Developpement 2 : Irréductibilité des polynômes cyclotomiques :

Schéma de la démonstration :

1) Soit ζ une racine primitive $n^{ème}$ de l'unité dans $\mathbb{C}$. On note $f(X)$ son polynôme minimal. Soit p premier tel que $n \wedge p = 1$
On montre que si u est une racine de f alors u^p aussi. (par l'absurde)

2) Donc pour tout $k \in \{1, \dots, n-1\} \mid k \wedge n = 1$, ζ^k est racine de f
On en déduit que $f = \Phi_n$ donc Φ_n irréductible.

---

1) f polynôme minimal de ζ. pq $f \in \mathbb{Q}[X]$?
On a alors : $f(X) \mid X^n - 1$ dans $\mathbb{Q}[X]$.
Donc $X^n - 1 = f(X)h(X)$; $(h(X) \in \mathbb{Q}[X])$
On $f(X)$ unitaire
$X^n - 1 \in \mathbb{Z}[X]$ et unitaire $\Big\} \Rightarrow h(X) \in \mathbb{Z}[X]$ (et unitaire)

Soit u une racine de f (dans $\mathbb{C}$) et soit p premier ne divisant pas n. Alors, puisque $f(X) \mid X^n - 1$ on a $u^n - 1 = 0$
u est donc une racine $n^{ème}$ de l'unité dans $\mathbb{C}$.
Donc u^p est aussi une racine $n^{ème}$ de l'unité.
On a donc $0 = (u^p)^n - 1 = f(u^p)h(u^p)$.

Supposons $f(u^p) \neq 0$: donc $h(u^p) = 0$

Or u est racine de $f \in \mathbb{Q}[X]$ qui est irréductible
donc f est le polynôme minimal de u.

Donc $f(X) \mid h(X^p)$ dans $\mathbb{Q}[X]$.
Par conséquent : $h(X^p) = f(X)g(X)$ $(g(X) \in \mathbb{Q}[X])$
On $h(X^p) \in \mathbb{Z}[X]$ unitaire
$f(X) \in \mathbb{Z}[X]$ unitaire $\Big\} \Rightarrow g(X) \in \mathbb{Z}[X]$ unitaire.

Par réduction modulo p ; on a dans $\mathbb{F}_p[X]$:

$\bar{h}(X^p) = \overline{h(X^p)} = \bar{f}(X)\bar{g}(X)$

Or $\bar{h}(X^p) = (\bar{h}(X))^p$ (Frobenius)

Donc $(\bar{h}(X))^p = \bar{f}(X)\bar{g}(X)$ dans $\mathbb{F}_p[X]$.

Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\bar{f}$.

Alors $\theta \mid \bar{h}^p \Rightarrow \theta \mid \bar{h} \Rightarrow \theta^2 \mid \bar{f}\bar{h} = X^n - \bar{1}$ dans $\mathbb{F}_p[X]$.

Donc $\theta \mid X^n - \bar{1}$.
$\theta \mid (X^n - \bar{1})' = \bar{n}X^{n-1}$ } donc $\theta \mid (X^n - \bar{1}) \wedge \bar{n}X^{n-1} = \bar{1}$.

(car $-(\bar{n})^{-1} \cdot X)\,\bar{n}X^{n-1} + X^n - \bar{1} = \bar{1}$)

ce qui est absurde.

Donc $f(u^p) = 0$.

2) Donc pour tout $k \in \mathbb{N}$ $f(\zeta^{p^k}) = 0$ (par récurrence)

Or toute racine primitive $n^{ième}$ de l'unité peut s'écrire sous la forme ζ^m avec $m \wedge n = 1$

On décompose m en produit de facteurs premiers $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$f(\zeta^{p_1^{\alpha_1}}) = 0$ donc $f((\zeta^{p_1^{\alpha_1}})^{p_2^{\alpha_2}}) = 0$ ie $f(\zeta^{p_1^{\alpha_1} p_2^{\alpha_2}}) = 0$ ($p_i \wedge n = 1$)

--- puis par récurrence :

$$f(\zeta^m) = f(\zeta^{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}) = 0$$

Donc toute racine primitive $n^{ième}$ est racine de f

Donc $\phi_n \mid f$; d'où $\phi_n = f$ irréductible dans $\mathbb{Q}[X]$.

Références bibliographiques :

- I. GOZARD : Théorie de Galois.
- D. PERRIN : Cours d'Algèbre.
- D. GUIN : Tome 1 : Groupes et anneaux
  Tome 2 : Corps et théorie de Galois