Factorisation des polynômes sur les corps finis

1 L'algorithme de Berlekamp

Soit $K = \mathbb{F}_q$ un corps fini, et soit $P \in K[X]$ un polynôme. On souhaite factoriser P ; l'algorithme de Berlekamp prend P en entrée, et ressort soit P si celui-ci est irréductible, soit un diviseur non trivial de P. Les étapes sont les suivantes :

(1) si $P' = 0$ alors il existe Q tel que $P(X) = Q(X^p)$. Soit R le polynôme dont les coefficients sont les racines des coefficients de Q (bien déterminés car le Frobenius F est un isomorphisme de K), alors $P(X) = (R(X))^p$ et l'algorithme renvoie R et s'arrête.

(2) si $P \wedge P' \neq 1$ alors c'est un facteur non trivial de P donc l'algorithme renvoie $P \wedge P'$ et s'arrête.

(3) sinon, P a ses facteurs irréductibles distincts. Soit $A = K[X]/P$ qui est une K-algèbre de dimension n, et considérons l'endomorphisme de K-ev $F - \mathrm{Id}$. Soit r la dimension de $N = \ker(F - \mathrm{Id})$; on a $r \geq 1$ car $K \subset N$. Si $r = 1$ alors P est irréductible, l'algorithme le dit et s'arrête. Si $r \geq 2$ on prend un élément de $N \setminus K$, classe d'un polynôme $Q \in K[X]$. On décrit alors tous les $\alpha \in K$ et on calcule le pgcd de P et $Q - \alpha$. Un lemme montre que pour un certain α on trouve un truc non trivial, l'algorithme le renvoie et s'arrête.

2 Mise en pratique

Voici une question (hyper classique) posée à l'oral pour la leçon sur les racines des polynômes : factoriser $P = X^9 + X^6 - X + 1$ sur $K = \mathbb{F}_3$.

La première chose à faire est de voir s'il a une racine dans K. C'est vite fait car K n'a que 3 éléments, et on trouve qu'il n'y a pas de racine. Appliquons maintenant l'algorithme :

(1) $P' = -1$.

(2) $P \wedge P' = 1$ car $P' = -1$.

(3) On est donc dans le vif du sujet. L'algèbre qui nous intéresse est
$$A = K[X]/(X^9 + X^6 - X + 1) .$$

C'est un K-ev de dimension 9 dont une base est $\{1, X, X^2, \dots, X^8\}$. Pour calculer la matrice de l'endomorphisme $F - \mathrm{Id}$ on aura besoin des puissances de X^3 jusqu'à X^{24}. Je vais calculer aussi X^{10} et X^{11}, vous verrez tout de suite pourquoi en suivant le calcul :

$$\begin{aligned}
&X^9 = -X^6 + X - 1\\
&X^{10} = -X^7 + X^2 - X\\
&X^{11} = -X^8 + X^3 - X^2\\
&X^{12} = -(-X^6 + X - 1) + X^4 - X^3 = X^6 + X^4 - X^3 - X + 1\\
&X^{15} = (-X^6 + X - 1) + X^7 - X^6 - X^4 + X^3 = X^7 + X^6 - X^4 + X^3 + X - 1\\
&X^{18} = (-X^7 + X^2 - X) + (-X^6 + X - 1) - X^7 + X^6 + X^4 - X^3 = X^7 + X^4 - X^3 + X^2 - 1\\
&X^{21} = (-X^7 + X^2 - X) + X^7 - X^6 + X^5 - X^3 = -X^6 + X^5 - X^3 + X^2 - X\\
&X^{24} = -(-X^6 + X - 1) + X^8 - X^6 + X^5 - X^4 = X^8 + X^5 - X^4 - X + 1
\end{aligned}$$

On peut alors écrire la matrice de $F - \mathrm{Id}$:

$$\begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 & -1 & 1 & -1 & -1 & 0 & 1 \\ 0 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & -1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} & \begin{array}{c} 1 \\ X \\ X^2 \\ X^3 \\ X^4 \\ X^5 \\ X^6 \\ X^7 \\ X^8 \end{array} \end{array}$$

Le noyau contient la droite engendrée par la première colonne ; il faut décider s'il est plus gros. Utilisons le pivot de Gauss ; c'est long mais on trouve le vecteur $(0, 1, -1, -1, 1, 1, -1, 0, 1)$ (par exemple). Un représentant polynôme est

$$Q(X) = X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X$$

On calcule ensuite $P \wedge (Q - \alpha)$. Gardons α général au début, on fera $\alpha = 0$, 1 ou 2 en temps utile. On utilise l'algorithme d'Euclide : la première division est

$$X^9 + X^6 - X + 1 = (X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X - \alpha)X + (X^7 - X^5 + X^4 + X^3 - X^2 + (\alpha - 1)X + 1)$$

La seconde est

$$X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X - \alpha = (X^7 - X^5 + X^4 + X^3 - X^2 + (\alpha - 1)X + 1)X - \alpha(X^2 + 1)$$

C'est gagné car si $\alpha = 0$, on a un reste nul, donc $X^7 - X^5 + X^4 + X^3 - X^2 - X + 1$ divise P :

$$P(X) = (X^7 - X^5 + X^4 + X^3 - X^2 - X + 1)(X^2 + 1)$$

On pourrait imaginer de continuer l'algorithme avec $\alpha \neq 0$, mais on ne trouverait rien d'autre (je ne sais pas si c'est un fait général de l'algorithme de Berlekamp), car on poursuivrait avec $X^2 + 1$ comme reste, or on sait déjà qu'il divise P.

Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{F}_3$. Il faut ensuite recommencer avec le facteur $P_1 = X^7 - X^5 + X^4 + X^3 - X^2 - X + 1$. Avec moins de détail cette fois :

$$\begin{aligned} X^7 &= X^5 - X^4 - X^3 + X^2 + X - 1 \\ X^9 &= -X^6 + X - 1 \\ X^{12} &= X^6 + X^4 - X^3 - X + 1 \\ X^{15} &= X^6 + X^5 + X^4 + X^2 - X + 1 \\ X^{18} &= X^5 + X^3 - X^2 + X + 1 \end{aligned}$$

Matrice de $F - \mathrm{Id}$

$$\begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 & -1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & -1 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} & \begin{array}{c} 1 \\ X \\ X^2 \\ X^3 \\ X^4 \\ X^5 \\ X^6 \end{array} \end{array}$$

Ici on voit très rapidement que le système formé par les six colonnes de droite est de rang maximal, donc la dimension du noyau est 1 et P est irréductible. En conclusion la décomposition en facteurs irréductibles de $X^9 + X^6 - X + 1$ est $(X^7 - X^5 + X^4 + X^3 - X^2 - X + 1)(X^2 + 1)$.

3 Décomposition sur les exemples simples

Dans les cas simples, soit on aura une racine dans le corps de base, soit il y aura suffisamment de facteurs irréductibles de petit degré (i.e. 2 ou 3) qui sont facilement détectables et permettent de conclure. Dans ce cas-là, on “va à la pêche” ce qui nécessite tout de même de la méthode.

Rappelons tout d'abord la remarque utile :

Lemme : *Soit K un corps et $P \in K[X]$ de degré n. Alors P est réductible ssi il est divisible par un polynôme de degré $\leq n/2$.*

D'abord notons qu'il est facile de tester si un polynôme de degré ≤ 3 est irréductible, car cela équivaut à dire qu'il n'a pas de racine. On voit alors, par exhaustion, que sur $\mathbb{F}_3$, les polynômes irréductibles unitaires de degré 2 sont : X^2+1, X^2+X-1, X^2-X-1.

Remarque : comme on est en caractéristique différente de 2, à translation près sur la variable, dans tout polynôme unitaire de degré 2 on peut camoufler le terme en X puisque $X^2+aX = (X+\frac{1}{2}a)^2+\dots$ Par ailleurs il est clair que P est irréductible ssi $P(X+a)$ l'est. Donc partant des polynômes irréductibles de degré 2 et sans terme en X (il n'y en a qu'un : X^2+1), on les trouve tous en susbtituant $X+a$ ($a \in \mathbb{F}_3$) à X. On trouve ainsi X^2+X-1 et X^2-X-1 sans calcul.

Pour trouver les polynômes irréductibles de degré 3 on peut utiliser le fait que X^3-X induit la fonctions nulle sur $\mathbb{F}_3$. Si P est un polynôme irréductible unitaire de degré 3, alors $P-(X^3-X)$ est un polynôme de degré ≤ 2 dont la fonction associée ne s'annulle pas. Il est donc de la forme aQ avec $a \in \mathbb{F}_3^\times$ et Q unitaire sans racine, i.e. égal à 1 ou irréductible de degré 2. En sens inverse, partant de $Q=1$ ou Q de degré 2 unitaire irréductible, le polynôme $P = X^3-X+aQ$ est irréductible unitaire de degré 3. On trouve ainsi :

$$\begin{array}{ll}
X^3-X+1\ , & (X^3-X)+(X^2+X-1) = X^3+X^2-1\ , \\
X^3-X-1\ , & (X^3-X)-(X^2+X-1) = X^3-X^2+X+1\ , \\
 & \\
(X^3-X)+(X^2+1)\ , & (X^3-X)+(X^2-X-1) = X^3+X^2+X-1\ , \\
(X^3-X)-(X^2+1)\ , & (X^3-X)-(X^2-X-1) = X^3-X^2+1\ .
\end{array}$$

Remarque : vérifions que les polynômes trouvés sont en nombre correct à l'aide de la formule

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

On trouve $\operatorname{card} I(2,3) = \frac{1\times 3^2+(-1)\times 3}{2} = 3$ et $\operatorname{card} I(3,3) = \frac{1\times 3^3+(-1)\times 3}{3} = 8$.