Irréductibilité des polynômes cyclotomiques

Leçons : 141

Références : PERRIN, *Cours d'algèbre* (p.82) et DEMAZURE, *Cours d'algèbre* (p.206)

Prérequis :

- la division euclidienne dans $\mathbb{Z}[X]$
- $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$
- les polynômes cyclotomiques sont dans $\mathbb{Z}[X]$
- lien entre l'irréductibilité sur $\mathbb{Z}$ et sur $\mathbb{Q}$ (voir Appendice)

Notations :

- $\mu_n^\times(\mathbb{C})$ désignent les racines $n^{\text{ième}}$ primitives de l'unité sur $\mathbb{C}$, autrement dit, les générateurs du groupe $\mathbb{U}_n$ des racines $n^{\text{ième}}$ de l'unité.
- $\mu_n(\mathbb{C})$ désignent l'ensemble de toutes les racines $n^{\text{ième}}$ de l'unité sur $\mathbb{C}$.

Introduction :

On va montrer que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$ et unitaires donc irréductibles aussi sur $\mathbb{Z}$.

Pour $n \in \mathbb{N}$, on définit le polynôme cyclotomique par

$$\phi_n(X) = \prod_{\zeta \in \mu_n^\times(\mathbb{C})} (X - \zeta)$$

Ainsi ϕ_n est de degré $\varphi(n)$ où $\varphi(n)$ est l'indicatrice d'Euler.

Théorème 1. Soit $n \in \mathbb{N}^*$. Le polynôme cyclotomique ϕ_n est dans $\mathbb{Z}[X]$ et est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Idée de la preuve : On commencera par montrer que ϕ_n est dans $\mathbb{Z}[X]$ et unitaire. Ainsi il suffit de montrer qu'il est irréductible sur $\mathbb{Q}$ pour avoir le résultat du théorème (voir Appendice). Pour montrer que ϕ_n est irréductible sur $\mathbb{Q}$, on va montrer qu'il est égal au polynôme minimal d'une racine $n^{\text{ième}}$ primitive de l'unité. Pour cela, on montrera qu'il divise ϕ_n, qu'il est unitaire et qu'il est de degré égal au degré de ϕ_n.

Démonstration.
Étape 1 : *Montrons que tous les $\phi_n \in \mathbb{Z}[X]$ et sont unitaires.*

On procède par récurrence forte sur $n \in \mathbb{N}^*$.
Initialisation : Pour $n = 1$, on a

$$\phi_1(X) = X - 1 \in \mathbb{Z}[X] \text{ unitaire}$$

car 1 est la seule racine unième de l'unité.

Hérédité : Soit $n > 1$. On suppose que pour tout $k \in [\![1; n-1]\!]$, on a $\phi_k \in \mathbb{Z}[X]$ et unitaire.

Or on sait que dans $\mathbb{C}[X]$, on a

$$\phi_n = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d \neq n}} \phi_d}$$ [1]

On note $F = \prod\limits_{\substack{d|n \\ d \neq n}} \phi_d$ qui est, par hypothèse de récurrence, dans $\mathbb{Z}[X]$ et unitaire [2].

On a donc

$$X^n - 1 = F\phi_n \text{ dans } \mathbb{C}[X]$$

Comme F est unitaire, on peut faire la division euclidienne dans $\mathbb{Z}[X]$, on a donc

$$X^n - 1 = FP + R \text{ avec } \deg R < \deg F$$

Or c'est la même division que dans $\mathbb{C}[X]$, donc $P = \phi_n$ et $R = 0$. Ainsi, comme P est dans $\mathbb{Z}[X]$ et unitaire (car on divise un polynôme unitaire par un polynôme unitaire), on a $\phi_n \in \mathbb{Z}[X]$ et unitaire.

Conclusion : Ainsi pour tout $n \in \mathbb{N}^*$, le polynôme ϕ_n est dans $\mathbb{Z}[X]$ et est unitaire.

Étape 2 : *Définition des polynômes minimaux de racines $n^{ième}$ primitives de l'unité.*

Soit ζ une racine $n^{\text{ième}}$ primitive de l'unité. Soit p un nombre premier qui est premier avec n, *i.e.* $p \wedge n = 1$. On note $\omega = \zeta^p$, qui est donc aussi une racine $n^{\text{ième}}$ primitive de l'unité.

On note Π_ζ (respectivement Π_ω) le polynôme minimal de ζ (resp. ω) sur $\mathbb{Q}$.

Étape 3 : *Montrons que Π_ζ et Π_ω sont dans $\mathbb{Z}[X]$ et divisent ϕ_n.*

On utilise le caractère factoriel de $\mathbb{Z}[X]$ [3]. On peut donc écrire

$$\phi_n = \prod_i F_i^{\alpha_i}$$

où les (F_i) sont irréductibles sur $\mathbb{Z}$ et on peut les supposer unitaires car ϕ_n est unitaire.

On a $\phi_n(\zeta) = \phi_n(\omega) = 0$ car ce sont des racines $n^{\text{ième}}$ de l'unité. Il existe donc deux indices i_0 et i_1 dans $[\![1; r]\!]$ tels que

$$F_{i_0}(\zeta) = 0 \quad \text{et} \quad F_{i_1}(\omega) = 0$$

Or comme les polynômes F_{i_0} et F_{i_1} sont irréductibles, unitaires dans $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, on a

$$\Pi_\zeta = F_{i_0} \in \mathbb{Z}[X] \quad \text{et} \quad \Pi_\omega = F_{i_1} \in \mathbb{Z}[X]$$ [4]

Par définition des (F_i), on a donc

$$\Pi_\zeta \mid \phi_n \quad \text{et} \quad \Pi_\omega \mid \phi_n \text{ dans } \mathbb{Z}[X].$$

1. car $X^n - 1$ a pour racine toutes les racines $n^{\text{ième}}$ de l'unité et donc en partitionnant $\mu_n(\mathbb{C})$ par les $\mu_d^\times(\mathbb{C})$ avec $d \mid n$, on trouve $X^n - 1 = \prod_{d \mid n} \phi_d$
2. comme produit de polynômes unitaires
3. car $\mathbb{Z}$ l'est et on a un théorème qui dit que A est factoriel si et seulement si $A[X]$ est factoriel
4. car les polynômes minimaux sont irréductibles (voir Appendice)

Étape 4 : *Montrons que* $\Pi_\zeta = \Pi_\omega$.

Raisonnons par l'absurde, on suppose que $\Pi_\zeta \neq \Pi_\omega$. On sait qu'ils sont irréductibles dans $\mathbb{Z}[X]$ (par l'étape 3). On a donc

$$\Pi_\zeta \Pi_\omega \mid \phi_n \text{ dans } \mathbb{Z}[X]$$ [5]

Or par définition de ω et de Π_ω, on a

$$\Pi_\omega(\zeta^p) = 0$$

Donc

$$\Pi_\zeta \mid \Pi_\omega(X^p) \text{ dans } \mathbb{Z}[X]$$

A première vue, on a pour l'instant que

$$\Pi_\zeta \mid \Pi_\omega(X^p) \text{ dans } \mathbb{Q}[X]$$

C'est-à-dire

$$\Pi_\omega(X^p) = \Pi_\zeta(X)Q(X)$$

avec $Q \in \mathbb{Q}[X]$. Mais par la même technique qu'à l'étape 1, on peut effectuer la division euclidienne de $\Pi_\omega(X^p)$ par $\Pi_\zeta(X)$ dans $\mathbb{Z}[X]$

$$\Pi_\omega(X^p) = \Pi_\zeta(X)S(X) + R(X)$$

d'où $S = Q$ et $R = 0$. Donc $Q \in \mathbb{Z}[X]$. Ainsi

$$\Pi_\zeta \mid \Pi_\omega(X^p) \text{ dans } \mathbb{Z}[X]$$

On va noter $\overline{P} \in \mathbb{F}_p[X]$ la réduction du polynôme $P \in \mathbb{Z}[X]$ modulo p. Notre but est de prendre un facteur irréductible A de $\overline{\Pi_\zeta(X)}$, de montrer qu'il est forcément de degré 0 et inversible, donc il y aura contradiction car un facteur irréductible ne peut pas être inversible par définition.

On a par ce qui précède que

$$\overline{\Pi_\zeta(X)} \mid \overline{\Pi_\omega(X^p)} = \overline{\Pi_\omega(X)}^p \text{ dans } \mathbb{Z}[X]$$

Soit A un facteur irréductible de $\overline{\Pi_\zeta(X)}$ dans $\mathbb{F}_p[X]$. D'où

$$A \mid \overline{\Pi_\omega(X)}^p$$

Mais, par le caractère irréductible de A, on a

$$A \mid \overline{\Pi_\omega(X)} \text{ dans } \mathbb{F}_p[X]$$

Comme on a $\Pi_\zeta \Pi_\omega \mid \phi_n$ dans $\mathbb{Z}[X]$, on a

$$\overline{\Pi_\zeta \Pi_\omega} \mid \overline{\phi_n} \text{ dans } \mathbb{F}_p[X]$$

Donc

$$A^2 \mid \overline{\phi_n} \text{ dans } \mathbb{F}_p[X]$$

Puis

$$A^2 \mid \overline{X^n - 1} \text{ dans } \mathbb{F}_p[X] \tag{1}$$

5. puisque les indices i_0 et i_1 sont différents.

Il existe donc $B \in \mathbb{F}_p[X]$ tel que $\overline{X^n - 1} = A^2 B$. En dérivant, on trouve

$$\overline{nX^{n-1}} = A(2A'B + AB')$$

Ainsi, on a

$$A \mid \overline{nX^{n-1}} \tag{2}$$

On peut alors trouver à partir de (**??**) et (**??**) [6] que

$$A \mid \overline{nX^n} \quad \text{et} \quad A \mid \overline{nX^n - n}\,[7]$$

En utilisant la propriété $a \mid b$ et $a \mid c$ implique $a \mid b + c$, on a

$$A \mid \overline{n} \neq 0, \quad \overline{n} \neq 0 \text{ car } n \wedge p = 1$$

Ainsi A est de degré 0, et non nul, ce qui contredit l'irréductibilité de A (puisque $\mathfrak{p}$ est un corps).

On peut donc en conclure que

$$\Pi_\zeta = \Pi_\omega$$

Étape 5 : *Montrons que toute racine $n^{ième}$ primitive de l'unité est racine de Π_ζ.*

Toutes les racines $n^{\text{ième}}$ primitive de l'unité peuvent s'écrire ζ^m où $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ et $m \wedge n = 1$. Il faut remarquer qu'on a donc $p_i \wedge n = 1$ pour tout $i \in [\![1; s]\!]$.

Par l'étape 4, on sait que

$$\Pi_\zeta(\zeta) = 0 \implies \Pi_\zeta(\zeta^p) = 0$$

On peut donc prouver par récurrence sur le nombre de facteurs premiers de m que $\Pi_\zeta(\zeta^m) = 0$.

En effet, on va commencer par montrer que $\Pi_\zeta(\zeta) = 0 \implies \Pi_\zeta(\zeta^{p_1}) = 0$ car $\Pi_\zeta = \Pi_{\zeta^{p_1}}$. Puis on va montrer que $\Pi_\zeta(\zeta^{p_1}) = 0 \implies \Pi_\zeta(\zeta^{p_1^2}) = 0$ [8], etc jusqu'à $\Pi_\zeta(\zeta^{p_1^{\alpha_1}}) = 0$. Ensuite, on continue en montrant que $\Pi_\zeta(\zeta^{p_1^{\alpha_1}}) = 0 \implies \Pi_\zeta(\zeta^{p_1^{\alpha_1} p_2}) = 0$ [9], etc jusqu'à montrer que $\Pi_\zeta(\zeta^m) = 0$.

Étape 6 : *Conclusion.*

On sait que par l'étape 5, toute racine primitive est racine de Π_ζ donc $\deg \Pi_\zeta \geqslant \varphi(n)$. De plus, on a

$$\Pi_\zeta \mid \phi_n$$

Ainsi $\deg \Pi_\zeta = \varphi(n)$. Comme Π_ζ et ϕ_n sont unitaires, de même degré et que l'un divise l'autre, on a

$$\phi_n = \Pi_\zeta$$

On peut conclure que ϕ_n est irréductible sur $\mathbb{Q}$ car par définition des polynômes minimaux Π_ζ est irréductible sur $\mathbb{Q}$.

Enfin, comme ϕ_n est unitaire, à coefficients entiers et irréductible sur $\mathbb{Q}$, il est irréductible sur $\mathbb{Z}$ (voir Appendice). □

6. on a simplement multiplier la partie de droite par quelque chose, ça ne change donc pas le fait que A divise quelque chose de plus gros

7. car pour la deuxième divisibilité, on a $A \mid \overline{n(X^n - 1)}$

8. ici le ζ^{p_1} joue le rôle de ζ de l'étape 4 et $\zeta^{p_1^2} = (\zeta^{p_1})^{p_1}$ joue le rôle de ω

9. ici le $\zeta^{p_1^{\alpha_1}}$ joue le rôle de ζ de l'étape 4 et $(\zeta^{p_1^{\alpha_1}})^{p_2}$ joue le rôle de ω

Remarques :

Les premiers polynômes cyclotomiques sont

$$\begin{aligned}\phi_1(X) &= X-1\\ \phi_2(X) &= X+1\\ \phi_3(X) &= X^2+X+1\\ \phi_4(X) &= X^2+1\\ \phi_5(X) &= X^4+X^3+X^2+X+1\\ \phi_6(X) &= X^2-X+1\end{aligned}$$

Pour p premier,

$$\phi_p(X) = X^{p-1}+X^{p-2}+\cdots+X+1$$

On peut définir les polynômes cyclotomiques sur d'autres corps que sur $\mathbb{C}$. En effet, on pose alors la définition

$$\phi_{n,k}(X) = \prod_{\zeta\in\mu_n^\times(\mathbb{K}_n)} (X-\zeta)$$

où $\mathbb{K}_n$ est le corps de décomposition de X^n-1 sur le corps k.

Astuces de l'agrégatif :

Il faut faire attention aux espaces dans lesquels on vit [10], notamment lorsque l'on écrit $\Pi_\zeta \mid \Pi_\omega(X^p)$, est ce que l'on est dans $\mathbb{Z}[X]$ ou dans $\mathbb{Q}[X]$? La division euclidienne vit dans $\mathbb{C}[X]$, $\mathbb{Q}[X]$ ou $\mathbb{Z}[X]$, etc. La division euclidienne n'est licite que dans un anneau euclidien et $K[X]$ est euclidien si et seulement si K est un corps. Cependant, on peut effectuer la division euclidienne dans $A[X]$ où A est un anneau si on divise par un polynôme unitaire (c'est ce qu'on fait ici dans l'étape 1).

Le polynôme minimal d'un élément n'a de sens que dans un anneau principal puisqu'il est élément générateur de l'idéal annulant. Donc on ne peut pas définir le polynôme minimal sur $\mathbb{Z}[X]$. Le polynôme minimal est irréductible (voir Appendice).

L'étape 4 peut paraître longue et pas très intuitive, mais si on a dans la tête que si $a \mid b$ alors $a \mid bc$, on comprend bien comment cela s'enchaîne.

10. comme dans la vraie vie finalement