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

Théo Jaudon

Lemme 1. *Soit $P \in \mathbb{Z}[X]$ et $A, B \in \mathbb{Q}[X]$ tels que $P = AB$ et A et P soient unitaires. Alors A et B sont à coefficients entiers.*

Preuve. Comme A et P sont unitaires, B l'est. On note $d \in \mathbb{N}^*$ le ppcm des dénominateurs des coefficients de A et B de sorte que $d^2P = \widetilde{A}\widetilde{B}$ où les polynômes $\widetilde{A} = dA \in \mathbb{Z}[X]$ et $\widetilde{B} = dB \in \mathbb{Z}[X]$ ont pour coefficient dominant d. On en déduit que $c(\widetilde{A})$ et $c(\widetilde{B})$ divise d. Par multiplicativité du contenu on a aussi $c(d^2P) = d^2c(P) = d^2 = c(\widetilde{A})c(\widetilde{B})$ car P est unitaire. On en déduit que $c(\widetilde{A}) = c(\widetilde{B}) = d$ donc les polynômes $A = \frac{1}{d}\widetilde{A}$ et $B = \frac{1}{d}\widetilde{B}$ sont à coefficients entiers.

Théorème 2. *Pour $n \in \mathbb{N}^*$, le polynôme $\Phi_n \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.*

Preuve. Comme Φ_n est unitaire donc primitif, il suffit de montrer que Φ_n est irréductible dans $\mathbb{Q}[X]$, ce qui équivaut à montrer que Φ_n est le polynôme minimal d'une racine primitive n-ième.
On se donne ω une racine primitive n-ième de l'unité et on note $f \in \mathbb{Q}[X]$ le polynôme minimal de ω sur $\mathbb{Q}$. Par minimalité on sait déja que f divise Φ_n dans $\mathbb{Q}[X]$ et comme ces deux polynômes sont unitaires il nous reste à montrer que Φ_n divise f dans $\mathbb{Q}[X]$ pour obtenir $f = \Phi_n$. Pour cela on va montrer que toute racine primitive n-ième de l'unité est racine de f.
Par minimalité f divise $X^n - 1$ dans $\mathbb{Q}[X]$. On écrit $X^n - 1 = f(X)h(X)$ où $h \in \mathbb{Q}[X]$ et d'après le lemme les polynômes f et h sont en fait à coefficients entiers. On se donne $u \in \mathbb{C}$ une racine de f et p un nombre premier qui ne divise pas n. Comme u est racine de f, u est racine de de $X^n - 1$ i.e u est une racine n-ième de l'unité donc u^p est encore une racine n-ième de l'unite et $f(u^p)h(u^p) = 0$.
Supposons par l'absurde que $h(u^p) = 0$. Par minimalité, f divise $h(X^p)$ dans $\mathbb{Q}[X]$ i.e $h(X^p) = f(X)g(X)$ où $g \in \mathbb{Q}[X]$ et comme précédemment le polynôme g est en fait à coefficients entiers. La projection canonique $\mathbb{Z} \mapsto \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ s'étend en un morphisme d'anneaux qui réduit les coefficients modulo p.

$$\begin{array}{rcll} \mathbb{Z}[X] & \to & \mathbb{F}_p[X] & \\ Q = \sum a_k X^k & \mapsto & \overline{Q} = \sum \overline{a_k} X^k & \end{array}$$

Il vient $\overline{h}(X^p) = \overline{f}(X)\overline{g}(X)$ et les propriétés du Frobenius sur $\mathbb{F}_p$ assurent que $\overline{h}(X^p) = \overline{h(X)}^p = \overline{f}(X)\overline{g}(X)$.
On se donne $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}$. Alors θ divise $\overline{h}^p$ donc θ divise $\overline{h}$. D'autre part on a $\overline{X^n - 1} = X^n - \overline{1} = \overline{f}(X)\overline{h}(X)$ de sorte que θ^2 divise $X^n - \overline{1}$ dans $\mathbb{F}_p[X]$. On en déduit que le polynôme $X^n - \overline{1}$ possède une racine double dans une clôture algébrique $\overline{\mathbb{F}_p}$. Comme p ne divise pas n cela fournit une contradiction car le polynôme dérivé $(X^n - \overline{1})' = \overline{n}X^{n-1} \neq 0$ n'a pas de racines communes avec $X^n - \overline{1}$ dans $\overline{\mathbb{F}_p}$.
Ainsi $h(u^p) \neq 0$ donc $f(u^p) = 0$. Par récurrence immédiate on en déduit que ω^{p^α} est racine de f pour tout $\alpha \geq 0$. Plus généralement pour tout nombres premiers $p_1, \ldots, p_r$ qui ne divise pas n et pour tout $\alpha_1, \ldots, \alpha_r \geq 0$, le nombre complexe $\omega^{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}$ est racine de f. Mais comme ω est une racine primitive n-ième de l'unité, l'ensemble des racines primitives n-ièmes de l'unité est

$$\{\ \omega^m \quad | \quad m \in \mathbb{N},\, m \wedge n = 1\ \}$$

qui est aussi égal à l'ensemble

$$\{\ \omega^{p_1^{\alpha_1}\cdots p_r^{\alpha_r}} \quad | \quad r \in \mathbb{N}^*,\ p_1, \ldots, p_r \text{ premiers qui ne divise pas } n \text{ et } \alpha_1, \ldots, \alpha_r \geq 0\ \}.$$

Autrement dit toute racine primitive n-ième de l'unité est racine de f ce qui termine la preuve.

Quelques remarques et compléments sur ce développement :

Il faut être à jour sur les propriétés du contenu pour les polynômes à coefficients entiers et sur les propriétés usuelles des polynômes cyclotomiques.
La preuve du théorème utilise un joli argument de réduction modulo p. Dans cette même veine, citons le résultat suivant.

Proposition 3. *Soit $Q \in \mathbb{Z}[X]$ un polynôme unitaire et p un nombre premier. Si $\overline{Q}$ est irréductible dans $\mathbb{F}_p[X]$, alors Q est irréductible dans $\mathbb{Z}[X]$.*

Preuve. Soient $P, R \in \mathbb{Z}[X]$ tels que $Q = PR$. Comme Q est unitaire, les coefficients dominants de Q et R valent ± 1, en particulier $\deg(P) = \deg(\overline{P})$. En reprenant les notations précédentes il vient $\overline{Q} = \overline{PR} = \overline{P} \times \overline{R}$ et comme $\overline{Q}$ est irréductible dans $\mathbb{F}_p[X]$ on peut supposer (vu les rôles symétriques joués par P et R) que $\overline{P}$ est constant et donc que P est constant. Ainsi $P = \pm 1$ et Q est irréductible dans $\mathbb{Z}[X]$.

Remarque 4. *La réciproque du résultat précédent est fausse en général, les contres exemples canoniques sont justement donnés par les polynômes cyclotomiques.*

Proposition 5. *Le polynôme $\Phi_8 = X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_p[X]$ pour tout premier p.*

Preuve. On utilise le fait que le produit de deux non carrés de $\mathbb{F}_p^*$ est un carré. On distingue ensuite selon que -1 est un carré dans $\mathbb{F}_p$, que 2 est un carré dans $\mathbb{F}_p$ ou que -1 et 2 ne sont pas des carrés dans $\mathbb{F}_p$. Dans le dernier cas -2 est un carré dans $\mathbb{F}_p$ et on conclut.

Théorème 6. *Soit $n \in \mathbb{N}^*$ et p un nombre premier qui ne divise pas n. On note r l'ordre de $\overline{p}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors $\overline{\Phi_n} \in \mathbb{F}_p[X]$ se décompose en produits de polynômes irréductibles tous de degré r.*

Les extensions de $\mathbb{Q}$ de la forme $\mathbb{Q}(\omega)$ où ω est une racine de l'unité sont dites cyclotomiques. Ces extensions interviennent par exemple :
- en arithmétique pour étudier des équations diophantiennes type $x^3 + y^3 = z^3$.
- en géométrie pour étudier les polygones constructibles à la règle et au compas.

Un corollaire immédiat du théorème 2. est le suivant.

Corollaire 7. *Soit ω une racine primitive n-ième de l'unité. Alors Φ_n est le polynôme minimal de ω sur $\mathbb{Q}$ et le degré de l'extension cyclotomique $\mathbb{Q}(\omega)/\mathbb{Q}$ vaut $\deg(\Phi_n) = \varphi(n)$.*

Le calcul du degré d'une extension cyclotomique est une première étape importante dans la démonstration du théorème de Gauss-Wantzel portant sur les polygones constructibles à la règle et au compas. En utilisant le critère nécessaire de constructibilité (être algébrique de degré une puissance de 2) on en déduit facilement que si le polygône régulier à p cotés (p premier) est constructible, alors p est un nombre premier de Fermat. La réciproque se démontre en étudiant le groupe de Galois de l'extension cyclotomique qui est alors un 2-groupe.

Un dernier résultat pour finir.

Lemme 8. *L'indicatrice d'Euler vérifie* $\lim_{n\to+\infty} \varphi(n) = +\infty$.

Preuve. Soit $M > 0$. Il s'agit de montrer que l'ensemble $\{\ n \in \mathbb{N} \quad | \quad \varphi(n) \leq M\ \}$ est fini. On considère n dans l'ensemble précédent et p un facteur premier de n. Alors $p-1$ divise $\varphi(n)$ donc $p \leq M+1$. On note $\mathcal{P}_M$ l'ensemble $\{\ p \text{ premier} \quad | \quad p \leq M+1\ \}$ et on peut donc écrire

$$n = \prod_{p\in\mathcal{P}_M} p^{\nu_p(n)}.$$

On en déduit

$$\varphi(n) = \prod_{p\in\mathcal{P}_M} p^{\nu_p(n)}(1-p^{-1}) = n \prod_{p\in\mathcal{P}_M} (1-p^{-1})$$

d'où

$$n \leq \frac{M}{\prod_{p\in\mathcal{P}_M}(1-p^{-1})}$$

et l'ensemble $\{\ n \in \mathbb{N} \quad | \quad \varphi(n) \leq M\ \}$ est donc fini en tant que partie majorée de $\mathbb{N}$.

Proposition 9. *Soit K une extension finie de $\mathbb{Q}$. Alors K ne possède qu'un nombre fini de racines de l'unité.*

Preuve. On note $M = [K : \mathbb{Q}]$ et $\mathcal{U}_n^\times$ l'ensemble des racines primitives n-ièmes de l'unité. D'après le lemme précédent, il existe $N \in \mathbb{N}$ tel que

$$\{\ n \in \mathbb{N} \quad | \quad \varphi(n) \leq M\ \} \subset [\![0, N]\!].$$

On se donne $\zeta \in K$ une racine de l'unité. Alors ζ est une racine primitive n-ième de l'unité pour un certain $n \in \mathbb{N}^*$. Par multiplicativité du degré on sait que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ divise M et en particulier $\varphi(n) \leq M$ donc $n \leq N$. Ainsi l'ensemble des racines de l'unité dans K est inclus dans l'ensemble $\bigcup_{1\leq n\leq N} \mathcal{U}_n^\times$ qui est fini comme union fini d'ensembles finis.

Recasages : 102, 141, 120, 144 etc ?

Références : Gozard, Théorie de Galois.