

# Sur l'irréductibilité des polynômes cyclotomiques

Daniel Ferrand

Janvier 2007

Pour un corps  $K$ , notons  $\mu'_n(K)$  l'ensemble des racines *primitives*  $n$ -èmes de l'unité dans  $K$ , c'est-à-dire l'ensemble des éléments d'ordre exactement  $n$  dans le groupe multiplicatif  $K^\times$ . Cet ensemble n'est évidemment pas un groupe, mais, s'il n'est pas vide, il en est cependant très proche puisque le groupe  $(\mathbf{Z}/n\mathbf{Z})^\times$  des éléments inversibles de l'anneau  $\mathbf{Z}/n\mathbf{Z}$  opère sur cet ensemble de façon simplement transitive<sup>1</sup> : plus explicitement, si  $\zeta$  et  $\eta$  sont deux racines primitives  $n$ -èmes de l'unité il existe un unique  $s \in (\mathbf{Z}/n\mathbf{Z})^\times$  tel que  $\eta = \zeta^s$ . Ainsi, le choix d'un élément  $\zeta \in \mu'_n(K)$  conduit à une bijection  $(\mathbf{Z}/n\mathbf{Z})^\times \xrightarrow{\sim} \mu'_n(K)$ ,  $s \mapsto \zeta^s$ . Les liens sont donc étroits entre ce groupe  $(\mathbf{Z}/n\mathbf{Z})^\times$  et le polynôme cyclotomique  $\Phi_n(X)$ . Cette note illustre ces liens, et, en particulier, elle conduit au résultat suivant qui n'a, semble-t-il, pas encore été remarqué :

*Soit  $K$  un corps, et soit  $n$  un entier inversible dans  $K$ . On suppose que le polynôme cyclotomique  $\Phi_n(X)$  est irréductible dans  $K[X]$ . Alors, pour tout diviseur  $d$  de  $n$ ,  $\Phi_d(X)$  est irréductible dans  $K[X]$ .*

Cela peut être proposé en développement dans les leçons concernant l'anneau  $\mathbf{Z}/n\mathbf{Z}$ , ou les racines de l'unité, ou l'irréductibilité des polynômes ou encore l'action d'un groupe sur un ensemble . . .

Ceux qui connaissent un peu la théorie de Galois reconnaîtront une méthode qu'elle utilise souvent, mais la démonstration qui suit est détaillée et autonome ; elle reste dans le cadre du programme de l'agrégation.

**Proposition 1.** *Soient  $a, b$  et  $c$  des entiers tels que  $c \neq 0$  et  $\text{pgcd}(a, b, c) = 1$ . Alors il existe un entier  $x$  tel que  $\text{pgcd}(a + bx, c) = 1$ .*

Si  $c = \pm 1$ , l'entier  $x = 0$  convient. Lorsque tout diviseur premier de  $c$  divise  $a$ , on peut prendre  $x = 1$ . Sinon, on prend pour  $x$  le produit des nombres premiers qui divisent  $c$  et qui ne divisent pas  $a$ .

**Proposition 2.** *Soient  $n$  un entier  $\geq 1$  et  $d$  un diviseur de  $n$ , de sorte qu'il y a un morphisme (surjectif) d'anneaux  $\mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{Z}/d\mathbf{Z}$ . Alors l'homomorphisme de groupes multiplicatifs*

$$(\mathbf{Z}/n\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/d\mathbf{Z})^\times$$

*est surjectif.*

Il s'agit de vérifier ceci : pour tout  $\alpha \in (\mathbf{Z}/d\mathbf{Z})^\times$  il existe  $\alpha' \in (\mathbf{Z}/n\mathbf{Z})^\times$  dont l'image modulo  $d$  est égale à  $\alpha$  ; cela se traduit de la façon suivante : pour tout  $a \in \mathbf{Z}$  tel que  $\text{pgcd}(a, d) = 1$ , il existe  $a' \in \mathbf{Z}$  tel que  $a' \equiv a \pmod{d}$  (pour que la classe de  $a'$  modulo  $d$  soit égale à celle de  $a$ ), et tel que  $\text{pgcd}(a', n) = 1$  ; il s'agit donc de montrer l'existence d'un  $x \in \mathbf{Z}$  tel que  $\text{pgcd}(a + xd, n) = 1$ . Or, on a  $\text{pgcd}(a, d, n) = 1$  ; il suffit donc d'utiliser la proposition qui précède.

**Corollaire** *Soit  $L$  un corps tel que  $\mu'_n(L)$  soit non vide. Soit  $d$  un diviseur de  $n$ . Alors l'application*

$$\zeta \longmapsto \zeta^{n/d}$$

*définit une application surjective  $\mu'_n(L) \longrightarrow \mu'_d(L)$ .*

---

<sup>1</sup>Cette situation est tout-à-fait comparable à celle d'un espace affine et de son groupe des translations.

Pour tout entier  $m$ , on a  $\text{ord}(\zeta^m) = \text{ord}(\zeta) / \text{pgcd}(\text{ord}(\zeta), m)$ ; par suite,  $\zeta^{n/d}$  est une racine primitive  $d$ -ème de l'unité, et l'application envisagée est bien définie. Posons  $e = n/d$ . Il faut vérifier que tout  $\eta \in \mu'_d$  est de la forme  $\eta = \zeta^e$ , avec  $\zeta \in \mu'_n$ . Or, pour un élément  $\omega \in \mu'_n$ , on a  $\omega^e \in \mu'_d$ ; il existe donc un entier  $t$ , premier à  $d$  tel que  $\eta = (\omega^e)^t$ ; d'après le résultat qui précède, il existe un entier  $s$ , premier à  $n$  et congru à  $t$  modulo  $d$ ; on a donc

$$\eta = (\omega^e)^t = (\omega^e)^s = (\omega^s)^e,$$

et on a  $\omega^s \in \mu'_n$  puisque  $s$  est premier à  $n$ .

Concernant les **polynômes cyclotomiques**, une certaine confusion apparaît parfois, dans le discours étudiant - et dans certains manuels utilisés - entre la *définition/caractérisation* de ces polynômes (qui ne fait pas intervenir de racines de l'unité), et leur *construction* qui, elle, utilise les racines de l'unité dans  $\mathbf{C}$ , ou dans une clôture algébrique de  $\mathbf{Q}$ . Pour fixer les choses, séparons l'énoncé (crucial) de sa démonstration (qu'on peut oublier) :

**Théorème** *Il existe une unique suite  $(\Phi_n(X))_{n \geq 1}$  de polynômes de  $\mathbf{Z}[X]$  telle que pour tout entier  $n \geq 1$ , on ait*

$$(\star_n) \quad X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Toutes les propriétés de ces polynômes proviennent de ces relations.

Pour tout corps  $L$ , il y a un unique morphisme d'anneaux  $\mathbf{Z}[X] \rightarrow L[X]$ , de sorte qu'on peut considérer les images des  $\Phi_n$  dans  $L[X]$ ; on les désigne par les mêmes symboles. Les relations  $(\star_n)$  sont vérifiées dans  $L[X]$ . Bien entendu, les racines de l'unité ne sont pas loin :

**Proposition 3.** *Soit  $L$  un corps dans lequel un entier  $n$  est inversible. Alors toute racine de  $\Phi_n$  dans  $L$  est une racine primitive  $n$ -ème de l'unité; autrement dit, l'ensemble des racines de  $\Phi_n$  dans  $L$  est égal à  $\mu'_n(L)$ .*

Soit  $\zeta$  une racine de  $\Phi_n$ . La relation  $(\star_n)$  montre d'abord que l'on a  $\zeta^n = 1$ , donc que l'ordre  $m$  de  $\zeta$  divise  $n$ ; par suite, la relation  $(\star_m)$  montre que  $\zeta$  est racine d'un  $\Phi_d$  pour un  $d$  divisant  $m$ . Comme  $n$  est inversible dans  $L$ , et que la dérivée du polynôme  $X^n - 1$  est  $nX^{n-1}$ , on voit que les racines de  $X^n - 1$  sont simples; par suite, la relation  $(\star_n)$  montre que la racine  $\zeta$  de  $\Phi_n$  n'est pas racine d'un  $\Phi_d$  pour un diviseur strict de  $n$ . Son ordre est donc exactement  $n$ .

**Exercice** (Inutile pour la suite) *Soit  $p$  un nombre premier, et  $m$  un entier non multiple de  $p$ . Montrer que dans  $\mathbf{Z}[X]$  on a  $\Phi_{p^s m}(X) \Phi_m(X^{p^s-1}) = \Phi_m(X^{p^s})$ . En déduire que dans  $\mathbf{F}_p[X]$ , on a*

$$\Phi_{p^s m}(X) = \Phi_m(X)^{p^s - p^{s-1}}.$$

*Autrement dit, les racines de  $\Phi_{p^s m}(X)$  dans une extension de  $\mathbf{F}_p$  sont les racines primitives  $m$ -èmes de l'unité affectées de la multiplicité  $\varphi(p^s)$ .*

Avant d'aborder la démonstration du résultat annoncé au début, il convient de dégager le principe général qui la guide :

**Principe** *Soit  $F(X)$  un polynôme unitaire à coefficients dans un corps  $K$ . Soit  $K \rightarrow L$  une extension de corps telle que  $F$  soit scindé à racines simples  $z_1, \dots, z_m$  dans  $L[X]$ . On suppose que pour tout couple  $i, j$  il existe un*

automorphisme  $\sigma$  du corps  $L$ , qui induit l'identité sur  $K$ , et tel que  $\sigma(z_i) = z_j$ . Alors  $F$  est irréductible dans  $K[X]$ .

En effet, soit  $P(X) = X^d + a_{d-1}X^{d-1} + \dots + a_0$  un diviseur unitaire non constant de  $F(X)$  dans  $K[X]$ ; il s'agit de montrer que  $P = F$ . Le polynôme  $P$  est, lui aussi, scindé dans  $L[X]$ , et il faut vérifier que toutes les racines  $z_j$  de  $F$  sont aussi racines de  $P$ . Or, soit  $z_i$  l'une des racines de  $P$ ; pour tout  $j$ , soit  $\sigma$  un automorphisme comme dans l'énoncé. On a

$$0 = \sigma(P(z_i)) = \sigma(z_i)^d + a_{d-1}\sigma(z_i)^{d-1} + \dots + a_0 = P(z_j).$$

D'où le résultat.

Signalons une application immédiate de ce principe aux polynômes cyclotomiques sur les corps finis.

**Proposition 4.** Soit  $\mathbf{F}_q$  un corps fini, où  $q = p^s$ . Soit  $n$  un entier non multiple de  $p$ . Alors le polynôme  $\Phi_n(X)$  est irréductible dans  $\mathbf{F}_q[X]$  si et seulement si la classe de  $q$  dans le groupe (multiplicatif)  $(\mathbf{Z}/n\mathbf{Z})^\times$  engendre ce groupe.

Posons  $K = \mathbf{F}_q$  et soit  $K \rightarrow L$  une extension de décomposition de  $\Phi_n(X)$ . L'automorphisme de Frobenius  $\sigma : L \rightarrow L$  défini par  $\sigma(x) = x^q$  est l'identité sur  $K$ . L'ensemble des racines de  $\Phi_n(X)$  dans  $L$  est égal à  $\mu'_n(L)$ , et le groupe  $(\mathbf{Z}/n\mathbf{Z})^\times$  opère simplement et transitivement sur cet ensemble.

Si tout élément de ce groupe est la classe d'une puissance convenable de  $q$ , alors, pour deux racines  $\zeta$  et  $\eta$ , il existe un entier  $m$  tel que  $\zeta^{q^m} = \eta$ , soit  $\sigma^m(\zeta) = \eta$ . Le principe signalé plus haut permet donc de conclure que  $\Phi_n(X)$  est irréductible dans  $\mathbf{F}_q[X]$ .

Réciproquement, supposons que  $\Phi_n(X)$  soit irréductible dans  $\mathbf{F}_q[X]$ . Soit  $\omega \in \mu'_n(L)$  une racine de ce polynôme, et posons  $U = \{\omega, \omega^q, \omega^{q^2}, \dots\} \subset \mu'_n(L)$ . Par construction, pour  $u \in U$ , on a  $u^q \in U$ ; par suite les coefficients  $c_i$  du polynôme  $P(X) = \prod_{u \in U} (X - u)$  vérifient la relation  $c_i^q = c_i$ ; ils sont donc dans  $\mathbf{F}_q$ , et  $P$  est un diviseur de  $\Phi_n(X)$  dans  $\mathbf{F}_q[X]$ ; comme on a supposé que  $\Phi_n(X)$  est irréductible dans  $\mathbf{F}_q[X]$ , on voit que  $P = \Phi_n$ , donc que  $U = \mu'_n(L)$ , et finalement que la classe de  $q$  dans le groupe (multiplicatif)  $(\mathbf{Z}/n\mathbf{Z})^\times$  engendre ce groupe.

**Proposition 5.** Soit  $K$  un corps et soit  $n$  un entier inversible dans  $K$ . On suppose que le polynôme cyclotomique  $\Phi_n(X)$  est irréductible dans  $K[X]$ . Alors, pour tout diviseur  $d$  de  $n$ ,  $\Phi_d(X)$  est irréductible dans  $K[X]$ .

Posons  $L = K[X]/(\Phi_n(X))$ , et désignons par  $\omega \in L$  la classe de  $X$ ; c'est une racine de  $\Phi_n(X)$  dans  $L$ . Par hypothèse,  $L$  est un corps et  $n$  est inversible dans  $L$ ; par suite (prop. 3)  $\Phi_n(X)$  est scindé dans  $L[X]$  et l'ensemble de ses racines est  $\mu'_n(L)$ . Comme  $d$  est un diviseur de  $n$  le corollaire montre que le polynôme  $\Phi_d(X)$  est lui aussi scindé dans  $L[X]$  et que ses racines sont les éléments  $\zeta^e$  où  $\zeta$  parcourt  $\mu'_n(L)$ , et où  $e = n/d$ . Pour pouvoir appliquer le principe de démonstration évoqué plus haut, il suffit donc de montrer que pour  $\zeta$  et  $\eta$  dans  $\mu'_n(L)$ , il existe un automorphisme de corps  $\sigma : L \rightarrow L$  qui est l'identité sur le sous-corps  $K$  et tel que  $\sigma(\zeta) = \eta$ . Pour construire  $\sigma$ , on choisit un entier  $s$  premier à  $n$  tel que  $\eta = \zeta^s$ . Reprenons la racine primitive  $\omega$  définie comme la classe de  $X$  dans  $L = K[X]/(\Phi_n(X))$ , et considérons le morphisme de  $K$ -algèbres

$$(\star) \quad K[X] \longrightarrow L, \quad F(X) \longmapsto F(\omega^s).$$

Comme  $\omega^s$  est une racine primitive  $n$ -ème de l'unité, c'est une racine du polynôme  $\Phi_n(X)$ , lequel est supposé irréductible dans  $K[X]$ ; le noyau du morphisme  $(\star)$  est donc engendré par ce polynôme, et, en passant au quotient, on obtient un morphisme injectif de  $K$ -algèbres

$$L = K[X]/(\Phi_n(X)) \longrightarrow L.$$

Comme le  $K$ -espace vectoriel  $L$  est de dimension finie, ce morphisme injectif est aussi bijectif; c'est l'automorphisme  $\sigma$  cherché; en effet, comme  $\sigma(\omega) = \omega^s$ , et que  $\zeta$  est une puissance de  $\omega$ , on a aussi  $\sigma(\zeta) = \zeta^s = \eta$ .