leçons:	Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$. (37)	Références:
102 : Groupe des nb $\mathbb{C}$x de module 1 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications. 121 : Nombres premiers. Applications. 141 : Polynômes irréductibles à une indeterminée.		Gourdon algèbre page 91

Thm : Pour tout $n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Q}$.

Prérequis :

- $\phi_n := \prod_{\xi \in \Pi_n} (X - \xi)$ où Π_n est l'ensemble des racines primitives n-ième de l'unité.
- $X^n - 1 = \prod_{d \mid n} \phi_d$
- $\forall n \in \mathbb{N}^*$, $\phi_n \in \mathbb{Z}[X]$ et ϕ_n unitaire.

<u>preuve</u> : Soit $n \in \mathbb{N}^*$.

$\mathbb{Q}[X]$ est factoriel : $\phi_n = \prod_{i=1}^{r} Q_i$ avec $Q_i \in \mathbb{Q}[X]$, irréductibles dans $\mathbb{Q}[X]$, unitaires.

L'objectif est de montrer que $r = 1$.

① <u>lemme</u> : Soit $F \in \mathbb{Z}[X]$ et p un nombre premier.

Alors $\overline{F}(X^p) = (\overline{F}(X))^p$ dans $\mathbb{Z}/p\mathbb{Z}[X]$.

<u>preuve du lemme</u> : $F(X) = \sum_{i=0}^{d} a_i X^i$, $a_i \in \mathbb{Z}$

$$\overline{F}(X) = \sum_{i=0}^{d} \overline{a_i} X^i$$

$$(\overline{F}(X))^p = \left(\sum_{i=0}^{d} \overline{a_i} X^i\right)^p \underset{\substack{\uparrow \\ \text{morphisme} \\ \text{de Frobenius}}}{=} \sum_{i=0}^{d} \overline{a_i}^p (X^i)^p \underset{\substack{\uparrow \\ \text{petit théorème} \\ \text{de Fermat}}}{=} \sum_{i=0}^{d} \overline{a_i} (X^p)^i = \overline{F}(X^p)$$

② $\forall i \ \exists \alpha_i \in \mathbb{N}^* \ \alpha_i Q_i \in \mathbb{Z}[X]$

$$\prod_i \alpha_i \phi_n = \prod_i (\alpha_i Q_i)$$

$$c\left(\prod_i \alpha_i \phi_n\right) = \prod_i c(\alpha_i Q_i) = \prod_i \alpha_i$$

D'où $\phi_n = \prod_i \underbrace{\left(\frac{\alpha_i Q_i}{c(\alpha_i Q_i)}\right)}_{= F_i} = \prod_i F_i$ où $F_i \in \mathbb{Z}[X]$, unitaires, irréductibles sur $\mathbb{Q}$.

(3) MQ si p est premier, $p \nmid n$ et $\overline{Q}^2 \mid \overline{\Phi_n}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ alors $\overline{Q}$ est constant

On a $X^n - 1 = \prod_{d|n} \Phi_d$.

$\overline{Q}^2 \mid \overline{\Phi_n} \Rightarrow \overline{Q}^2 \mid \overline{X^n - 1} \Rightarrow \exists \overline{R} \in \mathbb{Z}/p\mathbb{Z}[X] \ \overline{X^n - 1} = \overline{Q}^2 \overline{R}$

On dérive : $\overline{Q} \mid \overline{n} X^{n-1}$

Donc $\overline{Q} \mid X^{n-1}$ ($\overline{n} \neq 0$ donc inversible dans $\mathbb{Z}/p\mathbb{Z}$ car $p \nmid n$)

Donc $\overline{Q} \mid X^n$ et finalement $\overline{Q} \mid 1$. D'où $\overline{Q}$ constant.

(4) Soit $\xi \in \Pi_n$. ξ est une racine de Φ_n et quitte à renuméroter, on peut supposer que $F_1(\xi) = 0$. Soit p premier, $p \nmid n$. MQ $F_1(\xi^p) = 0$.

$\Phi_n(\xi^p) = 0$ car $p \wedge n = 1$ donc $\xi^p \in \Pi_n$

Supposons $F_1(\xi^p) \neq 0$. Alors $\exists i \neq 1 \ F_i(\xi^p) = 0$

F_1 | irréductible sur $\mathbb{Q}$ et $F_1(\xi) = 0$ donc F_1 est le polynome minimal
| unitaire

de ξ sur $\mathbb{Q}$. $F_i(X^p)$ annule ξ donc $F_1 \mid F_i(X^p)$ dans $\mathbb{Q}[X]$.

Ces polynomes sont unitaires donc $F_1 \mid F_i(X^p)$ dans $\mathbb{Z}[X]$.

On a alors $\overline{F_1} \mid \overline{F_i}(X^p) = (\overline{F_i}(X))^p$ par le lemme (1).

Soit $\overline{P}$ un facteur irréductible de $\overline{F_1}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\overline{P} \mid \overline{F_1} \Rightarrow \overline{P} \mid (\overline{F_i}(X))^p \Rightarrow \overline{P} \mid \overline{F_i}$

$\overline{\Phi_n} = \prod_{j=1}^{\wedge} \overline{F_j} \Rightarrow \overline{P}^2 \mid \overline{\Phi_n} \Rightarrow \overline{P}$ constant par (3)

$\overline{P}$ irréductible et constant, c'est absurde car $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Donc $F_1(\xi^p) = 0$

(5) Par récurrence sur le cardinal d'une famille $(p_1, \dots, p_\ell)$ de nombres premiers, on a $\forall \ell, \forall p_1, \dots, p_\ell$ premiers

$(\forall j \ p_j \nmid n) \Rightarrow F_1(\xi^{p_1 \cdots p_\ell}) = 0$

Par décomposition en facteurs premiers, on obtient $F_1(\xi^k) = 0 \ \forall k \wedge n = 1$

Ainsi $\forall \omega \in \Pi_n \ F_1(\omega) = 0$. D'où $\Phi_n \mid F_1$ (*) et $F_1 \mid \Phi_n$ dans $\mathbb{C}$.

Ces polynomes sont unitaires donc $F_1 = \Phi_n$.

Φ_n est irréductible sur $\mathbb{Q}$.

explication de (*) : les racines de Φ_n sont simples et toutes les racines de Φ_n sont racines de F_1.