# Retour TP 7 : Factorisation des polynômes sur $\mathbf{F}_p[X]$

► **Prérequis** : *Chapitre 5 du poly.*

## Exercice I

Dans cet exercice, $p$ est un nombre premier et on considère des polynômes en une variable $X$ à coefficients dans $\mathbf{F}_p$. On stockera la valeur de $p$ dans une variable globale. On s'intéresse à la factorisation d'un tel polynôme $P \in \mathbf{F}_p[X]$ : on voudrait être capable d'écrire une fonction qui renvoie la factorisation complète de $P$ sous la forme d'une liste de polynômes irréductibles.

Jusqu'à la question **3.** incluse, on suppose que le polynôme $P$ est non constant et séparable et on va lui appliquer l'algorithme de Berlekamp pour en déterminer un facteur irréductible.

**4.** On peut même démontrer cette équivalence. On a clairement que

$$(1 + X^3 + X^6)(X^3 - 1) = X^9 - 1$$

et que $P$ est irréductible sur $\mathbf{Z}[X]$ (par le critère d'Eisenstein appliqué à $P(X+1)$ et $p = 3$ par exemple, le calcul de $P(X+1)$ étant effectué dans le Notebook). On en déduit donc que $P$ est un polynôme cyclotomique et on peut vérifier que $P = \Phi_9$. On peut alors utiliser le résultat suivant[1] concernant la factorisation de $\Phi_n$ dans $\mathbf{F}_p$ avec $p \nmid n$ : le polynôme cyclotomique $\Phi_n$ se factorise en un produit de $\frac{\varphi(n)}{d}$ facteurs irréductibles 2 à 2 non associés et tous de même degré où $d$ est l'ordre de $p$ modulo $n$. Ici $\varphi(9) = 6$, on obtient donc que $P$ est scindé modulo $p$ si, et seulement si, l'ordre de $p$ modulo $9$ est 1, ce qui équivaut à demander que[2] $p \equiv 1 \pmod 9$.

**5.** Ici, il suffit d'extraire la partie sans facteur carré de $P$ et d'appliquer notre algorithme de factorisation à cette partie sans facteur carré. Enfin, pour obtenir les multiplicités, il suffit en effectuant des divisions euclidiennes de déterminer le plus grand entier $m$ tel qu'un facteur irréductible donné à la puissance $m$ divise $P$. Le seule problème est donc de savoir extraire la partie sans facteur carré d'un polynôme $P$. On sait que $P$ est séparable si, et seulement si, $\mathrm{Res}(P, P') \neq 0$ et l'algorithme mis en œuvre dans le TP 2 consistait à renvoyer $\frac{P}{\mathrm{pgcd}(P,P')}$. Malheureusement, en caractéristique positive, il va falloir être plus subtil car il est possible que $P' = 0$. Par exemple, dans le cas de $P(X) = (1+X)^7$ dans $\mathbf{F}_7$, on va avoir $\frac{P}{\mathrm{pgcd}(P,P')} = 1$.
On fixe le corps de base comme étant $\mathbf{F}_p$ avec $p$ un nombre premier. On utilise alors la propriété immédiate qu'un polynôme $P \in \mathbf{F}_p[X]$ s'écrit de manière unique sous la forme $P = Q \times R^p$ avec $Q, R \in \mathbf{F}_p[X]$ premiers entre eux et $Q$ produit d'irréductibles de multiplicité première à $p$. On a alors $P' = Q'R^P$ car on est en caractéristique $p$ et ainsi $\mathrm{pgcd}(P, P') = \mathrm{pgcd}(QR^p, Q'R^p) = R^p\mathrm{pgcd}(Q, Q')$. Il s'ensuit que

$$\frac{P}{\mathrm{pgcd}(P, P')} = \frac{Q}{\mathrm{pgcd}(Q, Q')}.$$

Or, on peut montrer que $Q' \neq 0$ car si $Q' = 0$, on obtient que $Q$ serait de la forme $S(X^p) = S(X)^p$ avec $S \in \mathbf{F}_p[X]$, ce qui est exclu. Dans ce cas, on a alors bien par le raisonnement habituel que $Q_{\mathrm{sfc}} = \frac{Q}{\mathrm{pgcd}(Q,Q')}$ est la partie sans facteur carrée de $Q$. On obtient alors $R^p$ en divisant $P$ par $Q_{\mathrm{sfc}}$ pour obtenir un nouveau polynôme $P_1$ et en réappliquant ce procédé jusqu'à ce que que $\frac{P_i}{\mathrm{pgcd}(P_i,P_i')} = 1$. On utilise alors le fait que $R(X)^p = R(X^p)$ pour obtenir $R$ et on réapplique l'algorithme à $R$ jusqu'à ce que[3] $R = 1$.

**6.** On conjecture que $X^4 + 1$ est scindé dans $\mathbf{F}_p[X]$ pour les premiers nombres premiers $p \equiv 1 \pmod 8$ et produit de deux polynômes irréductibles de degré 2 lorsque $p \not\equiv 1 \pmod 8$. Par ailleurs, $X^4 + 1 \equiv (X+1)^4 \pmod 2$. On peut facilement voir que si $p \equiv 3 \pmod 4$, comme $-1$ n'est pas un carré modulo $p$, que $P = X^4 + 1$ est soit irréductible soit un produit de deux irréductibles de degré 4. Mais pour tout $p$, le polynôme $P$ n'est jamais irréductible modulo $p$. En effet, on l'a vu pour $p = 2$ et on peut désormais supposer que $p$ est impair. Alors $8 \mid p^2 - 1$ si bien que le groupe cyclique $\mathbf{F}_{p^2}^\times$ est d'ordre divisible par 8. Par ailleurs,

$$X^8 - 1 = (X^4 - 1)(X^4 + 1)$$

si bien que toute racine $x$ de $P$ (dans un corps de décomposition) est racine de $X^8 - 1$ et vérifie donc $x^8 = 1$ et $x^4 = -1$ de sorte que $x$ est d'ordre 8. Or on vient de voir que le groupe cyclique $\mathbf{F}_{p^2}^\times$ est d'ordre divisible par 8 donc il contient un élément d'ordre 8 et $P$ a une racine dans $\mathbf{F}_{p^2}$, ce qui prouve que $P$ n'est pas irréductible (si $P$ était irréductible, une racine donnerait lieu à une extension de degré 4). Ainsi, pour $p \equiv 3 \pmod 4$, $P$ est produit de deux polynômes irréductibles de degré 2. Reste donc le cas le cas $p \equiv 1 \pmod 4$. Dans ce cas (et en fait on aurait aussi pu utiliser cet argument dans le cas précédent), on peut conclure comme en question 4 car $P = \Phi_8$. Mais à nouveau $P$ est irréductible sur $\mathbf{Z}[X]$ soit à l'aide d'Eisenstein à $P(X+1)$ avec $p = 2$ soit en utilisant les résultats classiques sur les polynômes cyclotomiques.

1. Que vous pouvez trouver dans la littérature ou ici `http://agregmaths.free.fr/doc/docs_nicolas/developpement%20Algebre/Condition%20d%27irreductibilite%20des%20polynomes%20cyclotomiques%20sur%20les%20corps%20finis.pdf`, la démonstration étant très élémentaire et classique.

2. Le théorème de la progression arithmétique de Dirichlet garantit qu'il existe une infinité de tels nombres premiers.

3. Noter que simplement dans l'optique de factoriser $P$, on peut appliquer Berlekamp à $Q_{\mathrm{sfc}}$ puis déterminer les multiplicités des facteurs irréductibles et en déduire $R^p$ donc $R$ par simple division, auquel on applique récursivement notre algorithme, $R$ n'étant pas nécessairement sans facteur carré.

**7.** Si la réduction du polynôme dans $\mathbf{F}_p[X]$ est irréductible pour un certain $p$ variant parmi les nombres premiers compris entre 3 et $N$ (où $N$ est un entier à préciser dans les entrées), alors le polynôme de $\mathbf{Z}[X]$ en question est irréductible sur $\mathbf{Q}[X]$. Bien sûr, l'exemple de la question précédente montre que la réciproque est fausse et ce test ne s'appliquera pas à ce polynôme (ni le test de la question suivante).

**8.** On va voir dans cette question qu'il est possible d'être plus subtil[4]. On constate en réduisant que modulo des nombres premiers inférieurs à 10 que le polynôme $Q = X^4 + 8X + 12 \in \mathbf{Z}[X]$ est parfois produit d'un polynôme irréductible de degré 3 par un polynôme de degré 1 et parfois produit de deux polynômes irréductibles de degré 2. Cela implique que $Q$ est irréductible sur $\mathbf{Q}[X]$ car sinon, soit il est produit de deux polynômes irréductibles de degré 2 sur $\mathbf{Q}[X]$, auquel cas sa réduction modulo $p$ ne peut jamais donner un produit d'un facteur de degré 3 par un facteur de degré 1 (et idem pour le produit d'un facteur de degré 2 et deux facteurs de degré 1) soit il est produit d'un facteur irréductible de degré 3 et d'un facteur de degré 1 auquel cas sa réduction modulo $p$ ne peut pas donner lieu à un produit de deux facteurs irréductibles de degré 2 car notamment $Q$ aura une racine modulo $p$.
Cette méthode ne marche pas pour $P = X^4 + 1$ car les deux factorisations possible (scindé et produit de deux facteurs de degré 2) ne sont pas incompatibles. Cela exclut que $P$ soit un produit d'un facteur de degré 3 par un facteur linéaire et de plus on sait que $P$ n'a pas de racine mais n'exclut pas la factorisation comme produit de deux irréductibles de degré 2. La différence entre les deux polynômes peut s'expliquer en termes de structure du groupe de Galois associé et grâce à de la théorie algébrique des nombres. Je vous renvoie pour cela à l'article Integer Polynomials that are Reducible Modulo all Primes de Rolf Brandl qui est aussi dans Dokéos. Les lemmes 1 et 2 de cet article ainsi que le fait que les polynômes $P$ et $Q$ donnent lieu à deux extensions galoisiennes de groupes de galois respectif $\mathbf{Z}/2\mathbf{Z}$ et $\mathfrak{A}_4$ montrent que $P$ et $Q$ ne peuvent pas être irréductible modulo $p$ car leur groupes de Galois ne contient aucun 4 cycle.

**9.** La version initiale convient en réalité déjà. On peut donner en entrée un polynôme à coefficients entiers de n'importe quelle variable.

**10.** La première étape de l'algorithme est d'écrire la matrice de l'endomorphisme $\Phi_P$ de $\mathbf{F}_P[X]/(P)$ défini par $y \longmapsto y^p - y$. On notera $n$ le egré de $P$ dans la suite. Étudions la complexité de cette étape. L'algorithme du polycopié consiste à calculer d'abord $X^p$ modulo $P$, ce qui coûte $O(pn)$ opérations puis à effectuer ensuite $X^{2p} = X^p \times X^p$ modulo $P$, puis $X^{3p} = X^{2p} \times X^p$ modulo $P$ jusqu'à $X^{(n-1)p}$. On a donc $O(n)$ étapes et à chaque étape on multiplie deux polynômes de degrés plus petit que $n$ suivi d'une division euclidienne, le tout coûtant $O(n^2)$ opérations élémentaires. Au final, on obtient $O(pn + n^3)$, ce à quoi on peut inclure l'algèbre linéaire[5] qui coûte $n^3$. On peut améliorer cela en utilisant une exponentiation rapide qui fournit la matrice[6] en $O(\log(p)n^2 + n^3)$.
Une fois la matrice et un vecteur du noyau obtenu, chaque essai du pgcd coûte[7] $O(n^2)$ et il fait en faire au plus $p$ donc on trouve un facteur non trivial en $O((p + n)n^2)$. Si le polynôme possède $k$ facteurs irréductibles, alors il faut itérer $2k - 1$ fois et on obtient (on peut être plus fins mais ce n'est pas nécessaire) une complexité au pire de $O(k(p + n)n^2))$.

## Exercice II

Soit $P \in \mathbf{F}_p[X]$ sans facteur carré. On s'intéresse dans cet exercice à *la factorisation de $P$ en degrés distincts*. On rappelle que pour tout $d \geqslant 1$, $x^{p^d} - x$ est le produit de tous les polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ dont le degré divise $d$. On appelle alors *factorisation de $P$ en degrés distincts* la suite $(g_1, \ldots, g_s)$ de polynômes $g_i \in \mathbf{F}_p[X]$ où $g_i$ est le produit de tous les polynômes irréductibles unitaires de degré $i$ divisant $P$, avec $g_s \neq 1$.
On propose l'algorithme suivant tant que $P_i \neq 1$ et avec $P_0 = P$ :

(i) On calcule $h_i = x^{p^i} - x$ ;

(ii) On calcule $g_i = \text{pgcd}(h_i, P_{i-1})$ ;

(iii) On pose $P_i = \frac{P_{i-1}}{g_i}$.

**1.** Il est clair que $g_i$ est le produit des polynômes unitaires irréductibles qui divisent $P$ et que $s \leqslant n$ (avec $n$ le degré de $P$) si bien que l'algorithme s'arrête après au plus $n$ étapes et fournit bien la factorisation en degrés distincts.

**4.** Cet algorithme requiert au plus $n$ étapes et chaque étape requiert un calcul de pgcd et une division euclidienne qui coûtent $O(np^i)$ ce qui donne après sommation un $O(np^{n-1})$, ce qui est très mauvais ! Mais en fait on peut remplacer $\text{pgcd}(P_{i-1}, h_i)$ par

$$\text{pgcd}(P_{i-1}, h_i \pmod{P_{i-1}})$$

et calculer $h_i \pmod{P_{i-1}}$ par exponentiation rapide et division euclidienne en $O(i\log(p)n^2)$ à chaque itération ce qui donne une complexité dans le pire des cas en $O(\log(p)n^4)$, ce qui est rapidement meilleur que Berlekamp dès que $p$ est grand. En particulier on passe d'une complexité linéaire en $p$ avec Berlekamp à une complexité logarithmique ici !

4. En effet, le polynôme $Q$ n'est également jamais irréductible modulo $p$ soit en raisonnant avec son groupe de Galois et en traitant les premiers divisant le discriminant à la main.

5. Ce que l'on peut améliorer et pour cela, je vous renvoie à la référence [5] du polycopié.

6. Noter qu'on peut également améliorer la multiplication avec Karatsuba ou la FFT.

7. Là aussi on peut faire mieux en montrant qu'une division ne coûte pas plus cher qu'une multiplication et je vous renvoie pour cela à [5].

On suppose à présent que $p$ un nombre premier impair et on présente un algorithme probabiliste, dit de **Cantor-Zassenhaus** pour factoriser $P$. On rappelle que dans $\mathbf{F}_q$, si on tire $a$ au hasard, $a^{\frac{q-1}{2}}$ vaut 1 ou $-1$ avec probabilité $\frac{1}{2}$. L'idée de l'agorithme est la suivante. Imaginons que $P$ se décompose en produit de facteurs irréductibles **tous de même degré**, disons $d$. On a alors que $P = P_1 \cdots P_r$ avec $dr = n$ et les $P_i$ irréductibles deux à deux non associés. On rappelle qu'on a alors un isomorphisme

$$\mathbf{F}_p[X]/(P) \cong \prod_{i=1}^{r} \mathbf{F}_p[X]/(P_i)$$

où chaque $\mathbf{F}_p[X]/(P_i)$ est isomorphe à $\mathbf{F}_{p^d}$. On propose alors l'algorithme probabiliste suivant. Soit $k$ un nombre d'étape fixé en entrée. Jusqu'à atteindre $k$ étapes ou trouver un facteur irréductible non trivial, on tire $a \in \mathbb{F}_p[X]$ de degré strictement inférieur à celui de $P$ uniformément au hasard. On calcule alors $g_1 = \mathsf{pgcd}(a, P)$. Si $g_1 \neq 1$, on renvoie $g_1$ qui est un facteur non trivial de $P$. Sinon, on calcule $b = a^{\frac{p^d-1}{2}}$ modulo $P$ et on calcule $g_2 = \mathsf{pgcd}(b-1, P)$. Si $g_2 \neq 1$ et $g_2 \neq P$, on retourne $g_2$ et sinon on recommence.

**5.** On échoue à trouver un facteur non trivial à une étape donnée avec une probabilité inférieure à la probabilité que $g_2 = 1$ ou $P$. Or, $g_2 = P$ si, et seulement si, $b \equiv 1 \pmod{P}$, et par théorème chinois si, et seulement si, $b \equiv 1 \pmod{P_i}$ pour tout $i \in \{1, \ldots, r\}$. On a alors $\mathbf{F}_p[X]/(P_i) = \mathbf{F}_{p^d}$ et dans $\mathbf{F}_{p^d}^{\times}$, tout élément $x$ a probabilité $\frac{1}{2}$ de vérifier $x^{\frac{p^d-1}{2}} = 1$ si bien que $g_2 = P$ avec probabilité $\frac{1}{2^r}$ et de même on obtient que $g_2 = 1$ avec probabilité $\frac{1}{2^r}$ (car $g_2 = 1$ si, et seulement si, $b - 1$ est non nul modulo $P_i$ pour tout $i$ soit $b \equiv 1 \pmod{P_i}$ pour tout $i \in \{1, \ldots, r\}$) si bien que $g_2 = 1$ ou $P$ avec probabilité $2^{1-r}$ et en itérant $k$ fois on obtient bien une probabilité d'échec inférieure à $2^{(1-r)k} \leqslant 2^{-k}$ dès que $r \geqslant 2$. On commence donc par utiliser l'algorithme de factorisation en degré distincts et on applique Cantor-Zassenhaus à chaque $g_i$.

**7.** Le problème pour $p = 2$ est que tout élément est un carré et non plus avec probabilité $\frac{1}{2}$ comme dans le cas impair.
SOit $g_i$ de degré $n$. La complexité de Cantor-Zassenhaus appliqué à $g_i$ est donnée par le calcul de deux pgcd en $O(n^2)$ et le calcul de $b$ que l'on peut effectuer en $O(d \log(p) n^2)$ par exponentiation rapide par exemple. Il vient alors une complexité ee $O(kd \log(p) n^2)$ pour trouver un facteur non trivial de $P$ avec probabilité $\leqslant 2^{-k}$. Il reste alors à itérer cela au plus $r$ fois pour obtenir la factorisation de $g_i$ et on obtient une complexité en $O(krd \log(p) n^2) = O(k \log(p) n^3)$. Pour conclure il suffit de sommer ces contributions sur tous les $g_i$ qui sont de degré $\leqslant N = \deg(P)$ ce qui fournit du $O(k \log(p) N^4)$. À nouveau, on bat Berlekamp en terme de dépendance en $p$.