102

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

I) Structure du groupe des nombres complexes de module 1

1) Exponentielle complexe

Définition 1 : On note $\mathbb{U}$ le noyau du morphisme de groupes $\begin{cases} (\mathbb{C}^*, \times) \longrightarrow (\mathbb{R}^*, \times) \\ z \longmapsto |z| \end{cases}$. Il s'agit du groupe des nombres complexes de module 1.

Proposition 2 : $\exp : \begin{cases} (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times) \\ t \longmapsto e^{it} \end{cases}$ est un morphisme de groupes injectif, de noyau $2\pi\mathbb{Z}$.

Corollaire 3 : $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{R}/\mathbb{Z}$. $[t] \in \mathbb{R}/2\pi\mathbb{Z}$ est appelé argument de e^{it}.

Remarque 4 : Lorsqu'on identifie $\mathbb{C}$ à $\mathbb{R}^2$, $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{S}^1$. Il s'agit d'un homéomorphisme pour la topologie induite par $\mathbb{C}$ sur $\mathbb{U}$. On a le théorème de relèvement : si $\varphi : \mathbb{R} \longrightarrow \mathbb{U}$ est continue, il existe $\theta \in \mathcal{C}(\mathbb{R}, \mathbb{R})$ tq $\varphi = \exp \circ \theta$.

. trigonométrie :

Définition 5 : $\forall x \in \mathbb{R}$, $\cos x = \mathrm{Re}(\exp x)$ et $\sin x = \mathrm{Im}(\exp x)$

Proposition 6 : - cos et sin sont 2π-périodiques (on peut les définir sur $\mathbb{R}/2\pi\mathbb{Z}$ par passage au quotient).

- Formules d'Euler : $\forall t \in \mathbb{R}$, $\cos(t) = \dfrac{e^{it}+e^{-it}}{2}$, $\sin(t) = \dfrac{e^{it}-e^{-it}}{2i}$
- $\cos^2 + \sin^2 = 1$
- $\forall a, b \in \mathbb{R}$, $\begin{cases} \cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b) \\ \sin(a+b) = \sin(a)\cos(b) + \cos(a)\sin(b) \end{cases}$
- $\forall a \in \mathbb{R}$, $\cos(a) = \sin\left(a + \frac{\pi}{2}\right)$, $\sin(a) = \cos\left(a - \frac{\pi}{2}\right)$

Remarque 7 : Les formules trigonométriques usuelles se déduisent à partir de celles ci-dessus.

Application 8 : Calcul des noyaux de Dirichlet et de Fejér :

$\forall t \in \mathbb{R}$, $D_n(t) = \sum_{k=-n}^{n} e^{ikt} = \dfrac{\sin[(n+1/2)t]}{\sin[t/2]}$, $K_n(t) = \dfrac{1}{n}\sum_{k=0}^{n-1} D_k(t) = \dfrac{\sin[nt/2]^2}{n\sin[t/2]^2}$

Application 9 : Polynômes de Tchebychev :

$\forall n \in \mathbb{N}$, $\exists ! P_n \in \mathbb{R}_n[X]$, $\forall \theta \in \mathbb{R}$, $P_n(\cos\theta) = \cos(n\theta)$

les racines de P_n sont exactement les $\cos\left(\frac{2k+1}{2n}\pi\right)$, pour $k \in [\![0, n-1]\!]$.

On peut linéariser $\cos(k\theta)$ et $\sin(k\theta)$ en fonction de $\cos(\theta)$ et $\sin(\theta)$.

Par exemple, $\cos(5\theta) = 16\cos^5\theta - 15\cos^3\theta + 10\cos\theta$

Application 10 : Localisation de racines de polynômes :

$X^n - Y^n = \prod_{k=0}^{n-1}\left(X - e^{\frac{2ik\pi}{n}}Y\right)$

le polynôme $P(X) = \sum_{k=0}^{n}\binom{n}{k}\sin(k\theta)X^k$ n'a que des racines réelles.

2) Rotations et angles orientés du plan

Proposition 11 : L'action de $SO_2(\mathbb{R})$ sur $\mathbb{U}$ identifié à $\mathbb{S}^1$ par multiplication à gauche est simplement transitive. $\mathbb{U}$ est donc en bijection avec $SO_2(\mathbb{R})$.

Proposition 12 : $\begin{cases} \mathbb{R}/2\pi\mathbb{Z} \longrightarrow SO_2(\mathbb{R}) \\ \theta \longmapsto R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{cases}$ est un isomorphisme de groupes et un isomorphisme d'action.

Exemple 13 : Pour tout $\theta \in \mathbb{R}/2\pi\mathbb{Z}$, $\exp(\theta I_2) = R_\theta$

Définition 14 : On appelle angle orienté de vecteurs une orbite sous l'action produit de $SO_2(\mathbb{R})$ sur $\mathbb{U}^2$. On note $\mathcal{A}$ l'ensemble des angles orientés.

Proposition 15 : L'action de $SO_2(\mathbb{R})$ sur $\mathbb{U}^2$ est libre. En particulier, $\mathcal{A} \simeq \mathbb{R}/2\pi\mathbb{Z}$

Définition 16 : On appelle mesure de l'angle orienté $\widehat{(u,v)}$ l'image de $\widehat{(u,v)}$ par la bijection $\mathcal{A} \xrightarrow{\sim} \mathbb{R}/2\pi\mathbb{Z}$. On définit le cosinus et le sinus de $\widehat{(u,v)}$ comme ceux de sa mesure.

Exemple 17 : - $\widehat{(e_1, e_2)}$ est de mesure $\frac{\pi}{2}$; $\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$ (annexe 1)

- $\widehat{(\overrightarrow{OA}, \overrightarrow{OB})}$ est de mesure l'argument du complexe $\frac{z_B}{z_A}$.

3) Sous-groupes de $\mathbb{U}$

Proposition 18 : Tout sous-groupe de $(\mathbb{R}, +)$ est soit de la forme $a\mathbb{Z}$, avec $a \in \mathbb{R}$, soit dense dans $\mathbb{R}$, pour la topologie définie par la valeur absolue.

Exemple 19 : Tout sous-groupe de $\mathbb{U}$ est dense ou cyclique (ou les deux).

Exemple 20 : - $\left(e^{\frac{2ik\pi}{n}}\right)_{k \in [\![0, n-1]\!]}$ est cyclique et fini.

- $(e^{iz})_{z \in \mathbb{Z}}$ est dense dans $\mathbb{U}$, et cyclique.

Application 21 : $\{\cos(n), n \in \mathbb{Z}\}$ et $\{\sin(n), n \in \mathbb{Z}\}$ sont denses dans $[-1, 1]$.

Proposition 22 : Les sous-groupes compacts de $(\mathbb{C}^*, \times)$ sont $\mathbb{U}$ et ses sous-groupes cycliques, qui sont finis ou denses dans $\mathbb{U}$.

II) Racines de l'unité

1) Etude algébrique des sous-groupes finis de $\mathbb{U}$

Proposition 23 : $\forall n \in \mathbb{N}^*$, $\mathbb{U}$ admet un unique sous-groupe d'ordre n, noté μ_n. Il s'agit de l'ensemble des racines du polynôme $X^n - 1 \in \mathbb{C}[X]$, et :

$\mu_n = \left\{e^{\frac{2ik\pi}{n}}, k \in [\![0, n-1]\!]\right\}$.

. Dans toute la suite, n désigne un entier naturel non nul.

Remarque 24 : - $\forall z \in \mu_n$, $\overline{z} \in \mu_n$ et $\overline{z} = z^{-1}$
- Si $n \geq 2$, $\sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = 0$
- Si $a \in \mathbb{C}$, $z^n = a \iff z \in \left\{ |a|^{\frac{1}{n}} e^{\frac{2ik\pi + \arg(a)}{n}}, k \in [\![0, n-1]\!] \right\}$

Proposition 25 : $\begin{cases} (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (\mu_n, \times) \\ \overline{k} \longmapsto \exp\left(\frac{2ik\pi}{n}\right) \end{cases}$ est un isomorphisme de groupes.

Corollaire 26 : Les générateurs de μ_n sont les $e^{\frac{2ik\pi}{n}}$, avec $k \wedge n = 1$. Si φ désigne l'indicatrice d'Euler, il y a $\varphi(n)$ générateurs de μ_n.

Exemple 27 : - $\mu_3 = \{1, j, \overline{j}\}$, avec $j = e^{\frac{2i\pi}{3}}$. $\mu_3 \simeq \mathbb{Z}/3\mathbb{Z}$, et a pour générateurs j et $\overline{j}$. $X^3 - 1 = (X-1)(X^2+X+1)$, donc j et $\overline{j}$ sont les racines complexes conjuguées de $X^2 + X + 1$.

- $\mu_4 = \{1, i, -1, -i\} \simeq \mathbb{Z}/4\mathbb{Z}$, et a pour générateurs i et $-i$.

Corollaire 28 : Lemme de prolongement des caractères :
Soit G un groupe fini et H un sous-groupe de G. Soit χ un caractère de H (morphisme de H dans $(\mathbb{C}^*, \times)$). Il existe un unique caractère $\widetilde{\chi} : G \longrightarrow \mathbb{C}^*$ tel que $\widetilde{\chi}_{|H} = \chi$.

Théorème 29 : Théorème de structure des groupes abéliens finis :
Soit G un groupe abélien fini. Il existe $d_1 | \cdots | d_n \in \mathbb{Z}$ tels que, de manière unique à permutation des facteurs près, $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$.

Application 30 : Classification des groupes abéliens d'ordre $600 = 2^3 \times 3 \times 5^2$:
$\mathbb{Z}/600\mathbb{Z}$; $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/300\mathbb{Z}$; $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/150\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

2) Spectres de matrices d'ordre fini

Proposition 31 : Les valeurs propres d'une matrice d'ordre fini (de $M_n(\mathbb{C})$) sont des racines de l'unité.

Exemple 32 : L'application $\begin{cases} (\mathfrak{S}_n, \circ) \longrightarrow (GL_n(\mathbb{C}), \times) \\ \sigma \longmapsto M_\sigma \end{cases}$, avec $[M_\sigma]_{i,j} = \delta_{i,\sigma(j)}$ $(1 \leq i, j \leq n)$ est un morphisme de groupes. Alors, $Sp(M_\sigma) \subset \mu_{(n!)}$

Exemple 33 : Si $M = \begin{pmatrix} a & b & c & \cdots & c \\ c & a & b & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & c \\ b & \ddots & \ddots & a & b \\ c & \cdots & c & b & a \end{pmatrix}$ (matrice circulante) $\in M_n(\mathbb{C})$, $Sp(M) = \mu_n$.

Application 34 : Soit $z^{(0)} = (z_1^{(0)}, \ldots, z_n^{(0)}) \in \mathbb{C}^n$, et la suite $z^{(k)}$ définie par récurrence :
$\forall k \geq 0$, $z^{(k+1)} = \left(\frac{z_1^{(k)} + z_2^{(k)}}{2}, \frac{z_2^{(k)} + z_3^{(k)}}{2}, \ldots, \frac{z_n^{(k)} + z_1^{(k)}}{2} \right)$ (annexe 2)
Si $g = \sum_{j=1}^{n} \frac{z_i}{n}$, $(z^{(k)})_{k \geq 0}$ converge dans $\mathbb{C}^n$ vers $(g, \ldots, g)$

DEVELOPPEMENT 1

Exemple 35 : Soit G un groupe fini et $\rho : G \longrightarrow GL(V)$ une représentation de G (linéaire) dans V un $\mathbb{C}$-espace vectoriel de dimension finie. Pour tout $g \in G$, les valeurs propres de $\rho(g)$ sont des racines $|G|$-ièmes de l'unité.

3) Cyclotomie

Définition 36 : μ_n^* est l'ensemble des éléments de μ_n d'ordre n. Il s'agit de l'ensemble des générateurs de μ_n, et en particulier, $|\mu_n^*| = \varphi(n)$.

Définition 37 : On définit le n-ième polynôme cyclotomique dans $\mathbb{C}[X]$ par :
$$\Phi_n(X) = \prod_{\lambda \in \mu_n^*} (X - \lambda)$$
En particulier, Φ_n est unitaire et $\deg \Phi_n = \varphi(n)$.

Proposition 38 : $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d | n} \Phi_d(X)$

Application 39 : Calcul récursif des polynômes cyclotomiques :

$\Phi_1(X) = X - 1$ $(\mu_1^* = \{1\})$	$\Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$
$\Phi_2(X) = X + 1$ $(\mu_2^* = \{-1\})$	$\Phi_4(X) = \frac{X^4 - 1}{(X-1)(X+1)} = X^2 + 1$

Remarque 40 : $\Phi_n(X) \in \mathbb{Z}[X]$

Application 41 : Théorème de Wedderburn :
Tout corps fini est commutatif

DEVELOPPEMENT 2

- Irréductibilité :

Proposition 42 : Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$.

Contre-exemple 43 : Ceci est faux sur un corps fini : $\Phi_8 = X^4 + 1$ est réductible sur tout $\mathbb{F}_q$.

Théorème 44 (Kronecker) : Soit $P \in \mathbb{Z}[X]$, unitaire, tel que $P(0) = 0$, et dont les racines sont de module inférieur ou égal à 1. Alors, ses racines sont des racines de l'unité, et P est un produit de polynômes cyclotomiques.
Si P est irréductible, P est un polynôme cyclotomique.

III) Applications à divers domaines de l'algèbre

1) Algorithmique : Transformée de Fourier rapide

On se fixe $\omega \in \mu_n^*$ (une racine primitive n-ième de l'unité).

Proposition 45 : $DFT_\omega : \begin{cases} \mathbb{C}[X]/(X^n - 1) \longrightarrow \mathbb{C}^n \\ F \longmapsto (F(1), \ldots, F(\omega^{n-1})) \end{cases}$ est un isomorphisme de $\mathbb{C}$-algèbres.

Proposition 46: Dans les bases $\{1, X, \dots, X^{n-1}\}$ sur $\mathbb{C}[X]/(X^n-1)$ et canonique sur $\mathbb{C}^n$, $\mathrm{mat}(\mathrm{DFT}_\omega) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{pmatrix} = V_\omega$, d'inverse $V_\omega^{-1} = \frac{1}{n} V_{\omega^{-1}}$.

Algorithme 47: Soient $n = 2^d$, $F = \sum_{j=0}^{n-1} f_j X^j$ et ω^j calculées pour $0 \le j \le n-1$.
- Si $n=1$, renvoyer f_0.
- Sinon, poser $k = n/2$ (stratégie "diviser pour régner"). Calculer :
  $R_0(X) = \sum_{j=0}^{k-1} (f_j + f_{j+k}) X^j$
  $R_1(X) = R_0(\omega X) = \sum_{j=0}^{k-1} (f_j - f_{j+k}) \omega^j X^j$
- Calculer récursivement $\{R_0(1), R_0(\omega^2), \dots, R_0(\omega^{2(k-1)})$
  $\{R_1(1), R_1(\omega^2), \dots, R_1(\omega^{2(k-1)})$
- Renvoyer $(R_0(1), R_1(1), \dots, R_0(\omega^{(k-1)}), R_1(\omega^{(k-1)}))$

Application 48: Multiplication de polynômes en $O(n \log_2 n)$ opérations.

$P_1(X) = X^2 + 5X + 3$ $\Rightarrow$ $\mathrm{DFT}_i(P_1) = (9, 2+5i, -1, 2-5i)$
$P_2(X) = 6X + 7$ $\Rightarrow$ $\mathrm{DFT}_i(P_2) = (13, 7+6i, 1, 7-6i)$

$\Rightarrow \mathrm{DFT}_i(P_1 P_2) = (117, -16+47i, -1, -16-47i)$

$\Rightarrow \mathrm{DFT}_{-i}[\mathrm{DFT}_i(P_1 P_2)] = (84, 212, 148, 24) = \frac{1}{4}(21, 53, 37, 6)$

$\Rightarrow (P_1 P_2)(X) = 6X^3 + 37X^2 + 53X + 21$

2) Géométrie : Constructibilité à la règle et au compas

Définition 49: Un nombre complexe est dit constructible s'il est contenu dans une extension quadratique itérée de $\mathbb{Q}$.

Exemples 50:
- 1 et $\cos(\frac{2\pi}{5})$ sont constructibles.
- Si z est constructible, $\frac{1}{z}$ et $\sqrt{|z|}$ le sont
- Si z et z' sont constructibles, $z+z'$ et zz' le sont.
- e, $\sqrt[3]{2}$ et $\cos(\frac{\pi}{9})$ ne sont pas constructibles.

Remarque 51: Cela revient à dire qu'un nombre est constructible si, et seulement s'il est à l'intersection de droites ou de cercles tracés à partir d'un ensemble lui-même constitué de nombres constructibles (on parle de construction à la règle et au compas d'un nombre constructible).

Définition 52: Un polygone est dit constructible si ses sommets le sont.

Proposition 53: le polygone régulier à n côtés est constructible si, et seulement si $e^{\frac{2i\pi}{n}}$ est un nombre constructible.

Théorème 54 (Gauss-Wantzel): le polygone régulier à n côtés est constructible si, et seulement si $n = 2^\alpha p$, avec $\alpha \in \mathbb{N}$ et p un produit de nombres premiers de la forme $(1 + 2^{2^\beta})$, $\beta \in \mathbb{N}$.

Application 55 : Construction du pentagone régulier à la règle et au compas (annexe 3)

3) Représentations : Intégralité des tables de caractères

Dans cette partie, on se donne G un groupe fini et χ un caractère de G, i.e. un morphisme de G dans $(\mathbb{C}^*, \times)$. On note $n = |G|$.

Proposition 56 : Pour tout $g \in G$, $\chi(g)$ est un entier algébrique.

Corollaire 57 : Les degrés des représentations irréductibles de G divisent l'ordre de G.

Corollaire 58 : Si χ est à valeurs dans $\mathbb{Q}$, alors χ est à valeurs dans $\mathbb{Z}$.

- Condition nécessaire et suffisante d'intégralité :

Soit ω une racine primitive n-ième de l'unité.

Proposition 59 : Pour tout k tel que $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$, il existe un unique automorphisme de corps $\sigma_k : \mathbb{Q}[X]/(\Phi_n) \longrightarrow \mathbb{Q}[\omega]$ qui fixe $\mathbb{Q}$ et qui envoie ω sur ω^k (Φ_n désigne le n-ième polynôme cyclotomique).

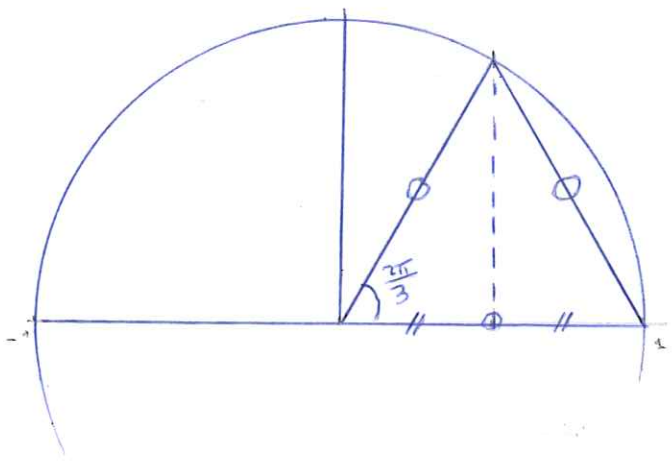
Proposition 60 : Pour tout $\alpha \in \mathbb{Q}[\omega]$ (resp. $\mathbb{Z}[\omega]$), $\sigma_k(\alpha) = \alpha$ pour tout k tel que $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ si, et seulement si $\alpha \in \mathbb{Q}$ (resp. $\alpha \in \mathbb{Z}$).

Proposition 61 : χ est invariant par $(\mathbb{Z}/n\mathbb{Z})^*$ si, et seulement si χ est à valeurs dans $\mathbb{Z}$ (pour tout $g \in G$, $\chi(g^k) = \sigma_k(\chi(g))$).

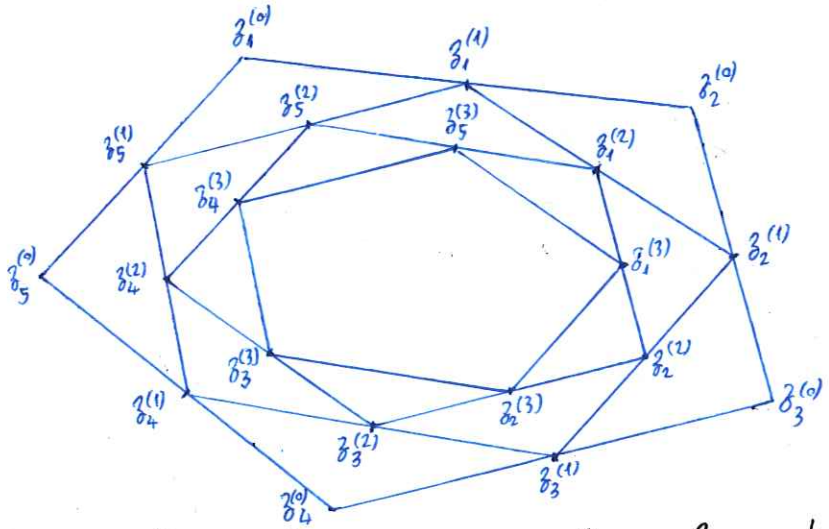
Corollaire 62 : La table de caractères de G est à valeurs dans $\mathbb{Z}$ si, et seulement si pour tout $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ et tout $g \in G$, g et g^k sont conjugués.

Application 63 : Si $G = \mathfrak{S}_n$, le corollaire 62 s'applique : pour tout $n \in \mathbb{N}$, la table de caractères de $\mathfrak{S}_n$ est entière.

Annexe 1

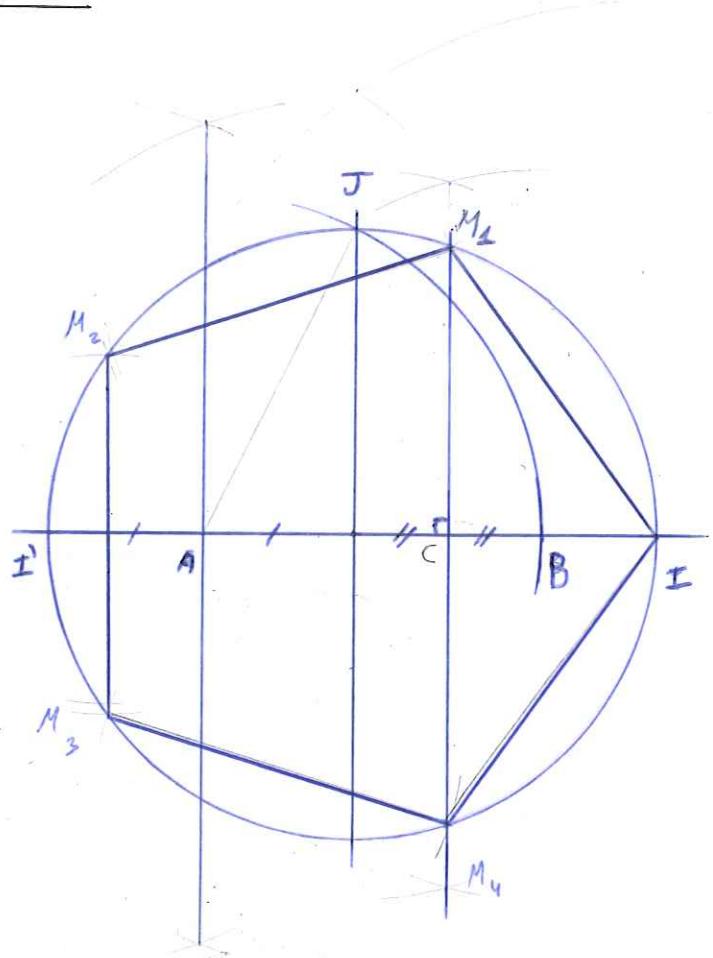


Annexe 2



Convergence d'une suite de polygones vers leur isobarycentre

Annexe 3



Construction du pentagone régulier à la règle et au compas