Irréductibilité des polynômes cyclotomiques

Références : [Gou94] p.92-94 ([Mé06]).

Pour tout $n \in \mathbb{N}$, on pose $\mathcal{U}_n = \{e^{\frac{2i\pi k}{n}}, k \in \mathbb{Z}\}$.

Définition 0.1 *On dit qu'un élément $x \in \mathcal{U}_n$ est une racine primitive n-ième de l'unité si x engendre le groupe multiplicatif $\mathcal{U}_n$.*

NOTATION : Π_n l'ensemble des racines primitives n-ième de l'unité.

Définition 0.2 *On pose $\phi_n = \prod_{\xi \in \Pi_n}(X - \xi)$ le polynôme cyclotomique d'indice n.*

Théorème 0.1 *Les polynômes cyclotomiques ϕ_n sont irréductibles dans $\mathbb{Q}[X]$.*

Démonstration

Étape 1 Montrons que :

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

Et déduisons-en que $\forall n \in \mathbb{N}^*$, $\phi_n \in \mathbb{Z}[X]$.
On pose $\omega = e^{\frac{2i\pi}{n}}$. Soit $0 \leq k \leq n-1$. Soit d l'ordre de ω^k dans $\mathcal{U}_n$. Alors on a $d|n$.
Par ailleurs, $(\omega^k)^d = 1$ donc $\omega^k \in \mathcal{U}_d$ et ω^k étant d'ordre d, on a même que $\omega^k \in \Pi_d$.
On en déduit que $(X - \omega^k)|\phi_d$ donc $(X - \omega^k)|\prod_{d|n} \phi_d$.
Les ω^k pour $0 \leq k \leq n-1$ étant distincts, on en déduit que :

$$X^n - 1 = \prod_{k=0}^{n-1}(X - \omega^k)|\prod_{d|n} \phi_d$$

Ces polynômes étant de plus unitaires et de même degré (car $\deg(\prod_{d|n} \phi_d) = \sum_{d|n} \deg(\phi_d) = \sum_{d|n} \phi(d) = n$), ils sont égaux.
Montrons que $\forall n \in \mathbb{N}^*$, $\phi_n \in \mathbb{Z}[X]$ par récurrence.

- $\mathbf{n = 1}$ $\phi_1 = X - 1 \in \mathbb{Z}[X]$.
- On suppose le résultat vrai au rang $n-1$, montrons-le au rang n.
  D'après l'hypothèse de récurrence, le polynôme $P = \prod_{d|n, d \neq n} \phi_d \in \mathbb{Z}[X]$.
  Par ailleurs $X^n - 1 = \phi_n P$, P étant unitaire, on peut effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$, ie $\exists Q, R \in \mathbb{Z}[X]$, $X^n - 1 = PQ + R$ avec $\deg(R) < \deg(Q)$.
  Il y a de plus unicité du couple (Q, R) dans $\mathbb{C}[X]$ donc dans $\mathbb{Z}[X]$ et nécessairement $Q = \phi_n$ et $R = 0$. Donc $\phi_n \in \mathbb{Z}[X]$ (car $Q \in \mathbb{Z}[X]$).

Étape 2 Montrons qu'on peut écrire $\phi_n = F_1 F_2 \dots F_r$ avec les $F_i \in \mathbb{Z}[X]$ unitaires irréductibles dans $\mathbb{Q}[X]$.
Soit $\phi_n = G_1 G_2 \dots G_r$ la décomposition de ϕ_n en facteurs irréductibles unitaires de $\mathbb{Q}[X]$.
On sait que $\forall i$, il existe $\alpha_i \in \mathbb{N}^*$ (prendre α_i égal au maximum des dénominateurs des coefficients de G_i) tel que $\alpha_i G_i \in \mathbb{Z}[X]$.
On a donc $\alpha_1 \alpha_2 \dots \alpha_r \phi_n = (\alpha_1 G_1) \dots (\alpha_r G_r)$.
Or d'après le lemme de Gauss, on sait que :

$$\alpha_1 \dots \alpha_r = c(\alpha_1 \dots \alpha_r \phi_n) = \prod_{i=1}^{r} c(\alpha_i G_i)$$

Or $\forall i$, le polynôme $F_i = \dfrac{\alpha_i G_i}{c(\alpha_i G_i)} \in \mathbb{Z}[X]$ et on a $\phi_n = F_1 \dots F_r$.
De plus pour tout i, $F_i \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ et est unitaire puisque ϕ_n l'est.

Étape 3 Soit ξ une racine de F_1 dans $\mathbb{C}$. Soit p premier tel que p ne divise pas n. Montrons que $\exists i \in \{1,\dots,r\}$ tel que $F_i(\xi^p)=0$.
L'élément ξ est racine de F_1 donc de ϕ_n donc $\xi \in \Pi_n$.
Or p est premier et p ne divise pas n, donc p est premier avec n et donc $\xi^p \in \Pi_n$, d'où ξ^p racine de ϕ_n, ie $\exists i \in \{1,\dots,r\}$ tel que $F_i(\xi^p)=0$.

Étape 4 (à ne pas faire lors du développement) Pour tout $F=\sum_{k=0}^m a_k X^k \in \mathbb{Z}[X]$, on pose $\overline{F}=\sum_{k=1}^m \overline{a_k}X^k \in \mathbb{Z}/p\mathbb{Z}[X]$. Montrons que $\forall F \in \mathbb{Z}[X]$, $\overline{F}(X^p)=(\overline{F}(X))^p$.
On montre cette relation par récurrence sur $m=\deg(F)$.

- $\mathbf{m=1}$ c'est évident.
- Supposons le résultat vrai jusqu'au rang $m-1$ et montrons-le au rang m.
  On écrit : $F=\sum_{k=0}^m a_k X^k = a_m X^m + G$. D'après l'hypothèse de récurrence, on a $\overline{G}(X)^p=\overline{G}(X^p)$.
  Or :
  $$\overline{F}^p=(\overline{G}+\overline{a_m}X^m)^p=\overline{G}^p+\overline{a_m}^p X^{mp}+\sum_{k=1}^{p-1} C_k^p \overline{G}^k \overline{a_m}^{p-k} X^{(p-k)m}$$
  et comme pour $1\le k\le m-1$, $p|C_k^p$ et d'après le théorème de Fermat $\overline{a_m}^p=\overline{a_m}$, on en déduit :
  $$\overline{F}(X)^p=\overline{G}(X)^p+\overline{a_m}X^{mp}=\overline{G}(X^p)+\overline{a_m}(X^p)^m=\overline{F}(X^p)$$

Étape 5 Montrons que dans $\mathbb{Z}/p\mathbb{Z}[X]$, $\overline{\phi_n}$ n'est divisible par le carré d'aucun polynôme non constant.
Supposons que $\overline{\phi_n}=\overline{Q}^2\overline{P}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Si $R=\prod_{d|n,d\neq n}\phi_d \in \mathbb{Z}[X]$, on a $X^n-1=\phi_n R$ d'après l'étape 1.
Ainsi $X^n-\overline{1}=\overline{\phi_n R}=\overline{Q}^2\overline{S}$ (avec $S=PR$) d'où par dérivation :
$$\overline{n}X^{n-1}=2\overline{QQ'}\overline{S}+\overline{Q}^2\overline{S'}$$
donc $\overline{Q}|\overline{n}X^{n-1}$, donc $\overline{Q}|\overline{n}X^n$.
Or $\overline{Q}|(\overline{n}X^n-\overline{n})$ (car $\overline{Q}|(X^n-\overline{1})$) donc $\overline{Q}$ divise la différence, ie $\overline{Q}|\overline{n}$.
Or p ne divise pas n donc $\overline{n}\neq\overline{0}$ et donc $\overline{Q}$ est constant.

Étape 6 Montrons que $F_1(\xi^p)=0$.
Comme $F_i(\xi^p)=0$, $F_1(X)$ et $F_i(X^p)$ ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.
En effet, si on suppose le contraire, d'après le théorème de Bézout $\exists U,V\in\mathbb{Q}[X]$ tels que $U(X)F_1(X)+V(X)F_i(X^p)=1$.
D'où $U(\xi)F_1(\xi)+V(\xi)F_i(\xi^p)=0=1$, ce qui fournit une contradiction.
De plus, F_1 est irréductible dans $\mathbb{Q}[X]$ donc $F_1(X)|F_i(X^p)$ dans $\mathbb{Q}[X]$.
Comme F_1 est unitaire, $F_1(X)$ divise $F_i(X^p)$ dans $\mathbb{Z}[X]$. On en déduit que $\overline{F_1}(X)|\overline{F_i}(X^p)=\overline{F_i}(X)^p$ d'après l'étape 4.
Ceci étant, soit $\overline{P}\in\mathbb{Z}/p\mathbb{Z}[X]$ un facteur irréductible de $\overline{F_1}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. On a alors $\overline{P}|\overline{F_i}(X)^p$ donc $\overline{P}|\overline{F_i}$.
Par conséquent si $i\neq 1$, on voit que $\overline{P}^2|\overline{\phi_n}=\overline{F_1}\dots\overline{F_r}$; ce qui est impossible d'après l'étape 5.
Donc $i=1$.

Étape 7 Montrons que $\forall k$ entier premier avec n, on a $F_1(\xi^k)=0$.
Soit k un entier premier avec n. Écrivons $k=p_1p_2\dots p_s$, les p_i étant des nombres premiers. Montrons par récurrence sur s que $F_1(\xi^k)=0$.

- $\mathbf{s=1}$ c'est le résultat de l'étape 6.
- Supposons le résultat vrai au rang $s-1$ et montrons-le au rang s.
  Comme k est premier avec n, on a $p_1p_2\dots p_{s-1}$ est premier avec n donc d'après l'hypothèse de récurrence $F_1(\xi^{p_1\cdots p_{s-1}})=0$.
  Or p_s est aussi premier avec n, donc $F_1((\xi^{p_1\cdots p_{s-1}})^{p_s})=0$, d'où le résultat.

Conclusion Pour tout nombre entier k premier avec n, on a $F_1(\xi^k)=0$. Or $\xi\in\Pi_n$, donc $\Pi_n=\{\xi^k, k\wedge n=1\}$. Tous les éléments de Π_n sont donc des racines de F_1, ce qui prouve que $\phi_n=F_1$, donc ϕ_n est irréductible dans $\mathbb{Q}[X]$.

Lemmes utilisés

Lemme 0.1 (Lemme de Gauss) *Soient $P, Q \in \mathbb{Z}[X]$. Alors $c(PQ) = c(P)c(Q)$, où $c(P)$ désigne le pgcd des coefficients de P.*

Démonstration On pose :

$$P_1 = \frac{P}{c(P)} \in \mathbb{Z}[X] \qquad Q_1 = \frac{Q}{c(Q)} \in \mathbb{Z}[X]$$

Alors $c(P_1) = 1$ et $c(Q_1) = 1$.
Si $c(P_1Q_1) > 1$, alors il existe un nombre premier p divisant $c(P_1Q_1)$. Mais alors on a $p|c(P_1)$ ou $p|c(Q_1)$, ce qui est absurde, donc $c(P_1Q_1) = 1$.
Donc $c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$.
Montrons maintenant que si $p|c(PQ)$ alors $p|c(P)$ ou $p|c(Q)$.
Si $P = \sum_{k=0}^{m} a_k X^k \in \mathbb{Z}[X]$, on note $\overline{P} = \sum_{k=0}^{m} \overline{a_k} X^k \in \mathbb{Z}/p\mathbb{Z}[X]$. Si $p|c(PQ)$, alors p divise tous les coefficients de PQ, donc on a $\overline{PQ} = \overline{P}\,\overline{Q} = 0$. Or comme $\mathbb{Z}/p\mathbb{Z}$ est intègre (car p étant premier c'est un corps), alors $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre, donc $\overline{P} = 0$ ou $\overline{Q} = 0$. D'où le résultat.

Lemme 0.2 *Si A est un anneau intègre, alors $A[X]$ et $A[[X]]$ le sont aussi.*

Démonstration Montrons-le pour $A[[X]]$ par contraposée.
Soient $P, Q \in A[[X]]$ non nuls. Supposons que le premier terme non nul de P soit $p_k X^k$ et que le premier terme non nul de Q soit $q_l X^l$. Alors le coefficient de X^{k+l} dans PQ est $p_k q_l$, qui est non nul puisque A est intègre. Donc PQ est non nul.

Lemme 0.3 *Soit p un nombre premier. Soit $1 \leq k \leq p-1$, alors p divise C_k^p.*

Démonstration

$$C_k^p = \frac{p!}{k!(p-k)!}$$

donc $p! = k!(p-k)!C_k^p$.
Et $p|p!$ donc $p|k!(p-k)!C_k^p$.
Or p est premier avec $k!(p-k)!$ car $k!(p-k)! = 1 \dots k \times 1 \dots (p-k)$ et dans ce produit aucun terme ne divise p car $k \leq p-1$. Donc d'après le théorème de Gauss p divise C_k^p.

Lemme 0.4 (Théorème de Gauss) *Soient a et b deux entiers non nuls premiers entre eux et n un entier. Si $a|bn$, alors $a|n$.*

Démonstration Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au - bv = 1$.
Comme $a|bn$ alors $\exists x \in \mathbb{Z}$ tel que $ax = bn$, d'où $axv = bnv = (au-1)n$. D'où $n = aun - avx = a(un - vx)$.
D'où le résultat.

Lemme 0.5 *Pour tout $n \geq 2$:*

$$\sum_{d|n} \deg(\phi_d) = \sum_{d|n} \phi(d) = n$$

où ϕ désigne l'indicatrice d'Euler, ie $\phi(d) = \{k, k \wedge d = 1\}$.

Démonstration Montrons pour $n \geq 2$ que $\sum_{d|n} \phi(d) = n$.
On considère les fractions $\frac{1}{n}, \frac{2}{n}, \dots \frac{n-1}{n}, \frac{n}{n}$ et on cherche à les mettre sous la forme irréductible $\frac{a}{d}$ avec d divisant n.
Pour chaque d divisant n, il y a $\phi(d)$ possibilités pour le numérateur a, car le nombre d'entier a tel que a soit premier avec d est $\phi(d)$ (on peut seulement choisir a parmi ceux-ci car sinon la fraction ne sera pas irréductible).
Comme il y a en tout n fractions, on en déduit le premier résultat.
Montrons que $\sum_{d|n} \deg(\phi_d) = \sum_{d|n} \phi(d)$.
Comme $\phi_d = \sum_{\xi \in \Pi_d} (X - \xi)$, alors $\deg(\phi_d) = \operatorname{card} \Pi_d$.
Or $\Pi_d = \{\omega^k, 1 \leq k \leq d-1, k \wedge d = 1\}$, donc $\deg(\phi_d) = \phi(d)$.

Lemme 0.6 (théorème au programme dans le cas d'un corps) *Soit A un anneau. Soient $U, V \in A[X]$.*
On suppose que $V \neq 0$ de coefficient dominant inversible dans A.
Alors $\exists Q, R \in A[X]$ tels que $U = VQ + R$ avec soit $R = 0$, soit $\deg(R) < \deg(V)$.
De plus, si A est intègre, on a unicité du couple (Q, R).

Démonstration **Existence** On procède par récurrence sur le degré de U.
- Si U est nul ou $\deg(U) < \deg(V)$, il suffit de prendre $Q = 0$ et $R = U$.
- Supposons que $\deg(U) \geq \deg(V)$ et que le terme dominant de U soit uX^m et celui de V, vX^s.
  On pose $\overline{U} = U - (uv^{-1}X^{n-s})V$. Il est clair que $\overline{U}$ est nul ou de degré strictement inférieur à celui de V. Par hypothèse de récurrence, il existe $\overline{Q}, R \in A[X]$ tels que $\overline{U} = \overline{Q}V + R$, avec $R = 0$ ou $\deg(R) < \deg(V)$. Ainsi $U = (uv^{-1}X^{n-s} + \overline{Q})V + R$.

Unicité On suppose que $U = VQ + R$ avec $R = 0$ ou $\deg(R) < \deg(V)$ et que $U = VQ' + R'$ avec $R' = 0$ ou $\deg(R') < \deg(V)$.
Alors $V(Q - Q') = R - R'$.
Si $R \neq R'$, alors $R - R'$ est de degré strictement inférieur à celui de V, or $V|(R - R')$ ce qui est absurde car A intègre.
Si $R = R'$ alors $Q = Q'$ par intégrité de A car $V \neq 0$.

Lemme 0.7 *Soient $P, Q \in \mathbb{Q}[X]$. Si $P|Q$ dans $\mathbb{Q}[X]$ et P unitaire, alors $P|Q$ dans $\mathbb{Z}[X]$.*

Démonstration Dans $\mathbb{Z}[X]$, on sait $\exists A, R \in \mathbb{Z}[X]$ tels que $Q = PA + R$ (d'après le théorème précédent sans se soucier de l'unicité, on va utiliser un autre moyen de la prouver) mais on n'a pas unicité du couple (A, R).
Or $P|Q$ dans $\mathbb{Q}[X]$, donc $\exists X \in \mathbb{Q}[X]$ tel que $Q = PX$. De plus, on a unicité de la division euclidienne dans $\mathbb{Q}[X]$ car $\mathbb{Q}$ est un corps, donc nécessairement $A = X$ et $R = 0$. Donc $P|Q$ dans $\mathbb{Z}[X]$.
Le fait que P soit unitaire est important sinon on ne pourrait pas appliquer le théorème précédent.

Références

[Gou94] Xavier Gourdon. *Algèbre*. Ellipses, 1994.

[Mé06] Jean-Yves Mérindol. *Nombres et algèbre*. EDP Sciences, 2006.