Polynômes

BCPST Spé 2 Lycée Champollion Grenoble

Novembre 2023

Table des matières

I Rappels sur les complexes et la trigonométrie

Dans toute la suite lorsque l'on introduira un complexe sous la forme $a = a + \mathbf{i}\, b$, il est sous entendu que a et b sont des réels.

I.1 Définitions et premières propriétés.

Définition 1 (Forme algébrique)**.**
Tout complexe z peut se mettre de façon unique sous la forme $z = a + \boldsymbol{i}\, b$. où a et b sont des réels. Cette forme est unique

- *a est la **partie réelle** de z, elle est notée $Re(z)$.*
- *b est la **partie imaginaire** de z, elle est notée $Im(z)$.*
- *On dit que z est un **imaginaire pur** si et seulement si $Re(z) = 0$. On note $\boldsymbol{i}\mathbb{R}$*

l'ensemble des imaginaires purs.

Définition 2 (Conjugaison)**.**
*Soit $z = a + \boldsymbol{i}\, b$ un complexe, on appelle **conjugué** de z, que l'on note $\overline{z}$ l'unique complexe :*

$$\overline{z} = a - \boldsymbol{i}\, b$$

Proposition 1 (Propriétés de la partie réelle et de la partie imaginaire.)**.**
Soit z et z' deux complexes, α et β deux réels.

- $Re(\alpha \cdot z + \beta \cdot z) = \alpha Re(z) + \beta Re(z)$
- $Im(\alpha \cdot z + \beta \cdot z) = \alpha Im(z) + \beta Im(z)$
- *$z \in \boldsymbol{i}\mathbb{R}$ si et seulement si $z = \boldsymbol{i}\, Im(z)$.*
- *$z \in \mathbb{R}$ si et seulement si $z = Re(z)$.*
- *$z \in \mathbb{R}$ si et seulement si $0 = Im(z)$.*

Proposition 2 (Propriétés du conjugué)**.**
Soit z et z' deux complexes, α et β deux réels.

- $\overline{\overline{z}} = z$
- $\overline{\alpha \cdot z + \beta \cdot z'} = \alpha \cdot \overline{z} + \beta \cdot \overline{z'}$
- $z + \overline{z} = 2Re(z)$
- *$z \in \mathbb{R}$ si et seulement si $z = \overline{z}$.*
- $z - \overline{z} = 2\boldsymbol{i}\, Im(z)$
- *$z \in \boldsymbol{i}\mathbb{R}$ si et seulement si $z = -\overline{z}$.*
- $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$

On remarque que si $z = a + \mathbf{i} \cdot b$ alors $z \cdot \overline{z} = a^2 + b^2$ est un réel positif.

Définition 3 (module)**.**
*Soit $z \in \mathbb{C}$, on appelle **module** de z et on note $|z|$ l'unique réel positif tel que :*

$$|z|^2 = z \cdot \overline{z}$$

On a aussi de façon équivalente si $z = a + \boldsymbol{i}\, b$

$$|z| = \sqrt{a^2 + b^2}$$

Proposition 3 (Propriétés du module)**.**

Soit z et z' deux complexes et α un réel.

1. $|z| \geqslant 0$ *et de plus* $|z| = 0$ *si et seulement si* $z = 0$.
2. *Si* $z \in \mathbb{C}^*$*, alors;* $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$
3. $\left|z \cdot z'\right| = |z| \cdot \left|z'\right|$
4. $\left|\overline{z}\right| = |z|$
5. $z = |z|$ *si et seulement si z est un réel positif*
6. $|Re(z)| \leqslant |z|$ *et il y a égalité dans l'inégalité si et seulement si z est réel.*
7. $Re(z) \leqslant |z|$ *et il y a égalité dans l'inégalité si et seulement si z est réel positif.*
8. $|Im(z)| \leqslant |z|$ *et il y a égalité dans l'inégalité si et seulement si z est un imaginaire pur.*
9. ***Inégalité triangulaire :***
$$\left|z + z'\right| \leqslant |z| + \left|z'\right|$$
De plus il y a égalité dans l'inégalité si et seulement si :
$$\exists \lambda \in \mathbb{R}_+ \qquad z = \lambda z' \quad ou \quad z' = \lambda z$$

Définition 4 (Exponentielle de $\mathbf{i}\,\theta$)**.**
Soit $\theta \in \mathbb{R}$ on pose :

$$e^{\boldsymbol{i}\theta} = \cos\theta + \boldsymbol{i} \sin\theta$$

Proposition 4 (Propriétésd e l'exponentielle complexe)**.**

Soit α et β deux réels

1. ***Formule d'Euler***.
$$\cos\alpha = Re(e^{i\alpha}) = \frac{e^{\boldsymbol{i}\alpha}+e^{-\boldsymbol{i}\alpha}}{2} \qquad \sin\alpha = Im(e^{\boldsymbol{i}\alpha}) = \frac{e^{\boldsymbol{i}\alpha}-e^{-\boldsymbol{i}\alpha}}{2i}$$
2. $e^{\boldsymbol{i}\alpha}e^{i\beta} = e^{\boldsymbol{i}(\alpha+\beta)}$
3. $e^{\boldsymbol{i}\alpha} \neq 0$
4. $\overline{e^{\boldsymbol{i}\alpha}} = \dfrac{1}{e^{\boldsymbol{i}\alpha}} = e^{-\boldsymbol{i}\alpha}$
5. *Si $k \in \mathbb{Z}$ alors*
$$e^{\boldsymbol{i}(\alpha+k2\pi)} = e^{\boldsymbol{i}\alpha}$$
6. ***Formule de Moivre.*** *Si $n \in \mathbb{N}$ alors* $\left(e^{\boldsymbol{i}\alpha}\right)^n = e^{\boldsymbol{i}n\alpha}$

Proposition 5 (Forme trigonométrique et exponentielle)**.**

1. *Soit $z \in \mathbb{C}$ tel que $|z| = 1$ alors il existe $\theta \in \mathbb{R}$ tel que*
$$z = e^{i\theta} = \cos\theta + \boldsymbol{i}\sin\theta$$
2. *Soit $z \in \mathbb{C}^*$ alors il existe $\theta \in \mathbb{R}$ tel que :*
$$z = |z|e^{i\theta} = |z|(\cos\theta + \boldsymbol{i}\sin\theta)$$

Remarque : θ n'est défini qu'à 2π près.

Définition 5 (Argument)**.**
Soit $z \in \mathbb{C}^*$, si z est de la forme $\rho e^{\boldsymbol{i}\theta}$ avec $\rho \in \mathbb{R}_+^*$, on dit alors que θ est ***un argument*** *de z.*

Remarque : 0 n'a pas d'argument.

Proposition 6 (Égalité)**.**
Deux nombres complexes non nuls sont égaux si et seulement si ils ont même argument à 2π prés et même module.
Soit $z_1 = \rho_1 e^{\boldsymbol{i}\theta_1}$ et $z_2 = \rho_2 e^{\boldsymbol{i}\theta_2}$ avec ρ_1 et ρ_2 positifs alors :
$$z = z' \text{ si et seulement si } \quad \rho_1 = \rho_2 \quad et \quad \exists k \in \mathbb{Z}, \qquad \theta_1 + 2k\pi$$

I.2 Applications à la trigonométrie.

Les formules et d'Euler permettent de retrouver les formules de trigonométrie classiques, il faut savoir les utiliser

Méthode : Linéarisation de $\cos(x)^p \sin(x)^q$

Pour écrire sous forme d'une somme ces quantités .

- On remplace $\sin(x)$ et $\cos(x)$ en utilisant la formule d'Euler.
- On développe en utilisant les formules du binôme.
- En rassemble des termes $\mathrm{e}^{\mathbf{i}\,nx}$ et $\mathrm{e}^{-\mathbf{i}\,nx}$ pour faire apparaître des cosinus $\cos(nx)$ et des sinus $\sin(nx)$ grâce aux formules d'Euler.
- Ces formules sont utiles par exemple lorsque l'on veut intégrer des produit de sinus et de cosinus

Méthode : simplification de $\cos(px)$ ou $\sin(px)$

Pour écrire sous forme d'une somme ces quantités .

- On utilise la formule de Moivre .

$$\cos(px) = \mathrm{Re}\left(\left(\mathrm{e}^{\mathbf{i}\,x}\right)^p\right) \qquad \sin(px) = \mathrm{Im}\left(\left(\mathrm{e}^{\mathbf{i}\,x}\right)^p\right)$$

- On remplace $\mathrm{e}^{\mathbf{i}\theta} = \cos(\theta) + \mathbf{i}\,\sin(\theta)$
- On développe en utilisant les formules du binôme.
- On identifie les parties réelles et imaginaires

Méthode résolution de $a\cos\varphi + b\sin\varphi = c$

Pour résoudre cette équation on commence par écrire

$$a\cos\varphi + b\sin\varphi = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}}\cos\varphi + \frac{b}{\sqrt{a^2+b^2}}\sin\varphi\right)$$

Puis on cherche un réel θ tel que

$$\cos(\theta) = \frac{a}{\sqrt{a^2+b^2}} \qquad \sin(\theta) = \frac{b}{\sqrt{a^2+b^2}}$$

Ce réel existe toujours mais n'a pas forcément une forme simple.
Et on s'est ramené à un équation du type

$$\cos(\varphi - \theta) = c'$$

II Polynômes

II.1 Des fonctions polynomiales aux polynômes

L'année dernière vous avez étudié les fonctions polynomiales réelles, c'est à dire les fonctions que l'on peut écrire sous la forme

$$x \mapsto a_0 + a_1 x + \cdots + a_n x^n$$

Où les a_i sont des coefficients réels

Définition 6 (Notation X)**.**
On note X la fonction définie sur $\mathbb{R}$ telle que

$$X : x \mapsto x$$

Attention : *X n'est pas une inconnue ni une variable, on dit que c'est* ***l'indéterminée***

On peut alors écrire toute fonction polynomiale réelle sous la forme

$$\sum_{i=0}^{n} a_i X^i$$

ou même

$$\sum a_i X^i \qquad \text{les } a_n \text{ sont nuls à partir d'un certain rang}$$

II.2 Polynômes à coefficients complexes

Définition 7 (Polynômes complexes)**.**
Dans l'écriture précédente rien n'interdit de remplacer les coefficients par des complexes. Un ***polynôme à coefficients complexes*** *s'écrit sous la forme*

$$\sum_{i=0}^{n} a_i X^i \qquad a_0,\ a_1, \ldots,\ a_n \qquad \textbf{\textit{complexes}}$$

ou même

$$\sum a_i X^i \ \textit{ les } a_i \textit{ sont des complexes nuls à partir d'un certain rang}$$

Définition 8 (Les ensembles $\mathbb{R}[X]$, $\mathbb{C}[X]$ et $\mathbb{R}[X]$.)**.**
On note

1. *L'ensemble des polynômes à coefficients réels est noté $\mathbb{R}[X]$:*

$$\mathbb{R}[X] = \left\{ \sum_{i=0}^{n} a_i X^i \Big/ n \in \mathbb{N}, a_0,\ a_1,\ \ldots,\ a_n \textit{ des réels} \right\}$$

2. *L'ensemble des polynômes à coefficients complexes est noté* $\mathbb{C}[X]$ *:*

$$\mathbb{R}[X] = \left\{ \sum_{i=0}^{n} a_i X^i \Big/ n \in \mathbb{N}, a_0,\, a_1, \ldots, a_n \text{ des complexes} \right\}$$

3. *Si on n'a pas besoin de préciser l'ensemble auquel appartiennent les coefficients on utilise la notation* $\mathbb{K}[X]$.

Remarque : La notation $\mathbb{K}[X]$ n'apparait pas dans le programme, dans vos sujets il sera précisé si on étudie des polynômes à coefficients réels ou complexes (**scalaire**).

Vocabulaire

- les **scalaires** a_n sont les **coefficients**.
- X^i est le **monôme de degré** i.

Définition 9 (Polynôme nul)**.**
Le ***polynôme nul*** *est l'unique polynôme dont tous les coefficients sont nuls, on le note* 0 *ou* $O_{\mathbb{R}[X]}$

Définition 10 (Degré)**.**
Soit $P = \sum a_k X^k$ *un polynôme à coefficients dans* $\mathbb{K}$ ***non nul***

- *Le degré de* P *est le plus grand entier* n*, tel que* a_n *est non nul.*
- *Le coefficient associé est le* ***coefficient dominant****.*
- *Le polynôme nul à pour degré* $-\infty$.
- *Un polynôme de degré 0 est* ***constant****.*
- *Un polynôme de coefficient dominant égal à un est dit* ***unitaire****.*

Proposition 7 (Égalité de deux polynômes)**.**
Soit $P = \sum a_k X^k$ *et* $Q = \sum b_k X^k$ *deux éléments de* $\mathbb{K}[X]$

- $P = 0$ *si et seulement si tous ses coefficients sont nuls.*
- $P = Q$ *si et seulement si*

II.3 Propriétés

Définition 11 (Opérations)**.**
On munit l'ensemble $\mathbb{K}[X]$ des opérations suivantes : Soit $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux éléments de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ un réel ou un complexe.

1. ***Addition***

$$P + Q = \sum (a_k + b_k) X^k$$

On évite de noter $P \cdot \lambda$

2. ***Multiplication par un scalaire***

$$\lambda \cdot P = \sum \qquad X^k$$

3. ***Multiplication***

$$PQ = \sum c_k X^k \quad \text{où} \quad \forall k \in \mathbb{N} \qquad c_k =$$

Démonstration :

Proposition 8 (Propriétés des opérations)**.**
On admet que ces opérations ont les propriétés calculatoires usuelles (distributivité, associativité, commutativité)

On décide pour ce chapitre des conventions suivantes :

- Pour $n \in \mathbb{N}$, on a $-\infty < n$.
- Pour $n \in \mathbb{N}$, on a $-\infty + n = -\infty$.
- $-\infty + (-\infty) = -\infty$.

Proposition 9 (Degré et opérations)**.**

*Soit $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux éléments de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ un scalaire **non nul***

1. $$deg(P + Q) \leqslant \max(deg(P), deg(Q))$$

   *Il y a égalité **notamment** si $deg(Q) \neq deg(P)$*

2. $$deg(\lambda \cdot P) = deg(P)$$

3.
$$deg(PQ) = deg(P) + deg(Q)$$

Définition 12 (Ensemble des polynômes de degré inférieur à n)**.**
On note
$$\mathbb{K}_n[X] = \left\{P \in \mathbb{K}[X] \;/\; deg(P) \leqslant n\right\}$$

Les notations $\mathbb{R}_n[X]$ *et* $\mathbb{C}_n[X]$ *sont des cas particuliers utilisées si on veut préciser quel cas on étudie.*

On remarque que $\mathbb{K}_n[X]$ est stable par somme et par multiplication par un scalaire.

II.4 Autres opérations

Composée

Définition 13 (composée de deux polynômes)**.**
Soit $P = \sum_{k=0}^{n} a_k X^k$ *et* $Q = \sum_{k=0}^{m} b_k X^K$.
Alors on définit la composée de P *et* Q *par :*
$$P \circ Q = P(Q) = \sum_{k=0}^{n} a_k Q^k$$

Attention : A priori dans le cas général $P \circ Q \neq Q \circ P$

Remarque : Lorsque l'on écrit $P(X^2)$ cela revient à remplacer tous les X par des X^2

Proposition 10 (Degré d'une composée)**.**
Soit $P \in \mathbb{K}[X]$ *et* $Q \in K[X]$ *et* Q *non constant*
$$deg(P(Q)) =$$

Dérivation

Définition 14 (Dérivation)**.**

Soit P un polynôme $P = \sum_{k=0}^{n} a_k X^k$.
On définit le polynôme dérivé de P par

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}$$

Proposition 11 (Propriétés de la dérivation)**.**

Soit P et Q deux polynômes à coefficients dans $\mathbb{K}$ et λ et μ deux scalaires. Alors :

1. *Si $deg(P) \geqslant 1$ alors $deg(P') = deg(P) - 1$*
2. $\left(\lambda \cdot P + \mu \cdot Q\right)' = \lambda \cdot P' + \mu \cdot Q'$
3. $(PQ)' = P'Q + Q'P$
4. $(P \circ Q)' = Q'\left(P' \circ Q\right)$
5. *$P' = 0$ si et seulement si P est un polynôme constant.*
6. *Si $P' = Q'$ alors il existe $\lambda \in \mathbb{K}$ tel que $P = Q + \lambda$*

Définition 15 (Dérivées successives)**.**
Soit P un polynôme. On définit la dérivée n-ième de P que l'on note $P^{(n)}$ par :

$$\begin{cases} P^{(0)} = P \\ P^{(n+1)} = \left(P^{(n)}\right)' \end{cases}$$

III Racines et factorisation

III.1 Racines

Définition 16 (Racine)**.**
*Soit $P \in \mathbb{K}[X]$ on dit que $\alpha \in \mathbb{K}$ est **racine** de P si et seulement si $P(\alpha) = 0$*

Théorème 1 (Racine et factorisation)**.**
Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ alors les deux propositions suivantes sont équivalentes :

- *α est racine de P*
- *P s'écrit sous la forme $P = (X - \alpha)Q$ où Q est un polynôme*

Proposition 12 (Extension à plusieurs racines distinctes)**.**

Si $P \in \mathbb{K}[X]$ *est un polynôme non nul et si* α_1, $\alpha_2 \dots \alpha_n$ *sont des racines, distinctes deux à deux, de ce polynôme alors on peut trouver un polynôme Q tel que*

$$P = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) Q$$

Théorème 2 (Principe d'identification)**.**
Soit $P \in \mathbb{K}[X]$

- *Un polynôme non nul admet au maximum* $\deg(P)$ *racines distinctes.*
- *Si* P *est un polynôme qui admet strictement plus de racines que son degré alors* P *est nul*
- *Si* P *un polynôme tel que pour tout* α *réel* $P(\alpha) = 0$, *alors* P *est le polynôme nul, c'est à dire que tous ses coefficients sont nuls*
- *Si* $P = \sum a_n X^n$ *et* $Q = \sum b_n X^n$ *sont tels que pour une infinité de réels* α, $P(\alpha) = Q(\alpha)$ *alors*

$$\forall n \in \mathbb{N} \qquad a_n = b_n$$

III.2 Racines multiples

Définition 17 (Racines multiples)**.**
Soit $P \in \mathbb{K}[X]$. *On dit que* $\alpha \in \mathbb{K}$ *est une racine de multiplicité* n_α *de* P *si on peut factoriser* $(X - \alpha)^{n_\alpha}$ *dans* P *mais que l'on ne peut pas factoriser* $(X - \alpha)^{n_\alpha + 1}$

Proposition 13 (Caractérisation d'une racine multiple)**.**
. α *est une racine multiple de* P *si et seulement si* $P(\alpha) = P'(\alpha) = 0$

III.3 Factorisation

Théorème 3 (D'Alembert-Gauss)**.**
Soit $P \in \mathbb{C}[X]$ *si* P *n'est pas constant alors il existe* $\alpha \in \mathbb{C}$ *tel que* $P(\alpha) = 0$

Démonstration :
Admis (dur)

Attention : Ce théorème est faux dans $\mathbb{R}[X]$

III.3.a Dans $\mathbb{C}[X]$

Proposition 14 (Factorisation dans $\mathbb{C}[X]$)**.**
Soit P un polynôme de $\mathbb{C}[X]$ non nul alors il existe $\lambda \in \mathbb{C}$ et $z_1, z_2, \ldots, z_p$ des complexes tous distincts et $n_1, \ldots, n_p$ des entiers non nuls tels que

$$P = \lambda \prod_{i=1}^{p} (X - z_i)^{n_i}$$

Dans ce cas là, les z_i sont alors les racines de P et n_i est la multiplicité de z_i

Démonstration :

III.3.b Dans $\mathbb{R}[X]$

On a très souvent besoin de ce lemme, **à connaitre** et à savoir démontrer

***lemme* 1.**
Soit $P \in \mathbb{C}[X]$ tel que tous les coefficients de P soient réels. On suppose que α est racine de P.
Alors $\overline{\alpha}$ est racine de P de plus l'ordre de multiplicité de α et $\overline{\alpha}$ sont identiques.

Démonstration :

Proposition 15 (HP Factorisation dans $\mathbb{R}[X]$)**.**
Soit P un polynôme de $\mathbb{R}[X]$ non nul alors il existe $\lambda \in \mathbb{C}$,$a_1, a_2, \ldots a_p$ des réels tous disctincts ; et $n_1, \ldots, n_p$ des entiers naturels non nuls et $P_1, \ldots, P_r$ des polynômes de degré 2 sans racines et des entiers naturels non nuls $m_1 \ldots m_r$ tels que

$$P = \lambda \left[\prod_{i=1}^{p} (X - z_i)^{n_i} \right] P_1^{m_1} P_2^{m_2} \cdots P_r^{m_r}$$

Les z_i sont alors les racines de P et les n_i les multiplicités des z_i

Exemple : Factorisez X^3, $X^3 + X^2 + X + 1$, $X^4 + 2X^2 + 2$ dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

III.3.c HP Cas général du procédé d'indentification

Proposition 16 (Nombre maximum de racine)**.**
Soit $P \in \mathbb{K}[X]$ non nul alors le nombre de racines comptées avec leur multiplicité est inférieur au degré de P.
Dans le cas de $\mathbb{C}[X]$ il y a égalité.

Démonstration :
Cela découle rapidement de la factorisation d'un polynôme

IV Résultats classiques qui ne sont pas au programme

Attention : Les résultats suivants ne peuvent pas être utilisés directement, dans le programme officiel ils sont décrits comme "ne sont pas des attendus du programme"

IV.1 Racines de l'unité

Soit n un entier naturel non nul, on cherche à résoudre dans $\mathbb{C}$, l'équation :

$$z^n = 1 \tag{E.1}$$

On cherche z sous la forme exponentielle *i.e.* $z = \rho e^{\mathbf{i}\theta}$ avec $\rho \geqslant 0$

$$\begin{aligned}
z^n = 1 &\Leftrightarrow \left(\rho e^{\mathbf{i}\theta}\right)^n \\
&\Leftrightarrow \rho^n e^{\mathbf{i}n\theta} && \text{à l'aide de la formule de Moivre} \\
&\Leftrightarrow \left\{ \begin{array}{ccc} \rho^n & = & 1 \\ n\theta & \equiv & 0[2\pi] \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{ccc} \rho & = & 1 \\ \exists k \in \mathbb{Z} \quad \theta & = & k\dfrac{2\pi}{n} \end{array} \right. && \text{car } \rho \text{ est un réel positif}
\end{aligned}$$

Comptons le nombre de solutions différentes.

$$\left\{ e^{\mathbf{i}\cdot k\frac{2\pi}{n}} \Big/ k \in \mathbb{Z} \right\}$$

Soit ω une solution, et soit $k \in \mathbb{Z}$ tel que $\omega = e^{\mathbf{i}\,k\frac{2\pi}{n}}$. On effectue la division euclidienne de k par n, alors on trouve q et r deux entiers qui vérifient :

$$k = q \cdot n + r \qquad 0 \leqslant r < n$$

Donc :

$$e^{\mathbf{i}\,k\frac{2\pi}{n}} = e^{\mathbf{i}\,r\frac{2\pi}{n}}$$

Toutes les solutions sont de la forme

$$e^{\mathbf{i}\,r\frac{2\pi}{n}} \qquad r \in [\![0, n-1]\!]$$

Ces complexes sont tous différents.
On effet soit $k \in [\![0, n-1]\!]$ et $\ell \in [\![0, n-1]\!]$ tels que

$$e^{\mathbf{i}\,k\frac{2\pi}{n}} = e^{\mathbf{i}\,\ell\frac{2\pi}{n}}$$

alors

$$k\frac{2\pi}{n} \equiv \ell\frac{2\pi}{n}\,[2\pi]$$

Soit $m \in \mathbb{Z}$ tel que :

$$k\frac{2\pi}{n} = k\frac{2\pi}{n} + m2\pi$$

et donc on obtient :

$$k - \ell = mn$$

or

$$0 \leqslant k \leqslant n-1 \qquad 0 \leqslant \ell \leqslant n-1$$

et donc

$$1 - n \leqslant k - \ell \leqslant n - 1$$

donc

$$1 - n \leqslant mn \leqslant n - 1$$

ce qui montre [1]

$$m = 0$$

et finalement

$$k = \ell$$

Résultat à utiliser directement

Proposition 17 (Racines n-ième de l'unité)**.**

1. en faisant une démonstration par l'absurde

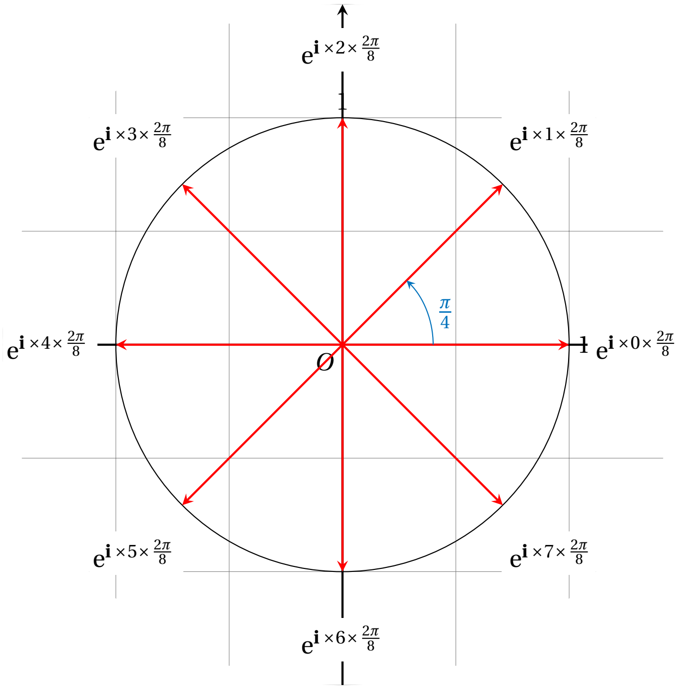
Soit $n \in \mathbb{N}^*$, alors l'équation :

$$z^n = 1$$

admet exactement n racines distinctes qui sont

$$\left\{ e^{\boldsymbol{i} \cdot k \frac{2\pi}{n}} \Big/ k \in [\![0, n-1]\!] \right\}$$

*Ce sont les **racines** n**-ièmes de l'unité**.*



racines 8 ièmes de l'unité

Annexe : formules de trigonométrie

Proposition 18 (formules d'addition)**.**
Soit α et β des réels tels que les quantités suivantes soient définies. Alors

1. $\cos\left(\alpha+\beta\right) = \cos(\alpha)\cos\left(\beta\right) - \sin(\alpha)\sin\left(\beta\right)$
2. $\cos(2\alpha) = \cos^2\alpha - \sin^2\alpha = 1 - 2\sin^2\alpha = 2\cos^2\alpha - 1$
3. $\sin\left(\alpha+\beta\right) = \sin(\alpha)\cos\left(\beta\right) + \sin\left(\beta\right)\cos(\alpha)$
4. $\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$
5. * $\tan\left(\alpha+\beta\right) = \dfrac{\tan\alpha+\tan\beta}{1-\tan\alpha\tan\beta}$
6. *$\tan 2\alpha = \dfrac{2\tan\alpha}{1-\tan^2\alpha}$

Proposition 19 (Formule de factorisation)**.**
Soit α et β des réels

1. $\cos\alpha + \cos\beta = 2\cos\dfrac{\alpha+\beta}{2}\cos\dfrac{\alpha-\beta}{2}$
2. $\cos\alpha - \cos\beta = -2\sin\dfrac{\alpha+\beta}{2}\sin\dfrac{\alpha-\beta}{2}$
3. $\sin\alpha + \sin\beta = 2\sin\dfrac{\alpha+\beta}{2}\cos\dfrac{\alpha-\beta}{2}$
4. $\sin\alpha - \sin\beta = 2\sin\dfrac{\alpha-\beta}{2}\cos\dfrac{\alpha+\beta}{2}$

Proposition 20 (Formules de l'arc moitié)**.**
Soit $\alpha \in \mathbb{R}\setminus\{\frac{\pi}{4} + k\frac{\pi}{2} \;/\; k \in \mathbb{Z}\}$; on pose $t = \tan\dfrac{\alpha}{2}$.
Alors :

$$\cos\alpha = \frac{1-t^2}{1+t^2} \qquad \sin\alpha = \frac{2t}{1+t^2}$$

Si de plus $t \neq \pm 1$

$$\tan\alpha = \frac{2t}{1-t^2}$$