Irréductibilité des polynômes cyclotomiques

ref: Gozard, Théorie de Galois p.69 | Perrin, Cours d'algèbre 82.
X. Gourdon, Algèbre. §1 | Demazure, cours d'algèbre, §12

Théorème: Par $n \in \mathbb{N}^*$, $k \in [\![0, n-1]\!]$ premier avec n alors $\Phi_{n,\mathbb{Q}}$ est le polynôme minimale de $\exp(2i\pi\frac{k}{n})$ sur $\mathbb{Q}$. En particulier il est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$ car unitaire.

Preuve: réf. Gozard

- Soit f le pol minimale de $\omega = \exp(2i\pi\frac{k}{n})$ sur $\mathbb{Q}$. Alors $f \mid X^n - 1$ dans $\mathbb{Q}[X]$ ainsi il existe $h \in \mathbb{Q}[X]$, unitaire tq:

$$\underbrace{X^n - 1}_{\in \mathbb{Z}[X]} = f(X)\underbrace{h(X)}_{\text{unitaires}} \quad (1)$$

Ainsi en particulier $f, h \in \mathbb{Z}[X]$.

- Soit u une racine de f et p premiers tq $p \nmid n$, montrons que u^p est racine de f.

Or $(u^p)^q - 1 = (u^n)^{k} - 1 = 0$ donc $f(u^p)h(u^p) = 0$

Supposons $f(u^p) \neq 0$.

Ainsi $h(u^p) = 0$, ainsi $h(X^p)$ admet pour racine u. Or u est une racine de f qui est unitaire et irréductible sur $\mathbb{Q}$, ainsi c'est son polynôme minimal sur $\mathbb{Q}[X]$. Donc $f \mid h(X^p)$ dans $\mathbb{Q}[X]$ or $h(X^p) \in \mathbb{Z}[X]$ unitaire et f est unitaire ainsi:

$$h(X^p) = \underbrace{f(X)}_{\in \mathbb{Z}[X]}\underbrace{g(X)}_{\in \mathbb{Z}[X]} \quad (2)$$

On réduit les égalités (1) et (2) modulo p alors:

$$X^n - 1 = \bar{f}(X)\bar{h}(X) \text{ et } \bar{h}(X^p) = \bar{f}(X)\bar{g}(X).$$

$$\text{donc } \bar{f}(X)\bar{g}(X) = \bar{h}(X^p) = \bar{h}(X)^p.$$

Ainsi soit Θ un facteur irréductible de $\bar{f}$ alors $\Theta \mid \bar{h}^p$ donc $\Theta \mid \bar{h}$ dans $\mathbb{F}_p$. Ainsi

$$\Theta^2 \mid \bar{f}\bar{h} = X^n - 1.$$

Donc $\Theta^2 \mid X^n - 1$ dans $\mathbb{F}_p[X]$.

(Donc $X^n - 1$ possède une racine double dans une extension $\mathbb{F}_q$ de $\mathbb{F}_p$.) pas besoin

Ceci est absurde car $X^n - 1$ est premier avec $\bar{n} X^{n-1}$ dans $\mathbb{F}_p[X]$ car $p \nmid n$ donc $\bar{n}$ inversible dans $\mathbb{F}_p[X]$, en effet $\bar{n}$ inversible dans $\mathbb{Z}/p\mathbb{Z}$ car $p \nmid \bar{n}$ donc.

$$\frac{1}{\bar{n}} X \bar{n} X^{n-1} - (X^n - 1) = 1.$$

Donc par Bezout $\text{pgcd}(X^n - 1, \bar{n} X^{n-1}) = 1$.

Ainsi $h(u^p) \neq 0$ donc $f(u^p) = 0$ $\forall p$ premier et $p \nmid n$.

. Or soit ω' une racine primitive de l'unité, il existe k premier avec n tel que $\omega' = \omega^k$. Ainsi en décomposant $k = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec $p_i \wedge n = 1$, on sait que ω^k est racine de f (car ω^{p_1} racine puis $\omega^{p_1^2}$ etc...)

Ainsi $\deg(f) \geq \varphi(n)$, f unitaires, $f \mid \Phi_n$ unitaires donc

$$f = \Phi_n.$$

D'où le résultat. ∎

Corollaire : Soit $\mathbb{Q}(\mathbb{U}_n)$ alors soit ζ une racine primitive de l'unité :

$$\mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(\zeta) \quad \text{et} \quad [\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$$

) ref : Gozard

Preuve : $\Phi_n = \text{Irr}(\zeta, \mathbb{Q})$ on a :

$$\mathbb{Q}(\zeta) = \frac{\mathbb{Q}[X]}{\langle \Phi_n \rangle} \text{ donc } [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$$

Or pour $\omega \in \mathbb{U}_n$, il existe m tq $\omega = \zeta^m$ donc $\omega \in \mathbb{Q}(\zeta)$ ainsi $\mathbb{Q}(\mathbb{U}_n) \subset \mathbb{Q}(\zeta)$. D'où le résultat. ∎

Théorème : Soit $n \in \mathbb{N}^*$.

$$\text{Aut}(\mathbb{Q}(\mathbb{U}_n)) \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

) ref : Gozard

Preuve : Soit ω une racine primitive n-ième de l'unité on sait que $\mathbb{Q}(\mathbb{U}_n) \simeq \mathbb{Q}(\zeta)$ ce qui donne que

$$\text{Aut}(\mathbb{Q}(\mathbb{U}_n)) = \text{Aut}(\mathbb{Q}(\zeta))$$

Or $\mathbb{Q}(\zeta) = \frac{\mathbb{Q}[X]}{\langle \Phi_n \rangle}$ donc par un résultat précédent $\text{Aut}(\mathbb{Q}(\zeta))$ correspond bijectivement avec racines de Φ_n donc ω^k avec $1 \leq k < n$ et $k \wedge n = 1$. Ainsi on définit la bijection qui sont des morphismes de groupes

$$\text{Aut}(\mathbb{Q}(\mathbb{U}_n)) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \quad \text{et} \quad (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \text{Aut}(\mathbb{Q}(\mathbb{U}_n)) \quad \text{d'où l'isomorphisme.}$$

$$\omega_n^k \longmapsto \overline{k} \qquad \overline{k} \longmapsto \sigma_{\overline{k}} : \omega \longmapsto \omega^k$$

∎

ref : Cours d'Algèbre de Demazure, p 218

Théorème : $\Phi_{n,K}$ avec $\#K = q = p^\alpha$ et $p \nmid n$ alors soit r l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$ alors $\Phi_{n,K}$ se décompose en $\frac{\varphi(n)}{r}$ polynômes irréductibles distincts tous de degrés r.

Preuve : Soit P un facteur irréductible de $\Phi_{n,\mathbb{F}_q}$ et on note $s := \deg(P)$.

But : Montrer que $s = r$ où r est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Soit ξ une racine de P dans un corps de décomposition K_n de $X^n - 1$ sur $\mathbb{F}_q$ alors comme P est irréductible, c'est le polynôme minimale de ξ sur $\mathbb{F}_q$, ainsi :

$$[\mathbb{F}_q(\xi) : \mathbb{F}_q] = s$$

donc $|\mathbb{F}_q(\xi)^*| = q^s - 1$

Donc l'ordre de ξ dans K_n divise $q^s - 1$ (Lagrange)

$= n$ car $P(\xi) = 0$ donc ξ racine de $\Phi_{n,\mathbb{F}_q}$ i.e racine primitive n-ième de l'unité dans $\mathbb{F}_q$.

Ainsi $n \mid q^s - 1$ donc $q^s \equiv 1 \,[n] \Rightarrow r \mid s$.

- Montrons que $s \mid r$.

Pour cela montrons que (1) $\mathbb{F}_q(\xi)$ est contenue dans un corps de décomposition D de $X^{q^r} - X$ sur $\mathbb{F}_q$,

En effet : cela nous donne :

$$\underbrace{[D : \mathbb{F}_q]}_{= r \text{ (voir corps finis)}} = [D : \mathbb{F}_q(\xi)]\,\underbrace{[\mathbb{F}_q(\xi) : \mathbb{F}_q]}_{= s} \Rightarrow s \mid r.$$

Et pour montrer (1), il suffit de montrer que $\xi^{q^r} - \xi = 0$ or $q^r \equiv 1 \,[n]$ ainsi

$n \mid q^r - 1$ donc $\xi^{q^r - 1} = 1$, d'où le résultat

Ainsi tous les facteurs irréductibles sont de degré r or $p \nmid n$ donc $\Phi_{n,\mathbb{F}_q}$ n'admet pas de racine double. (1)

$\Rightarrow$ Les facteurs irréductibles sont 2 à 2 distincts

$\Rightarrow$ Il y en a $\frac{\varphi(n)}{r}$ facteurs irréductibles de degré r.

(2)

Lemme : $\Phi_{n,\mathbb{F}_q}$ admet une racine double alors $p \mid n$.

Preuve : ref Gourdon

Soit a une racine double de $\Phi_{n,\mathbb{F}_q}$, en particulier :

$$X^n - 1 = (X - a)^2 h(X)$$

dc $(X+a)^n - 1 = X^2 h(X+a)$ ou $(X+a)^n - 1 = \sum_{k=1}^{n} \binom{n}{k} X^k a^{n-k} + a^n - 1$.

donc

$$a^n - 1 = 0 \text{ dans } \mathbb{F}_q \quad \text{et} \quad n a^{n-1} = 0 \text{ dans } \mathbb{F}_q .$$

or si $a^{n-1} = 0$ dans $\mathbb{F}_q$ $a^n = 0 \neq -1$ dans $\mathbb{F}_q$ donc $n = 0$ dans $\mathbb{F}_q$ i.e $p \mid n$. ☒

Corollaire: Φ_n est irréductible sur $\mathbb{F}_q$ $\iff$ $\mathrm{ord}(q)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est égale à $\varphi(n)$

$\iff$ q en engendre $(\mathbb{Z}/n\mathbb{Z})^\times$

Preuve: Il faut $r = \varphi(n)$ d'où l'équivalence.

Exemple: $\Phi_8 = X^4 + 1$ réductible sur tout $\mathbb{F}_q$

car $(\mathbb{Z}/8\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

↳ pas d'élément d'ordre 4 d'où le résultat.

Corollaire: $\exists \alpha \in \mathbb{F}_q$ tq $\Phi_n(\alpha) = 0$ $\iff$ $\mathrm{ord}(q)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est 1.

$\iff q = 1 [n]$

Preuve: Direct par le théorème.

Application: Petit théorème de Dirichlet.

Pour l'absurde voir Gourdon, Algèbre p. 90.

Pour $n \in \mathbb{N}^*$ il existe une infinité de nombres premiers p tq $p \equiv 1 [n]$.

Preuve: Tout d'abord comme Φ_n non constant et $\Phi_n(0) = \pm 1$ et $N \mid \Phi_n(N) - \Phi_n(0)$ alors :

$\Phi_n(N) \equiv \pm 1 [N]$.

Ainsi $\Phi_n(N) \wedge N = 1$.

De plus pour p facteur premier de $\Phi_n(N)$ alors $\Phi_n(N) = 0 [p]$ donc $p \equiv 1 [n]$ par le corollaire.

Supposons que les p sont finis, on les notes $p_1 \dots p_r$.

On considère $N = \alpha p_1 \dots p_r$ alors $\Phi_n(N) \wedge N = 1$ et α assez grand tel que $\Phi_n(N) \neq \pm 1$.

Soit p premier tel que $p \mid \Phi_n(N)$ alors $p \equiv 1 [n]$ et $p \wedge N = 1$ donc $\forall i$ $p \neq p_i$.

Absurde

☒

Lemme: Soient $P, A, B \in \mathbb{Q}[X]$ non nuls. On suppose $P \in \mathbb{Z}[X]$, $P = AB$ avec P et A unitaire.
Alors $A, B \in \mathbb{Z}[X]$ et B unitaires.

Preuve:
Il est clair que B est unitaire
On note : $A(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ avec $a_i \in \mathbb{Q}$ donc $a_i = \frac{p_i}{q_i}$ et $p_i \wedge q_i = 1$.
Soit $q = \text{ppcm}(q_0, \dots, q_{n-1})$ alors

$$A(X) = X^n + \frac{1}{q} \sum_{i=0}^{n-1} z_i X^i \text{ avec } z_i \in \mathbb{Z}.$$

Quitte à diviser par $\text{pgcd}(z_0, \dots, z_{n-1}, q)$, $z_0, \dots, z_{n-1}$ et q ops que :

$$\text{pgcd}(z_0, \dots, z_{n-1}, q) = 1.$$

On note $A_1(X) = qX^n + \sum_{i=0}^{n-1} z_i X^i \in \mathbb{Z}[X]$ et $c(A_1) = 1$.

De même il existe $r \in \mathbb{N}^*$ tel que $B(X) = \frac{1}{r} B_1(X)$ où $B_1 \in \mathbb{Z}[X]$ et $c(B_1) = 1$.
On a donc :

$$qrP = A_1 B_1 \implies c(qrP) = c(A_1)\, c(B_1).$$

$$\implies qr = 1.$$

Donc $q = r = 1$ ainsi $A = A_1 \in \mathbb{Z}[X]$
et $B = B_1 \in \mathbb{Z}[X]$.

□