Université de Rennes

Mémoire - Préparation à l'agrégation

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

Alice MORINIÈRE

Mémoire encadré par Matthieu Romagny

Année 2023-2024

Table des matières

Introduction

Si les nombres complexes ont été introduits initialement afin de résoudre des équations polynomiales, notamment de degré 3, ils ont depuis leur apparition permis de faire avancer ou de simplifier de nombreux domaines des mathématiques. Ils sont par exemple utilisés en géométrie plane ou pour l'analyse de Fourier ; ils ont permis le développement de toute l'analyse complexe, qui elle-même fait avancer d'autres domaines ; leur ensemble offre l'exemple le plus simple de corps algébriquement clos ; et l'on pourrait continuer la liste encore longtemps.
Le groupe des nombres complexes de module 1 ne déroge pas à cette règle : il est omniprésent dans beaucoup de champs des mathématiques. Il s'interprète sous différents points de vue complémentaires. On peut le considérer comme étant le cercle unité du plan complexe, et étudier ses propriétés topologiques, ou le voir comme l'un des exemples les plus basiques de sous-variété. On peut l'observer avec un regard plus algébrique, en considérant par exemple ses sous-groupes contenant des racines de l'unité, qui ont de nombreuses applications comme nous le verrons. Et l'on peut mêler la géométrie à tout ça, en l'utilisant pour faire de la géométrie plane, et pour étudier des problèmes de constructibilité à la règle et au compas. De nouveau, il n'est pas possible de tout passer en revue, et il ne sera pas possible de le faire non plus à travers ce plan, mais nous allons tout de même essayer d'adopter différents points de vue sur ce groupe, et d'observer diverses applications.

1 Le plan complexe

1.1 Fonctions trigonométriques [Jea92]

Avant de parler du groupe des nombres complexes de module 1, effectuons quelques rappels sur les fonctions trigonométriques qui nous seront utiles pour la suite.

Définition 1.1.1. *On définit l'exponentielle comme la fonction entière suivante :*

$$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}. \end{aligned}$$

On définit également cosinus et sinus par $\cos(x) = \mathrm{Re}(e^{ix})$ *et* $\sin(x) = \mathrm{Im}(e^{ix})$ *pour* $x \in \mathbb{R}$*, on a donc* $e^{ix} = \cos(x) + i\sin(x)$.

De ces définitions découlent des formules classiques utiles pour jongler avec les fonctions trigonométriques.

Proposition 1.1.2. •*Soit* $x \in \mathbb{R}$*, alors*

$$\cos^2(x) + \sin^2(x) = 1.$$

•***Formule de Moivre :*** *Soit* $x \in \mathbb{R}$ *et* $n \in \mathbb{Z}$*, alors*

$$e^{inx} = \cos(nx) + i\sin(nx).$$

•***Formule d'Euler :*** *Soit* $x \in \mathbb{R}$*, alors*

$$\cos(x) = \frac{e^{ix} + e^{-ix}}{2} \quad et \quad \sin(x) = \frac{e^{ix} - e^{-ix}}{2i}.$$

Application 1.1.3. *Ces formules peuvent être utilisées pour linéariser* $\cos^n(x)$ *ou* $\sin^n(x)$ *pour* $x \in \mathbb{R}$ *et* $n \in \mathbb{Z}$*, c'est à dire les exprimer comme une combinaison linéaire de cosinus et sinus de multiples de* x*, ou également pour exprimer* $\cos(nx)$ *et* $\sin(nx)$ *comme des polynômes en* $\cos(x)$ *et* $\sin(x)$ *respectivement.*

Application 1.1.4. *Ces formules permettent également de calculer par exemple le noyau de Dirichlet qui apparaît dans l'étude des séries de Fourier : pour* $N \in \mathbb{N}$*, et* $x \in \mathbb{R}$*,*

$$D_N(x) = \sum_{k=-N}^{N} e^{ikx} = 1 + 2\sum_{k=1}^{N} \cos(kx) = \frac{\sin(\frac{2N+1}{2}x)}{\sin(\frac{x}{2})}.$$

1.2 Groupe des nombres complexes de module 1 [Jea92]

Nous allons maintenant définir le groupe des nombres complexes de module 1.

Définition 1.2.1. *On définit* $\mathbb{U}$ *le groupe des nombres complexes de module 1 comme le noyau du morphisme de groupes :*

$$\begin{aligned} |.| : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}_+^*, \times) \\ z &\longmapsto |z|. \end{aligned}$$

Il s'agit donc d'un sous-groupe multiplicatif de $(\mathbb{C}^*, \times)$*, qui contient les* $z \in \mathbb{C}^*$ *tel que* $|z| = 1$*.*

Exemple 1.2.1. *Les nombres* 1*,* -1*,* i*,* $-i$ *sont dans* $\mathbb{U}$*.*

Remarque 1.2.2. *Si l'on identifie* $\mathbb{C}$ *à* $\mathbb{R}^2$*, le groupe* $\mathbb{U}$ *représente le cercle unité* $\mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2, x^2 + y^2 = 1\}$*. On notera donc le groupe* $\mathbb{U}$ *lorsque l'on évoquera ses propriétés plutôt algébriques, et* $\mathbb{S}^1$ *lorsque l'on évoquera ses propriétés plutôt topologiques, ou sa représentation dans le plan.*

Théorème 1.2.3. *L'application*

$$\begin{aligned} \mathbb{R}_+^* \times \mathbb{U} &\longrightarrow \mathbb{C}^* \\ (r, u) &\longmapsto ru \end{aligned}$$

définit un isomorphisme de groupe.

Grâce à l'exponentielle redéfinie précédemment, nous pouvons obtenir une nouvelle description du groupe $\mathbb{U}$.

Théorème 1.2.4. *L'application*

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{U} \\ x &\longmapsto e^{ix} \end{aligned}$$

est un morphisme de groupes surjectif de noyau $2\pi\mathbb{Z}$*. Ainsi, grâce au premier théorème d'isomorphisme,*

$$\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z}.$$

Enfin, on peut s'intéresser à des propriétés topologiques du groupe. On sait que $\mathbb{U}$ est muni de la topologie issue de la topologie usuelle sur $\mathbb{C}$, de même pour $\mathbb{S}^1$ munie de la topologie issue de la topologie usuelle sur $\mathbb{R}^2$, et on peut munir $\mathbb{R}/2\pi\mathbb{Z}$ de la topologie quotient. La bijection entre $\mathbb{U}$ et $\mathbb{S}^1$ est alors un homéomorphisme, et l'isomorphisme de groupes obtenu dans le théorème précédent définit en fait un homéomorphisme entre les deux groupes. S'intéresser aux propriétés topologiques du cercle unité $\mathbb{S}^1$ nous permet donc d'en déduire des propriétés sur notre groupe.

Proposition 1.2.5. *L'ensemble $\mathbb{S}^1$ est compact et connexe par arcs.*

1.3 Géométrie plane [Jea92] [Aud98] [Com21] [Rom21]

Les nombres complexes de module 1 ont de nombreuses applications en géométrie plane, nous allons ici en voir quelques-unes. Tout d'abord, grâce au théorème 1.2.4, on peut définir la notion d'argument d'un nombre complexe.

Définition 1.3.1. *Soit $z \in \mathbb{C}^*$. On appelle argument de z un réel θ tel que $e^{i\theta} = \frac{z}{|z|}$. L'ensemble des arguments de z sera noté $\arg(z)$. Si $\theta \in \arg(z)$, on appelle forme polaire ou forme trigonométrique de z la décomposition $z = |z|e^{i\theta}$.*

Remarque 1.3.2. *La forme polaire est pratique pour multiplier des complexes, ou les élever à une certaine puissance.*

Proposition 1.3.3. *Si $z \in \mathbb{C}^*$, alors $\arg(z)$ est non vide et pour tout θ_0 dans $\arg(z)$, on a*

$$\arg(z) = \theta_0 + 2\pi\mathbb{Z}.$$

Définition 1.3.4. *Soit $z \in \mathbb{C}^*$. On appelle argument principal de z et on note $\mathrm{Arg}(z)$ l'unique élément de $\arg(z) \cap [-\pi, \pi[$.*

Remarque 1.3.5. *Cette notion d'argument principal permet notamment de définir la détermination principale du logarithme complexe.*

Proposition 1.3.6. *Soit $z \in \mathbb{S}^1 \setminus \{(-1,0)\}$, les coordonnées de z sont données par*

$$\cos(\theta) = \frac{1-t^2}{1+t^2} \quad et \quad \sin(\theta) = \frac{2t}{1+t^2},$$

où θ est l'argument principal de z, et $t = \tan(\frac{\theta}{2})$. On obtient alors deux paramétrisations de $\mathbb{S}^1$:

$$\begin{aligned} [-\pi, \pi[&\longrightarrow \mathbb{S}^1 \\ \theta &\longmapsto (\cos(\theta), \sin(\theta)) \end{aligned}$$

et

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{S}^1 \\ t &\longmapsto (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}). \end{aligned}$$

Application 1.3.7. *La seconde paramétrisation est utile pour trouver les triplets pythagoriciens, c'est à dire les triplets (a,b,c) d'entiers naturels non nuls vérifiant la relation de Pythagore : $a^2+b^2=c^2$. On obtient alors que tous les triplets qui fonctionnent sont de la forme $\Big(d(u^2-v^2), 2duv, d(u^2+v^2)\Big)$, où $u, v \in \mathbb{N}^*$ sont premiers entre eux, et $d \in \mathbb{Z}$.*

Enfin, nous allons définir la notion d'angle orienté, que l'on pourra facilement relier à la notion d'argument.

Proposition 1.3.8. *Soit $u, v \in \mathbb{S}^1$. Il existe une unique rotation qui envoie u sur v.*

Remarque 1.3.9. *En termes d'action de groupe, cela signifie que $SO_2(\mathbb{R})$ agit simplement transitivement sur $\mathbb{S}^1$.*

Définition 1.3.10. *On définit sur $\mathbb{S}^1$ la relation d'équivalence $\mathscr{R}$, où $(u,v)\mathscr{R}(u',v')$ si et seulement s'il existe une rotation qui envoie u sur v et u' sur v'. La classe d'équivalence de (u,v) pour cette relation est appelée angle orienté de u et v. On note $\mathscr{A}$ l'ensemble des angles orientés, i.e. l'ensemble des classes d'équivalence sous $\mathscr{R}$.*

Proposition 1.3.11. *L'application de $\mathscr{A}$ dans $SO_2(\mathbb{R})$ qui a un couple (u,v) associe l'unique rotation qui envoie u sur v est une bijection.*

Remarque 1.3.12. *Cette bijection permet de munir $\mathscr{A}$ d'une structure de groupe.*

Puisque $SO_2(\mathbb{R})$ est isomorphe à $\mathbb{R}/2\pi\mathbb{Z}$, on peut explicitement définir des mesures d'angles orientés.

Définition 1.3.13. *Soit $u, v \in \mathbb{S}^1$. On dit que $\theta \in \mathbb{R}$ est une mesure de l'angle orienté de u et v si $R(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$ est la rotation envoyant u sur v.*
On dit que θ est la mesure principale de l'angle orientée de u et v si θ est dans $[-\pi, \pi[$.

On peut maintenant faire le lien entre cette notion de mesure d'un angle entre deux vecteurs et la notion d'argument définie précédemment. Pour cela, nous allons faire le parallèle entre le plan complexe et $\mathbb{R}^2$.

Définition 1.3.14. *Si M est un point de $\mathbb{R}^2$ de coordonnées (x, y), on dit que $z = x + iy$ est l'affixe de M. On dit de même que z est l'affixe de $\overrightarrow{OM}$, où O est le point de coordonnées $(0, 0)$.*
L'affixe d'un vecteur $\overrightarrow{AB}$ de $\mathbb{R}^2$ est alors $b - a$ où a est l'affixe de A et b est l'affixe de B.

Proposition 1.3.15. *•Si θ est un argument de $z \in \mathbb{C}$ affixe d'un vecteur $\vec{v} \in \mathbb{R}^2$, alors c'est une mesure de l'angle orienté de $\vec{v}$ et $\vec{e_1} = (1, 0)$.*
•Si $\vec{v_1}$ et $\vec{v_2}$ sont deux vecteurs non nuls d'affixes respectives z_1 et z_2 alors un argument de $\frac{z_2}{z_1}$ est une mesure de l'angle orienté de $\vec{v_1}$ et $\vec{v_2}$, et on a :

$$\cos(\theta) = \frac{\vec{v_1} \cdot \vec{v_2}}{||\vec{v_1}||\,||\vec{v_2}||} \quad et \quad \sin(\theta) = \frac{\det(\vec{v_1}, \vec{v_2})}{||\vec{v_1}||\,||\vec{v_2}||}$$

Grâce à toutes ces notions d'affixes, d'angles, etc., on peut traiter des problèmes de géométrie plane grâce aux complexes. Voyons par exemple une version avec les nombres complexes du théorème de Pythagore.

Application 1.3.16. *Soit T le triangle ABC, où A, B, C sont des points d'affixes respectives a, b et c. Il y a équivalence entre les assertions suivantes :*

1. *le triangle T est rectangle en A ;*
2. $\mathrm{Re}((b - a)(\bar{c} - \bar{a})) = 0$;
3. $|b - c|^2 = |c - a|^2 + |b - a|^2$
4. *$AD = \frac{BC}{2}$, où D est le milieu de $[B, C]$.*

Remarque 1.3.17. *On peut trouver le même type de caractérisations pour les triangles isocèles et équilatéraux.*

2 Racines de l'unité

2.1 Définition et premières propriétés [Com21] [Jea92] [Goz09]

Nous allons désormais nous intéresser à des sous-groupes particuliers du groupe des nombres complexes de module 1 : les racines $n-$ièmes de l'unité pour $n \geq 1$.

Définition 2.1.1. *Soit n dans $\mathbb{N}^*$. On définit l'ensemble des racines n-ièmes de l'unité comme $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$. Il s'agit du noyau du morphisme de groupes surjectif*

$$\begin{aligned} f : \mathbb{U} &\longrightarrow \mathbb{U} \\ z &\longmapsto z^n. \end{aligned}$$

Cet ensemble est facile à étudier au vu de ses propriétés.

Proposition 2.1.2. *Soit n dans $\mathbb{N}^*$. L'ensemble $\mathbb{U}_n$ est un sous-groupe cyclique d'ordre n de $\mathbb{U}$. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ via l'isomophisme :*

$$\begin{aligned} \varphi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{U}_n \\ \bar{k} &\longmapsto e^{\frac{2ik\pi}{n}}. \end{aligned}$$

Les générateurs de ce sous-groupe, c'est-à-dire les éléments z tels que $z^n = 1$, mais $z^d \neq 1$ pour $1 \leq d < n$, sont les éléments de la forme $e^{\frac{2ik\pi}{n}}$ pour $1 \leq k \leq n$, premier avec n.

Donnons un nom à l'ensemble des générateurs, qui nous sera d'une grande utilité par la suite.

Définition 2.1.3. *Soit n dans $\mathbb{N}^*$. On définit l'ensemble des racines primitives n-ièmes de l'unité comme $\mathbb{U}_n^* = \{e^{\frac{2ik\pi}{n}}, k \wedge n = 1\}$.*

Proposition 2.1.4. *Soit n dans $\mathbb{N}^*$. Si ξ est une racine primitive n-ième de l'unité, alors les racines primitives n-ièmes de l'unité sont les ξ^k pour $1 \leq k \leq n$, premier avec n.*

Exemple 2.1.1. *Pour se faire une idée de ces ensembles, on peut voir ce que cela donne pour $n = 1, 2, 3, 4$:*

- $\mathbb{U}_1 = \{1\}$ *et* $\mathbb{U}_1^* = \{1\}$.
- $\mathbb{U}_2 = \{1, -1\}$ *et* $\mathbb{U}_2^* = \{-1\}$.
- $\mathbb{U}_3 = \{1, j, j^2\}$ *et* $\mathbb{U}_3^* = \{j, j^2\}$, *où* $j = e^{\frac{2i\pi}{3}}$.
- $\mathbb{U}_4 = \{1, -1, i, -i\}$ *et* $\mathbb{U}_3^* = \{i, -i\}$.

On obtient directement à partir de ce qui précède des informations sur les cardinaux de ces ensembles.

Proposition 2.1.5. *Soit n dans $\mathbb{N}^*$. Le cardinal de $\mathbb{U}_n$ est $\varphi(n)$ où φ désigne l'indicatrice d'Euler. De plus, $\mathbb{U}_n = \bigsqcup_{d|n} \mathbb{U}_d^*$, et on en déduit donc $n = \sum_{d|n} \varphi(d)$.*

Remarque 2.1.6. *En plus d'être facile à étudier, le sous-groupe des racines $n-$ièmes de l'unité pour $n \geq 1$ est facile à représenter. En effet, dans le plan, les racines $n-$ièmes de l'unité peuvent se représenter comme les sommets d'un polygone régulier à n côtés inscrit dans $\mathbb{S}^1$, voir figures 2 et 3 de l'annexe.*

Enfin, on peut de nouveau faire un pont entre l'algèbre et la topologie, grâce à ces sous-groupes, en remarquant que l'on a alors trouvé tous les sous groupes compacts de $\mathbb{C}^*$.

Théorème 2.1.7. *Soit G un sous groupe compact de $(\mathbb{C}^*, \times)$. Alors soit $G = \mathbb{U}$, soit il existe n dans $\mathbb{N}^*$ tel que $G = \mathbb{U}_n$.*

2.2 Polynômes cyclotomiques [Goz09] [Per96] [Ser07]

Nous allons maintenant étudier les polynômes minimaux des racines primitives de l'unité, qui nous seront utiles pour la suite dans les applications, notamment pour les questions de constructibilité à la règle et au compas.

Définition 2.2.1. *Soit n dans $\mathbb{N}^*$. On définit le n-ième polynôme cyclotomique de la façon suivante :*

$$\phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi).$$

Remarque 2.2.2. *On voit directement que pour tout n dans $\mathbb{N}^*$, ϕ_n est un polynôme unitaire de degré $\varphi(n)$.*

Exemple 2.2.1. *Puisque l'on a vu précédemment les racines primitives n-ièmes pour $n = 1, 2, 3, 4$, on peut déduire directement les premiers polynômes cyclotomiques : $\phi_1(X) = X - 1$, $\phi_2(X) = X + 1$, $\phi_3(X) = X^2 + X + 1$ et $\phi_4(X) = X^2 + 1$.*

Proposition 2.2.3. *Soit n dans $\mathbb{N}^*$. On a*

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Remarque 2.2.4. *Cette écriture nous permet de calculer par récurrence les polynômes cyclotomiques en écrivant pour $n \geq 1$:*

$$\phi_n = \frac{X^n - 1}{\prod_{d|n, d \neq n} \phi_d}.$$

De plus, on en déduit que pour p premier,

$$\phi_p = \frac{X^p - 1}{X - 1} = \sum_{i=0}^{p-1} X^i.$$

Et on peut même aller plus loin en déduisant une expression explicite de ϕ_q pour $q = p^n$ avec n dans $\mathbb{N}^*$:

$$\phi_{p^n}(X) = \frac{X^q - 1}{\prod_{d|q, d \neq q} \phi_d},$$

or $\prod_{d|q, d \neq q} \phi_d = \prod_{d|p^{n-1}} \phi_d = X^{p^{n-1}} - 1$, *d'où*

$$\phi_q(X) = \frac{(X^{p^{n-1}})^p - 1}{X^{p^{n-1}} - 1} = \sum_{i=0}^{p-1} (X^{p^{n-1}})^i.$$

Nous allons maintenant montrer par étapes l'irréductibilité des polynômes cyclotomiques, ce qui fera l'objet du premier développement, rédigé à la fin du document.

Proposition 2.2.5. *Pour tout n dans $\mathbb{N}^*$, ϕ_n est dans $\mathbb{Z}[X]$.*

Voici une variante du lemme de Gauss pour les polynômes qui nous sera utile pour la preuve de l'irréductibilité.

Lemme 2.2.6. *Soient P, A et B des polynômes non nuls de $\mathbb{Q}[X]$. On suppose que P est dans $\mathbb{Z}[X]$, que $P = AB$ et que P et A sont unitaires. Alors A et B sont dans $\mathbb{Z}[X]$.*

Et nous avons désormais tous les ingrédients pour aboutir au théorème principal.

Théorème 2.2.7. *Pour tout n dans $\mathbb{N}^*$, ϕ_n est irréductible dans $\mathbb{Q}[X]$, et donc dans $\mathbb{Z}[X]$.*

Application 2.2.8. *Soit n dans $\mathbb{N}^*$ et ξ une racine primitive n-ième de l'unité. Alors le théorème nous permet d'affirmer que ϕ_n est le polynôme minimal de ξ sur $\mathbb{Q}$, et donc $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.*

Puisque l'on connait maintenant les polynômes minimaux sur $\mathbb{Q}$ des racines primitives de l'unité, on en déduit ce corollaire sur le nombre de racines de l'unité d'un corps de nombres.

Corollaire 2.2.9. *Si K une extension finie de $\mathbb{Q}$, alors il y a un nombre fini de racines de l'unité dans K.*

Enfin, on peut utiliser les polynômes cyclotomiques pour obtenir le théorème suivant, qui est une version faible du théorème de la progression arithmétique de Dirichlet.

Théorème 2.2.10. *Soit n dans $\mathbb{N}^*$. Il existe une infinité de nombres premiers de la forme $\lambda n + 1$ avec λ entier.*

3 Applications

3.1 Matrices circulantes [Gou21]

On retrouve tout d'abord les nombres complexes de module 1, et en particulier les racines de l'unité, dans l'étude de matrices particulières que l'on appelle les matrices circulantes.

Définition 3.1.1. *On définit l'ensemble $\mathscr{C}$ des matrices circulantes comme l'ensemble des matrices de $M_n(\mathbb{C})$ de la forme :*

$$C = \begin{bmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_3 & c_2 \\ c_2 & c_1 & c_0 & \cdots & c_4 & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{n-2} & c_{n-3} & c_{n-4} & \cdots & c_0 & c_{n-1} \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_1 & c_0 \end{bmatrix}.$$

Remarque 3.1.2. *On les appelle de la sorte puisque chaque ligne est obtenue par permutation cyclique de la ligne précédente.*

On peut alors réduire facilement ces matrices, ce qui fait apparaître les racines de l'unité.

Proposition 3.1.3. *Les matrices de $\mathscr{C}$ sont simultanément diagonalisables, et si C est la matrice de la définition précédente, alors ses valeurs propres sont les $P(1), P(\omega), \dots P(\omega^{n-1})$, où $\omega = e^{\frac{2i\pi}{n}}$ (ainsi les ω^k pour $0 \leq k \leq n-1$ sont les racines n-ièmes de l'unité), et $P(X) = \sum_{k=0}^{n-1} a_k X^k$. Et alors,*

$$\det(C) = \prod_{k=0}^{n-1} P(\omega^k).$$

On en déduit un corollaire géométrique inattendu sur le barycentre d'un polygone, qui montre une nouvelle fois l'utilité des nombres complexes pour la géométrie.

Proposition 3.1.4. *Soit P un polygone du plan complexe dont les sommets ont pour affixe $z_1, \dots, z_n$. On définit par récurrence la suite de polygones $(P_k)_{k\in\mathbb{N}}$ avec $P_0 = P$ et pour tout $k \in \mathbb{N}$, les sommets de P_{k+1} sont les milieux des arêtes de P_k. La suite $(P_k)_{k\in\mathbb{N}}$ converge vers l'isobarycentre de $z_1, \dots, z_n$.*

On pourra retrouver une illustration de ce théorème en figure 4 de l'annexe.

3.2 Applications aux polynômes [Gou21] [Ser07] [Pra01]

Les nombres complexes de module 1 apparaissent naturellement dans certains résultats sur les polynômes, et pas seulement à travers l'étude des polynômes cyclotomiques. Voyons tout d'abord le théorème de Kronecker.

Théorème 3.2.1. *Soit P un polynôme unitaire de $\mathbb{Z}[X]$ de degré supérieur ou égal à 1, dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose $P(0) \neq 0$. Alors toutes les racines de P sont des racines de l'unité.*

Et si en plus le polynôme considéré est irréductible, on en déduit qu'il s'agit alors d'un polynôme cyclotomique.

Corollaire 3.2.2. *Soit P un polynôme unitaire de $\mathbb{Z}[X]$ de degré supérieur ou égal à 1, irréductible dans $\mathbb{Q}[X]$, dont les racines complexes sont toutes de module inférieur ou égal à 1. Alors soit $P = X$, soit il existe $d \in \mathbb{N}^*$ tel que P soit le d-ième polynôme cyclotomique.*

Nous allons maintenant introduire une mesure sur les polynômes, qui nous donnera d'ailleurs une autre interprétation du théorème de Kronecker.

Définition 3.2.3. *Soit P un polynôme de $\mathbb{C}[X]$ défini par $P(X) = a_d(X-\alpha_1)\dots(X-\alpha_d)$. On définit la mesure de Mahler de P par la formule :*

$$M(f) = |a_d| \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

Si l'on écrit P sous la forme $P = \sum_{i=0}^{d} a_i X^i$, on définit également la hauteur de P :

$$H(P) = \max |a_i|.$$

Remarque 3.2.4. *La mesure de Mahler d'un polynôme cyclotomique est égal à 1, et le théorème de Kronecker nous montre donc que si P est un polynôme unitaire de $\mathbb{Z}[X]$ irréductible sur $\mathbb{Q}[X]$ de mesure de Mahler égale à 1, alors il s'agit soit du monôme X, soit d'un polynôme cyclotomique.*

Estimer la hauteur d'un polynôme peut s'avérer utile, par exemple dans l'étude des nombres transcendants, mais la hauteur n'est pas pratique à manipuler : elle n'est par exemple pas multiplicative, contrairement à la mesure de Mahler.

Proposition 3.2.5. *Soit P et Q deux polynômes de $\mathbb{C}[X]$, alors*

$$M(PQ) = M(P)M(Q).$$

En plus d'être facilement manipulable, cette mesure est pratique car elle permet d'encadrer la hauteur. Afin d'estimer la hauteur d'un polynôme il suffit donc d'estimer sa mesure de Mahler.

Proposition 3.2.6. *Soit P un polynôme de $\mathbb{C}[X]$ de degré d, alors*

$$\frac{M(P)}{\sqrt{d+1}} \leq H(P) \leq 2^{d-1} M(P).$$

Mais quel est donc le lien entre cette mesure et les nombres complexes de module 1 ? Il s'agit du théorème suivant.

Théorème 3.2.7. *Soit P un polynôme de $\mathbb{C}[X]$. Alors*

$$M(P) = \exp\Big(\int_0^1 \ln |P(e^{2i\pi t})| \mathrm{d}t \Big).$$

Ce théorème nous montre donc que pour mesurer P selon la mesure de Mahler, il suffit de regarder le polynôme sur le disque unité !

3.3 Constructibilité à la règle et au compas [Car89] [Goz09]

Nous allons de nouveau utiliser les nombres complexes de module 1, et en particulier les racines de l'unité, à des fins géométriques. Avant de passer aux théorèmes phares de cette partie, nous allons définir la notion de constructibilité et voir quelques propriétés de base.

Dans toute la suite, P désigne un plan euclidien orienté, $\mathscr{R} = (O, \vec{i}, \vec{j})$ est un repère orthonormé direct de P, et on note $I = (1, 0)$, et $J = (0, 1)$. On identifiera de même chaque point M de P avec le couple de ses coordonnées dans $\mathbb{R}^2$.

Définition 3.3.1. *Soit X une partie de P de cardinal supérieur ou égal à 2. On définit les courbes de X comme les droites (AB), où A et B sont deux points distincts de X, et les cercles $\mathscr{C}(C, ||CD||)$ où C et D sont deux points distincts de X. On dit que $M \in P$ est constructible en un pas à partir de X s'il est l'intersection de deux courbes distinctes de X.*

Définition 3.3.2. *Soit B_0 une partie de P de cardinal supérieur ou égal à 2. On dit qu'un point M est constructible à partir de B_0 s'il existe une suite finie de points $M_1, \dots, M_n$ telle que $M = M_n$, et pour tout $i \in [\![1, n]\!]$, M_i est constructible en un pas à partir de A_{i-1}, où $A_0 = B_0$, et pour $i \in [\![1, n]\!]$, $A_i = A_{i-1} \cup \{M_i\}$.*

Dans toute la suite, on prendra $B_0 = \{O, I\}$, et on dira simplement "constructible" pour "constructible à partir de B_0".
A partir de ces définitions, on montre que l'on sait construire plusieurs figures géométriques de base.

Proposition 3.3.3.
1. *J est constructible.*
2. *Si M est constructible, son symétrique par rapport à l'origine l'est également.*
3. *Si A et B sont constructibles distincts, le milieu de $[A, B]$ est constructible, ainsi que la médiatrice de $[A, B]$.*
4. *Si A, B et C sont constructibles distincts, on peut construire la perpendiculaire à (AB) passant par C, et également la parallèle à (AC) passant par C.*

On retrouvera en figure 5 de l'annexe l'exemple de la construction de la perpendiculaire à (AB) passant par C.

On peut maintenir définir la notion de réel constructible à partir de la notion de point constructible.

Proposition 3.3.4. *Soit $x \in \mathbb{R}$. Le point $(x, 0)$ est constructible si et seulement si le point $(0, x)$ est constructible. Si tel est le cas, on dit que x est un nombre constructible.*

Remarque 3.3.5. *Cette notion s'articule bien avec la notion de point constructible comme on peut s'y attendre : le point $M = (x, y)$ est constructible si et seulement si x et y sont constructibles.*

Exemple 3.3.1. *Les nombres $0, 1, -1$ sont constructibles car ce sont les abscisses des points constructibles O, I, I', ainsi que $\sqrt{3}$ qui est l'ordonnée du point K puisqu'il se situe sur le cercle d'équation $(x-1)^2 + y^2 = 4$, voir la figure 6 de l'annexe pour la représentation de ces points.*

Théorème 3.3.6. *L'ensemble des nombres réels constructibles est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ stable par racine carrée.*

Nous parvenons désormais au théorème le plus important de cette partie : le théorème de Wantzel.

Théorème 3.3.7. ***(Wantzel)*** *Le réel x est constructible si et seulement s'il existe une suite finie $(L_0, L_1, \dots L_p)$ de sous corps de $\mathbb{R}$ vérifiant $L_0 = \mathbb{Q}$, $x \in L_p$, et pour tout i dans $[\![0, p-1]\!]$, L_{i+1} est une extension quadratique de L_i autrement dit une extension de L_i de degré 2. On dit alors que la suite $(L_0, L_1, \dots L_p)$ est une tour d'extension quadratique.*

Corollaire 3.3.8. *Tout nombre constructible est algébrique sur $\mathbb{Q}$, et son degré est une puissance de 2.*

Exemple 3.3.2. *Ce résultat est très utile pour montrer qu'un réel n'est pas constructible. On peut par exemple en déduire que le nombre π n'est pas constructible puisqu'il n'est même pas algébrique, ou encore que le nombre $\sqrt[3]{2}$ n'est pas constructible puisque son degré sur $\mathbb{Q}$ est 3. Cela permet de répondre à des problèmes historiques très importants : la quadrature du cercle et la duplication du cube sont impossibles.*

Remarque 3.3.9. *On peut montrer que la réciproque du corollaire 3.3.8 est fausse.*

Revenons maintenant à notre sujet principal.

Définition 3.3.10. *On dit qu'un angle orienté $\hat{\theta}$ (que l'on confondra avec sa mesure principale $\theta \in [-\pi, \pi[$) est constructible si le point $M_\theta = (\cos(\theta), \sin(\theta))$ est constructible.*

Remarque 3.3.11. *L'angle θ est constructible si et seulement si $\cos(\theta)$ est constructible, si et seulement $\sin(\theta)$ est constructible. Cela implique que l'ensemble des angles constructibles est un groupe.*

Définition 3.3.12. *Si $n \geq 3$, on dit que le polygone régulier à n côtés est constructible si l'angle $\frac{2\pi}{n}$ est constructible.*

Nous allons maintenant chercher les entiers pour lesquels le polygone régulier associé est constructible.

Lemme 3.3.13. *•Soit m et n dans $\mathbb{N}^*$ premiers entre eux, alors $\frac{2\pi}{mn}$ est constructible si et seulement si $\frac{2\pi}{m}$ et $\frac{2\pi}{n}$ sont constructibles.*
•Si $n \geq 3$ a pour décomposition en facteurs premiers $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Alors le polygone régulier à n côtes est constructible si et seulement si les angles $\frac{2\pi}{p_1^{\alpha_1}} \dots \frac{2\pi}{p_k^{\alpha_k}}$ sont constructibles.

On définit des nombres remarquables qui apparaîtront dans la suite.

Définition 3.3.14. *On pose, pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$. On appelle F_n le nombre de Fermat d'indice n.*

Remarque 3.3.15. *On sait que si $2^q + 1$ est premier, pour $q \in \mathbb{N}$, alors $q = 0$ ou q est une puissance de 2. En revanche, tous les nombres de Fermat ne sont pas premiers : ils le sont si n vaut $1, 2, 3$ ou 4, mais ce n'est plus le cas pour $n = 5$, et ce au moins jusqu'à $n = 21$. Pour l'instant, aucun autre premier n'a été découvert.*

Grâce au lemme précédent, nous sommes ramenés à étudier les angles constructibles de la forme $\frac{2\pi}{p^\alpha}$ où p est premier et α est un entier non nul. Le théorème suivant qui étudie ce problème constituera le deuxième développement, détaillé à la fin du document.

Théorème 3.3.16. *1. Pour $\alpha \in \mathbb{N}^*$, le polygone régulier à 2^α côtés est constructible.*

2. Soit p un nombre premier supérieur ou égal à 3, et $\alpha \in \mathbb{N}^*$. Le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre de Fermat (premier).

Et en cumulant ce théorème au lemme précédent, on obtient directement le théorème suivant, que l'on doit à Gauss.

Théorème 3.3.17. *Soit n un entier supérieur ou égal à 2. On peut construire le polygone régulier à n côtés si et seulement si soit $n = 2^\alpha$ pour $\alpha \in \mathbb{N}^*$, soit $n = 2^\alpha p_1 \dots p_k$, où $\alpha \in \mathbb{N}$, et les $p_1, \dots, p_k$ sont des nombres de Fermat premiers distincts.*

Exemple 3.3.3. *Ainsi, pour $n \in \{2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20\}$, le polygone régulier à n côtés est constructible. Pour $n \in \{7, 9, 11, 13, 14, 18, 19\}$, le polygone régulier à n côtés n'est pas constructible. En figure 7 de l'annexe, on pourra retrouver la construction du pentagone.*

4 Développements

4.1 Irréductibilité des polynômes cyclotomiques [Goz09] [Per96]

Nous allons démontrer dans cette partie la proposition 2.2.5, le lemme 2.2.6 et le théorème 2.2.7 que nous allons rappeler au fur et à mesure.

Proposition 4.1.1. *Pour tout n dans $\mathbb{N}^*$, ϕ_n est dans $\mathbb{Z}[X]$.*

Démonstration. Nous allons montrer le résultat par récurrence forte sur n dans $\mathbb{N}^*$.
Initialisation : Pour $n = 1$, $\phi_1 = X - 1$, qui est bien dans $\mathbb{Z}[X]$.
Hérédité : Soit $n \geq 2$ tel que le résultat soit vrai pour tout $d < n$. On pose $F(X) = \prod_{d|n, d\neq n} \phi_d(X)$. Alors F est unitaire, et par hypothèse de récurrence, F est dans $\mathbb{Z}[X]$. On peut donc effectuer, puisque F est unitaire, la division euclidienne de $X^n - 1$ par F dans $\mathbb{Z}[X]$: il existe $(R, Q) \in (\mathbb{Z}[X])^2$ avec $R = 0$ ou $\deg(R) < \deg(F)$ tels que $X^n - 1 = F(X)Q(X) + R(X)$. Or on sait que dans $\mathbb{C}[X]$, on a $X^n - 1 = F(X)\phi_n(X)$. Donc par unicité de la division euclidienne sur $\mathbb{C}[X]$, on en déduit que $R = 0$, et $\phi_n = Q \in \mathbb{Z}[X]$, ce qui conclut l'hérédité.
Ainsi par récurrence, on a obtenu que ϕ_n est dans $\mathbb{Z}[X]$ pour tout n dans $\mathbb{N}^*$. □

Passons maintenant à la variante du lemme de Gauss.

Lemme 4.1.2. *Soient P, A et B des polynômes non nuls de $\mathbb{Q}[X]$. On suppose que P est dans $\mathbb{Z}[X]$, que $P = AB$ et que P et A sont unitaires. Alors A et B sont dans $\mathbb{Z}[X]$.*

Démonstration. On note $A(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, où pour tout $0 \leq i \leq n-1$, a_i est dans $\mathbb{Q}$. Pour $0 \leq i \leq n-1$, on écrit $a_i = \frac{p_i}{q_i}$, où $p_i \in \mathbb{Z}$, et $q_i \in \mathbb{N}^*$ sont premiers entre eux. On prend q un multiple commun des $q_0, \dots q_{n-1}$, alors $qA(X) = qX^n + \sum_{i=0}^{n-1} z_i X^i$, où pour tout $0 \leq i \leq n-1$, z_i est dans $\mathbb{Q}$. Quitte à diviser par $\text{pgcd}(q, z_0, \dots z_{n-1})$, on peut supposer $\text{pgcd}(q, z_0, \dots z_{n-1}) = 1$. Ainsi, $A_1 := qA$ est un polynôme primitif de $\mathbb{Z}[X]$.
Puisque A et P sont unitaires, on voit directement que B l'est aussi, et on peut donc effectuer le même procédé sur B. Ainsi, il existe de même $r \in \mathbb{N}^*$ tel que $B_1 := rB$ soit un polynôme primitif de $\mathbb{Z}[X]$.
Puisque A_1 et B_1 sont primitifs, le lemme de Gauss nous permet de conclure que $A_1 B_1$ est également primitif. Donc comme $qrP = A_1 B_1$, et puisque P est unitaire :

$$1 = c(qrP) = qrc(P) = qr.$$

Ainsi, $qr = 1$, donc $q = r = 1$, c'est à dire $A = A_1 \in \mathbb{Z}[X]$ et $B = B_1 \in \mathbb{Z}[X]$. □

Et nous arrivons au but : l'irréductibilité des polynômes cyclotomiques.

Théorème 4.1.3. *Pour tout n dans $\mathbb{N}^*$, ϕ_n est irréductible dans $\mathbb{Q}[X]$, et donc dans $\mathbb{Z}[X]$.*

Démonstration. Soit n dans $\mathbb{N}^*$. Soit ω une racine primitive n-ième de l'unité. Notons f le polynôme minimal de ω sur $\mathbb{Q}$. Nous allons montrer que $f = \phi_n$.
Premièrement, f divise ϕ_n dans $\mathbb{Q}[X]$ puisque par définition, $\phi_n(\omega) = 0$. Nous allons donc montrer que $\deg(f) \geq \varphi(n) = \deg(\phi_n)$, ce qui nous permettra de conclure puisque f et ϕ_n sont unitaires.
Nous allons essayer de réduire le problème au maximum. Pour montrer $\deg(f) \geq \varphi(n)$, nous allons montrer que toutes les racines primitives n-ièmes de l'unité sont racines de f. D'après la proposition 2.1.4, cela équivaut à montrer que pour tout $k \in [\![0, n-1]\!]$ premier avec n, $f(\omega^k) = 0$. Il suffit donc de montrer que si u est racine de f, et si p est un nombre premier ne divisant pas n, alors $f(u^p) = 0$. En effet, si $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, alors $f(\omega) = 0$ impliquera $f(\omega^{p_1}) = 0$, qui impliquera $f(\omega^{{p_1}^2}) = 0$, etc jusqu'à obtenir $f(\omega^{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}) = f(\omega^k) = 0$.
Maintenant que le problème est réduit, nous pouvons nous lancer dans la preuve. Remarquons tout d'abord une relation de divisibilité. Puisque ω est racine de $X^n - 1$, f divise $X^n - 1$ dans $\mathbb{Q}[X]$: il existe h dans $\mathbb{Q}[X]$ tel que

$$X^n - 1 = f(X)h(X). \tag{1}$$

Comme $X^n - 1$ et f sont unitaires, et $X^n - 1$ est dans $\mathbb{Z}[X]$, on en déduit grâce au lemme précédent que h et f sont dans $\mathbb{Z}[X]$.
Soit u une racine de f, et p un nombre premier ne divisant pas n. Comme f divise $X^n - 1$ dans $\mathbb{Q}[X]$ (et même dans $\mathbb{Z}[X]$ même si ce n'est pas nécessaire ici), on a $u^n - 1 = 0$, donc u est une racine n-ième de l'unité , donc u^p également :

$$0 = (u^p)^n - 1 = f(u^p)h(u^p).$$

Supposons $f(u^p) \neq 0$. Alors nécessairement $h(u^p) = 0$. Or u est racine de f, qui est unitaire et irréductible dans $\mathbb{Q}[X]$, donc f est le polynôme minimal de u sur $\mathbb{Q}$. Puisque u est racine de $h(X^p)$, f divise $h(X^p)$ dans $\mathbb{Q}[X]$, donc il existe g dans $\mathbb{Q}[X]$ tel que

$$h(X^p) = f(X)g(X). \tag{2}$$

Or $h(X^p)$ est dans $\mathbb{Z}[X]$ et $h(X^p)$ et f sont unitaires, donc encore une fois grâce au lemme précédent, g est dans $\mathbb{Z}[X]$.
Réduisons modulo p l'équation 2 :

$$(\bar{h}(X))^p = \overline{h(X^p)} = \bar{f}(X)\bar{g}(X).$$

Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\bar{f}$. Alors d'après l'égalité précédente, θ divise $\bar{h}^p$, et donc divise $\bar{h}$ dans $\mathbb{F}_p[X]$. Ainsi, si l'on reprend l'égalité 1 que l'on passe modulo p, on obtient

$$X^n - \bar{1} = \overline{X^n - 1} = \bar{f}(X)\bar{h}(X),$$

et donc θ^2 divise $X^n - \bar{1}$ dans $\mathbb{F}_p[X]$. Cela implique que $X^n - \bar{1}$ aurait une racine double dans un corps de décomposition sur $\mathbb{F}_p$, et cela est impossible car $X^n - \bar{1}$ est premier avec sa dérivée $(X^n - \bar{1})' = \bar{n}X^{n-1}$ dans $\mathbb{F}_p[X]$ (on peut écrire la relation de Bézout suivante puisque p ne divise pas n : $(\bar{n})^{-1}X \times \bar{n}X^{n-1} - (X^n - \bar{1}) = \bar{1}$).
Nous sommes donc parvenus à une contradiction, ainsi $f(u^p) = 0$. D'après ce que l'on a dit au début de la preuve, cela permet donc de conclure que $\phi_n = f$, ce qui conclut puisque f est irréductible sur $\mathbb{Q}[X]$ en tant que polynôme minimal de ω. On déduit ensuite que ϕ_n est irréductible sur $\mathbb{Z}[X]$ puisque ϕ_n est unitaire donc primitif. □

4.2 Polygones constructibles, [Goz09] [Car89]

Nous allons démontrer dans cette partie le théorème 4.2.1 que nous rappelons.

Théorème 4.2.1. *1. Pour $\alpha \in \mathbb{N}^*$, le polygone régulier à 2^α côtés est constructible.*

2. Soit p un nombre premier supérieur ou égal à 3, et $\alpha \in \mathbb{N}^*$. Le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre de Fermat (premier).

Démonstration. 1. Montrons le résultat par récurrence sur $\alpha \in \mathbb{N}^*$.
Initialisation : Pour $\alpha = 1$, $\cos(\frac{2\pi}{2}) = -1$, qui est constructible. Pour $\alpha = 2$, $\cos(\frac{2\pi}{4}) = 0$, qui est également constructible.
Hérédité : Soit $\alpha \geq 2$ tel que l'angle $\frac{2\pi}{2^\alpha}$ soit constructible. On obtient alors l'angle $\frac{2\pi}{2^{\alpha+1}}$ en construisant la bissectrice de l'angle $\frac{2\pi}{2^\alpha}$ que l'on peut construire de la façon suivante : on considère $M_\alpha = (\cos(\frac{2\pi}{2^\alpha}), \sin(\frac{2\pi}{2^\alpha}))$, puis l'on construit A le milieu de $[I, M_\alpha]$, et l'on prend enfin le point à l'intersection entre la droite (OA) et le cercle de centre O passant par I. Ainsi, $\frac{2\pi}{2^{\alpha+1}}$ est constructible, ce qui conclut l'hérédité.
Ainsi par récurrence, on a obtenu que pour tout $\alpha \in \mathbb{N}^*$, $\frac{2\pi}{2^\alpha}$ est constructible.

2. Soit p un nombre premier supérieur ou égal à 3.
•Supposons qu'il existe $\alpha \in \mathbb{N}$ tel que $\frac{2\pi}{p^\alpha}$ soit constructible. Alors $\cos(\frac{2\pi}{p^\alpha})$ est un nombre constructible, donc d'après le théorème de Wantzel, il existe un entier m tel que :

$$[\mathbb{Q}(\cos(\frac{2\pi}{p^\alpha})) : \mathbb{Q}] = 2^m.$$

Pour alléger l'écriture, notons $q = p^\alpha$. Alors $\omega = \cos(\frac{2\pi}{q}) + i\sin(\frac{2\pi}{q})$ est une racine q-ième primtive de l'unité. Son polynôme minimal sur $\mathbb{Q}$ est donc ϕ_q le q-ième polynôme cyclotomique, de degré $\varphi(q) = p^{\alpha-1}(p-1)$. Ainsi,

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1).$$

Or $\omega + \omega^{-1} = 2\cos(\frac{2\pi}{q})$, donc $\cos(\frac{2\pi}{q}) \in \mathbb{Q}(\omega)$ et $\omega^2 - 2\cos(\frac{2\pi}{q}) + 1 = 0$. Donc ω est de degré 2 sur $\mathbb{Q}(\cos(\frac{2\pi}{p^\alpha}))$, et ainsi d'après le théorème de la base téléscopique, on obtient :

$$p^{\alpha-1}(p-1) = [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}(\cos(\frac{2\pi}{p^\alpha}))] \times [\mathbb{Q}(\cos(\frac{2\pi}{p^\alpha})) : \mathbb{Q}] = 2^{m+1}.$$

Ainsi puisque p est premier différent de 2, on en déduit que $\alpha = 1$ et $p = 1 + 2^{m+1}$. Cela permet donc de conclure que p est un nombre premier de Fermat (cf remarque 3.3.15).
•Supposons que p soit un nombre premier de Fermat. Ainsi, $p = 1 + 2^n$ pour $n \geq 1$. Nous allons essayer de créer une tour d'extension quadratique sur $\mathbb{Q}$ tel que le dernier sous-corps contienne $\cos(\frac{2\pi}{p})$, et cela conclura grâce au théorème de Wantzel. Et pour cela, nous allons considérer $K = \mathbb{Q}(\omega)$, où $\omega = e^{\frac{2\pi}{p}}$ est une racine primitive p-ième de l'unité, et plus précisement le groupe des automorphismes de K.
Soit $\sigma \in \mathrm{Aut}(K)$. Puisque σ fixe $\mathbb{Q}$, et est un morphisme, on en déduit que

$$\phi_p(\sigma(\omega)) = \sigma(\phi_p(\omega)) = \sigma(0) = 0.$$

Ainsi $\sigma(\omega)$ est une racine de ϕ_p, et donc par définition, une racine primitive p-ième de l'unité. Il existe donc $k \in [\![1, p-1]\!]$ tel que $\sigma(\omega) = \omega^k$. Réciproquement, si $k \in [\![1, p-1]\!]$, l'application

$$\begin{aligned} \mathbb{Q}[X] &\longrightarrow K \\ P &\longmapsto P(\omega^k), \end{aligned}$$

est un morphisme d'anneaux surjectif (car $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$), de noyau $\langle \phi_p \rangle$. Ainsi, on peut passer au quotient, et on obtient alors un automorphisme de corps :

$$\begin{aligned} \sigma_k : \mathbb{Q}[X]/\langle \phi_p \rangle \simeq K &\longrightarrow K \\ \omega &\longmapsto \omega^k. \end{aligned}$$

Puisqu'un automorphisme σ de $\mathrm{Aut}(K)$ est entièrement déterminé par l'image de ω, on en déduit que l'application

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow \mathrm{Aut}(K) \\ \bar{k} &\longmapsto \sigma_k \end{aligned}$$

est un isomorphisme de groupes. Comme p est premier, $(\mathbb{Z}/p\mathbb{Z})^\times$, et donc $\mathrm{Aut}(K)$ sont cyliques d'ordre $p-1 = 2^n$. Soit g un générateur de $\mathrm{Aut}(K)$. On peut donc définir pour $i \in [\![0, n]\!]$, $K_i = \{z \in K, g^{2^i}(z) = z\}$. Alors pour tout $i \in [\![0, n]\!]$, K_i est un sous-corps de K et $K_i \subset K_{i+1}$. On obtient donc une suite d'extension de corps :

$$\mathbb{Q} \subset K_0 \subset K_1 \subset K_2 \subset \dots K_n = K.$$

Montrons que pour tout $i \in [\![0, n-1]\!]$, $K_i \neq K_{i+1}$. Regardons tout d'abord le cas $K_0 \neq K_1$. On considère

$$z = \omega + g^2(\omega) + g^4(\omega) + \cdots + g^{2^n-2}(\omega) = \sum_{k=0}^{2^{n-1}-1} g^{2k}(\omega).$$

Alors

$$g^2(\omega) = g^2(\omega) + g^4(\omega) + \cdots + g^{2^n-2}(\omega) + \omega = z,$$

mais

$$g(z) = g(\omega) + g^3(\omega) + \dots g^{2^n-1}(\omega) \neq z,$$

par unicité de l'écriture de z dans la base $\{g^k(\omega), 0 \leq k \leq p-2\} = \{\omega^k, 1 \leq k \leq p-1\}$ de K. Ainsi $z \in K_1 \setminus K_0$. De même dans le cas général, on considère

$$z = \omega + g^{2^{i+1}}(\omega) + g^{2^{i+2}}(\omega) + \cdots + g^{2^{i+1}(2^{n-i-1}-1)}(\omega) = \sum_{k=0}^{2^{n-i-1}-1} g^{2^{i+1}k}(\omega),$$

et de même, $g^{2^{i+1}}(z) = z$, mais $g^{2^i} \neq z$, et donc $z \in K_{i+1} \setminus K_i$. Ainsi, d'après le théorème de la base téléscopique, on obtient :

$$2^n = p - 1 = [K : \mathbb{Q}] = \prod_{k=0}^{n-1} [K_{i+1} : K_i] \times [K_0 : \mathbb{Q}].$$

Or, aucun des indices $[K_{i+1} : K_i]$ ne peut être égal à 1 d'après ce qu'il précède, et donc nécessairement, $[K_{i+1} : K_i] = 2$ pour tout $0 \leq i \leq n-1$, et $[K_0 : \mathbb{Q}] = 1$, donc $K_0 = \mathbb{Q}$.
Ainsi, on a obtenu une tour d'extensions quadratiques $\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n$. Nous allons montrer que $K_{n-1} = \mathbb{Q}(\cos(\frac{2\pi}{p}))$, ce qui conclura d'après le théorème de Wantzel.
On a $K_{n-1} = \{z \in K, f(z) = z\}$, où $f = g^{2^{n-1}}$. On note $f(\omega) = \omega^\lambda$, alors comme $f^2 = \mathrm{Id}_K$, on a $\omega = f^2(\omega) = f(\omega^\lambda) = \omega^{\lambda^2}$, i.e. $\omega^{\lambda^2-1} = 1$, donc p divise $\lambda^2 - 1$ c'est-à-dire modulo p, $\bar{\lambda} = \pm\bar{1}$. Mais $\bar{\lambda} = \bar{1}$ est impossible car $f \neq \mathrm{Id}_K$. Ainsi $\bar{\lambda} = -\bar{1}$, i.e. $f(\omega) = \omega^{-1}$. On en déduit :

$$f(\cos(\frac{2\pi}{p})) = f(\frac{1}{2}(\omega + \omega^{-1})) = \frac{1}{2}(f(\omega) + f(\omega^{-1})) = \frac{1}{2}(\omega^{-1} + \omega) = \cos(\frac{2\pi}{p}).$$

Donc $\cos(\frac{2\pi}{p}) \in K_{n-1}$, donc $\mathbb{Q}(\cos(\frac{2\pi}{p})) \in K_{n-1} \subsetneq K_n = K$. Or nous avons déjà vu précédemment que $[K : \mathbb{Q}(\cos(\frac{2\pi}{p}))] = 2$, donc $\mathbb{Q}(\cos(\frac{2\pi}{p})) = K_{n-1}$. Ainsi, d'après le théorème de Wantzel, $\cos(\frac{2\pi}{p})$ est constructible, ce qui termine la preuve.

□

5 Annexes

5.1 Figures

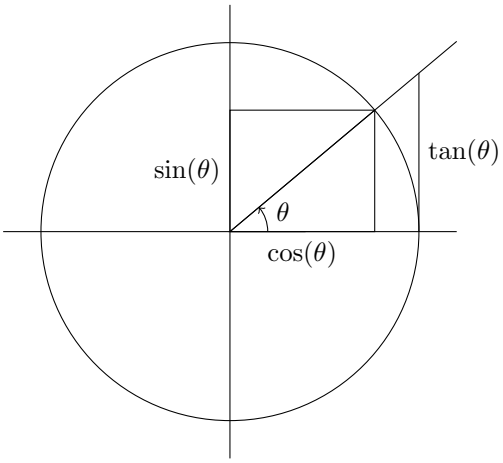

FIGURE 1 – Représentation d'un angle $\theta \in \mathbb{R}$ sur le cercle trigonométrique.

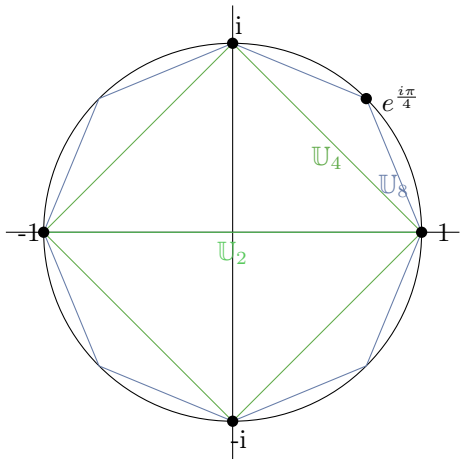

FIGURE 2 – Représentation de $\mathbb{U}_n$ pour $n = 2, 4, 8$.

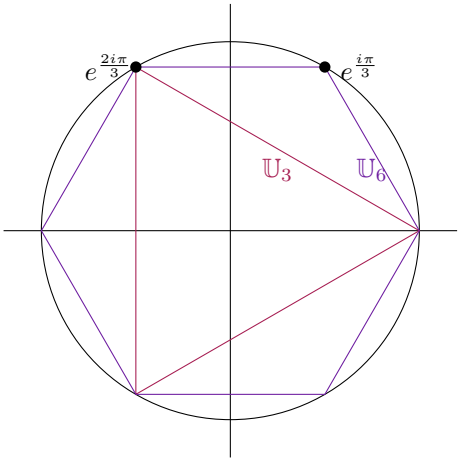

FIGURE 3 – Représentation de $\mathbb{U}_n$ pour $n = 3, 6$.

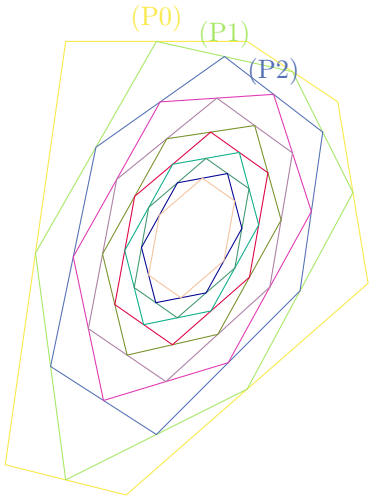

FIGURE 4 – Suite de polygones convergeant vers l'isobarycentre.

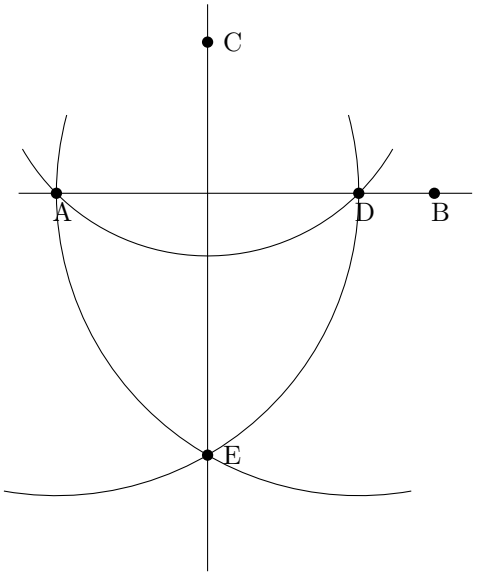

FIGURE 5 – Exemple de construction de la perpendiculaire à (AB) passant par C.

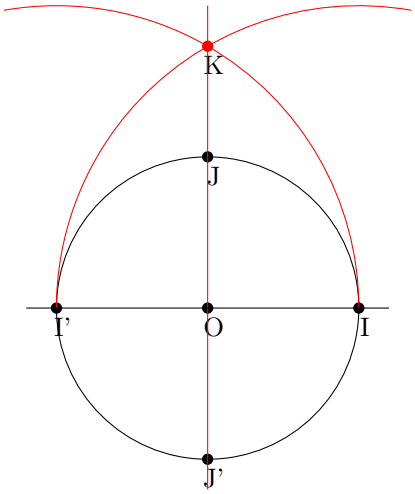

FIGURE 6 – Représentation de quelques points constructibles.

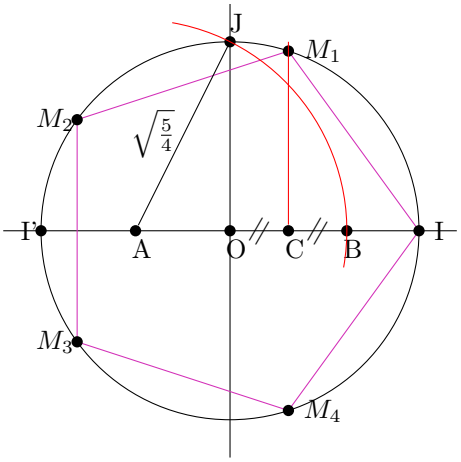

FIGURE 7 – Construction du pentagone.

5.2 Questions

Voici pour finir les questions qui ont été posées pendant la présentation de cette leçon en classe.

Première question : Est-ce que le polynôme $X^3 + X^2 + X + 1$ est cyclotomique ?
Réponse : Non, -1 est racine de ce polynôme, il n'est donc pas irréductible sur $\mathbb{Q}$ et ne peut donc pas être un polynôme cyclotomique.

Deuxième question : Soit $n \in \mathbb{N}^*$. Que vaut la somme des racines n-ièmes de l'unité ? Et la somme des racines primitives n-ièmes de l'unité ?
Réponse : Tout d'abord pour la somme des racines n-ièmes, on a :

$$\sum_{\omega \in \mathbb{U}_n} \omega = \sum_{k=0}^{n-1} e^{\frac{2i\pi k}{n}} = \frac{1 - (e^{\frac{2i\pi}{n}})^n}{1 - e^{\frac{2i\pi}{n}}} = 0.$$

Ensuite, on en déduit, en notant pour $d \in \mathbb{N}^*$, $S_d := \sum_{\omega \in \mathbb{U}_d^*} \omega$,

$$\sum_{d|n} S_d = 0, \quad \text{et} \quad S_1 = 1.$$

Et on reconnait la caractérisation de la fonction de Möbius ! Ainsi, $S_d = \mu(d)$.

Troisième question (culturelle) : On sait que les polynômes cyclotomiques sont à coefficients dans $\mathbb{Z}$, peut-on être encore plus précis ?
Réponse : Jusqu'à $n = 104$, les polynômes cyclotomiques sont à coefficients dans $\{-1, 0, 1\}$. Plus précisement, Migotti a démontré que si n a moins de deux facteurs premiers impairs alors ϕ_n est à coefficients dans $\{-1, 0, 1\}$ ($105 = 3 \times 5 \times 7$ est le plus petit entier ayant trois facteurs premiers impairs). Cependant, la réciproque est fausse, par exemple ϕ_{651} est à coefficients dans $\{-1, 0, 1\}$ alors que $651 = 3 \times 7 \times 31$.

Références

[Aud98] Michèle Audin. *Géométrie.* Belin, 1998.

[Car89] Jean-Claude Carrega. *Théorie des corps, La règle et le compas, 2ème édition.* Hermann, 1989.

[Com21] François Combes. *Algèbre et géométrie, 2ème édition.* Bréal, 2021.

[Gou21] Xavier Gourdon. *Les maths en tête, Algèbre Probabilités, 3ème édition.* Ellipses, 2021.

[Goz09] Ivan Gozard. *Théorie de Galois, 2ème édition.* Ellipses, 2009.

[Jea92] Jean-Marie Arnaudiès, Henri Fraysse. *Cours de mathématiques 1, Algèbre.* Dunod, 1992.

[Per96] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.

[Pra01] Victor V. Prasolov. *Polynomials.* Springer, 2001.

[Rom21] Jean-Etienne Rombaldi. *Mathématiques pour l'agrégation, Algèbre et géométrie, 2ème édition.* De Boeck Supérieur, 2021.

[Ser07] Serge Francinou, Hervé Gianella, Serge Nicolas. *Oraux X-ENS, Algèbre 1, 2ème édition.* Cassini, 2007.