Exposé

Katie Sweeney Martin Bacques

23 janvier 2023

1 Introduction

Dans cet exposé nous allons nous intéresser aux polynômes cyclotomiques ainsi qu'à la construction des polygones réguliers.

Dans une première partie sur les polynômes cyclotomiques on va commencer par parler des racines de l'unité. En effet les racines de l'unité sont à la base de la définition des polynômes cyclotomiques. Ensuite on va énoncer les propriétés importantes de ces polynômes, notamment le fait qu'ils soient des polynômes de $\mathbb{Z}[X]$ mais aussi des polynômes irréductibles sur $\mathbb{Z}$. C'est la démonstration de ce dernier résultat qui sera le plus compliqué mais dont les conséquences sont assez importantes.

En effet dans la deuxième partie nous allons parler des polygones réguliers et en particulier de leurs constructibilité. C'est le théorème de Gauss-Wantzel qui nous donnera la réponse à ce problème. La majorité des résultats de cette partie seront consacrées à démontrer ce théorème compliqué, on se servira de plus de l'irréductibilité des polynômes cyclotomiques afin de le prouver ce qui fera le lien entre la première et la deuxième partie.

De manière générale, c'est un exposé orienté sur des questions d'algèbre faisant intervenir la théorie des anneaux et des corps. Elle peut mener ensuite à des considérations plus générale notamment sur les extensions de corps, par exemple la théorie de Galois. Cette dernière est rapidement introduite à la fin de la deuxième partie sans pour autant rentrer dans les détails même si elle est liée à la démonstration du théorème de Gauss-Wantzel.

On va ici donner les résultats sans les démonstrations comme il a été demandé. Pour les polynômes cyclotomiques, nous avons surtout utilisé [2] et [5]. Pour ce qui est de la construction à la règle et au compas, nous avons utilisé [1], [4] mais la démonstration du théorème de Gauss-Wantzel est surtout basé sur [3].

2 Polynômes cyclotomiques

2.1 Racines de l'unité

Avant de parler des polynômes cyclotomiques on va commencer par parler des racines de l'unité que l'on abrégera en rdu ici.

Definition 1 Une racine de l'unité est un nombre complexe ζ tel qu'il existe $n \in \mathbb{N}^*$ qui vérifie $\zeta^n = 1$. On dit que c'est la n-ième racine de l'unité.

Dans le cas général si on résoud $\zeta^n = 1$ sous la forme polaire on voit qu'il y a n solutions. De plus :

$\{n$ racines de l'unité $\}=\{\ e^{\frac{2\pi k}{n}} | k \in [\![0; n-1]\!]\ \} = \{\ \zeta^k\ | k \in [\![0; n-1]\!]\ \}$.

Maintenant il y a des racines de l'unité qui nous intéressent plus que d'autres.

Definition 2 Une racine est primitive si son ordre (multiplicatif) est n. C'est équivalent à dire que les puissances de cette racine génère toutes les autres.

Prenons un exemple pour illustrer tout ça :

Exemple 2.1 *Pour le cas $n = 6$, les racines 6-ièmes de l'unité sont donc dans l'ensemble : $\{\ e^{\frac{2\pi k}{n}} | k \in [\![0; 5]\!]\ \}$.*

On regarde maintenant les puissances de ζ^k :

-Si $k = 0$ alors $\zeta^k = 1$ et ce n'est pas une racine primitive puisque les puissances de 1 valent toujours 1.

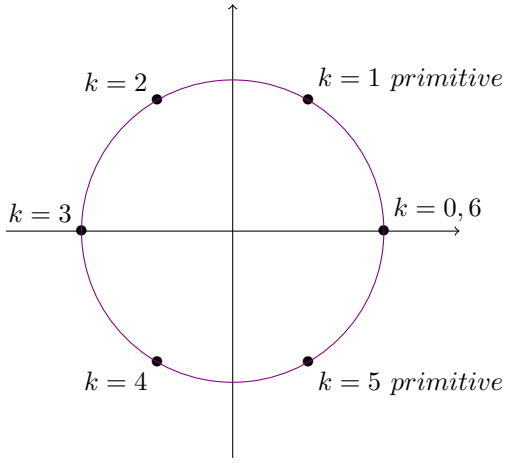
-Si $k = 1$ alors $\zeta^k = \zeta$ et donc c'est une racine primitive car son ordre est n. En effet, on a par définition que ζ génére les racines de l'unité.

-Si $k = 2$, on voit que $(\zeta^2)^3 = \zeta^6 = 1$ donc $\zeta^2)^4 = \zeta^2$ et par conséquent ζ^2 ne peut pas être racine de l'unité car elle génère seulement l'ensemble $\{1, \zeta^2, \zeta^4\}$.

-Si $k = 3$,on a $\zeta^3 = -1$ et donc l'ensemble que génère -1 est $\{-1, 1\}$ donc ce n'est pas une racine primitive.

Pour ce qui est de $k = 4, 5$ c'est équivalent à avoir $\zeta{-}2$ et ζ^{-1} et donc ont le même ordre respectivement que 2 et 1. On peut conclure que les seules racines primitives pour $n = 6$ sont ζ^1 et ζ^5.

Ce qui nous donne finalement le cercle trigonométrique suivant :



Proposition 1 *Il y a $\varphi(n)$ racines de l'unité, où φ est la fonction d'Euler. Ce qui est équivalent à : $|\{n^{ème}$ racines primitives de l'unité$\}| = \varphi(n)$. Le nombre de n-ièmes racines de primitive est égal à la fonction d'Euler en la valeur n.*

On peut maintenant passer aux polynômes cyclotomiques.

2.2 Définitions et exemples

Definition 3 Soit $n \in \mathbb{N}^*$. Le n-ième polynôme cyclotomique, $\Phi_n(X)$ est le polynôme ayant comme racines les racines primitives n-*ièmes* de l'unité.

Il est donc défini par :

$$\Phi_n(X) = \prod_{\zeta^k \ racine \ primitive} (X - \zeta^k) = \prod_{pgcd(k,n)=1} (X - \zeta^k)$$

avec $k \in [\![1; n]\!]$

Proposition 2 *Le polynôme cyclotomique $\Phi_n(X)$ est de degré $\varphi(n)$.*

La démonstration vient de la définition de la fonction φ d'Euler.

Exemple 2.2 *Regardons quelques exemples de polynômes cyclotomiques :*

-Pour $n = 1$, $\Phi_1(X) = X - 1$ (il y a une seule racine de l'unité qui est 1).

-Pour $n = 2$, $\Phi_2(X) = X + 1$ (la seule racine de l'unité est -1)

-Pour $n = 3$, $\Phi_3(X) = (X - e^{\frac{2i\pi}{3}})(X - e^{\frac{4i\pi}{3}}) = X^2 - (e^{\frac{2i\pi}{3}} + e^{\frac{4i\pi}{3}}) + e^{\frac{2i\pi}{3}} e^{\frac{4i\pi}{3}} = X^2 + X + 1$.

On peut voir maintenant un résultat important :

2.3 Propriétes des polynômes cyclotomiques

Théorème 2.1

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

c'est à dire qu'on peut factoriser $X^n - 1$ par des polynômes cyclotomiques.

Ce résultat est assez important puisqu'il permet la démonstration de nouveaux résultats.

Exemple 2.3 *Quelques nouveaux exemples de polynômes cyclotomiques :*
-$\Phi_4(X) = X^2 + 1$
-$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$
-$\Phi_6(X) = X^2 - X + 1$

Ce qui est surprenant c'est que l'on part de nombres complexes et que l'on obtient pour les 6 premiers termes des polynômes à coefficients entiers.

En fait on peut démontrer que c'est un fait plus général, c'est le résultat suivant :

Proposition 3 *Le polynôme $\Phi_n(X)$ est un polynôme de $\mathbb{Z}[X]$.*

Pour la démonstration on doit utiliser le théorème précédent ainsi que le lemme de Gauss pour pouvoir conclure.

C'est une des propriétés importantes des polynômes cyclotomiques. Mais ça ne s'arrête pas là puisqu'en fait les polynômes cyclotomiques ont des propriétés encore plus intéressantes.

Théorème 2.2 *Le polynôme $\Phi_n(X)$ est un polynôme irreductible de $\mathbb{Z}[X]$.*

La démonstration de ce théorème est assez complexe. On suppose d'abord que c'est faux et que $\Phi_n(X)$ est un produit de polynômes non constants. Puis on regarde les propriétés de ces nouveaux polynômes dans $\mathbb{F}_p[X]$ afin de montrer que l'un des polynômes du produit est en fait $\Phi_n(X)$. Etant donné qu'on peut supposer que ce polynôme est irréductible on déduit le résultat.

3 Construction à la règle et au compas

3.1 Introduction du problème

La construction des polygones réguliers est un problème qui occupe les mathématiciens depuis très longtemps (sûrement depuis les grecs).

C'est un problème très simple à exprimer :

> "Quels sont les polygones réguliers constructibles à la règle et au compas ?"

Historiquement c'est le théorème de Gauss-Wantzel (1837) qui a donné une réponse au problème de la construction des polygones réguliers.

Le théorème est le suivant :

Théorème 3.1 (Gauss-Wantzel) *:*

Un polygone à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 et de nombres premiers.

On précisera plus tard quels sont ces nombres premiers.

C'est ce théorème que nous allons montrer dans cette partie mais d'abord nous devons introduire ce que cela signifie pour un polygone d'être constructible.

3.2 Construction à la règle et au compas

On part du principe que l'on possède seulement une règle et un compas. La règle est marquée de 2 points et permet de définir l'unité de mesure. Le compas est muni de 2 pointes, une pour le centre du cercle et la seconde pour tracer le cercle.

On suppose que l'on se donne un point du plan (ici le plan euclidien $\mathbb{R}^2$), à partir de cela on peut tracer une droite passant par ce point. Grâce au compas on peut ensuite tracer sa perpendiculaire, on obtient donc un repère orthonormé.

Pour ce qui est des définitions on peut se permettre de ne pas les donner ici puisqu'elles sont assez intuitives. Cependant on doit quand même montrer un résultat concernant les constructions que l'on peut faire.

L'espace dans lequel on travaille ici est le plan euclidien, cependant nous allons intéresser seulement aux coordonnées des points de ce plan. Si l'on note (x, y) les coordonnées d'un tel point. On peut voir qu'en fait on peut s'intéresser seulement à une coordonnée car on peut faire la projection du point (x, y) sur l'axe des abscisses. Ensuite on construit la droite du plan d'équation $y = x$, on fait la projection de $(x, 0)$ sur cette droite, on obtient le point (x, x).

On vient donc de voir qu'il suffit qu'une des deux coordonnées soient constructibles pour que l'autre le soit aussi.

A partir de maintenant on peut considérer l'ensemble des points constructibles comme un sous-ensemble de $\mathbb{R}$ car l'étude des points comme couple peut être ramener à l'étude du nombre réel seul comme on vient de le voir.

On note à partir de maintenant $\mathcal{C}$ l'ensemble des nombres constructibles qui est un sous-ensemble de $\mathbb{R}$

Proposition 4 *L'ensemble $\mathcal{C}$ muni de l'addition et de la multiplication est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$.*

Maintenant afin de démontrer le théorème de Gauss-Wantzel on a besoin d'abord d'un résultat qui est dû à Wantzel et qui est en fait essentiel. Il utilise les extensions de corps pour caractériser les points constructibles à la règle et au compas.

Théorème 3.2 *Le nombre $a \in \mathbb{R}$ est constructible si il existe une suite finie de corps L_i telle que : $L_0 = \mathbb{Q}$, $[L_{i+1} : L_i] = 2$ et $a \in L_n$.*

Avec ce théorème il devient plus facile de démontrer le théorème de Gauss-Wantzel qui est le suivant :

Théorème 3.3 *Un polygône à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat.*

Les nombres premiers de Fermat sont de la forme $F_n = 2^{2^n} + 1$, on sait que les cinq premières valeurs sont des nombres premiers mais ensuite on ne connaît aucun nombre de cette forme qui soit premier.

La démonstration de ce théorème admet plusieurs démonstrations mais qui sont toutes basées sur le théorème de Wantzel. En effet celui-ci permet de faire le lien entre le problème géométrique et le problème algébrique. Or la théorie des extensions de corps est plus facile à étudier. Pour ce qui est de la condition nécessaire, on utilise le fait que le polynôme minimale de $e^{\frac{2i\pi}{n}} = \omega$ soit $\Phi_n(X)$. Ainsi cela nous donne la condition que $\varphi(n) = 2^\beta$ grâce au théorème de Wantzel. On en déduit ensuite la condition nécessaire.

Pour montrer que c'est une condition suffisante il faut plus travailler. Pour cela, on construit une suite d'extensions de corps qui vérifie le théorème de Wantzel. On prend pour ça une application g qui fixe les nombres rationnels mais qui permute les nombres les racines de l'unité. Le point est qu'on peut se ramener seulement au cas où n est un nombre premier de Fermat et donc utiliser le fait que ζ^k est toujours une n-ième racine primitive si n est premier. En considérant $K_i = Ker(g^{2^i} - Id)$ alors on obtient bien une suite d'extensions de corps qui vérifie le théorème de Wantzel. Le résultat le plus difficile est de montrer que $g^{n-1} = Id$, ce qui passe par l'étude du groupe de Galois $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ avec $\mathbb{Q}(\omega) = \mathbb{Q}[X]/(\Phi_n(X))$.

Ce qui est intéressant avec cette démonstration c'est qu'on donne aucune méthode pour construire les polygones réguliers. On résout le problème de manière purement algébrique.

Références

[1] Daniel Lines Alain Jeanneret. *Invitation à l'algèbre.* 2005.

[2] Marco Cavaleri. Vidéo sur les polynômes cyclotomiques. *https ://www.youtube.com/watch ?v=bTCA0uE5R1M*, 2021.

[3] Laura Gay Florian Lemonnier. Polygônes réguliers constructibles, théorème de gauss-wantzel. *https ://perso.eleves.ens-rennes.fr/ lgay/Agregation*, 2015.

[4] Patrice Tauvel. *Corps commutatifs et théorie de Galois.* Calvage & Mounet, 2021.

[5] Steven H. Weintraub. Several proofs of the irreducibility of the cyclotomic polynomial. *https ://www.lehigh.edu/ shw2/c-poly/several proofs.pdf*, 2000.