Perrin (p82)

IRRÉDUCTIBILITÉ DES POLYNÔMES CYCLOTOMIQUES

102, 125, 141

Pour tout $n \geq 1$, on note $\mathbb{U}_n$ le groupe des racines complexes de l'unité, μ_n^* l'ensemble de ses générateurs, $\zeta_n = e^{\frac{2i\pi}{n}}$. $\phi_n := \prod_{\zeta \in \mu_n^*} (X - \zeta) \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$. Plus précisément, c'est le polynôme minimal de ζ_n sur $\mathbb{Q}$.

Les parties en vert sont à admettre lors de la présentation, sauf s'il manque du temps. Il faut savoir les faire !

- $\phi_n \in \mathbb{Z}[X]$:
  - $n = 1$: $\phi_1 = X - 1 \in \mathbb{Z}[X]$.
  - Soit $n \in \mathbb{N}$, supposons que $\forall k \in [\![1, n]\!]$, $\phi_k \in \mathbb{Z}[X]$. Alors $Q := \prod_{\substack{d \mid n+1 \\ d < n+1}} \phi_d \in \mathbb{Z}[X]$ et Q est unitaire, donc il existe P et R dans $\mathbb{Z}[X]$ tels que $X^{n+1} - 1 = PQ + R$ et $\deg(R) < \deg(Q)$ (division euclidienne dans $\mathbb{Z}[X]$). Or on sait que $X^{n+1} - 1 = \phi_{n+1} Q$ (dans $\mathbb{Q}[X]$), donc $Q \times (\phi_{n+1} - P) = R$. Or $\deg(Q \times (\phi_{n+1} - P)) = \deg(Q) + \deg(\phi_{n+1} - P) > \deg(R) + \deg(\phi_{n+1} - P)$, donc nécessairement, $\deg(\phi_{n+1} - P) < 0$, i.e. $\phi_{n+1} = P \in \mathbb{Z}[X]$.

- Irréductibilité de ϕ_n : pour cela, montrons que $\phi_n = P_{\zeta_n, \mathbb{Q}}$:
  - Soit p premier ne divisant pas n. De cette manière, $\zeta_n^p \in \mu_n^*$. Par factorialité de $\mathbb{Z}[X]$, écrivons $\phi_n = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ la décomposition de ϕ_n en produit d'irréductibles dans $\mathbb{Z}[X]$. Comme ϕ_n est unitaire, supposons $P_1, \dots, P_r$ unitaires, quitte à ajouter un signe. De là, $\phi_n(\zeta_n) = \phi_n(\zeta_n^p) = 0$ car $(\zeta_n, \zeta_n^p) \in (\mu_n^*)^2$, donc il existe $(i, j) \in [\![1, r]\!]^2$ tel que $f_i(\zeta_n) = f_j(\zeta_n^p) = 0$. Or f_i et f_j sont irréductibles sur $\mathbb{Z}$ et unitaires, donc irréductibles sur $\mathbb{Q}$, donc $P_{\zeta_n, \mathbb{Q}} = f_i \in \mathbb{Z}[X]$ et $P_{\zeta_n^p, \mathbb{Q}} = f_j \in \mathbb{Z}[X]$.
  - Supposons que $P_{\zeta_n, \mathbb{Q}} \neq P_{\zeta_n^p, \mathbb{Q}}$: d'après ce qui précède, $P_{\zeta_n, \mathbb{Q}} \mid \phi_n$ et $P_{\zeta_n^p, \mathbb{Q}} \mid \phi_n$ dans $\mathbb{Z}[X]$. Par ailleurs, $P_{\zeta_n^p, \mathbb{Q}}(X^p)$ annule ζ_n, donc $P_{\zeta_n, \mathbb{Q}}(X) \mid P_{\zeta_n^p, \mathbb{Q}}(X^p)$ *a priori* dans $\mathbb{Q}[X]$.

  Lemme (de Gauss) : Soit A un anneau factoriel. Pour $P \in A[X]$, on note $c(P)$ un PGCD des coefficients de P. Pour tout $(P, Q) \in A[X]^2$, $c(PQ) = c(P) c(Q)$.

  Preuve : Supposons que $c(P) = c(Q) = 1$ et $c(PQ) \neq 1$. Il existe alors $\pi \in A$ irréductible qui divise tous les coefficients de PQ (car A est factoriel). Écrivons $P = \sum_{i=0}^{r} p_i X^i$ et $Q = \sum_{j=0}^{s} q_j X^j$. Comme $c(P) = c(Q) = 1$, il existe $i_0 \in [\![1, r]\!]$ et $j_0 \in [\![1, s]\!]$ tels que $\forall i < i_0$, $\forall j < j_0$, $\pi \mid p_i$, $\pi \mid q_j$, $\pi \nmid i_0$ et $\pi \nmid q_{j_0}$. Par hypothèse, $\pi \mid \sum_{i+j = i_0 + j_0} p_i q_j = p_{i_0} q_{j_0} + \sum_{\substack{i+j = i_0 + j_0 \\ i < i_0 \text{ ou } j < j_0}} p_i q_j$ donc $\pi \mid p_{i_0} q_{j_0}$ par définition de i_0 et j_0. Or π est aussi premier, donc $\pi \mid p_{i_0}$ ou $\pi \mid q_{j_0}$, ce qui est contradictoire. Donc $c(PQ) = 1 = c(P) c(Q)$.

  Dans le cas général : il existe $\tilde{P} \in A[X]$ et $\tilde{Q} \in A[X]$ tels que $P = c(P) \tilde{P}$, $Q = c(Q) \tilde{Q}$, $c(\tilde{P}) = c(\tilde{Q}) = 1$. On a montré que $c(\tilde{P}\tilde{Q}) = c(\tilde{P}) c(\tilde{Q}) = 1$, mais $PQ = c(P) c(Q) \tilde{P}\tilde{Q}$ donc $c(PQ) = c(P) c(Q) c(\tilde{P}\tilde{Q}) = c(P) c(Q)$ ■

Il existe $(a, b) \in \mathbb{Z}^2$ et $h \in \mathbb{Z}[X]$ tel que $c(h) = 1$ et $P_{\zeta_n^p, \mathbb{Q}}(X^p) = P_{\zeta_n, \mathbb{Q}}(X) \cdot \frac{a}{b} h(X)$. D'après le lemme, comme $P_{\zeta_n, \mathbb{Q}}$ est unitaire, $1 = c(P_{\zeta_n^p, \mathbb{Q}}(X^p)) = c(\frac{a}{b} P_{\zeta_n, \mathbb{Q}}(X) h(X)) = \frac{a}{b} c(P_{\zeta_n, \mathbb{Q}}(X)) c(h(X)) = \frac{a}{b} \times 1 \times 1$, donc $P_{\zeta_n, \mathbb{Q}}(X) \mid P_{\zeta_n^p, \mathbb{Q}}(X^p)$ dans $\mathbb{Z}[X]$. Modulo p, grâce au morphisme de Frobenius, on obtient $\overline{P_{\zeta_n, \mathbb{Q}}(X)}\, \overline{h(X)} = \overline{P_{\zeta_n^p, \mathbb{Q}}(X^p)} = \overline{P_{\zeta_n^p, \mathbb{Q}}(X)}^p$. Si φ est un facteur irréductible de $\overline{P_{\zeta_n, \mathbb{Q}}(X)}$ dans $\mathbb{F}_p[X]$, on a $\varphi \mid \overline{P_{\zeta_n^p, \mathbb{Q}}(X)}$ d'après la relation précédente. Comme $P_{\zeta_n, \mathbb{Q}}(X) \mid \phi_n(X)$ et $P_{\zeta_n^p, \mathbb{Q}}(X) \mid \phi_n(X)$, on a $\varphi^2 \mid \overline{\phi_n(X)}$. Ainsi, dans une extension de décomposition K, $\overline{\phi_n(X)}$ admet une racine double. Or

Φ_n divise X^n-1, et X^n-1 n'a que des racines simples : en effet, comme $\mathrm{car}(K)=p$, $(X^n-1)'=nX^{n-1}$ admet comme unique racine 0, qui n'est pas racine de X^n-1. On a conclut à une absurdité, donc $P_{\zeta_n,\mathbb{Q}}=P_{\zeta_n^p,\mathbb{Q}}$.

▷ Par une récurrence immédiate, pour tout k premier à n, on a $P_{\zeta_n,\mathbb{Q}}=P_{\zeta_n^k,\mathbb{Q}}$. En particulier toutes les racines primitives n-ièmes de l'unité sont annulées par $P_{\zeta_n,\mathbb{Q}}$, donc $\Phi_n \mid P_{\zeta_n,\mathbb{Q}}$, mais $\Phi_n(\zeta_n)=0$ donc $P_{\zeta_n,\mathbb{Q}} \mid \Phi_n$ par minimalité. Enfin, $P_{\zeta_n,\mathbb{Q}}$ et Φ_n sont unitaires, donc $P_{\zeta_n,\mathbb{Q}}=\Phi_n$, et en particulier Φ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$ puisque Φ_n est unitaire. $\blacksquare$