IRRÉDUCTIBILITÉ DE Φ_n

[Per96, §3.4, p81–83]

ÉNONCÉ

Soit $n \in \mathbb{N}^*$.

Proposition. $\Phi_n \in \mathbb{Z}[X]$.

Théorème. *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

Corollaire. *On a $\left[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}\right] = \varphi(n)$.*

DÉVELOPPEMENT

Pour montrer que $\Phi_n \in \mathbb{Z}[X]$, on procède par récurrence forte sur $n \in \mathbb{N}^*$.

- On a que $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.
- Si $n > 1$ et le résultat est vrai pour tout $d \mid n$ avec $d < n$, considérons

$$F(X) = \prod_{d|n, d\neq n} \Phi_d(X)\,.$$

Alors $F(X) \in \mathbb{Z}[X]$ par hypothèse de récurrence et est unitaire.
On peut effectuer la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$ et on a

$$X^n - 1 = F(X)P(X) + R(X)\,, \quad \text{avec } P, R \in \mathbb{Z}[X] \text{ et } \deg(R) < \deg(F)\,.$$

Or on sait que $X^n - 1 = \Phi_n(X)F(X)$ dans $\mathbb{Q}[X]$, donc $F(X)\cdot\big(\Phi_n(X) - P(X)\big) = R(X)$, ce qui implique, en considérant les degrés, que $\Phi_n = P \in \mathbb{Z}[X]$.

Passons maintenant au théorème.

Lemme. *Soit ζ une racine n-ième primitive de l'unité. Soit p un nombre premier tel que $p \nmid n$. On sait que ζ^p est une autre racine n-ième primitive de l'unité. Notons $Q \in \mathbb{Q}[X]$ (respectivement R) le polynôme minimal[a] de ζ (respectivement ζ^p) sur $\mathbb{Q}$.*
Alors $Q \in \mathbb{Z}[X]$, $Q \mid \Phi_n$ et $Q = R$.

a. le polynôme minimal est défini sur un anneau principal, donc pas sur $\mathbb{Z}[X]$!

Vérifions que ce lemme permet de conclure. On veut montrer que $Q = \Phi_n$.
Soit ζ une racine n-ième primitive de l'unité. On sait que les racines n-ièmes primitives de l'unité sont exactement les ζ^k telles que $k \wedge n = 1$. Soit ζ^k l'une d'entre elles, et écrivons $k = \prod_{i=1}^{\ell} p_i^{\alpha_i}$ où les $(p_i)_{1\leq i\leq \ell}$ sont premiers et ne divisent pas n.
Par le lemme, ζ a même polynôme minimal que ζ^{p_1}, puis que $(\zeta^{p_1})^{p_1}$, puis que $\zeta^{p_1^{\alpha_1}}$, puis que $(\zeta^{p_1^{\alpha_1}})^{p_2^{\alpha_2}} = \zeta^{p_1^{\alpha_1}p_2^{\alpha_2}}$, et finalement ζ et ζ^k ont même polynôme minimal.

Ainsi toutes les racines n-ièmes primitives de l'unité ont même polynôme minimal. Donc Q admet $\varphi(n)$ racines au moins, et comme $Q \mid \Phi_n$ qui a exactement $\varphi(n)$ racines, on a que $Q = \Phi_n$. Alors Φ_n est irréductible.

Finalement, il ne reste qu'à montrer le lemme.
Vérifions déjà que $Q, R \in \mathbb{Z}[X]$. $\mathbb{Z}[X]$ est factoriel, donc on peut écrire $\Phi_n = \prod_{i=1}^{s} P_i$ où les $(P_i)_{1\leq i\leq s}$ sont des polynômes irréductibles de $\mathbb{Z}[X]$. Φ_n étant unitaire, on peut supposer que les $(P_i)_{1\leq i\leq s}$ le sont aussi. ζ étant racine de Φ_n, on a que ζ annule l'un des $(P_i)_{1\leq i\leq s}$, qui est unitaire et irréductible sur $\mathbb{Z}$ *donc*[1] sur $\mathbb{Q}$. Ainsi $Q = P_i \in \mathbb{Z}[X]$ pour un $i \in [\![1, s]\!]$, et de même $R = P_j \in \mathbb{Z}[X]$ pour un $j \in [\![1, s]\!]$.
Notons de plus que Q et R divisent Φ_n dans $\mathbb{Z}[X]$, et donc que divise aussi Φ_n si $Q \neq R$.

On veut montrer que $Q = R$. Supposons que ce n'est pas le cas.
On a que ζ est racine de $R(X^p)$, donc $Q(X) \mid R(X^p)$ dans $\mathbb{Q}[X]$ [2].
Écrivons $R(X^p) = Q(X)H(X)$ puis $H(X) = \frac{a}{b}H'(X)$ où $H' \in \mathbb{Z}[X]$ est de contenu 1. Alors

$$1 = c\big(R(X^p)\big) = c(Q)\cdot\frac{a}{b}\cdot c(H') = \frac{a}{b}\,, \quad \text{et donc } H \in \mathbb{Z}[X]\,.$$

Si $R(X) = \sum_{i=0}^{r} a_i X^i$, on a alors $\overline{a_i} = \overline{a_i}^p$ dans $\mathbb{F}_p$ pour tout $i \in [\![0, r]\!]$, d'où

$$\overline{R}(X^p) = \left(\sum_{i=0}^{r} \overline{a_i} X^{ip}\right) = \left(\sum_{i=0}^{r} \big(\overline{a_i} X^i\big)^p\right) = \left(\sum_{i=0}^{r} \overline{a_i} X^i\right)^p = \overline{R}(X)^p\,,$$

l'avant-dernière égalité provenant du morphisme de Frobenius. Ainsi $\overline{R}(X)^p = \overline{Q}(X)\cdot\overline{H}(X)$.

Considérons un facteur irréductible T de $\overline{Q}$ sur $\mathbb{F}_p$. On a nécessairement que T divise $\overline{R}$ ou $\overline{R}^{p-1}$, et alors par récurrence $T \mid \overline{R}$.

On a vu que $QR \mid \Phi_n$, et donc dans $\mathbb{F}_p$ on a $T^2 \mid \overline{\Phi_n} \mid X^n - 1$. Ainsi, dans son corps de décomposition, $X^n - 1$ a une racine double, ce qui est faux puisque $p \nmid n$: en effet on vérifie que $(X^n - 1)' = \overline{n}X^{n-1}$ n'a pour racine que 0 qui n'est pas une racine de $X^n - 1$.

Ainsi $Q = R$. Ce qui démontre le lemme.

Enfin, pour le corollaire, il suffit de remarquer que $\zeta = \mathrm{e}^{2i\pi/n}$ est une racine n-ième primitive de l'unité. Son polynôme minimal sur $\mathbb{Q}$ est donc Φ_n, de degré $\varphi(n)$.

COMMENTAIRES

Une argumentation parfois plus détaillée est proposée dans le [Gou09, §2.5, p91], ce qui peut être une bonne lecture pour se remettre les idées en place.

Il faut savoir justifier que la division euclidienne d'un polynôme de $\mathbb{Z}[X]$ par un polynôme de $\mathbb{Z}[X]$ à coefficient dominant inversible donne des polynômes dans $\mathbb{Z}[X]$.

1. il faut en être convaincu
2. les divisions euclidiennes se font dans $\mathbb{Q}[X]$ euclidien. Lorsque le diviseur est unitaire, on montre en fait que l'on peut faire la division dans $\mathbb{Z}[X]$