Irréductibilité des polynômes cyclotomiques

↪ Refs : Perrin p 81 (prop), Gozard p 67-69 (le reste).

On note pour $n \in \mathbb{N}^*$, $\mu_n = \{z \in \mathbb{C}, z^n = 1\}$ les racines n-ièmes de l'unité dans $\mathbb{C}$, et $\mu_n^* = \{z \in \mathbb{C}, z^n = 1 \text{ et } z^d \neq 1 \text{ pour } 1 \leq d < n\}$ $= \{e^{\frac{2ik\pi}{n}}, 1 \leq k \leq n, k \wedge n = 1\}$ les racines primitives n-ièmes de l'unité dans $\mathbb{C}$. (ce sont les générateurs de μ_n, et si $\mu_n = \langle \xi \rangle$, $\mu_n^* = \{\xi^k, k \wedge n = 1\}$) On définit également $\Phi_{n,\mathbb{C}}$ $(= \Phi_n) := \prod_{\xi \in \mu_n^*} (X - \xi)$ le n-ième polynôme cyclotomique. On voit directement que Φ_n est un polynôme unitaire à coefficients dans $\mathbb{C}$ de degré $\varphi(n)$.
On obtient facilement $X^n - 1 = \prod_{d|n} \Phi_d(X)$ (car $\mu_n = \coprod_{d|n} \mu_d^*$).

Proposition : Pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Lemme : (variante du lemme de Gauss) Soient P, A, B des polynômes non nuls de $\mathbb{Q}[X]$. On suppose que $P \in \mathbb{Z}[X]$, que $P = AB$ et que P et A sont unitaires. Alors A et B sont dans $\mathbb{Z}[X]$.

Théorème : Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Q}[X]$, et donc aussi dans $\mathbb{Z}[X]$ puisque c'est un polynôme unitaire (et donc de contenu 1).

Preuve de la proposition : Nous allons montrer le résultat par récurrence forte sur $n \in \mathbb{N}^*$.

* Initialisation : Pour $n = 1$, $\Phi_1(X) = X - 1$ qui est bien dans $\mathbb{Z}[X]$.
* Hérédité : Soit $n \geq 2$ tel que le résultat soit vrai pour les $d < n$.

On pose $F(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$. Alors F est unitaire, et par hypothèse de récurrence, $F \in \mathbb{Z}[X]$. On effectue la division euclidienne de $X^n - 1$ par F dans $\mathbb{Z}[X]$ (ok car F unitaire) : $X^n - 1 = F(X)P(X) + R(X)$ avec $P, R \in \mathbb{Z}[X]$ et $\deg R < \deg F$. Or on sait que sur $\mathbb{C}[X]$, on a $X^n - 1 = F(X)\Phi_n(X)$ donc par unicité de la division euclidienne sur $\mathbb{C}[X]$, on obtient $R = 0$ et $\Phi_n = P \in \mathbb{Z}[X]$. (Si on veut le retrouver, on écrit $F(X)\Phi_n(X) = F(X)P(X) + R(X)$ ie $F(X)(\Phi_n(X) - P(X)) = R(X)$, et donc puisque $\deg F > \deg R$, nécessairement $\Phi_n = P$)
Cela conclut la récurrence.

Preuve du lemme : Puisque A et P sont unitaires, on voit directement que B l'est aussi. On note $A(X) = X^m + \sum_{i=0}^{m-1} a_i X^i$ où pour $i \in [\![0, m-1]\!]$, $a_i \in \mathbb{Q}$. Pour $i \in [\![0, m-1]\!]$, 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. Soit q un multiple commun de $q_0, \ldots, q_{m-1}$, alors $qA(X) = qX^m + \sum_{i=0}^{m-1} r_i X^i$ où les $r_i \in \mathbb{Z}$. Quitte à diviser par

$\mathrm{pgcd}(q, z_0, \dots, z_{n-1})$, on peut supposer $\mathrm{pgcd}(q, z_0, \dots, z_{n-1}) = 1$.
(C'est là que l'hypothèse unitaire est importante : $A = \frac{2}{3}X + \frac{2}{3}$, $3A = 2X+2$ même si on divise par $\mathrm{pgcd}(3,2)=1$, on n'a toujours pas $\mathrm{pgcd}(\text{coeffs})=1$)
Ainsi $A_1 = qA$ est un polynôme de $\mathbb{Z}[X]$ primitif (ie $c(A_1)=1$).
De même, il existe $r \in \mathbb{N}^*$ tel que $B_1 = rB$ soit un polynôme de $\mathbb{Z}[X]$ primitif. Puisque A_1 et B_1 sont primitifs, le lemme de Gauss (cf rappel en remarques) nous dit que A_1B_1 est également primitif.
Donc $qrP = A_1B_1$ est primitif, alors $1 = c(qrP) = qr\,c(P) = qr$ car P est unitaire (donc primitive), ainsi $qr = 1$, et donc $q = r = 1$ ce qui nous permet de conclure $A = A_1 \in \mathbb{Z}[X]$ et $B = B_1 \in \mathbb{Z}[X]$.

<u>Preuve du théorème</u> : Soit $\omega \in \mu_n^*$. Notons f le polynôme minimal de ω sur $\mathbb{Q}$. Nous allons montrer $f = \Phi_n$.
Premièrement, f divise Φ_n dans $\mathbb{Q}[X]$ puisque $\Phi_n(\omega) = 0$.
Montrons maintenant $\deg(f) \geq \varphi(n) = \deg(\Phi_n)$, ce qui nous permettra de conclure puisque f et Φ_n sont unitaires.
Pour montrer cela, nous allons montrer que tout $x \in \mu_n^*$ est racine de f, ie 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, pour la suite : si $k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ alors $f(\omega) = 0 \Rightarrow f(\omega^{p_1}) = 0 \Rightarrow f(\omega^{p_1^2}) = 0 \Rightarrow \cdots \Rightarrow f(\omega^{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}) = 0$)
Maintenant que l'on a bien réduit le problème, allons-y !
Puisque ω est racine de $X^n - 1$, f divise $X^n - 1$ dans $\mathbb{Q}[X]$:
$X^n - 1 = f(X)h(X)$ où $h \in \mathbb{Q}[X]$. Comme $X^n - 1$ et f sont unitaires, et $X^n - 1 \in \mathbb{Z}[X]$, on en déduit que $h \in \mathbb{Z}[X]$ et $f \in \mathbb{Z}[X]$ d'après le lemme.
Soit u racine de f, et p un nombre premier ne divisant pas n. Comme f divise $X^n - 1$ dans $\mathbb{Q}[X]$, on a $u^n - 1 = 0$, ainsi u est une racine n-ième de l'unité dans $\mathbb{C}$, donc u^p aussi : $0 = (u^p)^n - 1 = f(u^p)h(u^p)$.
Supposons $f(u^p) \neq 0$, alors $h(u^p) = 0$. Or u est racine 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 $g \in \mathbb{Q}[X]$ tel que $h(X^p) = f(X)g(X)$. Or $h(X^p)$ est dans $\mathbb{Z}[X]$, $h(X^p)$ et $f(X)$ sont unitaires, donc d'après le lemme, $g \in \mathbb{Z}[X]$.
Réduisons modulo p l'égalité $h(X^p) = f(X)g(X)$: on obtient $(\bar{h}(X))^p = \bar{h}(X^p) = \bar{f}(X)\bar{g}(X)$. Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\bar{f}$. Alors d'après l'égalité précédente, θ divise $\bar{h}^p$ dans $\mathbb{F}_p[X]$

et donc θ divise $\bar{h}$ dans $\mathbb{F}_p[X]$. Ainsi, si on reprend l'égalité (*), que l'on passe modulo p, on obtient $\overline{X^n-1} = \bar{f}(X)\bar{h}(X)$, et donc θ^2 divise $\overline{X^n-1} = X^n - \bar{1}$ dans $\mathbb{F}_p[X]$. On obtient alors une contradiction : $X^n-\bar{1}$ aurait alors 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 $\mathbb{F}_p[X]$ (Bézout : $(\bar{n})^{-1}X\,n X^{n-1} - (X^n-\bar{1}) = \bar{1}$, possible car $p \nmid n$ donc $\bar{n} \neq 0$).

Ainsi $f(\omega^p)=0$. D'après ce que l'on a dit au début, cela permet de conclure que $\deg(f) \geq \deg(\Phi_n)$, et donc $\Phi_n = f$, ce qui conclut puisque f est irréductible sur $\mathbb{Q}[X]$ (car polynôme minimal de ω). On déduit ensuite directement que Φ_n est irréductible sur $\mathbb{Z}[X]$ puisque Φ_n est unitaire donc primitif.

(cf Gozard)

Avant les remarques, quelques rappels sur le contenu : $(c(P))$

Pour A un anneau factoriel, on définit pour $P \in A[X]$ le contenu de P comme le pgcd des coef de P (unique modulo $A^\times$). On dit que P est primitif si $c(P)=1$

Lemme de Gauss : 1) Le produit de deux polynômes primitifs est primitif

2) Pour tout $(P,Q) \in (A[X]\setminus\{0\})^2$, $c(PQ) = c(P)c(Q)$ (modulo $A^\times$).

Pour la preuve de 1) : si P et Q primitifs, on suppose par l'absurde PQ pas primitif alors il existe p divisant tous les coef de PQ, on regarde modulo p : $0 = \overline{PQ} = \bar{P}\bar{Q}$ donc $\bar{P}=0$ ou $\bar{Q}=0$, donc $p \mid c(P)$ ou $p \mid c(Q)$ ↯, le 2) en découle

Autre fait utile : On note $K = \mathrm{Frac}(A)$ (A toujours factoriel). Soit $P \in A[X]$

P est irréductible dans $A[X]$ $\Leftrightarrow$ $\begin{cases} \deg P = 0 \text{ et } P \text{ est irréductible dans } A \end{cases}$ ou $\begin{cases} \deg P \geq 1,\ c(P)=1 \text{ et } P \text{ irréductible dans } K[X]. \end{cases}$

(sert à montrer A factoriel $\Rightarrow A[X]$ factoriel) → contre-ex : $2X$ pas irred dans $\mathbb{Z}[X]$

Remarques : * Quelques exemples de Φ_n : $\Phi_1 = X-1$, $\Phi_2 = X+1$, $\Phi_3 = X^2+X+1$, $\Phi_4 = X^2+1$, etc, et pour p premier, $\Phi_p = \sum_{i=0}^{p-1} X^i$, et plus généralement, pour $n=p^n$, $\Phi_{p^n} = \sum_{i=0}^{p-1} (X^{p^{n-1}})^i$.

* Il faut faire attention aux divisions euclidiennes que l'on fait au cours du développement ! La division euclidienne est normalement valide pour les anneaux euclidiens, donc pour $K[X]$ avec K un corps, mais on fait aussi l'effectuer sur $\mathbb{Z}[X]$ si le diviseur est unitaire (preuve par récurrence). De même, les polynômes minimaux n'ont de sens que sur des corps, car l'anneau des polynômes associé doit être principal (donc pas $\mathbb{Z}[X]$ par exemple).

* On déduit directement du théorème que le polynôme minimal sur $\mathbb{Q}$ de tout ω_n racine primitive n-ième de l'unité sur $\mathbb{C}$ est Φ_n, et alors $[\mathbb{Q}(\omega_n):\mathbb{Q}] = \varphi(n)$ (et donc $[\mathbb{Q}(\mu_n):\mathbb{Q}] = \varphi(n)$).

* On peut utiliser le critère d'Eisenstein pour mtq $\Phi_p(X+1) = \frac{(X+1)^p-1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$

est irréductible dans $\mathbb{Q}[X]$ et donc Φ_p aussi.

* Ce théorème est par exemple utile dans le théorème de Gauss-Wantzel sur les nombres constructibles ! (cf dev correspondant).

* On peut déduire du théorème le fait suivant : Si K est une extension finie de $\mathbb{Q}$, alors il y a un nombre fini de racines de l'unité dans K. En effet : Toute racine de l'unité étant une racine primitive de l'unité, il suffit de mtq il y a un nbr fini de racines primitives de l'unité dans K : si $u \in K$ est une racine primitive n-ième de l'unité, on a, puisque $\mathbb{Q}(u) \subset K$, $[K:\mathbb{Q}(u)]\underbrace{[\mathbb{Q}(u):\mathbb{Q}]}_{=\varphi(n)} = \underbrace{[K:\mathbb{Q}]}_{=:N}$ donc $\varphi(n) \mid N$ et en particulier $\varphi(n) \leq N$. Mais $X = \{n \in \mathbb{N},\ \varphi(n) \leq N\}$ est fini : Si $n \in X$, on écrit $n = \prod_{i=1}^{r} p_i^{m_i}$, alors $\varphi(n) = \prod_{i=1}^{r} (p_i - 1)p_i^{m_i - 1}$. Les p_i vérifient $p_i \leq N+1$ (sinon $p_i - 1 > N$ et $\varphi(n) > N$). Donc il existe un nombre fini de diviseurs p_i possibles pour n. De plus, pour tout $i \in [\![1, r]\!]$, $p_i^{m_i - 1} \leq \varphi(n) \leq N$, donc $m_i \leq 1 + \frac{\ln(N)}{\ln(p_i)} \leq 1 + \frac{\ln(N)}{\ln(2)}$, donc les m_i sont aussi en nombre fini, donc X est fini. (cf Maths Générales 2019)
Cela conclut car pour tout n, μ_n^* est fini.

* On peut définir la notion de polynôme cyclotomique sur un corps quelconque. Soit K un corps, K_n un corps de décomposition de $X^n - 1$ sur K, on note $\mu_n^*(K_n) = \{x \in K_n,\ x \text{ est d'ordre } n\}$ et on définit $\Phi_{n,K} = \prod_{\xi \in \mu_n^*(K_n)} (X - \xi) \in K_n[X]$.
On peut encore montrer $X^n - 1 = \prod_{d \mid n} \Phi_{d,K}(X)$ et $\Phi_{n,K} \in K[X]$.
Si on note $\sigma : \mathbb{Z}[X] \to K[X]$ (induit par $\mathbb{Z} \to K$, $1 \mapsto 1_K$) alors $\Phi_{n,K} = \sigma(\Phi_{n,\mathbb{Q}})$.
Enfin (cf Demazure ou cours de Théo Le's) on peut mtq que $\overline{\Phi_n}$ l'image de Φ_n dans $\mathbb{F}_q[X]$ se décompose en $\frac{\varphi(n)}{r}$ polynômes irréductibles distincts tous de degré r, où r est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

* Autres applications des polynômes cyclotomiques : le théorème de Wedderburn, le théorème de Dirichlet faible ($\forall n \geq 2$, il existe une infinité de nombres premiers $p \equiv 1 [n]$), et de façon générale, c'est utile pour la théorie des extensions cyclotomiques et la théorie de Galois mais bon, cela ne nous regarde pas !