# Polynômes cyclotomiques

Chen Thomas
t.chen.thomas1[at]gmail.com

16 mai 2024

## Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

## Leçons

- 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

## Références

[1] X. Gourdon. *Algèbre et Probabilités*. Ellipses, 2021.

[2] D. Perrin. *Cours d'algèbre*. Ellipses, 1996.

L'essentiel est dans [2].

**Théorème 1.** *Soit $n \in \mathbb{N}^*$. On note $\Phi_n = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta)$. Alors $X^n - 1 = \prod_{d|n} \Phi_d$, et $\Phi_n$ est unitaire, dans $\mathbb{Z}[X]$ et irréductible dans $\mathbb{Z}[X]$.*

Etape 1 : Identité $X^n - 1 = \prod_{d|n} \Phi_d$. Il suffit de montrer que $\{\mathbb{U}_d^* : d|n\}$ forment une partition de $\mathbb{U}_n$. Il est clair que l'union est disjointe et que les $\mathbb{U}_d^*$ sont non vides. Il suffit de montrer le résultat par double inclusion. Soit $\omega \in \mathbb{U}_d^*$ pour $d|n$. Alors $\omega^d = 1$. De fait, $d$ divisant $n$ *i.e.* $n = kd$, $\omega^{kd} = 1$ donc $z \in \mathbb{U}_n$. Réciproquement, soit $\omega \in \mathbb{U}_n$. On note $d$ son ordre. Alors par Lagrange, $d|n$ d'où la réciproque. De fait, pour $n = 1$, on a $\Phi_1 = X - 1$ et pour $n \geq 2$,

$$X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mathbb{U}_d^*} (X - \zeta) = \prod_{d|n} \Phi_d.$$

Etape 2 : Unitarité et $\mathbb{Z}[X]$. Par l'étape 1, on en déduit que

$$\forall n \in \mathbb{N}^*, X^n - 1 = \Phi_n \prod_{d|n, d \neq n} \Phi_d.$$

Par récurrence forte, $\Phi_n$ est le quotient dans $\mathbb{Q}[X]$ de $X^n - 1$ et $\prod_{d|n, d\neq n} \Phi_d := B$ qui sont deux polynômes unitaires de $\mathbb{Z}[X]$. On va montrer un résultat utile plus tard :

**Lemme 2.** Soit $A, B \in \mathbb{Z}[X]$ avec $B$ unitaire. On suppose que $B|A$ dans $\mathbb{Q}[X]$. Alors c'est vrai dans $\mathbb{Z}[X]$.

*Démonstration.* Soit $Q$, le quotient dans $\mathbb{Q}[X]$. Par unitarité de $Q$, il existe $C, R$ dans $\mathbb{Z}[X]$ tels que $A = BC + R$ avec $\deg(R) < \deg(B)$. Donc $(Q - C)B = R$. Par degré, $R = 0$ donc par intégrité, $Q = C$ et $Q \in \mathbb{Z}[X]$. $\square$

On applique donc le lemme pour $A = X^n - 1$ et $B = \prod_{\substack{d|n \\ d\neq n}} \Phi_d$ pour obtenir $\Phi_n \in \mathbb{Z}[X]$ (et unitaire par unitarité de $A$ et $B$.

Etape 3 : Irréductibilité. On se donne un $x$ racine $n$-ème primitive ($x \in \mathbb{C}$). On note $\pi_x$, polynôme minimal de $x$ sur $\mathbb{Q}$ (qui existe car $\Phi_n(x) = 0$. On va montrer

1. $\pi_x \in \mathbb{Z}[X]$.
2. Si $p \nmid n$ premier, $\Phi_n$ n'a pas de facteur carré (non constant) dans $\mathbb{F}_p[X]$ et alors $\pi_x = \pi_{x^p}$.
3. Puisqu'on a $\mathbb{U}_n^* = \{x^k : k \wedge n = 1\}$ [1], on déduira par récurrence que $\pi_x$ s'annule sur $\mathbb{U}_n^*$ et conclura.

1. Puisque $\mathbb{Z}[X]$ est factoriel, on sait que $\Phi_n = \prod_{i=1}^{r} P_i^{a_i}$ avec $P_i$ irréductible sur $\mathbb{Z}[X]$. Par unitarité de $\Phi_n$, ces polynômes $P_i$ le sont aussi. Mais $\zeta$ est racine de $\Phi_n$ donc est racine de l'un des $P_i$ pour un certain $i$ que l'on choisit. Puisque $P_i$ est unitaire irréductible sur $\mathbb{Z}[X]$ donc sur $\mathbb{Q}[X]$, c'est le polynôme minimal de $\zeta$ dans $\mathbb{Q}[X]$ : on a alors $P_i = \pi_x$ qui est donc dans $\mathbb{Z}[X]$.
2. Soit $p \nmid n$ premier. Premièrement [2], si $\overline{\Phi_n} = \overline{Q}^2 \overline{P}$ dans $\mathbb{F}_p[X]$, $\overline{Q}^2$ divise $X^n - \overline{1}$ dans $\mathbb{F}_p[X]$. On a donc $\overline{Q}$ qui divise $\overline{n}X^n - \overline{n}$ et en dérivant, on a $\overline{Q}|\overline{n}X^{n-1}|\overline{n}X^n$. Donc $\overline{Q}$ divise $\overline{n}$. $\overline{n}$ étant non nul (car $p \nmid n$), $\overline{Q}$ est donc constant.

   Supposons que $\pi_x \neq \pi_{x^p}$. On va montrer que $\Phi_n$ admet un facteur carré. Ils sont irréductibles distincts, donc $\pi_x \pi_{x^p}$ divise $\Phi_n$. Utilisons la minimalité de $\pi_x$. Un polynôme annulateur de $x$ nous tend les bras : c'est $\pi_{x^p}(X^p)$ ! De fait, $\pi_x | \pi_{x^p}(X^p)$ dans $\mathbb{Q}[X]$. Par le lemme, cela est vrai dans $\mathbb{Z}[X]$. Notons ce polynôme $Q$. En plongeant sur $\mathbb{F}_p$, on obtient par Frobenius, en notant $\pi_{\zeta^p} = \sum_{k=0}^{r} a_k X^k$,

   $$\overline{a_k} = \overline{a_k^p}, \left(\sum_{k=0}^{r} \overline{a_k} X^k\right)^p = \sum_{k=0}^{r} \overline{a_k^p} X^{kp} \text{ et donc } (\overline{\pi_{\zeta^p}}(X))^p = \overline{\pi_{\zeta^p}}(X^p) = \overline{\pi_x}\overline{Q}.$$

   Soit donc $R \in \mathbb{F}_p[X]$, facteur irréductible que $\overline{\pi_x}$. $R$ divise donc aussi $\overline{\pi_{\zeta^p}}^p$ donc $\overline{\pi_{\zeta^p}}$ par Euclide. Puisque $\pi_x \pi_{x^p}$ divise $\Phi_n$, $\overline{\pi_x \pi_{x^p}}$ divise $\overline{\Phi_n}$ donc $R^2$ divise $\overline{\Phi_n}$ ce qui est absurde ! Ainsi, $\pi_x = \pi_{x^p}$.
3. Il est temps de conclure. Soit $k \wedge n = 1$. Alors $x^k \in \mathbb{U}_n^*$ et $k$ s'écrit $p_1^{a_1} \cdots p_r^{a_r}$ avec $\forall 1 \leq i \leq r, p_i \nmid n$. De fait, par une récurrence immédiate, $\pi_x = \pi_{x^k}$. Ainsi $\pi_x$ est annulé par tout $\mathbb{U}_n^*$ donc $\deg(\pi_x) \geq \varphi(n)$. Or, $\pi_x | \Phi_n$ donc par unitarité, $\pi_x = \Phi_n$. En particulier, $\Phi_n$ est irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$ par unitarité.

1. Bien sûr, si $x^k$ est générateur, il génère $x$ ce qui signifie qu'il existe $u$ tel que $x^{ku-1} = 1$ donc $n|ku - 1$ et $k \wedge n = 1$. Réciproquement, soit $k \wedge n = 1$ et $d$, l'ordre de $x^k$. Alors $x^{kd} = 1$ donc $n|kd$ donc $n|d$. Mais $d|n$ puisque $x^{kn} = 1$ donc $d = n$ par positivité
2. [1], page 92, d)