Polynômes Cyclotomiques
Théorème de Gauss

Le but du devoir est de démontrer le théorème de Gauss sur la constructibilité à la règle et au compas des polygones réguliers :

Les polygones réguliers constructibles sont ceux dont le nombre de côtés n est de la forme, soit 2^α ($\alpha \geq 2$) soit $2^\alpha p_1 p_2 ... p_r$ avec $\alpha \geq 0$ et les p_i des nombres premiers de Fermat distincts.

Pour cela on utilisera la caractérisation des nombres constructibles sur la base d'une tour d'extensions quadratiques :

Soit t un réel. t est constructible *ssi* il existe un entier p non nul, et une suite de sous-corps de $\mathbf{R}$, $\mathbf{L}_1$, $\mathbf{L}_2$, .., $\mathbf{L}_p$ tels que :

(i) $\mathbf{L}_1 = \mathbf{Q}$ *(ii)* pour $1 \leq j \leq p-1$, $\mathbf{L}_j \subset \mathbf{L}_{j+1}$ et $[\mathbf{L}_{j+1} : \mathbf{L}_j] = 2$. *(iii)* $t \in \mathbf{L}_p$.

En particulier si un nombre ω est construtible, le degré de l'extension associée, [Q(ω) : Q] est une puissance de 2.

Définitions préalables et rappels

1. Racines $n^{ième}$ de l'unité

Ce sont les racines, dans **C** du polynômes $X^n - 1$ dont on sait qu'il possède les n racines $\omega_k = e^{\frac{2ik\pi}{n}}$ (pour k = 0 ... n-1).

Elles forment un groupe cyclique U_n engendré par ω_1.

La racine $n^{ième}$ de l'unité ω_k est un générateur de U_n ssi $k \wedge n = 1$.

On dit alors que ω_k est une racine $n^{ième}$ *primitive* de l'unité. Il y a donc φ(n) racines $n^{ième}$ primitives de l'unité, où φ est l'indicateur d'Euler.

2. Polynômes cyclotomiques

Pour n≥1, on note $\Phi_n(X)$ le polynôme unitaire de **C**[X] dont les racines sont les racines $n^{ième}$ *primitives* de l'unité.

Φ_n est appelé le n° polynome cyclotomique. Il est donc de degré φ(n).

Dans ce texte, le terme *polynôme minimal* contient le terme *unitaire*.

Le degré du polynome minimal d'un nombre algébrique ω est aussi le degré de l'extension **Q**(ω) sur **Q**.

Partie I. Généralités sur les polynomes $\Phi_n(X)$.

I.1. Calculer, à partir de la définition, les polynômes Φ_n pour $1 \leq n \leq 4$.

I.2. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Indication : On peut utiliser la relation connue $n = \sum_{d|n} \varphi(n)$. On peut aussi opérer autrement, cette relation en devenant alors une conséquence immédiate.

I.2. Pour p premier, aprés avoir calculé Φ_p , calculer Φ_{p^2}.

On remarquera que la relation I.2 permet un calcul par récurrence de $\Phi_n(X)$.

Complément "culturel"

On constatera que pour ces valeurs particulières de n, le polynôme Φ_n est à coefficients dans **Z**. *On notera plus précisément que les coefficients de ces polynômes sont uniquement 0, 1 ou -1. On peut se demander si c'est toujours le cas. La réponse est non, mais la plus petite valeur de n qui convient comme contre exemple est n = 105.*

I.3. Montrer, par récurrence sur n, que les polynômes Φ_n sont à coefficients dans **Z**.

Partie II. Irréductibilité sur Q des polynomes Φ_n.

On se propose de montrer que Φ_n est le polynôme minimal sur **Q** *de toute racine $n^{ième}$ primitive de l'unité. Et en conséquence Φ_n sera irréductible.*

Dans cette partie, on pourra utiliser sans démonstration le lemme suivant :

Lemme : si P et Q sont deux polynômes unitaires de **Q**[X], et que leur produit PQ est un polynôme de **Z**[X], alors P et Q sont tous deux dans **Z**[X].

II.1. Soit ω une racine $n^{ième}$ primitive de l'unité, et f son polynôme minimal sur **Q**. Justifier que f est élément de **Z**[X].

Soit p un nombre premier avec n, alors ω^p est aussi une racine $n^{ième}$ primitive de l'unité. Soit g son polynôme minimal. Comme ci-dessus, $g \in \mathbf{Z}[X]$. On veut montrer que ω^p est une racine de f. Pour cela, il suffit de voir que f = g.

II.2. On raisonne par l'absurde en supposant que $f \neq g$.

II.2.a. Montrer alors que f(x) divise $g(X^p)$ dans **Z**[X].

II.2.b. En prenant les classes modulo p, montrer que , si φ(X) est un diviseur irréductible de $\overline{f(X)}$ dans $\frac{Z}{pZ}[X]$, son carré divise $X^n - \overline{1}$ dans $\frac{Z}{pZ}[X]$.

II.2.c. Conclure à une contradiction en dérivant (au sens polynomial).

Donc f = g.

On vient donc de montrer que si $p \wedge n = 1$, ω^p est aussi racine de f.

II.3. Soit $u = \omega^h$ avec $h \wedge n = 1$, une racine $n^{ième}$ *primitive* de l'unité. En décomposant h en facteurs premiers, montrer que u est elle aussi une racine de f.

II.4. Conclure au théorème énoncé.

Partie III. Conditions nécéssaires pour être un angle constructible.

Rappel : Un angle est dit constructible si son cosinus l'est.

III.1. Montrer que pour $m \wedge n = 1$ l'angle $2\pi/mn$ est constructible *ssi* les angles $2\pi/m$ et $2\pi/n$ le sont. En déduire que, pour $n \geq 3$, $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, le polygone régulier à n côtés est constructible *ssi* les angles $2\pi/p_i^{\alpha_i}$ le sont.

On s'intéresse donc désormais aux angles $2\pi/p^{\alpha}$ où p est un nombre premier impair (le cas p=2 étant trivial). Soit alors p un nombre premier impair tel que, si on note $q = p^{\alpha}$, l'angle $2\pi/q$ soit constructible. On pose $\omega = \cos 2\pi/q + i \sin 2\pi/q$.

III.2. Montrer que $[\mathbf{Q}(\omega) : \mathbf{Q}(\cos 2\pi/q)] = 2$. En déduire, par les résultats du II, que l'exposant α est égal à 1 et que p est de la forme $2^k + 1$.
III.3. En déduire que si un angle $2\pi/p^{\alpha}$, où p est un nombre premier impair, est constructible, alors $\alpha = 1$, et p est un nombre premier de Fermat ($p = 1 + 2^{2^k}$).

Partie IV. La condition nécessaire est suffisante

À la question IV.2, on pourra utiliser sans démonstration le résultat suivant :

Soit L une extension d'un corps K et a et b deux éléments de L, algébriques sur K et de même polynôme minimal sur K. Alors il existe un isomorphisme de corps σ, de K(a) sur K(b), laissant K invariant et tel que $\sigma(a) = b$.

Soit $p = 1 + 2^n$, un nombre premier de Fermat (n est une puissance de 2 - c.f. III.3 - mais cela ne servira pas ici). On pose $\omega = \cos 2\pi/p + i \sin 2\pi/p$, et $K = \mathbf{Q}(\omega)$.

IV.1. Justifier que $\{1, \omega, \ldots, \omega^{p-2}\}$ est une base de K considéré comme **Q**-ev.
IV.2. On note G le groupe des automorphismes de K. Soit $g \in G$. Montrer que $g(\omega)$ est un élément de $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$, puis, en utilisant le résultat énoncé ci-dessus, que les g_k, définis par $g_k(\omega) = \omega^k$ sont de tels automorphismes. Quel est le cardinal de G ?
IV.3. Montrer que l'application $G \to (Z/pZ)^* : g_k \to \overline{k}$ est un isomorphisme de groupe. En déduire qu'il existe un élément g de G tel que $G = \{g^h / 1 \leq h \leq p-1\}$.
IV.4. Montrer que $\{g^h(\omega) / 1 \leq h \leq p-1\}$ est aussi une base de K sur **Q**.

À l'issue de cette première partie, on dispose d'un groupe cyclique d'ordre une puissance de 2. Avec son générateur g, on va construire une suite de sous-groupes emboités auxquels - par les invariants - on va faire correspondre une suite de sous-corps emboités. C'est à partir de cette suite de sous-corps que l'on va construire une tour d'extenstons quadratiques jusqu'à cos $2\pi/p$.

On note donc, pour $1 \leq i \leq n$, $G_i = < g^{2^i} >$ le sous groupe de G engendré par g^{2^i}. On pose $G_o = G$, on a $G_n = \{Id\}$. À cette suite de sous-groupes, on associe une suite de sous corps $K_i = \{ z \in K / g^{2^i}(z) = z\}$.

IV.5. Montrer que $K_i \subset K_{i+1}$. En déduire l'inclusion $K_0 \subset K_1 \subset \ldots \subset K_{n-1} \subset K_n = K$.
IV.6. En utilisant la base du IV.4, montrer que $K_0 = \mathbf{Q}$.
IV.7. En donnant un élément z de K tel que $g(z) \neq z$ et $g^2(z) = z$, montrer que l'inclusion $K_0 \subset K_1$ est *stricte*. (Considérer par exemple $z = \omega + g^2(\omega) + g^4(\omega) + \ldots + g^{2^n-2}(\omega)$)
Justifier de même que $K_i \subset K_{i+1}$ est elle aussi *stricte* pour tout i. ($z = \omega + g^{2^{i+1}}(\omega) + \ldots$)
IV.8. On pose $f = g^{2^{n-1}}$, soit $K_{n-1} = \{z \in K / f(z) = z\}$, et $f(\omega) = \omega^{\lambda}$.
IV.8.a. Montrer que $p \mid \lambda^2 - 1$. En déduire que $f(\omega) = \omega^{-1}$.
IV.8.b. Déduire de 8.a. que $\cos 2\pi/p \in K_{n-1}$.
IV.8.c. Calculer $[K : \mathbf{Q}(\cos 2\pi/p)]$ (c.f. III.2). En déduire que $K_{n-1} = \mathbf{Q}(\cos 2\pi/p)$.
IV.9. En utilisant IV.7, montrer que la suite $\mathbf{Q} = K_0 \subset K_1 \subset \ldots \subset K_{n-1}$ est une tour d'extension quadratique. Conclure alors au théorème de Gauss.