonormé direct.

**DEF 53** : Soit $X \subseteq P$, $\#X \geq 2$. On considère
a) les droites affines $(AB)$, $A \neq B \in X^2$
b) les cercles $C(A, \|AB\|)$, $(A, B) \in X^2$, $A \neq B$.
On dit que $M \in P$ est constructible (à la règle et au compas) en un pas à partir de $X$ si et seulement s'il existe
- deux droites de type a)
- deux cercles de type b)
- une droite de type a) et un cercle de type b)

dont $M$ soit un point d'intersection.

**DEF 54** : $x \in \mathbb{R}$ est constructible $\Leftrightarrow (x, 0)$ est constructible $\Leftrightarrow (0, x)$ est constructible.

**THM 55** : L'ensemble $\mathbb{E}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée : $\forall x \in \mathbb{E} \cap \mathbb{R}_+^*$, $\sqrt{x} \in \mathbb{E}$.

**THM 56 (Wantzel)** : Soit $t \in \mathbb{R}$. $t$ est constructible si et seulement si il existe une suite finie $(L_0, \dots, L_p)$ de sous-corps de $\mathbb{R}$ vérifiant :
- $L_0 \in \mathbb{Q}$
- $\forall i \in [\![0; p-1]\!]$, $L_{i+1}$ est une extension quadratique de $L_i$
- $t \in L_p$.

**COR 57** : Soit $x \in \mathbb{R}$. Si $x$ est constructible, il existe $e \in \mathbb{N}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^e$, d'où $x$ est algébrique.

**DEF 58** : Soit $n \in \mathbb{N}^*$. $\{M_0, \dots, M_{n-1}\} \in (\mathbb{R}^2)$ forment les sommets d'un polygone régulier lorsqu'il existe une rotation $r$ de centre $O$ d'angle $\frac{2\pi}{n}$ telle que $M_1 = r(M_0), \dots, M_{n-1} = r(M_{n-2}), M_0 = r(M_{n-1})$.

[GOBLOT]

**PROP 59** : $\{z_1, \dots, z_n\}$ est un polygone régulier ssi $\Omega Z = 0$ avec $\Omega$ la matrice à $n$ colonnes et $n-2$ lignes $\Omega = (\omega^{kk})$, $k \in [\![1; n-2]\!]$, $k \in [\![0; n-1]\!]$, $\omega = e^{\frac{2i\pi}{n}}$ et $Z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$

**DEF 60** : Le polygone régulier à $n$ côtés est constructible si $\cos(\frac{2\pi}{n})$ est constructible

**THM 61 (Gauss)** Les polygones réguliers constructibles sont ceux dont le nombre de côtés $n$ est de la forme $2^\alpha p_1 \cdots p_r$, $\alpha \in \mathbb{N}$ et $p_i$ premiers distincts : $p_i = 1 + 2^{2^{\beta_i}}$ sont les nombres de Fermat.

### 2) Réduction des endomorphismes unitaires

Soit $(E, \langle \cdot | \cdot \rangle)$ un espace hermitien. [GOU p254]

**DEF 62** : On appelle endomorphisme unitaire tout élément $f \in \mathcal{L}(E)$ tel que $\forall (x, y) \in E \times E$, $(f(x) | f(y)) = (x | y)$

**REM 63** : On a alors $f^* = f^{-1}$ et $\|f\| = 1$.
Les valeurs propres d'un opérateur unitaire sont de module 1

**Matriciellement** $\mathcal{B}$ une base orthonormée de $E$, $A = \mathcal{M}at_{\mathcal{B}}(f)$. ${}^t\bar{A}A = A\,{}^t\bar{A} = I_n$ et $\det(A) \in \{-1; 1\}$.

**THM 64** : Soit $U \in \mathcal{M}_n(\mathbb{C})$ une matrice unitaire (vérifiant l'égalité ${}^t\bar{M}M = M\,{}^t\bar{M} = I_n$). Alors il existe une matrice unitaire $P$ telle que

$$P^{-1} U P = \begin{pmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_n} \end{pmatrix} \quad \text{où } \forall i \in [\![1; n]\!],\ \theta_i \in \mathbb{R}$$

En d'autres termes $U$ est diagonalisable dans une base orthonormée et toutes ses valeurs propres sont de module 1.