Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ (et sur $\mathbb{Z}$)

Recasage : 102, 125, 141

Réf : Perrin p 82-83

$\phi_n := \phi_{n,\mathbb{Q}}$; $\mu_n^* = \{$racines primitives de l'unité$\}$ dans $\mathbb{C}$.

Théorème : $\forall n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$.

Si $\zeta \in \mu_n^*$, on sait que $\zeta' \in \mu_n^* \iff \exists m$ premier à n tq $\zeta' = \zeta^m$.
Si p est un premier ne divisant pas n, on a donc $\zeta^p \in \mu_n^*$ donc $\phi_n(\zeta) = \phi_n(\zeta^p) = 0$ et $\phi_n \in \mathbb{Q}[X]$, si bien que ζ et ζ^p sont algébriques sur $\mathbb{Q}$.

Soit $\begin{cases} f \in \mathbb{Q}[X] \\ g \in \mathbb{Q}[X] \end{cases}$ polynôme minimal de ζ / ζ^p qui est donc unitaire irréductible sur $\mathbb{Q}$.

① Montrons que $f, g \in \mathbb{Z}[X]$: ce sera utile pour projeter sur $\mathbb{F}_p$.

On sait que $\phi_n \in \mathbb{Z}[X]$ et que $\mathbb{Z}[X]$ est factoriel.
Soit donc $\phi_n = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ sa décomposition en facteurs irréductibles dans $\mathbb{Z}[X]$. Comme ϕ_n est unitaire, on peut supposer qu'il en va de même pour les f_i (quitte à les multiplier par -1).
Par conséquent, le contenu $c(f_i) = 1$ et f_i est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$. Or $\phi_n(\zeta) = 0 = \prod_{i \leq r} f_i(\zeta)^{\alpha_i}$ dans $\mathbb{C}$ donc par intégrité, $\exists i$ tq $f_i(\zeta) = 0$.
Or $f_i \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$ et unitaire donc par unicité du polynôme minimal, $f = f_i \in \mathbb{Z}[X]$. Idem pour g.

(Note en marge :
Si $f_i = QR$ dans $\mathbb{Q}[X]$ ($f_i = P$)
q = ppcm des dénom. de Q, r = [illegible] R
qQ, $rR \in \mathbb{Z}[X]$
$qrP = qQ\,rR$
$c(qrP) = qr$ car P primitif et $c(qQrR) = c(qQ)c(rR)$ car $Q, R \in \mathbb{Z}[X]$ et par Gauss.
On $\frac{qQ}{c(qQ)}, \frac{rR}{c(rR)} \in \mathbb{Z}[X]$
et $P = \frac{qQ}{c(qQ)} \cdot \frac{rR}{c(rR)}$ est réductible dans $\mathbb{Z}$ absurde.)

Rmq : une fois qu'on aura montré $\phi_n = f$, on aura directement que ϕ_n est irréductible sur $\mathbb{Z}$ car $f = f_i$ est irréductible sur $\mathbb{Z}$.

K_n = corps de décomposition de $X^n - 1$ sur k. On définit $\phi_{n,k}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$

De $\mu_n(K_n) = \bigsqcup_{d|n} \mu_d^*(K_n)$, on déduit $X^n - 1 = \prod_{d|n} \phi_{d,k}$.

② Montrons par l'absurde que $f = g$.

Sinon, comme f et g sont irréductibles dans $\mathbb{Z}[X]$ et distincts, et comme $f \mid \phi_n$ et $g \mid \phi_n$, on a encore $fg \mid \phi_n$ par unicité de la décomposition dans un anneau factoriel.

Divisions dans $\mathbb{Z}[X]$

Par ailleurs $g(\zeta^p) = 0$, ζ est racine du polynôme $g(X^p) \in \mathbb{Q}[X]$ donc $f(X)$ divise $g(X^p)$, a priori dans $\mathbb{Q}[X]$ mais aussi dans $\mathbb{Z}[X]$:

(car $f(X), g(X^p) \in \mathbb{Z}[X]$ voir détails)

$$\exists h \in \mathbb{Z}[X] \text{ tq } g(X^p) = f(X)\,h(X)$$

On projette cette égalité dans $\mathbb{F}_p$: $\overline{g(X^p)} = \overline{f(X)}\,\overline{h(X)}$.

En écrivant $g(X) = a_n X^n + \dots + a_0$ avec $a_i \in \mathbb{Z}$, on a $g(X^p) = a_n X^{pn} + \dots + a_0$ mais on sait que le morphisme de Frobenius est un automorphisme de $\mathbb{F}_p$ dans lui-même : $\overline{a_i} = \overline{a_i}^p$

donc $\overline{g(X^p)} = (\overline{a_n} X^n + \dots + \overline{a_0})^p = \overline{g(X)}^p$. Ainsi $\overline{g}^p = \overline{f} \cdot \overline{h}$.

Soit $\varphi(X)$ un facteur irréductible de $\overline{f}(X)$ dans $\mathbb{F}_p[X]$. Alors par le lemme d'Euclide, φ est un facteur irréductible de $\overline{g}^p$ et donc de $\overline{g}$.

On $fg \mid \phi_n$ dans $\mathbb{Z}[X]$ donc $\overline{f}\,\overline{g} \mid \overline{\phi_n}$ dans $\mathbb{F}_p[X]$ donc φ^2 divise $\overline{\phi_n} = \phi_{n, \mathbb{F}_p}$ dans $\mathbb{F}_p[X]$.

voir détails

Mais dans un corps de décomposition K de ϕ_n sur $\mathbb{F}_p$, $\overline{\phi_n} = \phi_{n, \mathbb{F}_p}$ admettrait donc une racine double.

On dans $\mathbb{F}_p[X]$, $P_n = X^n - 1 = \prod_{d \mid n} \phi_{d, \mathbb{F}_p}$ et $P_n' = n X^{n-1}$

donc comme la caractéristique p du corps $\mathbb{F}_p$ ne divise pas n par hypothèse, $P_n \wedge P_n' = 1$ i.e les racines de P_n dans K sont simples ce qui contredit le fait que $\phi_{n, \mathbb{F}_p}$ a une racine double.

Donc $g = f$ i.e le polynôme minimal de ζ^p dans $\mathbb{Q}[X]$ est le même que celui de ζ. On va montrer qu'il s'agit de ϕ_n.

③ Conclure que $\phi_n = f$.

Soit $\zeta' \in \mu_n^*$: $\exists m$ premier avec n tq $\zeta' = \zeta^m$.
On écrit $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_i \nmid n$.
Il résulte du point ② et d'une récurrence immédiate que ζ' et ζ ont même polynôme minimal f sur $\mathbb{Q}$, donc $f(\zeta') = 0$ i.e. f admet toutes les racines primitives $n^{\text{ème}}$ de l'unité comme zéros.
Comme $|\mu_n^*| = \varphi(n)$ par définition, $\deg f \geq \deg \varphi(n) = \deg \phi_n$ et comme $f \mid \phi_n$ et qu'ils sont unitaires, on a bien $f = \phi_n$.
Bref $\phi_n = f$ est bien irréductible sur $\mathbb{Q}$ et donc sur $\mathbb{Z}$.

Conséquence : Soit ζ une racine primitive $n^{\text{ième}}$ de l'unité dans un corps de caractéristique nulle (qui contient donc $\mathbb{Q}$), son polynôme minimal sur $\mathbb{Q}$ est ϕ_n si bien que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Application : Soit $\mathbb{Q} : K$ une extension finie. Alors K contient un nombre fini de racines de l'unité.

Ortiz, p 169

Dém : Si $\zeta^m = 1$ alors $\zeta \in \mu_d^*$ pour un $d \mid n$ donc il suffit de montrer qu'il y a un nombre fini de racines primitives de l'unité dans K.
Posons $N = [K : \mathbb{Q}]$. Si $\zeta \in \mu_n^*$ est dans K alors $\mathbb{Q}(\zeta) \subset K$ donc par multiplicativité des degrés, $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ divise N d'où $\varphi(n) \leq N$.

Il suffit donc de montrer que $X = \{n \geq 2 : \varphi(n) \leq N\}$ est fini.
Soit p un facteur premier de $n \in X$, alors $p - 1 \mid \varphi(n)$ donc a fortiori $p \leq \varphi(n) + 1 \leq N + 1$. Donc $\{p \in \mathcal{P} : p \mid n \text{ avec } n \in X\}$ est fini.

D'autre part si $n \geq 2$, $\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p \mid n}} \underbrace{\left(1 - \frac{1}{p}\right)}_{\leq 1} \geq n \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)$ donc

si $n \in X$, on a $n \leq \dfrac{N}{\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)}$ et X est bien fini.

□

Détails

$X^n - 1 = \prod_{d|n} \Phi_d(X)$. En outre, on a $\Phi_n \in \mathbb{Z}[X]$.

On remarque $\mathcal{U}_n = \bigsqcup_{d|n} \mu_d^*$: en effet si $z \in \mathcal{U}_n$, $z \in \mu_d^*$ avec d son ordre dans $\mathcal{U}_n$ et si $z \in \mu_d^*$ clairement $z \in \mathcal{U}_n$. L'union est disjointe par unicité de l'ordre d'un élément dans un groupe. Ainsi :

Perrin p 80-81

$$X^n - 1 = \prod_{z \in \mathcal{U}_n} (X - z) = \prod_{d|n} \prod_{z \in \mu_d^*} (X - z) = \prod_{d|n} \Phi_d(X).$$

On montre que $\Phi_n(X) \in \mathbb{Z}[X]$ par récurrence forte sur n. $\Phi_1 = X - 1$.
Par hypothèse de récurrence, $P = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X) \in \mathbb{Z}[X]$ et on sait que $X^n - 1 = P(X)\Phi_n(X)$.
Or P est unitaire donc on peut effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$: $\exists Q, R \in \mathbb{Z}[X]$ tq $X^n - 1 = PQ + R$ avec $\deg R < \deg P$. Ainsi $R(X) = P(X)(\Phi_n(X) - Q(X))$. Si $\Phi_n - Q \neq 0$ on a $\deg R \geq \deg P$ ce qui est impossible. Ainsi $\Phi_n = Q \in \mathbb{Z}[X]$.

$g(X^p) \in \mathbb{Q}[X]$ divise f dans $\mathbb{Q}[X]$ et $g(X^p), f \in \mathbb{Z}[X]$ donc la division a lieu dans $\mathbb{Z}[X]$.

On écrit $f = g(X^p)Q_1$ avec $Q_1 \in \mathbb{Q}[X]$. Or $g(X^p)$ est unitaire et dans $\mathbb{Z}[X]$: on peut effectuer la division euclidienne de f par $g(X^p)$ dans $\mathbb{Z}[X]$: $f = g(X^p)Q_2 + R$ avec $\begin{cases} Q_2, R \in \mathbb{Z}[X] \\ \deg R < \deg g(X^p) \end{cases}$
Alors $g(X^p)(Q_1 - Q_2) = R$ dans $\mathbb{Q}[X]$ ce qui impose (cf dessus) $Q_1 - Q_2 = 0$ puis $R = 0$. Donc $Q_1 = Q_2 \in \mathbb{Z}[X]$ et $g(X^p)$ divise bien f dans $\mathbb{Z}[X]$.

Perrin 81

Si k est un corps, $\sigma : \mathbb{Z} \to k$ le morphisme canonique, on a $\Phi_{n,k}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X))$. En particulier, $\Phi_{n,\mathbb{F}_p} = \overline{\Phi_n}$ (réd. mod p).

Par récurrence. Dans $\mathbb{Z}[X]$, $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{Q}} = \Phi_{n,\mathbb{Q}} F(X)$.
σ étant un morphisme, en se plaçant sur un corps de décomposition de $X^n - 1$ sur k, $X^n - 1 = \sigma(X^n - 1) = \sigma(\Phi_{n,\mathbb{Q}})\sigma(F)$. Par HR, $\sigma(F) = \prod_{\substack{d|n \\ d \neq n}} \sigma(\Phi_{d,\mathbb{Q}}) = \prod_{\substack{d|n \\ d \neq n}} \Phi_{d,k}$.

Or $X^n - 1 = \prod_{d|n} \Phi_{d,k}$ donc par intégrité de $k[X]$ on a bien $\Phi_{n,k} = \sigma(\Phi_{n,\mathbb{Q}})$.