Etude des polynômes cyclotomiques (coeffs entiers, unitaire et irréductible sur $\mathbb{Z}$)

Leçons : 102, 120, 121, 123, 141

Thm : Soit $n \in \mathbb{N}^*$, Φ_n le n^{e} polynôme cyclotomique à coefficients, unitaire et irréductible sur $\mathbb{Z}$.

Preuve :

Etape 1 On montre que $\Phi_n \in \mathbb{Z}[X]$ est unitaire

Par récurrence on définit la propriété $\mathcal{P}_n$: $\Phi_n \in \mathbb{Z}[X]$ est unitaire

- Si $n=1$ on a $\Phi_1(X) = X-1 \in \mathbb{Z}[X]$ est unitaire
- Supposons $\mathcal{P}_d$ vraie $\forall d < n$, on a $X^n - 1 = \Phi_n(X) \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(X)$

On a $g(X) \in \mathbb{Z}[X]$ unitaire par hypothèse de récurrence $g(X)$

Donc Φ_n est unitaire

De plus on effectue la division euclidienne de X^n-1 par $g(X)$ (car g est unitaire)

il existe $X^n - 1 = g(X)P(X) + R(X)$ avec $P, R \in \mathbb{Z}[X]$ et $\deg R < \deg g$

D'où $g(X)(\Phi_n(X) - P(X)) = R(X)$ donc par des raisons de degré on a nécessairement $\Phi_n = P \in \mathbb{Z}[X]$.

Etape 2 On montre que Φ_n est irréductible sur $\mathbb{Z}[X]$

- Soit ω racine primitive n^{e} de l'unité et $f(X)$ son polynôme minimal sur $\mathbb{Q}$.
  On a $f(X) \mid X^n - 1$ d'où il existe $h(X) \in \mathbb{Q}[X]$ tq $X^n - 1 = f(X)h(X)$. f, h $\in \mathbb{Z}[X]$
- Soit p premier, ω^p est aussi racine primitive n^{e} de l'unité car $p \wedge n = 1 \Rightarrow \omega = \omega^{kp+un} = (\omega^p)^k$
  Notons g son polynôme minimal sur $\mathbb{Q}$. On montre de même que $g \in \mathbb{Z}[X]$
  (En effet $\mathbb{Z}[X]$ est factoriel donc $\Phi_n(X) = f_1(X)^{\alpha_1} \dots f_r(X)^{\alpha_r}$, f_i unitaire irréductible $\in \mathbb{Z}[X]$ et on note $f = f_i$ qui annule ω, de même pour g.)
- On montre que $f = g$.
  On a $g(\omega^p) = 0$ donc ω est racine de $g(X^p)$ d'où $f(X) \mid g(X^p)$
  Donc il existe $\ell(X) \in \mathbb{Z}[X]$ tel que $g(X^p) = f(X)\ell(X)$

On regarde cette égalité modulo p on a dans $\mathbb{F}_p$

si $g(X) = a_r X^r + \dots + a_0$, $a_i \in \mathbb{Z}$ alors $\overline{g(X^p)} = \overline{g(X)}^p = (\overline{a_r} X^r + \dots + \overline{a_0})^p$

$= \overline{a_r}^p X^{pr} + \dots + \overline{a_0}^p$

$= \overline{a_r}(X^p)^r + \dots + \overline{a_0} = \overline{g(X^p)}$

(car $\overline{a_i}^p = \underbrace{(\overline{1} + \dots + \overline{1})^p}_{a_i \text{ fois}} = \underbrace{\overline{1}^p + \dots + \overline{1}^p}_{a_i \text{ fois}} = \overline{a_i}$)

On a alors $\overline{fg}(X)^p = \overline{f(X)}\,\overline{g(X)}$

- Soit $\varphi(X)$ un diviseur irréductible d'unité de $\overline{f}(X)$ sur $\mathbb{F}_p$.
Par lemme d'Euclide on a que $\varphi(X)$ divise $\overline{g}(X)$
De plus $\begin{cases} f(X) \mid X^n-1 \\ g(X) \mid X^n-1 \end{cases}$ d'où fg divise Φ_n d'où $\overline{f}\,\overline{g}$ divise $\overline{\Phi_n}$ d'où φ^2 aussi ; $\overline{X^n-1}$
Donc il existe $\psi(X) \in \mathbb{F}_p[X]$ tel que $X^n-\overline{1} = \varphi(X)^2\psi(X)$
On dérive et on obtient $nX^{n-1} = 2\varphi(X)\varphi'(X)\psi(X) + \varphi(X)^2\psi'(X)$
or $\varphi(X) \mid nX^{n-1}$ d'où $\varphi(X) = X$ mais $X \nmid X^n-1$ donc impossible
Contradiction obtenue par l'hypothèse que $f(X) \neq g(X)$ d'où $f = g$.
Donc on a vu que ω^p était racine de f

- Donc f a pour racines ω^p $\forall p$ premier et non diviseur de n.
On montre que toutes les racines primitives n^{e} de l'unité sont racines de $f(X)$.
Soit v une telle racine donc $v = \omega^h$, $h \in \mathbb{N}$ v est primitive donc il existe $h' \in \mathbb{N}$
tq $\omega = v^{h'}$ d'où $\omega = \omega^{hh'}$ $\Rightarrow$ $\omega^{hh'-1} = 1$ or $\omega^n = 1 \Rightarrow n \mid hh'-1$
$\Rightarrow$ $h \wedge n = 1$.
Soit $h = p_1 \cdots p_r$ la décomposition en facteurs premiers, $p_i \nmid n$ car $h \wedge n = 1$
On montre par récurrence sur r que $v = \omega^{p_1 \cdots p_r} = \omega^h$ est racine de $f(X)$.
- Si $r = 1$, on a $v = \omega^{p_1}$ qui est racine d'après ce qui précède
- Supposons la propriété vraie au rang $r-1$ donc $\omega^{p_1 \cdots p_{r-1}}$ est racines de $f(X)$.
Elle est racine primitive n^{e} car $p_1 \cdots p_{r-1} \wedge n = 1$ d'où $\omega' = \omega^{p_1 \cdots p_{r-1}}$
donc $v = \omega^{p_1 \cdots p_r} = \omega'^{p_r}$ est racine de $f(X)$ d'après ce qui précède.

- Donc toutes les racines primitives n^{e} de l'unité sont racines de $f(X)$.
Or $\Phi_n \mid f$ mais f est irréductible d'unité donc $\Phi_n = f$
Φ_n est donc le polynôme minimal sur $\mathbb{Q}$ de toutes les racines primitives n^{e} de l'unité
Donc Φ_n est irréductible sur $\mathbb{Q}[X]$ donc sur $\mathbb{Z}[X]$ car son contenu est 1
car unitaire.

□

Résultats supplémentaires

Rqi
Si $n \geq 1$, $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Preuve: Il suffit d'établir que $X^n - 1$ et $\prod_{d \mid n} \Phi_d(X)$ ont les mêmes racines dans $\mathbb{C}$ avec les mêmes multiplicités.

- ~~Soit ω racine primitive n^{e} de l'unité.~~
  Si ω est racine d'ordre d de $X^n - 1$ alors $d \mid n$
  et ω est racine d'une racine primitive donc une racine de Φ_d
- Si ω est une racine de Φ_d où $d \mid n$, c'est $n = kd$ d'où $\omega^n = (\omega^d)^k = 1$
  et ω est racine de $X^n - 1$.
- Les racines de $X^n - 1$ sont simples, il en est de même des racines de $\prod_{d \mid n} \Phi_d(X)$
  car $\Phi_d(X)$ a des racines simples et si les racines de Φ_d (d'ordre d) sont distinctes des racines de $\Phi_{d'}$ (d'ordre d') pour $d' \neq d$ □

Cours d'Algèbre, Perrin
Théorie des corps, Carrega