Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}[X]$:

I Le développement

Le but de ce développement est de montrer que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}[X]$ dans le but d'obtenir le degré d'une extension particulière.

Théorème 1 : [Perrin, p.82]
Le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Preuve :
$*$ Comme l'anneau $\mathbb{Z}$ est factoriel et que Φ_n est unitaire, par le théorème de transfert de Gauss il existe des polynômes irréductibles unitaires et irréductibles $F_1, ..., F_r \in \mathbb{Z}[X]$ tels que $\Phi = \prod_{i=1}^{r} F_i^{\alpha_i}$ $(*)$.

$*$ Soient $z \in \mathbb{C}$ une racine de F_1 et p un nombre premier qui est premier avec n.
Le nombre z^p est encore une racine de Φ_n (car c'est encore une racine primitive de l'unité). On raisonne désormais par l'absurde en supposant que z^p n'est pas racine de F_1.

Il existe alors $i \in [\![2; r]\!]$ tel que $F_i(z^p) = 0$. Le nombre $z \in \mathbb{C}$ est alors racine du polynôme $F_i(X^p)$ et par minimalité de F_1, on a alors F_1 qui divise $F_i(X^p)$ dans l'anneau $\mathbb{Q}[X]$ et donc dans $\mathbb{Z}[X]$ car $F_1 \in \mathbb{Z}[X]$ est unitaire (on peut faire la division euclidienne de $F_i(X^p)$ par F_1 dans $\mathbb{Z}[X]$). Il existe donc $H \in \mathbb{Z}[X]$ tel que $F_i(X^p) = F_1(X)H(X)$.

$*$ On réduit cette égalité dans $\mathbb{F}_p[X]$:
Comme $\mathbb{F}_p[X]$ est de caractéristique p, on a :

$$\overline{F_i(X)^p} = \overline{F_i}(X^p) = \overline{H}(X)\overline{F_1}(X)$$

On a ainsi $\overline{F_1}$ qui divise $\overline{F_i}^p$. De plus, si $\overline{P} \in \mathbb{F}_p[X]$ est un facteur irréductible de $\overline{F_1}$, on en déduit que l'on a $\overline{P}$ qui divise $\overline{F_1}$ et $\overline{P}$ qui divise $\overline{F_i}$ (car $\mathbb{F}_p[X]$ est factoriel), donc :

$$\overline{P}^2 \text{ divise } \overline{F_1}...\overline{F_r} \text{ qui divise } \overline{\Phi_n} \text{ qui divise } X^n - \overline{1}$$

On en déduit en dérivant que $\overline{P}$ divise $\overline{n}X^{n-1}$, donc par combinaison linéaire, le polynôme $\overline{P}$ divise $\overline{n} = \overline{n}X^{n-1}X - \overline{n}\left(X^n - \overline{1}\right)$. Or, on aboutit à une contradiction car p est premier avec n, donc $\overline{n}$ est non nul et ainsi $\overline{P}$ serait constant, mais P est irréductible sur $\mathbb{F}_p[X]$ avec $\mathbb{F}_p$ un corps, donc $\deg(P) \geq 1$.

Ainsi, on obtient que z^p est racine de F_1.

$*$ Par une récurrence immédiate qui découle de ce qui précède, on en déduit que pour tout $s \in \mathbb{N}^*$, on a la propriété suivante :
"Si $z \in \mathbb{C}$ est racine de F_1 et que $p_1, ..., p_s \in \mathbb{N}$ sont des nombres premiers ne divisant pas n alors $F_1\left(z^{p_1 \cdots p_s}\right) = 0$".

Finalement, puisque les racines de Φ_n sont exactement les z^m avec $m \in [\![1; n]\!]$ premier avec n et z une racine de F_1, on en déduit que $\Phi_n = F_1$ (par divisibilité et degré) et donc que Φ_n est irréductible sur $\mathbb{Z}[X]$.

$*$ De plus, on a Φ_n de contenu égal à 1 (car unitaire) et également irréductible sur $\mathbb{Q}[X]$ (car irréductible sur $\mathbb{Z}[X]$).

Finalement, les polynômes cyclotomiques Φ_n sont irréductibles dans $\mathbb{Q}[X]$.

■

Corollaire 2 : [Perrin, p.83]
Si ζ_n est une racine primitive n-ième de l'unité dans un corps commutatif de caractéristique nulle, son polynôme minimal sur $\mathbb{Q}$ est Φ_n et $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Preuve :
Soit ζ_n une racine primitive n-ième de l'unité dans un corps commutatif de caractéristique nulle.
Puisque Φ_n est unitaire, irréductible sur $\mathbb{Q}[X]$ et annule ζ_n (par définition), on en déduit que Φ_n est le polynôme minimal de ζ_n sur $\mathbb{Q}$. Ainsi, on a :

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$$

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Dans le développement, on a utilisé le théorème du transfert ainsi qu'un résultat sur le contenu que nous rappelons dans le cadre d'un anneau factoriel $(A, +, \times)$:

Définition 3 : Contenu d'un polynôme [Perrin, p.51] :
On considère un polynôme $P \in A[X]$.
On appelle **contenu de** P (et on note $c(P)$) le PGCD (défini modulo $A^\times$) des coefficients de P. De plus, P est dit **primitif** lorsque $c(P) = 1$.

Lemme 4 : Lemme de Gauss [Perrin, p.51] :
$*$ Pour tous polynômes P, Q de $A[X]$ non nuls, on a $c(PQ) = c(P)c(Q)$.
$*$ Le produit de deux polynômes primitifs est primitif.

Théorème 5 : [Perrin, p.51] :
Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont exactement :
$*$ Les constantes $p \in A$ irréductibles dans A.
$*$ Les polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$.

Théorème 6 : Théorème du transfert [Perrin, p.51] :
Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

II.2 Rappels sur les polynômes cyclotomiques

On donne ici quelques rappels sans démonstration sur les polynômes cyclotomiques :

On suppose que $\mathbb{K}$ est un corps commutatif quelconque de caractéristique p, on note $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \text{ tq } \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{K}$ et on suppose que $\mathrm{PGCD}(p, n) = 1$.

Définition 7 : n-ième polynôme cyclotomique [Perrin, p.80] :
On appelle **n-ième polynôme cyclotomique sur** $\mathbb{K}$ le polynôme :

$$\Phi_{n,\mathbb{K}}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$$

Remarque 8 : [Perrin, p.80]
$\Phi_n(X)$ est un polynôme unitaire et de degré $\varphi(n)$.

Proposition 9 : [Perrin, p.80 + 81]
On a la formule : $X^n - 1 = \prod_{d|n} \Phi_d(X)$ (on peut alors calculer les polynômes cyclotomiques par récurrence plutôt qu'explicitement).

Proposition 10 : [Perrin, p.81]
On a $\Phi_n(X) \in \mathbb{Z}[X]$.

II.3 Pour aller plus loin...

Remarque 11 :
Il faut être prudent car le polynôme $\Phi_{n,\mathbb{F}_q}$ n'est pas irréductible dans $\mathbb{F}_q[X]$ en général (en effet, on a l'irréductibilité si, et seulement si, la classe de q engendre le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$).

En utilisant le théorème de Wantzel et de la théorie de Galois, on peut également montrer que le polygone régulier à n côtés est constructible si, et seulement si, φ est une puissance de 2. Ainsi, le polygone régulier à n côtés est constructible si, et seulement si, n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts. Par exemple, on peut construire à la règle et au compas le pentagone et l'heptadécagone, mais on ne peut pas construire l'heptagone !

II.4 Recasages

Recasages : 102 - 125 - 141 - 144.

III Bibliographie

— Daniel Perrin, *Cours d'algèbre*.