Polynômes cyclotomiques

Définition 1. ***Groupe des racines n-ième de l'unité***

Soit $n \in \mathbb{N}^*$. On note $\mathbb{U}_n = \{z \in \mathbb{C}; z^n = 1\} = \left\{e^{\frac{2ik\pi}{n}}; k \in \mathbb{Z}\right\}$ le groupe multiplicatif des racines n-ièmes de l'unité.

Le groupe $\mathbb{U}_n$ est cyclique d'ordre n, engendré par $w = e^{\frac{2i\pi}{n}}$.

Définition 2. ***Racines primitives n-ième de l'unité***

On dit que $x \in \mathbb{U}_n$ est une racine primitive n-ième de l'unité si x engendre/est un générateur du groupe $\mathbb{U}_n$. On note $\mathbb{U}_n^*$ l'ensemble de ces racines.

Proposition 1. *On a $\mathbb{U}_n^* = \left\{e^{\frac{2ik\pi}{n}}; k \in [\![1; n]\!] \text{ et } k \wedge n = 1\right\}$. Ainsi $\mathbb{U}_n^*$ correspond aux racines n-ième de l'unité d'ordre n.*

Proposition 2. *On a l'égalité :* $\text{card}(\mathbb{U}_n^*) = \varphi(n) = \text{card}\{k \in [\![1; n]\!]; k \wedge n = 1\}$.

Définition 3. ***Polynôme cyclotomique d'indice n***

Soit $n \in \mathbb{N}^*$. On appelle polynôme cyclotomique d'indice n le polynôme :

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

On a donc : $\deg(\Phi_n) = \text{card}(\mathbb{U}_n^*) = \varphi(n)$.

Lemme 1. *L'ensembles des racines primitives n-ièmes de l'unité forme une partition des racines n-ièmes de l'unité. On a :*

$$\mathbb{U}_n = \bigsqcup_{d|n} \mathbb{U}_d^*.$$

Démonstration :

Soit $d|n$ et $z \in \mathbb{U}_d^*$. Alors $z^n = (z^d)^{\frac{n}{d}} = 1$. Donc $z \in \mathbb{U}_n$. Ainsi $\bigcup_{d|n} \mathbb{U}_d^* \subset \mathbb{U}_n$.

Réciproquement, soit $z \in \mathbb{U}_n$. Alors $z = e^{\frac{2ik\pi}{n}} = w^k$ avec $k \in [\![1; n]\!]$. Alors z est d'ordre $d = \frac{n}{n \wedge k}$ donc appartient à $\mathbb{U}_d^*$ avec $d|n$.

On obtient bien l'égalité $\bigcup_{d|n} \mathbb{U}_d^* = \mathbb{U}_n$.

Cette union est bien disjointe par unicité de l'ordre d'un élément dans un groupe. □

Remarque 1. On a montré que $\text{card}(\mathbb{U}_n) = \sum_{d|n} \text{card}(\mathbb{U}_n^*)$, on en déduit la relation : $n = \sum_{d|n} \varphi(d)$.

Théorème 1. *Pour tout $n \in \mathbb{N}^*$, on a :*

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

Démonstration :

Commes les $\mathbb{U}_d^*$ où $d|n$ forment une partition de $\mathbb{U}_n$, on obtient :

$$X^n-1=\prod_{z\in\mathbb{U}_n}(X-z)=\prod_{d|n}\prod_{z\in\mathbb{U}_d^*}(X-z)=\prod_{d|n}\Phi_d(X).$$

□

Remarque 2. Pour calculer le polynôme cyclotomique d'indice n si l'on connait ceux d'avant, on utilise la relation :

$$\Phi_n(X)=\frac{X^n-1}{\prod_{\substack{d|n\\ d\neq n}}\Phi_d(X)}.$$

Proposition 3. *Si $p\in\mathbb{N}^*$ est premier, alors $\Phi_p(X)=\sum_{k=0}^{p-1}X^k=1+X+\cdots+X^{p-1}$.*

Démonstration :

Si p est premier, alors :

$$X^p-1=\prod_{d|p}\Phi_d(X)=\Phi_p(X).\Phi_1(X)=\Phi_p(X).(X-1).$$

Donc $\Phi_p(X)=\frac{X^p-1}{X-1}=\sum_{k=0}^{p-1}X^k$. □

Exemple 1.

$$\Phi_1(X)=X-1.$$

$$\Phi_2(X)=\frac{X^2-1}{X-1}=X+1.$$

$$\Phi_3(X)=\frac{X^3-1}{X-1}=X^2+X+1.$$

$$\Phi_4(X)=\frac{X^4-1}{(X-1)(X+1)}=X^2+1.$$

$$\Phi_5(X)=\frac{X^5-1}{X-1}=X^4+X^3+X^2+X+1.$$

$$\Phi_6(X)=\frac{X^6-1}{\Phi_1\Phi_2\Phi_3}=\frac{X^6-1}{(X-1)(X+1)(X^2+X+1)}=\frac{X^6-1}{(X^3-1)(X+1)}=\frac{X^3+1}{X+1}=X^2-X+1.$$

$$\Phi_7(X)=\frac{X^7-1}{X-1}=X^6+X^5+X^4+X^3+X^2+X+1.$$

$$\Phi_8(X)=\frac{X^8-1}{\Phi_1\Phi_2\Phi_4}=\frac{X^8-1}{(X^2-1)(X^2+1)}=\frac{X^8-1}{X^4-1}=X^4+1.$$

Proposition 4. *Soit $n\in\mathbb{N}^*$. On a $\Phi_n(X)\in\mathbb{Z}[X]$.*

Démonstration :

On prouve le résultat par récurrence forte sur n.

Initialisation : pour $n=1$, on a $\Phi_n(X)=X-1\in\mathbb{Z}[X]$.

Hérédité : Soit $n\in\mathbb{N}^*$. On suppose que le résultat est vrai pour tout entier $0<d<n$. On montre que $\Phi_n(X)\in\mathbb{Z}[X]$.

Par hypothèse de récurrence, le polynôme $P=\prod_{\substack{d|n\\ d\neq n}}\Phi_d(X)$ est un élément de $\mathbb{Z}[X]$.

On sait que $X^n-1=\Phi_n(X).P(X)$. Comme P est unitaire, on peut effectuer la division euclidienne dans $\mathbb{Z}[X]$ de X^n-1 par P. Ainsi $X^n-1=PQ+R$ avec $Q,R\in\mathbb{Z}[X]$ et $\deg(R)<\deg(P)$.

On en déduit que $R(X)=(X^n-1)-P(X)Q(X)=P(X)\big(\Phi_n(X)-Q(X)\big)$. Ainsi par condition sur les degrés, on obtient que $\Phi_n(X)=Q(X)$ (car Φ_n est unitaire).

Finalement, $\Phi_n\in\mathbb{Z}[X]$.

(On aurait pû directement utiliser le lemme 2 car $X^n-1\in\mathbb{Z}[X]$, et $\Phi_n(X)$ et P sont unitaires).

Donc la propriété est héréditaire.

Conclusion : par principe de récurrence, on en conclut que $\Phi_n(X)\in\mathbb{Z}[X]$ pour tout $n\in\mathbb{N}^*$. □

Lemme 2. *Soit $P,Q\in\mathbb{Q}[X]$ non nuls. On suppose que $PQ\in\mathbb{Z}[X]$. On suppose que P et Q sont unitaires. Alors P et Q sont dans $\mathbb{Z}[X]$.*

Démonstration :

On pose m le PPCM des dénominateurs de P et Q. On a alors $mP=P_1\in\mathbb{Z}[X]$ et $mQ=Q_1\in\mathbb{Z}[X]$.

Donc $m^2PQ=P_1Q_1$ dans $\mathbb{Z}[X]$ et en passant aux contenus, on obtient : $m^2c(PQ)=c(P_1)c(P_2)$. Or $c(PQ)=1$ car PQ est unitaire dans $\mathbb{Z}[X]$. Ainsi $m^2=c(P_1)c(P_2)$, et $c(P_1)$ et $c(Q_1)$ divisent m car m est le coefficient dominant de ces polynômes (par définition).

Donc $c(P_1)=c(Q_1)=m$.

Finalement : $P=\frac{P_1}{c(P_1)}\in\mathbb{Z}[X]$ et $Q=\frac{Q_1}{c(Q_1)}\in\mathbb{Z}[X]$. □

Théorème 2. *Pour tout $n\in\mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

Démonstration :

Soit $\omega\in\mathbb{C}$ une racine n-ième primitive de l'unité : $\omega\in\mathbb{U}_n^*$.

Soit p un nombre premier ne divisant pas n.

Alors ω^p est une autre racine primitive n-ième de l'unité, car les générateurs de $\mathbb{U}_n$ sont les ω^m où $\text{pgcd}(m,n)=1$.

Soit $f\in\mathbb{Q}[X]$ le polynôme minimal de ω sur $\mathbb{Q}$.

Notre but va être de montrer que $\Phi_n=f$ pour en déduire l'irréductibilité de Φ_n.

Par minimalité de f, f divise X^n-1 dans $\mathbb{Q}[X]$:

$$X^n-1=f(X).h(X)\quad \text{avec } h(X)\in\mathbb{Q}[X].$$

Or $X^n-1\in\mathbb{Z}[X]$ et comme f et X^n-1 sont unitaires, h aussi. D'après le lemme 2, $h\in\mathbb{Z}[X]$ et $f\in\mathbb{Z}[X]$.

Montrons maintenant que si u est racine de f, alors u^p est aussi racine de f.

Comme f divise X^n-1 dans $\mathbb{Z}[X]$, on a alors $u^n-1=0$. Donc u est une racine n-ième de l'unité. On obtient alors que u^p est aussi une racine de l'unité. Ainsi :

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

Par l'absurde, on suppose que $f(u^p)\neq 0$.

Alors par intégrité de $\mathbb{C}$, on obtient que $h(u^p)=0$. D'où u est racine du polynôme $h(X^p)$.

Or u est racine de f, qui est unitaire et irréductible dans $\mathbb{Q}[X]$: f est donc le polynôme minimal de u sur $\mathbb{Q}$.

Ainsi par minimalité de f, f divise $h(X^p)$ dans $\mathbb{Q}[X]$:

$$h(X^p)=f(X).g(X) \quad \text{avec } g(X)\in\mathbb{Q}[X]. \tag{1}$$

Comme $h(X^p)\in\mathbb{Z}[X]$, et que f et $h(X^p)$ sont unitaires, toujours d'après le lemme 2, $g(X)\in\mathbb{Z}[X]$.

On peut alors réduire modulo p l'égalité (1). Il vient :

$$\left(\overline{h(X)}\right)^p=\overline{h(X^p)}=\overline{f(X)}\,\overline{g(X)} \quad \text{dans } \mathbb{F}_p[X].$$

En effet, si l'on écrit $h(X)=X^r+a_{r-1}X^{r-1}+\cdots+a_0\in\mathbb{Z}[X]$, on obtient $h(X^p)=X^{pr}+a_{r-1}X^{p(r-1)}+\cdots+a_1X^p+a_0$. Or d'après les propriétés du morphisme de Frobenius, comme $\bar{a_i}=\bar{a_i}^p$ dans $\mathbb{F}_p$, on a :

$$\begin{aligned}
\overline{h(X^p)} &= X^{pr}+\overline{a_{r-1}}X^{p(r-1)}+\cdots+\bar{a_1}X^p+\bar{a_0}\\
&= X^{pr}+(\overline{a_{r-1}}X^{r-1})^p+\cdots+(\bar{a_1}X)^p+\bar{a_0}^p\\
&= (X^r+\overline{a_{r-1}}X^{r-1}+\cdots+\bar{a_1}X+\bar{a_0})^p\\
&= \left(\overline{h(X)}\right)^p.
\end{aligned}$$

Maintenant soit $\theta\in\mathbb{F}_p[X]$ un facteur irréductible de $\overline{f(X)}$. Alors θ divise $\left(\overline{h(X)}\right)^p$ donc divise $\overline{h(X)}$ dans $\mathbb{F}_p[X]$. D'où θ^2 divise $\overline{f(X)}\overline{h(X)}=X^n-\bar{1}$ dans $\mathbb{F}_p[X]$.

Donc $X^n-\bar{1}$ possède une racine double θ dans $\mathbb{F}_p[X]$. Or la dérivée de $X^n-\bar{1}$ est $\bar{n}X^{n-1}$. Comme p ne divise pas n, alors 0 serait la seule racine du polynôme dérivé, et comme 0 n'annule pas $X^n-\bar{1}$, alors $X^n-\bar{1}$ n'admet que des racines simples dans $\mathbb{F}_p[X]$.

Contradiction. Donc $f(u^p)=0$ pour toute racine u de f.

D'après le travail fait précédemment, comme ω est racine de f, alors ω^p est racine de f. Or les racines primitives n-ièmes sont de la forme ω^m avec $m=\prod_{i=1}^r p_i^{\alpha_i}$ et $p_i\nmid n$. Par récurrence immédiate, ω^{p_1} puise $(\omega^{p_1})^{p_1}$ puis $\omega^{p_1^{\alpha_1}}$ puis $\left(\omega^{p_1^{\alpha_1}}\right)^{p_2^{\alpha_2}}$ sont racines de f. Donc toutes les racines primitives n-ièmes de l'unité sont racines de f.

D'où : $\deg(f)\geqslant\varphi(n)$.

Or comme ω est racine de $\Phi_n(X)$, alors par minimalité, $f(X)$ divise $\Phi_n(X)$ dans $\mathbb{Q}[X]$.

Comme $\deg(\Phi_n)=\varphi(n)$ et que $f(X)$ et $\Phi_n(X)$ sont tous les deux unitaires, on déduit que $f(X)=\Phi_n(X)$.

Finalement, $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$, donc dans $\mathbb{Z}[X]$ car il est primitif. □

Corollaire 1. *Le polynôme minimal sur $\mathbb{Q}$ de toute racine primitive n-ième de l'unité ω_n dans $\mathbb{C}$, est $\Phi_n(X)$. Donc $[\mathbb{Q}(\omega_n):\mathbb{Q}]=\varphi(n)$.*

En effet, $\Phi_n(\omega_n)=0$ et Φ_n est unitaire et irréductible sur $\mathbb{Q}[X]$.