Prérequis. Les polynômes cyclotomiques sont à coefficients entiers ; factorialité de $\mathbf{Z}[X]$.

Théorème 0.0.1. *Le polynôme cyclotomique Φ_n est irréductible sur $\mathbf{Q}$ (donc aussi sur $\mathbf{Z}$).*

Démonstration. Soient ζ une racine primitive n-ème de l'unité de p un nombre premier ne divisant pas n. Comme p et n sont premiers entre eux, ζ^p est aussi une racine primitive n-ème de l'unité.

Par factorialité de $\mathbf{Z}[X]$, on peut écrire $\Phi_n = f_1^{\alpha_1} \cdot \ldots \cdot f_r^{\alpha_r}$ avec les f_i irréductibles distincts. Φ_n est unitaire donc chaque f_i l'est aussi, et ζ est une racine de l'un d'eux, disons f_i qui est alors égal à μ_ζ. De même, ζ^p est racine de l'un d'eux, disons f_j qui est alors égal à μ_{ζ^p}. En particulier, les polynômes minimaux μ_ζ et μ_{ζ^p} sont à coefficients entiers. On va montrer que ces deux polynômes sont égaux.

S'ils sont différents, alors leur produit divise Φ_n. En fait ζ est aussi racine de $\mu_{\zeta^p}(X^p)$ donc μ_ζ le divise, dans $\mathbf{Q}[X]$ donc aussi dans $\mathbf{Z}[X]$. On écrit alors :

$$\mu_{\zeta^p}(X^p) = \mu_\zeta h, \text{ avec } h \in \mathbf{Z}[X].$$

On réduit cette égalité modulo p, ce qui avec le morphisme de Frobenius donne :

$$\overline{\mu_{\zeta^p}}^p = \overline{\mu_\zeta}\,\overline{h}.$$

Si φ est un facteur irréductible de $\overline{\mu_\zeta}$ dans $\mathbf{F}_p[X]$, il divise alors aussi $\overline{\mu_{\zeta^p}}$, et donc d'après la remarque au début du paragraphe, φ^2 divise $\overline{\Phi_n}$. Dans un corps de rupture de φ, le polynôme $\overline{\Phi_n}$ a donc une racine double... ce qui est impossible car $X^n - 1$ est à racines simples dans les corps de caractéristique p (sa dérivée s'annule uniquement en 0 qui n'est pas racine). C'est absurde.

Donc $\mu_\zeta = \mu_{\zeta^p}$. Toutes les racines primitives n-èmes de l'unité sont des puissances de ζ d'exposant premier avec n, donc elles ont toutes le même polynôme minimal, qui doit alors être multiple de Φ_n, donc leur polynôme minimal est Φ_n. En particulier, Φ_n est irréductible dans $\mathbf{Q}[X]$. Comme il est unitaire, il est donc aussi irréductible dans $\mathbf{Z}[X]$. □

Remarques.

- Il faut se souvenir de pourquoi les polynômes cyclotomiques sont à coefficients entiers. On le fait par récurrence avec la formule $X^n - 1 = \prod_{d|n} \Phi_d$, avec une division euclidienne licite dans $\mathbf{Z}[X]$ car le diviseur est unitaire.
- Il faut savoir expliquer pourquoi l'irréductibilité d'un polynôme unitaire dans $\mathbf{Q}[X]$ entraîne son irréductibilité dans $\mathbf{Z}[X]$. C'est à cause du lemme de Gauss sur le contenu. Ce même lemme de Gauss est celui qui permet de montrer que $\mathbf{Z}[X]$ est un anneau factoriel, ce que l'on utilise de manière cruciale au début du développement. De manière générale, si l'on expose ce développement il faut s'attendre à des questions sur les polynômes irréductibles dans $A[X]$ en fonction des irréductibles dans $\mathrm{Frac}(A)[X]$, lorsque A est un anneau factoriel. Ce sont les constantes irréductibles dans A, et les polynômes primitifs qui sont irréductibles dans $\mathrm{Frac}(A)[X]$.

— Une application de ce théorème est le théorème de Gauss-Wantzel qui énonce qu'un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est une puissance de deux multipliée par un produit de nombres premiers de Fermat distincts.
— C'est assez important pour les questions et le recul de savoir que ce n'est pas du tout comme ça que ça se passe sur les corps finis. Si le développement est trop court, on pourra même expliquer ce qui se passe. Par exemple, $\Phi_8 = 1 + X^4$ est réductible sur tous les corps finis. De manière générale, Φ_n se décompose en $\varphi(n)/r$ facteurs irréductibles dans $\mathbf{F}_q[X]$, chacun de degré r égal à l'ordre de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$. La démonstration est relativement courte et peut se rajouter ici (cf. Demazure, page 217).

Recasages.

— 102 : Les polynômes cyclotomiques sont par définition fortement reliés aux racines de l'unité. On peut de cette manière enchaîner ce développement avec le théorème de Gauss-Wantzel.
— 122 : On utilise des techniques vraies dans tous les anneaux factoriels, mais les théorèmes qui concernent le contenu des polynômes sont trop importants pour ne pas être mis dans cette leçon. Ainsi, on pourrait en profiter pour y mettre ce développement. Mais ce n'est bien sûr pas la meilleure leçon.
— 141 : Rien de mieux. On montre l'irréductibilité d'une classe importante de polynômes.
— 144 : Les relations entre les racines de Φ_n permettent de montrer qu'il est irréductible. Ce n'est pas forcément la meilleure leçon pour le développement, mais on peut l'imaginer quand même, avec d'autres résultats à propos des racines de l'unité vues comme des racines de polynômes cyclotomiques.