

## Décomposition en irréductibles et orbites sous l'action du groupe de Galois

Soit  $P \in K[X]$  un polynôme unitaire et séparable. Soit  $\alpha_1, \dots, \alpha_n$  ses racines dans un corps de décomposition  $L$  de  $P$  sur  $K$ . Nous avons vu que  $\text{Gal}(L/K)$  agissait sur les racines de  $P$ , ce qui permet de définir un morphisme injectif de groupes

$$\rho: \text{Gal}(L/K) \rightarrow \mathfrak{S}_n$$

où pour tout  $\sigma \in \text{Gal}(L/K)$ ,  $\rho(\sigma)$  est la permutation de  $\{1, \dots, n\}$  qui envoie  $i$  sur l'unique  $j$  tel que  $\sigma(\alpha_i) = \alpha_j$ . Ce morphisme  $\rho$  définit donc une action de  $\text{Gal}(L/K)$  sur l'ensemble  $\{1, \dots, n\}$ , et c'est relativement à cette action que nous parlons d'orbites dans l'énoncé ci-dessous.

**Théorème 1.** Notons  $\Omega_1, \dots, \Omega_m$  les orbites de  $\{1, \dots, n\}$  sous l'action de  $\text{Gal}(L/K)$ . Alors

$$P = \prod_{k=1}^m P_k \quad \text{où} \quad P_k = \prod_{i \in \Omega_k} (X - \alpha_i)$$

et les  $P_k$  sont des polynômes irréductibles de  $K[X]$ .

Étudions quelques exemples pour voir comment se manifeste concrètement ce théorème dans des situations au programme de l'agrégation.

**Exemple 2.** Racines conjuguées et factorisation dans  $\mathbf{R}[X]$

Si  $P \in \mathbf{R}[X]$  est un polynôme séparable, nous avons l'habitude d'obtenir ses facteurs irréductibles de degré 2 en regroupant les racines non-réelles par paires  $\{z, \bar{z}\}$ . Comme  $\text{Gal}(\mathbf{C}/\mathbf{R}) = \{\text{id}, z \mapsto \bar{z}\}$ , nous appliquons exactement la stratégie générale du Théorème 1 en regroupant les racines par orbites sous l'action du groupe de Galois.

**Exemple 3.** Factorisation sur  $\mathbf{F}_2$  de  $X^{32} - X$

Comme souvent en prépa agreg : *vous en rêviez ? Philippe Caldero l'a fait !* Cet exemple s'inspire donc de son document accessible ici :

<https://math.univ-lyon1.fr/~caldero/Factorisation-corps-fini.pdf>

Nous allons utiliser le Théorème 1 ci-dessus pour montrer que le polynôme  $X^{32} - X$  admet la factorisation en produits d'irréductibles suivante dans  $\mathbf{F}_2[X]$  :

$$X^{32} - X = X(X-1)(X^5 + X^3 + 1)(X^5 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X + 1)(X^5 + X^4 + X^2 + X + 1)(X^5 + X^3 + X^2 + X + 1)$$

— *Méthode 1* : Ce résultat est un cas particulier du fait général suivant : le polynôme  $X^{p^n} - X$  se factorise sur  $\mathbf{F}_p[X]$  comme

$$\prod_{d|n} \prod_{P \in \mathcal{I}(d,p)} P(X)$$

où  $\mathcal{I}(d, p)$  désigne l'ensemble des polynômes irréductibles unitaires de degré  $d$  à coefficients dans  $\mathbf{F}_p$ . On l'applique ici à  $p = 2$  et  $n = 5$ , donc les seuls diviseurs de  $n$  sont 1 et 5, et la factorisation ci-dessus revient à déterminer la liste des polynômes irréductibles de degré 1 et de degré 5 dans  $\mathbf{F}_2[X]$ . C'est plutôt cette approche qui est développée dans le texte de Philippe Caldero. Nous allons maintenant détailler les arguments plus « galoisiens » de son exercice 0.2, qui permettent de se contenter de la connaissance d'un seul polynôme irréductible de degré 5 et d'en déduire les autres.

- *Méthode 2* : On sait que le corps de décomposition  $L$  de  $X^{32} - X$  sur  $\mathbf{F}_2$  est une extension de degré 5 de  $\mathbf{F}_2$  (c'est comme ça que l'on a construit  $\mathbf{F}_{2^5}$  dans le cours sur les corps finis). En outre, on sait aussi que l'extension  $L$  n'est pas seulement engendrée sur  $\mathbf{F}_2$  par les racines de  $X^{32} - X$ , mais est exactement formée des racines. On a donc la factorisation suivante dans  $L[X]$ .

$$X^{32} - X = \prod_{\beta \in L} (X - \beta) \quad (1)$$

Le Théorème 1 permet de faire le lien entre cette factorisation en facteurs linéaires dans  $L[X]$  et sa factorisation dans  $\mathbf{F}_2[X]$  en regroupant les racines en orbites sous l'action du groupe de Galois de  $L/\mathbf{F}_2$ .

Afin de rendre les calculs plus explicites, il est plus pratique de voir  $L$  comme un corps de rupture. Pour cela, il suffit de connaître un seul polynôme irréductible de degré 5 à coefficients dans  $\mathbf{F}_2$ , disons par exemple  $X^5 + X^3 + 1$  (la preuve de l'irréductibilité de ce polynôme est faite dans le document de Philippe Caldero). On se place alors dans le corps de rupture  $L := \mathbf{F}_2[X]/(X^5 + X^3 + 1)$  et on note  $\alpha$  la classe de  $X$  dans ce quotient, de sorte que  $L = \mathbf{F}_2(\alpha)$ . Alors l'extension  $L/\mathbf{F}_2$  est de degré 5, c'est donc un corps de décomposition sur  $\mathbf{F}_2$  du polynôme  $X^{32} - X$ , dont tous les éléments s'expriment dans la base  $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ . C'est-à-dire que dans la factorisation (1), chaque  $\beta$  s'écrit  $\sum_{i=0}^4 a_i \alpha^i$  pour un certain  $(a_0, \dots, a_4) \in \mathbf{F}_2^5$ . La question est de déterminer comment regrouper les  $\beta$  pour obtenir des facteurs irréductibles dans  $\mathbf{F}_2[X]$ .

Le Théorème 1 nous dit qu'il suffit de les regrouper par orbites sous l'action de  $\text{Gal}(L/\mathbf{F}_2)$ . Or ce groupe est cyclique d'ordre 5, engendré par l'automorphisme de Frobenius  $\text{Frob}: x \mapsto x^2$ . Les éléments 0 et 1 sont seuls dans leur orbite, car ils sont fixés par le Frobenius, ce qui donne les deux facteurs irréductibles de degré 1. Ensuite, commençons par exemple par  $\alpha$ . Son orbite est  $\{\alpha, \text{Frob}(\alpha), \text{Frob}^2(\alpha), \dots, \text{Frob}^4(\alpha)\} = \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$  et donc le Théorème 1 nous dit que le facteur

$$\prod_{i=0}^4 (X - \alpha^{2^i})$$

est un diviseur irréductible de  $X^{32} - X$  dans  $\mathbf{F}_2[X]$ . Comme il s'annule en  $\alpha$ , c'est le polynôme minimal de  $\alpha$ , c'est-à-dire  $X^5 + X^3 + 1$ . Il est très facile avec un logiciel de calcul formel de déterminer l'écriture des  $\alpha^{2^i}$  dans la base  $\{1, \dots, \alpha^4\}$ . On obtient

$$(\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}) = (\alpha, \alpha^2, \alpha^4, \alpha + \alpha^3 + \alpha^4, \alpha^2 + \alpha^3).$$

Ensuite on peut prendre un autre élément de  $L$  qui n'intervient pas comme racine d'un des facteurs irréductibles  $X, X - 1$  et  $X^5 + X^3 + 1$  déjà déterminés. Par exemple  $1 + \alpha$ , et regarder son orbite sous l'action du groupe de Galois : à nouveau avec un logiciel de calcul formel, on obtient

$$(1 + \alpha, (1 + \alpha)^2, (1 + \alpha)^4, \dots, (1 + \alpha)^{16}) = (1 + \alpha, 1 + \alpha^2, 1 + \alpha^4, 1 + \alpha + \alpha^3 + \alpha^4, 1 + \alpha^2 + \alpha^3).$$

On en déduit un nouveau facteur irréductible

$$(X - (1 + \alpha))(X - (1 + \alpha^2))(X - (1 + \alpha^4))(X - (1 + \alpha + \alpha^3 + \alpha^4))(X - (1 + \alpha^2 + \alpha^3))$$

qui, une fois développé avec un logiciel de calcul formel, est égal à  $X^5 + X^4 + X^3 + X^2 + 1$ . Cela semble magique qu'il y ait autant de simplifications et qu'on finisse par obtenir un polynôme dont les coefficients sont 0 ou 1, mais c'est même encore plus magique parce qu'on obtient un polynôme qui est irréductible sur  $\mathbf{F}_2$  !

On peut continuer tant que l'on a pas utilisé tous les éléments de  $L$ . Par exemple ici on peut encore prendre  $1 + \alpha + \alpha^2$  et regarder son orbite, qui est

$$\{1 + \alpha + \alpha^2, 1 + \alpha^2 + \alpha^4, 1 + \alpha + \alpha^3, 1 + \alpha + \alpha^2 + \alpha^4, 1 + \alpha + \alpha^2 + \alpha^3\}$$

```

Entrée [25]: F.<x> = GF(2)[]
             K.<a> = GF(2**5, name='a', modulus=x^5 + x^3 + 1)
             K.<T> = K[]

Entrée [26]: L = []
             for i in range(5):
                 L += [(1+a + a^2)^(2^i)]

Entrée [27]: L

Out[27]: [a^2 + a + 1, a^4 + a^2 + 1, a^3 + a + 1, a^4 + a^2 + a + 1, a^3 + a^2 + a + 1]

Entrée [28]: S = 1
             for l in L:
                 S = S*(T-1)

Entrée [29]: S

Out[29]: T^5 + T^4 + T^2 + T + 1

```

FIGURE 1 – Le produit des  $X - \beta$  pour  $\beta$  variant dans l'orbite de  $1 + \alpha + \alpha^2$  donne le facteur irréductible  $X^5 + X^4 + X^2 + X + 1$

Le polynôme que l'on obtient en faisant le produit des facteurs linéaires associés à ces racines est alors  $X^5 + X^4 + X^2 + X + 1$  (cf. Figure 1). En continuant ainsi avec les racines pas encore prises en compte dans les facteurs précédents, on obtient tous les polynômes irréductibles de degré 5 de  $\mathbf{F}_2[X]$  et on retrouve la factorisation obtenue par la première méthode.

#### Exemple 4. Factorisation des polynômes cyclotomiques sur les corps finis

Le Théorème 1 permet aussi d'apporter un nouvel éclairage sur la forme de la factorisation des polynômes cyclotomiques sur les corps finis. Nous avons vu dans le cours sur la cyclotomie que pour tout entier  $n \geq 1$ , et pour tout corps fini  $\mathbf{F}_q$  dont la caractéristique ne divise pas  $n$ , le polynôme  $\Phi_{n, \mathbf{F}_q}$  se factorise en un produit de  $\varphi(n)/r$  facteurs irréductibles de degré  $r$ , où  $r$  est l'ordre de  $q$  dans  $(\mathbf{Z}/n\mathbf{Z})^\times$ . Voyons quel est le lien avec les orbites sous l'action d'un groupe de Galois.

Soit  $\zeta$  une racine primitive  $n^{\text{ème}}$  de l'unité dans un corps de décomposition de  $X^n - 1$  sur  $\mathbf{F}_q$ . Alors toutes les autres racines primitives  $n^{\text{ème}}$  sont de la forme  $\zeta^k$  pour  $k$  premier avec  $n$  et on a

$$\Phi_{n, \mathbf{F}_q} = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - \zeta^k)$$

dans  $\mathbf{F}_q(\zeta)[X]$ . Toute la question est de savoir comment regrouper les facteurs linéaires pour obtenir une factorisation en produits d'irréductibles dans  $\mathbf{F}_q[X]$ . Le Théorème 1 nous dit qu'il suffit de les regrouper en orbites sous l'action de  $\text{Gal}(\mathbf{F}_q(\zeta)/\mathbf{F}_q)$ . Ce groupe est cyclique<sup>1</sup>, engendré par l'automorphisme  $\text{Frob}_q: x \mapsto x^q$ . Partons donc d'une racine fixée  $\zeta^k$  pour un certain  $k \in (\mathbf{Z}/n\mathbf{Z})^\times$ , et appliquons lui les itérés de  $\text{Frob}_q$  :

$$\zeta^k, (\zeta^k)^q, (\zeta^k)^{q^2}, \dots, (\zeta^k)^{q^{m-1}}$$

On a parcouru une fois toute l'orbite de  $\zeta^k$  lorsque l'entier  $m$  est minimal pour la propriété  $(\zeta^k)^{q^m} = \zeta^k$ , c'est-à-dire lorsque  $kq^m \equiv k \pmod{n}$ . Puisque  $k$  est inversible modulo  $n$ , on peut simplifier cette égalité en  $q^m \equiv 1 \pmod{n}$  et donc le cardinal de chaque orbite est égal à  $m$  : l'ordre de  $q$  dans  $(\mathbf{Z}/n\mathbf{Z})^\times$ .

1. Attention, contrairement au cas de  $\mathbf{Q}(\zeta)/\mathbf{Q}$ , ce groupe n'est pas nécessairement de cardinal  $\varphi(n)$ , car le polynôme minimal de  $\zeta$  n'est pas forcément  $\Phi_{n, \mathbf{F}_q}$  puisque ce dernier n'est pas toujours irréductible.

Comme cela ne dépend pas de  $k$ , on en déduit que toutes les orbites ont le même cardinal, et on retrouve bien le résultat déjà vu : les facteurs irréductibles de  $\Phi_n, \mathbf{F}_q$  dans  $\mathbf{F}_q[X]$  ont tous le même degré, et ce degré commun est l'ordre de  $q$  dans  $(\mathbf{Z}/n\mathbf{Z})^\times$ .

**Exemple 5.** *Irréductibilité des polynômes cyclotomiques sur  $\mathbf{Q}$*

Soit  $n \geq 1$  et  $\Phi_n$  le  $n^{\text{ème}}$  polynôme cyclotomique sur  $\mathbf{Q}$ . L'irréductibilité sur  $\mathbf{Q}$  de ce polynôme peut s'interpréter comme une conséquence du Théorème 1, mais le serpent se mord la queue car pour appliquer ce théorème il faut comprendre le groupe de Galois de l'extension, ce que je ne sais pas faire sans l'irréductibilité des polynômes cyclotomiques.

Il est tout de même intéressant de voir le lien entre ces différents énoncés. Soit  $\zeta$  une racine primitive  $n^{\text{ème}}$  de l'unité dans  $\mathbf{C}$ . Alors l'extension  $\mathbf{Q}(\zeta)/\mathbf{Q}$  est un corps de décomposition de  $X^n - 1$  sur  $\mathbf{Q}$ , c'est donc une extensions galoisienne (en tant que corps de décomposition d'un polynôme séparable). De plus, le groupe de Galois de cette extension peut être déterminé sans faire appel à la théorie de Galois, et est isomorphe à  $(\mathbf{Z}/n\mathbf{Z})^\times$ . Un isomorphisme est donné par

$$\begin{array}{ccc} \varphi & : & (\mathbf{Z}/n\mathbf{Z})^\times \rightarrow \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \\ & & k \mapsto \varphi_k \end{array}$$

où  $\varphi_k$  est l'unique automorphisme qui envoie  $\zeta$  sur  $\zeta^k$  (cf. le complément sur la cyclotomie).

*Cependant, pour montrer que  $\varphi_k$  (que l'on définit seulement sur  $\mathbf{Q}$  et en  $\zeta$ ) est bien un automorphisme de  $\mathbf{Q}(\zeta)$ , je crains qu'il soit difficile d'éviter un argument du type «  $\zeta$  et  $\zeta^k$  ont le même polynôme minimal  $\Phi_n$ , et donc  $\varphi_k$  est un isomorphisme en tant que composée des applications d'évaluation naturelles  $\text{ev}_\zeta$  et  $\text{ev}_{\zeta^k}$  définies sur  $\mathbf{Q}[X]/(\Phi_n)$  », ou un argument de cardinalité du type « le groupe  $\text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$  est de cardinal  $\varphi(n)$  car c'est le degré de l'extension galoisienne  $\mathbf{Q}(\zeta)/\mathbf{Q}$  », qui utilise également l'irréductibilité.*

Après cette mise en garde, on peut tout de même se satisfaire de l'observation suivante, bien qu'elle ne constitue pas une preuve de l'irréductibilité des polynômes cyclotomiques : *le fait que  $\Phi_n$  soit irréductible est une manifestation du fait que l'action de  $(\mathbf{Z}/n\mathbf{Z})^\times$  soit transitive sur l'ensemble de ses racines.*

On peut donc interpréter la preuve classique de l'irréductibilité des polynômes cyclotomiques comme une application de la stratégie de preuve du Théorème 1 : en effet, on part d'un facteur irréductible  $f$  de  $\Phi_n$ , on veut montrer qu'il est égal à  $\Phi_n$ . Pour cela, on part d'une racine de  $f$ , et on construit plein d'autres racines en faisant agir un certain groupe, ici  $(\mathbf{Z}/n\mathbf{Z})^\times$ , dont on ne sait pas encore qu'il est le groupe de Galois de l'extension. C'est cela qu'on fait quand on montre que pour tout racine de  $f$  et tout  $p$  premier avec  $n$ , l'élément  $u^p$  est toujours une racine de  $f$ . Cependant la preuve est subtile car justement, on ne sait pas qu'élever une racine à la puissance  $p$  première avec  $n$  définit un automorphisme de  $\mathbf{Q}(\zeta)$  qui fixe donc le sous corps premier  $\mathbf{Q}$  (si on savait cela, il serait clair qu'on obtient de nouveau une racine de  $f$  puisqu'on ne fait qu'appliquer à l'égalité  $f(u) = 0$  un automorphisme qui préserve les coefficients de  $f$ ).