# Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$

Arnaud Girand

11 décembre 2011

Référence :
- [Gou94], p. 92 – 94

Leçons :
- 113 - Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
- 112 - Corps finis. Applications.
- 116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Prérequis :
- polynômes cyclotomiques.

Soit $n \geq 1$. Dans toute la suite on notera $\phi_n$ le $n$–ième polynôme cyclotomique sur $\mathbb{C}$. On rappelle que :

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

**Proposition 1**
*$\phi_n$ est irréductible sur $\mathbb{Q}$.*

Démonstration : Comme $\mathbb{Q}[X]$ est factoriel (car $\mathbb{Q}$ l'est [1]), il existe un (unique) $r$–uplet $(G_1, \dots, G_r) \in \mathbb{Q}[X]^n$ tel que :

$$\phi_n = \prod_{i=1}^{r} G_i$$

De plus, à $i \in [r]$ fixé, il existe $\alpha_i \in \mathbb{N}^*$ tel que $\alpha_i G_i \in \mathbb{Z}[X]$ (prendre le ppcm des coefficients de $G_i$, par exemple). De fait :

$$\left(\prod_{i=1}^{r} \alpha_i\right) \phi_n = \prod_{i=1}^{r} \alpha_i G_i$$

D'après le lemme de Gauss ( lemme 2 ), on a alors (la première égalité découlant du fait que $\phi_n$ est unitaire) :

$$\prod_{i=1}^{r} \alpha_i = c\left(\left(\prod_{i=1}^{r} \alpha_i\right) \phi_n\right) = \prod_{i=1}^{r} c(\alpha_i G_i)$$

Posons pour $i \in [r]$ $F_i := \dfrac{\alpha_i G_i}{c(\alpha_i G_i)}$. Alors :

$$\forall i \in [r],\ F_i \in \mathbb{Z}[X] \text{ est unitaire et irréductible sur } \mathbb{Q} \text{ et } \phi_n = \prod_{i=1}^{r} F_i$$

On se maintenant propose de démontrer par récurrence sur $s \geq 1$ la propriété suivante : *pour tout entier $s \geq 1$, pour tout entier $k$ premier avec $n$ de décomposition en produit de facteurs premiers [2] $k = p_1 \dots p_s$ et pour toute racine $\xi$ de $F_1$, on a $F_1(\xi^k) = 0$.*

1. C'est un corps !
2. Notons qu'alors aucun des $p_i$ ne peut diviser $n$.

– $s = 1$. Soit $\xi$ une racine de $F_1$ et soit $p$ un nombre premier tel que $p \nmid n$. On se propose de montrer que $F_1(\xi^p) = 0$. Pour commencer, remarquons que $\xi$ est une racine de $\phi_n$ donc une racine primitive $n$–ième de l'unité. Comme $p \wedge n = 1$, $\xi^p$ est également un racine primitive $n$–ième de l'unité donc une racine de $\phi_n$, ergo il existe $i \in [r]$ tel que $F_i(\xi^p) = 0$
  Supposons à présent que $F_1(X)$ et $F_i(X^p)$ soient premiers entre eux dans $\mathbb{Q}[X]$. Alors (lemme de Bézout) :
  $$\exists U, V \in \mathbb{Q}[X], \quad U(X)F_1(X) + V(X)F_i(X^p) = 1$$
  En évaluant cette égalité en "$X = \xi$", on obtient la contradiction[3] $1 = 0$. Or $F_1$ est irréductible sur $\mathbb{Q}$ donc on a nécessairement $F_1(X)|F_i(X^p)$ dans $\mathbb{Q}[X]$. Comme le coefficient dominant de $F_1$ est inversible dans $\mathbb{Z}$ on a de plus que $F_1(X)|F_i(X^p)$ dans $\mathbb{Z}[X]$ ( même raisonnement que dans l'hérédité du lemme 1 ). Si on note, pour $P \in \mathbb{Z}[X]$, $\overline{P} \in \mathbb{F}_p[X]$ la classe de $P$ modulo $p$, on a alors $\overline{F_1}(X)|\overline{F_i}(X^p) = \overline{F_i}(X)^p$ dans $\mathbb{F}_p[X]$.
  Soit à présent $\overline{P} \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{F_1}$ sur $\mathbb{F}_p$. Alors $\overline{P} \mid \overline{F_i}^p$ donc par irréductibilité[4] $\overline{P}|\overline{F_i}$ et donc si $i \neq 1$ $\overline{P}^2 \mid \overline{\phi_n}$. Posons :
  $$R := \prod_{d|n,\, d\neq n} \phi_d$$
  Alors $X^n - 1 = \phi_n R$ et donc $X^n - \overline{1} = \overline{P}^2\overline{S}$, où $S = PR$. En dérivant (formellement) cette égalité on obtient que $\overline{n}X^{n-} = 2\overline{PQ'} + \overline{P}^2\overline{S'}$, ergo $\overline{P}|\overline{n}X^{n-1}$ dans $\mathbb{F}_p[X]$. Or $\overline{P}|X^n - \overline{1}|\overline{n}X^n - \overline{n}$ ainsi par différence $\overline{P}|\overline{n} \neq 0$ donc $\overline{P}$ est constant ce qui est absurde. In fine $F_1(\xi^p) = 0$.
– Supposons la propriété vérifiée au rang $s \geq 1$. Soit $\xi$ une racine de $F_1$ et $k = p_1 \dots p_{s+1}$ un entier premier avec $n$. Alors l'entier $p_1 \dots p_s$ l'est également et donc par hypothèse de récurrence $F_1(\xi^{p_1 \cdots p_s}) = 0$. De plus $p_{s+1} \wedge n = 1$ (car $p_{s+1} \nmid n$) donc comme la propriété est vraie au rang 1 et que $\xi^{p_1 \cdots p_s}$ est une racine de $F_1$ on a $F(\xi^{(p_1 \cdots p_s)p_{s+1}}) = 0$, d'où le résultat.

Pour conclure, fixons une racine $\xi$ de $F_1$. Alors $\xi$ est une racine de $\phi_n$ et donc $\mu_n^*(\mathbb{C}) = \{\xi^k \mid k \wedge n = 1\}$. De fait, les racines de $\phi_n$ sont comprises dans celles de $F_1$ donc $\phi_n|F_1$. Or $F_1|\phi_n$ et ces deux polynômes sont élémentaires ergo $F_1 = \phi_n$, d'où le résultat.

**Détails supplémentaires :**

– Présentons d'abord un lemme sans lequel notre développement n'a pas grand sens :

  **Lemme 1**
  $\phi_n \in \mathbb{Z}[X]$.
  DÉMONSTRATION : On le démontre par récurrence sur $n \geq 1$.
  – $n = 1$. $\phi_1 = (X - 1) \in \mathbb{Z}[X]$.
  – Supposons la propriété validée pour tous $k \leq n$, avec $n \geq 1$. Alors, par hypothèse de récurrence :
  $$P := \prod_{d|n+1,\, d<n+1} \phi_d \in \mathbb{Z}[X]$$
  De plus, $X^{n+1} - 1 = P\phi_{n+1}$. $P$ est de coefficient dominant inversible dans $\mathbb{Z}$ donc il existe $Q, R \in \mathbb{Z}[X]$ tels que $X^{n+1} - 1 = PQ + R$, avec $\deg(R) < \deg(P)$. Par division euclidienne, de tels $Q, R$ sont uniques dans $\mathbb{C}[X]$ donc dans $\mathbb{Z}[X]$ et donc $R = 0$ et $Q = \phi_{n+1}$, d'où le résultat.
– On trouve le résultat suivant dans [Gou94], p.58 :

  **Lemme 2 (Gauss)**
  *Soient $P, Q \in \mathbb{Z}[X]$.*
  *Alors $c(PQ) = c(P)c(Q)$.*
  DÉMONSTRATION : Posons $P_1 := \dfrac{1}{c(P)}P$ et $Q_1 := \dfrac{1}{c(Q)}Q$. Alors $P_1, Q_1 \in \mathbb{Z}[X]$ et $c(P_1) = c(Q_1) = 1$.
  Supposons $c(P_1Q_1) > 1$. Alors il existe un nombre premier $p$ divisant $c(P_1Q_1)$, donc divisant tous les coefficients de $P$. De fait on a, dans $\mathbb{F}_p[X]$ :
  $$\overline{P_1Q_1} = \overline{P_1}\overline{Q_1} = \overline{0}$$

3. Car $\mathbb{Q}$ est un corps donc distinct de l'anneau trivial.
4. On se souviendra que si $P$ est irréductible sur $\mathbb{Z}$ il l'est modulo tout nombre premier.

Comme $\mathbb{F}_[X]$ est intègre, on a donc que $p$ divise tous les coefficients de $P_1$ ou tous les coefficients de $Q_1$, ce qui est impossible. Ainsi $c(P_1Q_1) = 1$. In fine :

$$c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$$

- Soit $\mathbb{K}$ un corps et soit $\xi \in \mu_n^*(\mathbb{K})$. Alors par définition $\{\xi^k \mid k \in \mathbb{N}\} = \mu_n(\mathbb{K})$. De plus, si on se donne $k$ premier avec $n$ et que l'on suppose qu'il existe $j < n$ tel que $(\xi^k)^j = 1$ alors par théorème de Lagrange appliqué à $\xi$ dans le groupe $\mu_n(\mathbb{K})$, $n|kj$ et donc comme $k \wedge n = 1$ par lemme de Gauss on a que $n|j$, ce qui est impossible. Donc $\{\xi^k \mid k \wedge n = 1\} \subset \mu_n^*(\mathbb{K})$. Réciproquement si $k$ et $n$ ont un diviseur commun non trivial $u$, avec $n = un_1$ et $k = uk_1$, alors $(\xi^k)^n_1 = \xi^{uk_1n_1} = \xi^{nk_1} = 1$, avec $n_1 < n$ ergo $\xi^k \notin \mu_n^*(\mathbb{K})$. In fine :

$$\{\xi^k \mid k \wedge n = 1\} = \mu_n^*(\mathbb{K})$$

- Soit $P \in \mathbb{Z}[X]$. Alors on a, dans $\mathbb{F}_p[X]$, $\overline{P}(X^p) = \overline{P}(X)^p$. Démontrons le par récurrence (forte) sur $m = \deg(P)$.
  - $m = -\infty$. Chut.
  - $m = 0$. Trivial
  - Supposons la propriété vraie au rang $m \geq 1$. Alors $P = G + aX^{m-1}$, avec $\deg(P) \leq m$. Le résultat découle alors de l'identité de Frobenius : *si $\mathbb{A}$ est un anneau commutatif de caractéristique p alors $x \mapsto x^p$ est un endomorphisme d'anneau.* Ce dernier résultat suinte à son tour de la tristement célèbre formule du binôme de Newton et du fait que si $1 \leq k \leq p-1$ alors comme $p|k!(p-k)!C_p^k = p!$ et que $p \wedge k!(p-k)! = 1$ le lemme de Gauss nous affirme [5] que $p|C_p^k$ et donc que $C_p^k \equiv 0[p]$.

# Références

[Gou94] Xavier Gourdon. *Algèbre.* Ellipses, 1994.

5. À raison.