Algèbre 1-NOTIONS DE THÉORIE DES CORPS

David Harari

Rappelons qu'un corps K est par définition un anneau commutatif dans lequel tout élément non nul est inversible, i.e. $K^* = K \setminus \{0\}$. La *caractéristique* de K est l'entier $n \in \mathbf{N}$ tel que le noyau de l'application $\mathbf{Z} \to K$, $x \mapsto x.1_K$ soit $n\mathbf{Z}$. Comme pour tout anneau intègre, la caractéristique d'un corps est zéro ou un nombre premier p.

Exemples.

- $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ sont des corps de caractéristique zéro.
- Pour p premier, $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z}(T)$ sont des corps de caractéristique p (noter que le second est infini).
- $\mathbf{Q}(i) := \{a + ib, (a, b) \in \mathbf{Z} \times \mathbf{Z}\}$ est un corps de caractéristique zéro; c'est le corps des fractions de l'anneau $\mathbf{Z}[i]$.

Dans ce court chapitre, on se limitera aux propriétés élémentaires des extensions de corps. Les résultats plus avancés (notamment la théorie de Galois) seront couverts dans le cours d'algèbre 2.

1. Corps et espaces vectoriels

Définition 1.1 Soit K un corps. Une *extension* de K est un corps L tel que K soit un sous-corps de L.

Si L est un extension de K, il est muni *ipso facto* d'une structure de K-espace vectoriel via la multiplication. D'autre part, si $\varphi : K \to L$ est un morphisme de corps, il est injectif et on peut considérer L comme une extension de K en identifiant K à $\varphi(K) \simeq K$.

Définition 1.2 Si L est de dimension finie sur K, on note $[L : K]$ la dimension du K-espace vectoriel L; c'est un entier > 0 qu'on appelle le *degré* de L sur K. On dit dans ce cas que L est *finie* sur K.[1]

Proposition 1.3 ("Base téléscopique") *Soient M un corps, L un sous-corps de M, K un sous-corps de L. Alors si $(e_i)_{i\in I}$ est une base de L sur K et $(f_j)_{j\in J}$ est une base de M sur L, la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.*

Démonstration : Si $\sum_{(i,j)\in I\times J} \lambda_{ij} e_i f_j = 0$ avec (λ_{ij}) famille presque nulle d'éléments de K, alors $\sum_{j\in J} f_j(\sum_{i\in I} \lambda_{ij} e_i) = 0$; comme (f_j) est une famille libre du L-ev M, on obtient pour tout $jdeJ$: $\sum_{i\in I} \lambda_{ij} e_i = 0$, et comme (e_i) est une famille libre du K-ev L, on a (j étant fixé) $\lambda_{ij} = 0$ pour tout i de I. Finalement la famille (λ_{ij}) est nulle et $(e_i f_j)$ est une famille libre du K-ev M. Si maintenant $x \in M$, on peut écrire $x = \sum_{j\in J} \alpha_j f_j$ avec (α_j) famille presque nulle d'éléments de L, puis en décomposant chaque α_j sur la base (e_i) du K-ev L, on voit que x est combinaison linéaire des $e_i f_j$. Finalement $(e_i f_j)$ est aussi une famille génératrice du K-ev M.

□

Corollaire 1.4 *Si L est fini sur K et M est fini sur L, alors M est fini sur K et on a*

$$[M : K] = [M : L].[L : K]$$

Bien que facile, ce corollaire est extrêmement utile, comme on le verra plus loin.

Définition 1.5 Soient L/K un extension de corps et $\alpha \in L$. On note

- $K[\alpha]$ le sous-anneau de L engendré par K et α; c'est aussi l'ensemble des $P(\alpha)$ avec $P \in K[T]$.
- $K(\alpha)$ le sous-corps de L engendré par K et α; c'est le corps des fractions de $K[\alpha]$, ou encore l'ensemble des $R(\alpha)$ avec $R \in K(T)$.

[1] Attention à ne pas confondre avec la notion d'extension de corps *de type fini*, qui signifierait qu'il existe des éléments $a_1, ..., a_n$ de L tels que L soit le plus petit corps contenant K et les a_i. Par exemple $K(T)$ est un corps de type fini sur K. Cette dernière notion est également différente de celle de K-algèbre de type fini : on peut démontrer que si L est un corps qui est une algèbre de type fini sur un sous-corps K, alors L est finie sur K.

Définition 1.6 Soient L/K une extension de corps et $\alpha \in L$. On définit un morphisme d'anneaux (et aussi de K-espaces vectoriels; c'est donc un morphisme de K-algèbres) $\varphi : K[T] \to L$ par $P \mapsto P(\alpha)$.

- Si φ est injectif, alors $K[\alpha] \simeq K[T]$ et $K(\alpha) \simeq K(T)$. On dit alors que α est *transcendant* sur K.
- Si φ n'est pas injectif, on note π le générateur unitaire de $\ker \varphi$. On dit que α est *algébrique* sur K et on appelle π le *polynôme minimal* de α sur K

Bien noter que les notions d'élément algébrique et transcendant dépendent du corps de base K (tout élément de L est évidemment algébrique sur L). Noter aussi que le polynôme minimal π est toujours irréductible sur K (car L est un anneau intègre donc si le produit de deux polynômes de $K[T]$ annule α, l'un de ces deux polynômes annule α).

Exemples.

- i est algébrique sur $\mathbf{Q}$, de polynôme minimal $X^2 + 1$.
- L'élément T de $K(T)$ est transcendant sur K (par définition !).
- On verra que l'ensemble des nombres complexes algébriques sur $\mathbf{Q}$ est dénombrable. Il y a donc beaucoup plus de nombres réels ou complexes transcendants sur $\mathbf{Q}$ que de nombres algébriques, bien qu'exhiber explicitement un nombre transcendant soit assez difficile !

Proposition 1.7 *Soient L/K une extension de corps et $\alpha \in K$. Il y a équivalence entre :*

1. *α est algébrique sur K.*
2. *$K[\alpha] = K(\alpha)$.*
3. *$K[\alpha]$ est un K-espace vectoriel de dimension finie.*

Si ces conditions sont satisfaites, alors l'entier $[K(\alpha) : K]$ est le degré du polynôme minimal de α; on l'appelle le degré de α sur K.

Démonstration : 1. implique 2. car dans ce cas $K[\alpha]$ est un anneau isomorphe à $K[T]/(\pi)$ avec π irréductible, donc comme $K[T]$ est un anneau principal, $K[\alpha]$ est un corps et il est égal à son corps des fractions $K(\alpha)$.

2. implique 1. car si α est transcendant, alors l'anneau $K[\alpha]$ est isomorphe à $K[T]$ qui n'est pas un corps.

1. implique 3. car si π est le polynôme minimal de α, alors le K-espace vectoriel $K[\alpha]$ est isomorphe à $K[T]/(\pi)$ qui est de dimension $\deg \pi$ (via la division euclidienne par π dans $K[T]$).

3. implique 1. car si α est transcendant, le K-espace vectoriel $K[\alpha]$ est isomorphe à $K[T]$ qui est de dimension infinie.

□

Définition 1.8 Une extension L/K est dite *algébrique* si tout élément de L est algébrique sur K.

Ainsi toute extension finie est algébrique, mais on verra que la réciproque est fausse.

Le théorème principal sur les éléments algébriques est le suivant :

Theorème 1.9 *Soit L/K une extension de corps. On note M l'ensemble des éléments de L qui sont algébriques sur K. Alors :*

1. *M est un sous-corps de L.*
2. *Tout élément de L qui est algébrique sur M est dans M; on dit que M est la clôture algébrique de K dans L.*
3. *En particulier, si L est algébriquement clos, M est algébriquement clos; on dit dans ce cas que M est une clôture algébrique de K.*

Remarque : Plus généralement on dit qu'une extension $\overline{K}$ de K est une *clôture algébrique* de K si $\overline{K}$ est algébriquement clos, et $\overline{K}/K$ est algébrique. D'après le théorème précédent, une telle clôture existe dès qu'il existe une extension L de K qui est algébriquement close; ceci est toujours vrai, mais la preuve nécessite le lemme de Zorn. D'autre part, la clôture algébrique est unique à isomorphisme près (non trivial).

Preuve du théorème : 1. Clairement $M \supset K$, donc 0 et 1 sont algébriques sur K. Si $x \in L$ est algébrique sur K, alors il existe un polynôme unitaire $X^n + ... + a_0$ dans $K[X]$ qui annule x. Alors $(-1)^n X^n + ... + a_0$ annule $-x$ et $1 + ... + a_0 X^n$ annule x^{-1}, donc $-x$ et x^{-1} sont algébriques sur K. Il s'agit maintenant de montrer que si x, y sont dans M, alors $x + y$ et xy sont encore dans M. Or $K[x] = K(x)$ est un corps, et y, qui est algébrique sur K l'est a fortiori sur $K[x]$, c'est-à-dire que $K[x, y] = K[x][y]$ est de dimension finie sur $K[x]$, donc aussi sur K via la base télescopique. Comme $K[x, y]$ contient $K[x + y]$ et $K[xy]$, il en résulte que ces deux derniers K-espaces vectoriels sont de dimension finie, ce qui signifie que $x + y$ et xy sont dans M.

2. Soit $x \in L$, algébrique sur M. Alors il existe un polynôme unitaire $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ de $M[X]$ qui annule x. Comme chaque a_i est algébrique sur K, on a par récurrence que $K[a_0, ..., a_{n-1}] = K(a_0, ..., a_{n-1})$ est un corps K' qui est de dimension finie sur K. Comme $P \in K'[X]$ est non nul et annule x, il en résulte que x est algébrique sur K', i.e. $K'[x]$ est de dimension finie sur K'; comme K'/K est finie, $K'[x]$ est aussi de dimension finie sur K, et $K[x]$ (qui en est un sev) aussi, i.e. x est algébrique sur K. Finalement $x \in M$.

3. Si $P \in M[X]$ est non constant, il admet une racine x dans le corps algébriquement clos L, mais x est alors algébrique sur M, donc $x \in M$ d'après 2.

□

Exemple. L'ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques sur $\mathbf{Q}$ est un corps algébriquement clos, c'est une clôture algébrique de $\mathbf{Q}$. Noter que $\overline{\mathbf{Q}}$ est dénombrable car $\mathbf{Q}[X]$ l'est (c'est la réunion pour $n \in \mathbf{N}$ des polynômes de $\mathbf{Q}[X]$ de degré au plus n), et chaque polynôme non nul de $\mathbf{Q}[X]$ n'a qu'un nombre fini de racines dans $\overline{\mathbf{Q}}$. L'ensemble $\mathbf{R} \cap \overline{\mathbf{Q}}$ des réels algébriques est donc également dénombrable ("presque tous les réels sont transcendants sur $\mathbf{Q}$").

2. Corps de rupture, corps de décomposition

Étant donnés K un corps et P un polynôme de $K[X]$, on cherche une extension L de K dans laquelle P a une racine. Cela amène la définition suivante :

Définition 2.1 Soit P un polynôme *irréductible* de $K[X]$. On dit qu'une extension L de K est un *corps de rupture* pour P sur K s'il existe une racine α de P dans L telle que $L = K[\alpha]$ $(= K(\alpha)$ puisque α est algébrique sur $K)$.

Ainsi un corps de rupture est une extension dans laquelle P a une racine, et qui est minimale pour cette propriété.

Theorème 2.2 *Pour tout polynôme irréductible $P \in K[X]$, il existe un corps de rupture L. De plus L est unique à K-isomorphisme près.*

Remarque : On n'aurait pas unicité si P n'était pas irréductible, prendre $P = (X^2 - 2)(X^2 - 3)$ sur $\mathbf{Q}$, et les corps $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ (ils ne sont pas isomorphes car 2 est un carré dans le premier et pas dans le second).

Démonstration : Comme P est irréductible, $L = K[X]/(P)$ est un corps. C'est une extension de K car l'application $\lambda \mapsto \bar{\lambda}$ de K dans L est un morphisme de corps. Enfin, si on prend pour α la classe de X dans $K[X]/(P)$, on a $P(\alpha) = 0$ et $L = K[\alpha]$, donc L est un corps de rupture pour P sur K. D'où l'existence.

Si maintenant L' est un corps de rupture pour P sur K, soit α' avec $L' = K[\alpha']$ et $P(\alpha') = 0$. Alors l'application $K[X] \to L'$, $Q \mapsto Q(\alpha')$ est surjective, de noyau (P) car le noyau contient (P) avec P irréductible (donc (P) maximal puisque $K[X]$ est principal). Finalement on obtient un isomorphisme de L sur L' qui induit l'identité sur K, i.e. un K-isomorphisme de L sur L'.

□

Examples.

1. $\mathbf{C}$ est le corps de rupture de $X^2 + 1$ sur $\mathbf{R}$.
2. $\mathbf{Q}(i)$ est le corps de rupture de $X^2 + 1$ sur $\mathbf{Q}$.
3. $\mathbf{Q}(\sqrt{3})$ est le corps de rupture [2] de $X^3 - 2$ sur $\mathbf{Q}$. Noter qu'ici le polynôme $X^3 - 2$ *n'est pas scindé* sur $\mathbf{Q}$. Ce phénomène ne se produit pas pour les polynômes de degré 2 parce que si $X^2 + aX + b$ possède une racine x dans L, alors l'autre racine $-x - a$ est encore dans L.

Le dernier exemple ci-dessus conduit à la définition suivante :

Définition 2.3 Soient K un corps et P un polynôme (qu'on ne suppose pas irréductible) de $K[X]$. On dit qu'une extension L/K est un *corps de décomposition* pour P sur K si L vérifie les deux proriétés suivantes :
i) P est scindé sur L.

[2] Ici on devrait vraiment dire "un" corps de rupture parce qu'il n'y a pas unicité même en tant que sous corps de $\mathbf{C}$: $\mathbf{Q}(j\sqrt{3})$ et $\mathbf{Q}(j^2\sqrt{3})$ conviennent aussi.

ii) L est engendré (comme corps ou comme anneau) par les racines de P sur L.

Ainsi un corps de décomposition est une extension minimale de K sur laquelle P est scindé.

Theorème 2.4 *Pour tout P de $K[X]$, il existe un corps de décomposition L, qui est unique à K-isomorphisme près.*

Démonstration : a) Existence. On procède par récurrence sur $\deg P$. Le cas $\deg P \leq 1$ est trivial. Soit Q un facteur irréductible de P. Alors Q admet un corps de rupture $K' = K[x] = K(x)$ sur K. Dans $K'[X]$, on a alors $P = (X - x)P_1$ avec $\deg P_1 < \deg P$. On applique alors l'hypothèse de récurrence à P_1 sur K' : il existe un corps de décomposition L pour P_1. Alors $P = (X - x)P_1$ est scindé sur L, et d'autre part $L = K'(x_2, ..., x_n)$, où $x_2, ..., x_n$ sont les racines de P_1 donc $L = K(x, x_2, ..., x_n)$ est engendré sur K par les racines de P, i.e. c'est un corps de décomposition de P sur K.

b) Unicité. On démontre par récurrence sur $\deg P$ l'assertion plus générale suivante : si $\varphi : K \to K'$ est un isomorphisme de corps, P est un polynôme de $K[X]$, et L, L' des corps de décomposition respectifs de P sur K, $\varphi(P)$ sur K', alors il existe un isomorphisme de corps $\psi : L \to L'$ qui prolonge φ. On obtiendra ensuite le résultat en faisant $K = K'$, $\varphi = \mathrm{Id}$. Si P est scindé (en particulier si $\deg P \leq 1$), on a $L = K$, $L' = K'$ et l'assertion est évidente. Sinon soit α racine de P dans $L \setminus K$, de polynôme minimal $Q \in K[X]$. Alors $\varphi(Q)$ admet une racine α' dans L' et $K[\alpha]$, $K[\alpha']$ sont des corps de rupture respectifs de Q, $\varphi(Q)$ sur K, K'. On prolonge φ en un isomorphisme $\varphi_1 : K[\alpha] \to K'[\alpha']$ en envoyant α sur α' : plus précisément pour tout polynôme R de $K[X]$, on définit $\varphi_1(R(\alpha)) = \varphi(R)(\alpha')$, ce qui a bien un sens puisque les polynômes minimaux de α, α' sur K, K' sont respectivement Q, $\varphi(Q)$. On écrit $P = (X-\alpha)P_1$ et $\varphi_1(P) = (X-\alpha')\varphi_1(P_1)$ avec $P_1 \in K[\alpha][X]$, puis on applique l'hypothèse de récurrence au polynôme P_1. L, L' sont des corps de décomposition respectifs de P_1, $\varphi_1(P_1)$ sur $K[\alpha]$, $K'[\alpha']$, d'où un isomorphisme $\psi : L \to L'$ qui prolonge φ_1, donc aussi φ.

□

Remarque : L'unicité est "meilleure" que celle du corps de rupture car si deux corps de décomposition L, L' d'un polynôme $P \in K[X]$ sont des sous-corps d'une même extension M de K, alors $L = L'$ vu que ces deux corps sont égaux à $K(x_1, ...x_n)$, où $x_1, ...x_n$ sont les racines de P dans L.

Exemples. Sur $\mathbf{R}$, le corps de décomposition d'un polynôme est $\mathbf{R}$ ou $\mathbf{C}$, suivant que le polynôme a ou non toutes ses racines réelles. Sur $\mathbf{Q}$, le

corps de décomposition de $X^3 - 2$ est $\mathbf{Q}(\sqrt{3}, j)$ (noter qu'il est de degré 6 sur $\mathbf{Q}$).

3. Corps finis

Les résultats ci-dessus vont nous permettre de construire les corps finis. Rappelons qu'un corps fini K est de caractéristique $p > 0$. Il peut être vu comme extension de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ via le morphisme $\mathbf{F}_p \to K$, $\bar{x} \mapsto x.1_K$. En particulier c'est un $\mathbf{F}_p$-espace vectoriel de dimension finie donc le cardinal de K est une puissance de p. En sens inverse, on a :

Theorème 3.1 *Soit $q = p^n$ avec $n \in \mathbf{N}^*$. Alors il existe un corps de cardinal q, unique à isomorphisme près. C'est le corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. On note ce corps $\mathbf{F}_q$.*

Démonstration : Soit K le corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. On note que l'ensemble K' des racines dans K de $X^q - X$ est déjà un corps, en vertu de l'identité $(x+y)^{p^n} = x^{p^n} + y^{p^n}$, qui se montre par récurrence sur n en utilisant le fait que tous les coefficients binomiaux C_p^k sont divisibles par p pour $0 < k < p$. Par définition du corps de décomposition, on a $K = K'$. D'autre part la dérivée de $X^q - X$ est $qX^{q-1} - 1 = -1$, donc toutes les racines sont simples et il y en a donc q. Finalement K est bien un corps de cardinal q.

Si maintenant L est un corps de cardinal q, alors tout élément x de L vérifie $x^q = x$ (c'est clair pour $x = 0$, et si $x \neq 0$ on a $x^{q-1} = 1$ parce que K^* est un groupe de cardinal $q - 1$). Ainsi $X^q - X$ est scindé sur L, et L contient donc un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$, i.e. un corps K_1 isomorphe à K. Par cardinalité $L = K_1$, et L est isomorphe à K.

□

Par exemple on a $\mathbf{F}_4 = \mathbf{F}_2[X]/(X^2 + X + 1)$, $\mathbf{F}_8 = \mathbf{F}_2[X]/(X^3 + X + 1)$, $\mathbf{F}_9 = \mathbf{F}_3[X]/(X^2 + 1)$. Il n'est pour l'instant pas clair qu'on peut faire apparaître tous les corps finis de caractéristique p comme corps de rupture sur $\mathbf{F}_p$. Pour cela, on a besoin de savoir qu'il y a des polynômes irréductibles de tout degré sur $\mathbf{F}_p$, ce qu'on va voir dans le dernier paragraphe de ce cours...

[Exercice : si K est un corps fini, et $P \in K[X]$ est irréductible, alors le corps de rupture de K coïncide avec son corps de décomposition.]

Remarques : -Toute algèbre à division finie est un corps (théorème de Wedderburn), autrement dit il n'y a pas de "corps non commutatifs" finis.

-Notons que $\mathbf{F}_{p^n}$ est une extension de $\mathbf{F}_{p^m}$ si et seulement si n divise m (et non pas p^n divise p^m). Par exemple $\mathbf{F}_8$ n'est pas une extension de $\mathbf{F}_4$.

4. Polynômes irréductibles, exemples

4.1. Le cas des corps finis

Le théorème suivant donne un résultat d'existence de polynômes irréductibles sur un corps fini. Trouver explicitement des polynômes irréductibles est en revanche une question difficile.

On définit la *fonction de Möbius* $\mu : N^* \to \{0, 1, -1\}$ par : $\mu(1) = 1$, $\mu(n) = 0$ si n possède un facteur carré, et $\mu(p_1...p_r) = (-1)^r$ si $p_1, ..., p_r$ sont des nombres premiers distincts.

Theorème 4.1 *Soit $\mathbf{F}_q$ le corps fini à q éléments. On note $I(n, q)$ le nombre de polynômes irréductibles unitaires de degré n de $\mathbf{F}_q[X]$. Alors pour tout $n \geq 1$, on a $I(n, q) > 0$. Plus précisément*

$$I(n, q) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d$$

Démonstration : Notons déjà que $\sum_{d|n} \mu(n/d) q^d \geq q^n - \sum_{d=1}^{n/2} q^d = q^n - \frac{q^{n/2}-q}{q-1}$ qui est strictement positif. Ainsi la formule qu'on veut montrer pour $I(n, q)$ implique bien $I(n, q) > 0$, c'est-à-dire qu'il y a des polynômes irréductibles de degré n dans $\mathbf{F}_q[X]$ pour tout $n \in \mathbf{N}^*$.

On va montrer :

$$q^n = \sum_{d|n} dI(d, q) \tag{1}$$

Considérons le polynôme $Q = X^{q^n} - X$ de $\mathbf{F}_q[X]$, et sa décomposition en produit de facteurs irréductibles unitaires

$$Q = P_1...P_r$$

On note qu'il n'y a pas de facteurs multiples dans cette décomposition, sinon un des P_i diviserait Q' alors que $Q' = -1$. Montrons que les P_i sont exactement les polynômes irréductibles de $\mathbf{F}_q[X]$ dont le degré divise n. Si P est irréductible de degré d, alors soit x une racine de P dans un corps de rupture. Ce corps de rupture est de degré d sur $\mathbf{F}_q$, donc il est isomorphe à $\mathbf{F}_{q^d}$, donc on a $x^{q^d} = x$, puis $x^{q^n} = x$ si d divise n. Comme P est le minimal de x sur $\mathbf{F}_q$ (puisqu'il est irréductible), il en résulte que P divise Q.

Réciproquement si P est irréductible de degré d et divise Q, alors toute racine x de P annule Q, donc le corps de décomposition $\mathbf{F}_{q^n}$ de Q contient $\mathbf{F}_{q^d} = \mathbf{F}_q[x]$, d'où d divise n via la base télescopique et les inclusions $\mathbf{F}_q \subset \mathbf{F}_{q^d} \subset \mathbf{F}_{q^n}$. En comparant le degré de Q et de $\prod_{i=1}^r P_i$, on obtient (1).

Pour terminer la preuve du théorème, il suffit alors de prouver :

Lemme 4.2 (Formule d'inversion de Möbius) *Soient $(A, +)$ un groupe abélien et f une application de $\mathbf{N}^*$ vers A. On pose $g(n) = \sum_{d|n} f(d)$. Alor*

$$f(n) = \sum_{d|n} \mu(n/d) g(d)$$

Démonstration : On remarque que

$$\sum_{d|n} \mu(d) = \delta_{1,n} \tag{2}$$

i.e. la somme vaut zéro pour tout entier $n \geq 2$, et 1 pour $n = 1$ (il est d'ailleurs facile de voir que ceci caractérise la fonction de Möbius). On a

$$\sum_{d|n} \mu(n/d) g(d) = \sum_{d|n} \mu(n/d) \sum_{d'|d} f(d') = \sum_{d'|n} f(d') \sum_{d'|d|n} \mu(n/d)$$

En posant $d_1 = n/d$, cette somme vaut

$$\sum_{d'|n} f(d') \sum_{d_1|(n/d')} \mu(d_1) = f(n)$$

d'après (2).

□

4.2. Irréductibilité sur Q et sur Z/pZ

Pour étudier l'irréductibilité d'un polynôme de $\mathbf{Q}[X]$, on peut toujours se ramener (en multipliant par un entier) à un polynôme primitif de $\mathbf{Z}[X]$. Le critère le plus efficace sera alors en général celui d'Eisenstein. Voici une autre façon d'utiliser la réduction modulo p :

Proposition 4.3 *Soit $P = a_n X^n + ... + a_0$ un polynôme de $\mathbf{Z}[X]$. Soit p un nombre premier. On suppose que p ne divise pas a_n. Alors, si la réduction $\overline{P}$ de P dans $\mathbf{Z}/p\mathbf{Z}[X]$ est irréductible, P est irréductible sur $\mathbf{Q}$.*

Remarque : On fera attention aux hypothèses ($2X^2 + X$ est irréductible modulo 2, mais il n'est pas irréductible dans $\mathbf{Q}[X]$) et à la conclusion (P n'est pas forcément irréductible sur $\mathbf{Z}$, par exemple $3X$ est irréductible modulo 2). Ce critère paraît séduisant, mais d'abord il ne donne qu'une condition suffisante, ensuite il n'est en général pas facile de déterminer si un polynôme de $\mathbf{Z}/p\mathbf{Z}[X]$ est irréductible si le degré est grand ! Bien entendu la proposition se généralise immédiatement à un anneau factoriel et à un idéal premier.

Démonstration : On a déjà $\deg P \geq 1$ sinon $\overline{P}$ ne serait pas irréductible sur $\mathbf{Z}/p\mathbf{Z}$. Si P était réductible sur $\mathbf{Q}$, il le serait donc aussi sur $\mathbf{Z}$ (d'après ce qu'on a vu dans le chapitre sur les anneaux factoriels) et on pourrait écrire $P = QR$ dans $\mathbf{Z}[X]$ avec Q et R de degré au moins 1. Mais comme p ne divise pas a_n, $\overline{P}$ a même degré que P, donc $\overline{Q}$ et $\overline{R}$ sont non constants, ce qui contredit l'irréductibilité de $\overline{P}$.

□

Rappelons que pour tout corps K, un polynôme de $K[X]$ de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine dans K. Voici un autre critère, souvent utile pour les corps finis :

Proposition 4.4 *Soit $P \in K[X]$. Si P n'a pas de racines dans toute extension de K de degré au plus $n/2$, alors P est irréductible.*

Démonstration : Si P est réductible, on peut l'écrire $P = QR$ avec P et Q non constants, et l'un des facteurs irréductibles π de P est donc de degré d au moins $n/2$. Comme π a une racine dans une extension de degré d de K (un corps de rupture), la proposition en résulte.

□

Par exemple $X^4 + X + 1$ est irréductible sur $\mathbf{F}_2$.

4.3. Polynômes cyclotomiques

Soit $\mu_n \subset \mathbf{C}^*$ le groupe multiplicatif des racines de l'unité. On note μ_n^* l'ensemble des racines *primitives* n-ièmes de l'unité, c'est l'ensemble des générateurs de $(\mu_n, \times)$. Le cardinal de μ_n^* est $\varphi(n)$, cet ensemble consiste en les $e^{2ik\pi/n}$ avec k entier premier à n.

Pour tout entier $n > 0$, on définit le *n-ième polynôme cyclotomique* Φ_n par

$$\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

Par exemple si p est premier, on a $\Phi_p = 1 + X + ... + X^{p-1}$.

Proposition 4.5 *On a $X^n - 1 = \prod_{d|n} \Phi_d$. Pour tout $n \in \mathbf{N}^*$, le polynôme Φ_n est dans $\mathbf{Z}[X]$.*

Démonstration : La première assertion vient de ce que $X^n - 1$ et $\prod_{d|n} \Phi_d$ sont deux polynômes unitaires, scindés et à racines simples dans $\mathbf{C}[X]$, qui ont les mêmes racines (en effet μ_n est la réunion des μ_d^* pour d divisant n, comme on le voit en triant les éléments de μ_n suivant leur ordre). La deuxième assertion se montre par récurrence sur n : pour $n = 1$, on a $\Phi_1 = X - 1$, et si tous les Φ_d sont dans $\mathbf{Z}[X]$ pour $d < n$, la formule précédente donne $X^n - 1 = R.\Phi_n$ (dans $\mathbf{C}[X]$), avec R dans $\mathbf{Z}[X]$ et unitaire; ainsi Φ_n est aussi dans $\mathbf{Z}[X]$ en considérant la division euclidienne de $X^n - 1$ par le polynôme *unitaire* R de $\mathbf{Z}[X]$.

□

Le théorème principal sur les polynômes cyclotomiques est le suivant :

Theorème 4.6 *Le polynôme Φ_n est irréductible sur $\mathbf{Q}$.*

Ainsi si ζ est dans μ_n^*, le polynôme minimal de ζ est Φ_n et le degré $[\mathbf{Q}(\zeta) : \mathbf{Q}]$ est $\varphi(n)$. Noter que $\mathbf{Q}(\zeta)$ est aussi le corps de décomposition de Φ_n.

Pour démontrer le théorème, la proposition-clef est la suivante :

Proposition 4.7 *Soit $\zeta \in \mu_n^*$. On fixe un nombre premier p ne divisant pas n, puis on appelle f, g les polynômes minimaux respectifs de ζ, ζ^p sur $\mathbf{Q}$. Alors*

1. *f et g sont dans $\mathbf{Z}[X]$.*
2. *$f = g$.*

Démonstration : 1. Il suffit de montrer le résultat pour f car comme p est premier à n, g est encore le polynôme minimal d'une racine primitive n-ième de l'unité. Comme $X^n - 1$ annule ζ, f divise $X^n - 1$. Comme $\mathbf{Z}[X]$ est factoriel, on peut décomposer $X^n - 1$ en un produit de facteurs irréductibles $P_1...P_r$ dans $\mathbf{Z}[X]$, et on peut choisir les P_i unitaires quitte à en multiplier certains par -1, vu que $X^n - 1$ est unitaire. alors $P_1...P_r$ est aussi

la décomposition en produit de facteurs irréductibles dans $\mathbf{Q}[X]$, donc f est l'un des P_i et $f \in \mathbf{Z}[X]$. [3]

2. Supposons le contraire. Alors f et g sont premiers entre eux et divisent Φ_n, donc fg divise Φ_n (dans $\mathbf{Q}[X]$, donc aussi dans $\mathbf{Z}[X]$ puisque tous ces polynômes sont unitaires). On observe que le polynôme $h = g(X^p)$ annule ζ. Par conséquent il est divisible par f (dans $\mathbf{Q}[X]$, ou dans $\mathbf{Z}[X]$, toujours parce que f est unitaire). Ainsi la réduction $\bar{h}$ de h modulo p est divisible par $\bar{f}$ dans $\mathbf{Z}/p\mathbf{Z}[X]$. Mais comme tout élément $\bar{a}$ de $\mathbf{Z}/p\mathbf{Z}$ vérifie $\bar{a}^p = \bar{a}$, on obtient $\bar{h} = \bar{g}^p$. Ainsi $\bar{f}$ divise $\bar{g}^p$. Le polynôme unitaire $\bar{f}$ n'est pas forcément irréductible dans $\mathbf{Z}/p\mathbf{Z}[X]$, mais il admet un facteur irréductible $\varphi \in \mathbf{Z}/p\mathbf{Z}[X]$. On a alors $\varphi \mid \bar{g}$. Comme d'autre part $\bar{f}\bar{g}$ divise $\bar{\Phi}_n$, on obtient a fortiori que φ^2 divise le polynôme $Q = X^n - \bar{1}$ dans $\mathbf{Z}/p\mathbf{Z}[X]$. Mais ceci n'est pas possible car Q est premier avec Q', via l'identité de Bezout dans $\mathbf{Z}/p\mathbf{Z}[X]$:

$$(X/\bar{n})Q' - Q = \bar{1}$$

qui a un sens parce que p ne divise pas n, donc $\bar{n}$ est inversible dans $\mathbf{Z}/p\mathbf{Z}$.

□

Preuve du théorème : Fixons une racine primitive n-ième ζ de l'unité, et appelons f son polynôme minimal sur $\mathbf{Q}$. Si ζ' est un autre élément de μ_n^*, on peut écrire $\zeta' = \zeta^m$ avec m premier à n; ainsi $m = \prod_{i=1}^r p_i^{\alpha_i}$ où les nombres premiers p_i ne divisent pas n. D'après la proposition précédente, le polynôme minimal de ζ' sur $\mathbf{Q}$ est encore f. Finalement f est divisible dans $\mathbf{C}[X]$ par tous les $(x - \zeta')$ avec $\zeta' \in \mu_n^*$, donc f est divisible par Φ_n (dans $\mathbf{C}[X]$, donc aussi dans $\mathbf{Q}[X]$). Comme $\Phi_n(\zeta) = 0$, Φ_n est multiple de f et finalement $\Phi_n = f$ donc Φ_n est irréductible sur $\mathbf{Q}$.

□

[3] Le même argument donne que pour tout anneau factoriel A, le polynôme minimal sur $K := \operatorname{Frac} A$ d'un élément x qui annule un polynôme *unitaire* à coefficients dans A est encore dans $A[X]$.