Références :
Algèbre, Xavier Gourdon

Déf. Soit $n \in \mathbb{N}^*$. Notons G_n le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. On appelle **indicateur d'Euler de** n l'entier $\phi(n) = Card(G_n)$. On a aussi que $\phi(n)$ est le nombre d'entiers $k \in [\![1, n]\!]$ tels que $k \wedge n = 1$.

Prop. *Si G est cyclique d'ordre n, $G =< a >$ alors*

$$< a^k >= G \Leftrightarrow k \wedge n = 1.$$

Théo (Lemme de Gauss)**.** *Soit $P \in \mathbb{Z}[X]$, on note $c(P)$ le pgcd des coefficients de P (et $c(P) = 1$ si $P = 0$). Si $P, Q \in \mathbb{Z}[X]$ alors $c(PQ) = c(P)c(Q)$.*

Déf. Pour tout $n \in \mathbb{N}^*$, on note

$$\mathbb{U}_n = \left\{ \exp\left(\frac{2ik\pi}{n}\right) k \in \mathbb{Z} \right\} \subset \mathbb{C}.$$

On dit qu'un élément $x \in \mathbb{U}_n$ est une **racine primitive $n^{\text{ième}}$ de l'unité** si x engendre le groupe multiplicatif $\mathbb{U}_n$. On note Π_n l'ensemble des racines primitives $n^{\text{ième}}$ de l'unité, et on définit le **polynôme cyclotomique d'indice** n par

$$\Phi_n = \prod_{\xi \in \Pi_n} (X - \xi)$$

Prop. *Pour tout $n \in \mathbb{N}^*$,*

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

En particulier, $\Phi_n \in \mathbb{Z}[X]$.

Démonstration. Soit $k \in [\![0, n-1]\!]$ et soit d l'ordre de w^k dans $\mathbb{U}_n$. On a nécessairement $d|n$. Par ailleurs, $(w^k)^d = 1$, on a donc $w^k \in \mathbb{U}_d$ et w^k étant d'ordre d, on a $| < w^k > | = d = |\mathbb{U}_d|$. On a donc $w^k \in \Pi_d$. Ainsi, $(X - w^k)$ divise Φ_d et, par conséquent, divise $\prod_{d|n} \Phi_d$.

Les valeurs w^k $(0 \leq k \leq n-1)$ étant distinctes, les polynômes $(X - w^k)$ sont donc premiers entre eux. On en déduit que $X^n - 1 = \prod_{k=0}^{n-1}(X - w^k)$ divise $\prod_{d|n} \Phi_d$. Ces polynômes étant, de plus, unitaires et de même degré (car $\sum_{d|n} \deg(\Phi_d) = \sum_{d|n} \phi(d) = n$), alors ils sont égaux.
Montrons maintenant, par récurrence sur $n \in \mathbb{N}^*$, que $\Phi_n \in \mathbb{Z}[X]$.
Pour $n = 1$, c'est vrai car $\phi_1 = X - 1$. Supposons le résultat vrai jusqu'au rang $n - 1$ et montrons le au rang n. D'après l'hypothèse de récurrence, le polynôme $P = \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in \mathbb{Z}[X]$. Par ailleurs, on a $X^n - 1 = \Phi_n P$. Comme P est unitaire, on peut effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$.

$$\exists Q, R \in \mathbb{Z}[X], X^n - 1 = PQ + R \text{ avec } \deg(R) < \deg(P).$$

Il y a unicité du couple (Q, R) dans $\mathbb{Z}[X]$ (car c'est un anneau intègre) donc dans $\mathbb{C}[X]$ et comme $X^n - 1 = P\Phi_n$, on en déduit que $R = 0$ et $\Phi_n = Q$. Donc $\Phi_n \in \mathbb{Z}[X]$ ce qui achève ce raisonnement par récurrence. □

Lemme. $\overline{\Phi}_n$ n'est pas divisible par le carré d'un polynôme non constant.

Démonstration. Montrons que dans $\mathbb{Z}/p\mathbb{Z}[X]$, $\overline{\Phi_n}$ n'est divisible par le carré d'aucun polynôme non constant.
Supposons $\overline{\Phi_n} = \overline{Q}^2\overline{P}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Si $R = \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in \mathbb{Z}[X]$, on a $X^n - 1 = \Phi_n R$ et donc $X^n - \overline{1} = \overline{\Phi_n R} = \overline{Q}^2\overline{S}$ (avec $S = PR$) d'où par dérivation au sens algébrique :

$$\overline{n}X^{n-1} = 2\overline{QQ'S} + \overline{Q}^2\overline{S} \text{ donc } \overline{Q}|\overline{n}X^{n-1}|\overline{n}X^n.$$

De plus, $\overline{Q}|\overline{n}X^n - \overline{n}$ donc $\overline{Q}$ divise la différence, ie $\overline{Q}|\overline{n}$. Or $p \nmid n$ donc $\overline{n} \neq 0$ et donc $\overline{Q}$ est constant. □

Théo. *Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$.*

Démonstration.

- Montrons tout d'abord que $\Phi_n = F_1...F_r$ avec $F_i \in \mathbb{Z}[X]$ unitaires et irréductibles dans $\mathbb{Q}[X]$.
  Soit $\Phi_n = G_1...G_r$ la décomposition de Φ_n en facteurs irréductibles unitaires de $\mathbb{Q}[X]$ (qui est factoriel). Pour tout $i \in [\![1, r]\!]$, il existe $\alpha_i \in \mathbb{N}^*$ tel que $\alpha_i G_i \in \mathbb{Z}[X]$. On a $\alpha_1...\alpha_r\Phi_n = (\alpha_1 G_1)...(\alpha_r G_r)$. Utilisons le lemme de Gauss. Comme $c(\Phi_n) = 1$ (car Φ_n est unitaire), on a

$$\alpha_1...\alpha_r = c(\alpha_1...\alpha_r\Phi_n) = \prod_{i=1}^{r} c(\alpha_i G_i).$$

  Pour tout $i \in [\![1, r]\!]$, on pose le polynôme $F_i = \frac{\alpha_i G_i}{c(\alpha_i G_i)}$ et d'après ce qui précède, on a $\Phi_n = F_1...F_r$. En effet,

$$F_1...F_r = \frac{\prod_{i=1}^{r} \alpha_i}{\prod_{i=1}^{r} c(\alpha_i G_i)} \prod_{i=1}^{r} G_i = \prod_{i=1}^{r} G_i = \Phi_n.$$

  Pour tout $i \in [\![1, r]\!], F_i \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ (car on ne multiplie G_i irréductible que par une constante) et est forcément unitaire car Φ_n est unitaire (En effet, les coefficients dominants des F_i sont égaux à 1 ou -1. Cependant, il doit y avoir un nombre pair de -1 pour que le produit soit égal à 1. Quitte à changer les F_i problématiques en $-F_i$, on obtient le résultat).

- Soit maintenant ξ une racine de F_1 dans $\mathbb{C}$ et p un nombre premier tel que $p \nmid n$. Montrons qu'il existe $i \in [\![1, r]\!]$ tel que $F_i(\xi^p) = 0$.
  L'élément ξ est racine de F_1 donc de Φ_n. On a donc $\xi \in \Pi_n$. Or p est premier et $p \nmid n$ donc $p \wedge n = 1$ et donc $\xi^p \in \Pi_n$, d'où ξ^p est racine de Φ_n. Il existe donc $i \in [\![1, r]\!]$ tel que $F_i(\xi^p) = 0$ (car $\mathbb{C}$ est un corps).

- Montrons que $i = 1$ ie $F_1(\xi^p) = 0$.
  Comme $F_i(\xi^p) = 0$, $F_1(X)$ et $F_i(X^p)$ ne sont pas premiers entre eux dans $\mathbb{C}[X]$. On a aussi que $F_1(X)$ et $F_i(X^p)$ ne sont pas premiers entre eux dans $\mathbb{Q}[X]$. (Si c'était le cas, on aurait l'existence de $U, V \in \mathbb{Q}[X]$ tels que $U(X)F_1(X)+V(X)F_i(X^p) = 1$ et on aurait donc le fait qu'ils sont premiers dans $\mathbb{C}[X]$). Il existe donc un facteur commun irréductible et unitaire (que l'on peut prendre dans le pgcd des deux polynômes). De plus, F_1 est irréductible dans $\mathbb{Q}[X]$ donc $F_1(X)|F_i(X^p)$. Comme, de plus, F_1 est unitaire, $F_1(X)$ divise $F_i(X^p)$ dans $\mathbb{Z}[X]$ (car on peut faire la division euclidienne dans $\mathbb{Z}[X]$ et utiliser l'unicité). On en déduit que $\overline{F_1}(X)|\overline{F_i}(X^p) = \overline{F_i}(X)^p$. Ceci étant, soit $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$ un facteur irréductible de $\overline{F_1}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. On a $\overline{P}|\overline{F_i}(X)^p$ donc $\overline{P}|\overline{F_i}(X)$ (les F_i sont irréductibles par construction). Par conséquent, si $i \neq 1$, on voit que $\overline{P}^2|\overline{\Phi_n} = \overline{F}_1...\overline{F}_r$, ce qui est impossible d'après ce qui précède. On a donc $i = 1$.

- Montrons que pour tout entier k premier avec n, $F_1(\xi^k) = 0$.
  Ecrivons $k = p_1...p_s$, les p_i étant des nombres premiers. Nous allons prouver par récurrence sur s que $F_1(\xi^k) = 0$. Pour $s = 1$, c'est ce qu'on a fait précédemment. Supposons le résultat vrai au rang $s-1$ et montrons le au rang s. Comme $k \wedge n = 1$, on a $p_1...p_{s-1} \wedge n = 1$, donc d'après l'hypothèse de récurrence $F_1(\xi^{p_1...p_{s-1}}) = 0$. Or $p_s \wedge n = 1$ donc

$$F_1[(\xi^{p_1...p_{s-1}})^{p_s}] = F_1(\xi^k) = 0$$

  ce qui achève le raisonnement par récurrence.
  Pour tout nombre entier k premier avec n, on a donc $F_1(\xi^k) = 0$. Or $\xi \in \Pi_n$ donc $\Pi_n = \{\xi^k, k \wedge n = 1\}$. Tous les éléments de Π_n sont donc des racines de F_1 ce qui prouve que $\Phi_n = F_1$ donc Φ_n est irréductible dans $\mathbb{Q}[X]$.

□

Leçons possibles : 141 - 144