Irréductibilité de Φ_p dans $\mathbb{Q}[X]$

Francinou-Gianella-Nicolas, *Oraux X-ENS Algèbre 1*, page 173

Exercice : Soit $\omega = e^{\frac{2i\pi}{p}}$ où p est premier et $\Phi_p = X^{p-1} + \ldots + X + 1$ (p-ième polynôme cyclotomique).

1. On admet que Φ_p est irréductible dans $\mathbb{Q}[X]$. Démontrer que l'ensemble $\mathcal{I}$ des polynômes annulateurs de ω dans $\mathbb{Q}[X]$ est $\Phi_p\mathbb{Q}[X]$.
2. Montrer que le polynôme $(X+1)^{p-1} + \ldots + (X+1) + 1$ est irréductible dans $\mathbb{Q}[X]$.
3. En déduire que Φ_p est irréductible dans $\mathbb{Q}[X]$.
4. Démontrer que $\mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right] = \{Q(\omega)\ ,\ Q \in \mathbb{Q}[X]\}$ est un corps, appelé *corps cyclotomique*. Quelle est sa dimension comme espace vectoriel sur $\mathbb{Q}$?

1. Posons $\mathcal{I} = \{Q \in \mathbb{Q}[X]\ ,\ Q(\omega) = 0\}$. $\mathcal{I}$ est un idéal de $\mathbb{Q}[X]$ en tant que noyau du morphisme d'algèbre $Q \in \mathbb{Q}[X] \mapsto Q(\omega) \in \mathbb{C}$. Nous savons que tout idéal de $\mathbb{Q}[X]$ est principal. Comme I est non nul, il existe donc un unique polynôme unitaire Q tel que $\mathcal{I} = Q\mathbb{Q}[X]$. Or, nous savons que $\Phi_p(\omega) = 0$, puisque $(\omega - 1)\Phi_p(\omega) = \omega^p - 1 = 1 - 1 = 0$. On en déduit que Q divise Φ_p, puisque $\Phi_p \in \mathcal{I}$. Comme $Q \neq 1$ et comme Φ_p est supposé irréductible, on a nécessairement $Q = \Phi_p$. On conclut

$$\boxed{\mathcal{I} = \Phi_p\mathbb{Q}[X]}$$

2. Posons $U = (X+1)^{p-1} + \ldots + (X+1) + 1 = \Phi_p(X+1)$, c'est-à-dire

$$\begin{aligned} U &= \frac{1-(X+1)^p}{1-(X+1)} = \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + \binom{p}{p-1}X^{p-2} + \ldots + \binom{p}{2}X + \binom{p}{1} \in \mathbb{Z}[X] \end{aligned}$$

Pour montrer que U est irréductible, nous allons utiliser le critère d'Eisenstein avec le nombre premier p.

Critère d'Eisenstein : *Soit $A = a_nX^n + \ldots a_1X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que*

(i) p ne divise pas a_0
(ii) p divise $a_0, a_1, \ldots, a_{n-1}$
(iii) p^2 ne divise pas a_0

Alors A est irréductible dans $\mathbb{Q}[X]$.

Les hypothèses (i) et (iii) sont clairement vérifiées ici. Il s'agit de vérifier (ii), c'est-à-dire que les $\binom{p}{k}$ sont divisibles par p pour $1 \leq k \leq p-1$. En effet, si $1 \leq k \leq p-1$, on a $k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$. Donc p divise $k!\binom{p}{k}$. Comme $k < p$, p est premier avec $k!$ donc divise $\binom{p}{k}$. On conclut à l'aide du critère d'Eisenstein que U est irréductible.

3. Supposons Φ_p composé et posons $\Phi_p = BC$ où B, C sont dans $\mathbb{Q}[X]$ avec $\deg B < \deg \Phi_p$ et $\deg C < \deg \Phi_p$. On a alors $U = \Phi_p(X+1) = B(X+1)C(X+1)$. Comme $\deg B(X+1) = \deg B < \deg U$ et $\deg C(X+1) = \deg C < \deg U$, il en résulte que U n'est pas irréductible, ce qui est faux.

Conclusion : $\Phi_p = X^{p-1} + \ldots + \ldots + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

4. Φ_p est le polynôme unitaire de plus petit degré annulant ω. Donc la famille $(1, \omega, \ldots, \omega^{p-2})$ est libre sur $\mathbb{Q}$ (toute combinaison linéaire non triviale nulle offrirait un polynôme non nul, de degré strictement inférieur à $p-1$, annulant ω). Si $Q \in \mathbb{Q}[X]$ et si on note R le reste de Q modulo Φ_p, il vient $Q(\omega) = R(\omega)$ puisque $\Phi_p(\omega) = 0$, ce qui montre que

$$\mathbb{Q}[\omega] = Vect(1, \omega, \ldots, \omega^{p-2})$$

Ainsi, le système $(1, \omega, \ldots, \omega^{p-2})$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\omega]$ et

$$\boxed{\dim \mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right] = p-1}$$

Reste à démontrer que $\mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right]$ est un corps. En premier lieu, $\mathbb{Q}[\omega]$ est l'image par le morphisme d'algèbre $P \mapsto P(\omega)$ de l'algèbre $\mathbb{Q}[X]$; c'est donc une sous-algèbre de la $\mathbb{Q}$-algèbre $\mathbb{C}$ et en particulier un sous-anneau de $\mathbb{C}$. Soit x un élément non nul de $\mathbb{Q}[\omega]$. Il existe $R \in \mathbb{Q}[X]$ non nul de degré strictement inférieur à $p-1$ tel que $x = R(\omega)$. Comme Φ_p est irréductible, il est premier avec R. Il existe donc $(U, V) \in \mathbb{Q}[X]^2$ tel que $U\Phi_p + VR = 1$. En ω, cela donne $U(\omega) \times 0 + V(\omega)x = 1$, soit $V(\omega)x = 1$ et $V(\omega) \in \mathbb{Q}[\omega]$ est l'inverse de x.

En conclusion, $\mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right]$ est un corps de dimension $p-1$ sur $\mathbb{Q}$.