Sandrine CARUSO

# Polynômes cyclotomiques

Référence(s) : la plupart des livres d'algèbre, par exemple Demazure

Pour un développement, l'ensemble est peut-être trop long. Ajuster en admettant un lemme, ou deux, ou le théorème 1...

Soient $n$ un entier supérieur à 1, et $\zeta$ une racine primitive $n$-ième de l'unité. Le $n$-ième polynôme cyclotomique est

$$\Phi_n = \prod_{\substack{k=1 \\ k\wedge n=1}}^{n} (X - \zeta^k).$$

**Théorème 1.** *Les polynômes cyclotomiques sont à coefficients dans $\mathbb{Z}$.*

**Lemme 1.1.** *On a*

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

*Démonstration.* Dans $\mathbb{C}$, on a $X^n - 1 = \prod_{k=1}^{n}(X - \zeta^k)$. On a la partition de $[\![1, n]\!]$ suivante :

$$[\![1, n]\!] = \bigsqcup_{d|n} \{k \in [\![1, n]\!], k \wedge n = d\}.$$

En utilisant cette partition, on écrit

$$\begin{aligned} X^n - 1 &= \prod_{d|n} \prod_{\substack{k=1 \\ k\wedge n=d}}^{n} (X - \zeta^k) = \prod_{d|n} \prod_{\substack{k=1 \\ k\wedge (n/d)=1}}^{n/d} (X - \zeta^{kd}) \\ &= \prod_{d|n} \prod_{\substack{k=1 \\ k\wedge d=1}}^{d} (X - \zeta^{nk/d}) = \prod_{d|n} \Phi_d \end{aligned}$$

la dernière égalité venant du fait que si $\zeta$ est une racine primitive $n$-ième de l'unité, $\zeta^{n/d}$ est une racine primitive $d$-ième. □

**Lemme 1.2.** *Soient $A$ un anneau commutatif unitaire intègre et $K$ un corps contenant $A$. Soient $F$ et $G$ dans $A[X]$, $G$ unitaire[1], tels qu'il existe $H \in K[X]$ vérifiant $F = GH$. Alors $H \in A[X]$.*

[1] Ou de coefficient dominant inversible.

*Démonstration.* Comme $G$ est unitaire, on peut faire la division euclidienne de $F$ par $G$ dans $A[X]$. On a ainsi

$$F = GQ + R$$

avec $Q, R \in A[X]$ et $\deg R < \deg G$. Cette division euclidienne est bien entendu également la division euclidienne dans $K[X]$ ; or, dans un tel anneau, la division euclidienne est unique. On en déduit que $R = 0$ et $Q = H$, et donc $H \in A[X]$. □

Démontrons à présent le théorème 1 par récurrence sur $n$. On a $\Phi_1 = X - 1$, qui est bien à coefficients dans $\mathbb{Z}$. Soit $n \geqslant 2$, et supposons que tous les $\Phi_d$ pour $d < n$ sont à coefficients entiers. D'après le lemme 1.1, on a

$$X^n - 1 = \Phi_n \prod_{\substack{d|n \\ d \neq n}} \Phi_d.$$

Par hypothèse de récurrence, $\prod_{d|n, d\neq n} \Phi_d$ est à coefficients entiers, et c'est également le cas de $X^n - 1$. Donc d'après le lemme 1.2, $\Phi_n \in \mathbb{Z}[X]$, ce qui conclut la récurrence.

**Théorème 2.** *Pour tout $n$, le polynôme $\Phi_n$ est irréductible dans $\mathbb{Z}[X]$ (donc dans $\mathbb{Q}[X]$).*

Soient $P \in \mathbb{Z}[X]$ un facteur irréductible de $\Phi_n$, et $Q \in \mathbb{Z}[X]$ tel que $\Phi_n = PQ$. Soit $\zeta$ une racine de $P$ dans $\mathbb{C}$. Nous allons montrer que pour tout nombre premier $p$ ne divisant pas $n$, $\zeta^p$ est aussi racine de $P$. Supposons que ce ne soit pas le cas. Alors $\zeta^p$ est racine de $Q$, donc $\zeta$ est racine de $Q(X^p)$. Comme $P$ est irréductible, c'est le polynôme minimal de $\zeta$, et par conséquent, $P|Q(X^p)$. Réduisons l'égalité $\Phi_n = PQ$ modulo $p$ : on a

$$\overline{\Phi}_n = \overline{PQ} \text{ dans } \mathbb{F}_p.$$

De plus, $\overline{Q(X^p)} = \overline{Q}^p$ ; comme $P$ divise $Q(X^p)$, $\overline{P}$ divise $\overline{Q}^p$ dans $\mathbb{F}_p$. En particulier, il existe $S \in \mathbb{F}_p[X]$, non constant, tel que $S$ divise $\overline{P}$ et $\overline{Q}$. Ainsi, $S^2$ divise $\overline{\Phi}_n$ et donc divise $X^n - \bar{1}$. Or, $(X^n - \bar{1})' = \bar{n}X^{n-1}$, qui est premier avec $X^n - \bar{1}$ car $p$ ne divise pas $n$. Par conséquent, $X^n - \bar{1}$ ne peut pas avoir de facteur carré non constant, ce qui contredit l'hypothèse faite au départ. Autrement dit, $\zeta^p$ est racine de $P$.

Maintenant, pour $k$ premier avec $n$, en écrivant $k = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et en appliquant récursivement le résultat précédent, on montre que $\zeta^k$ est racine de $P$. Finalement, $\Phi_n$ divise $P$ et donc $\Phi_n = P$ est irréductible.