Algorithme de Berlekamp

Julie Parreaux

2018-2019

Référence du développement : Objectif agrégation [1, p.244]

Leçons où on présente le développement : 123 (Corps fini) ; 141 (Polynômes irréductibles) ; 151 (Dimension d'un espace vectoriel).

1 Introduction

L'algorithme de Berlekamp, dont la correction repose sur le théorème chinois, est la base de la méthode de factoriser tous polynômes sur un corps fini. Il permet de décomposé en polynômes irréductibles tout polynôme sans facteur carrés à coefficient dans un corps finis. L'idée de cet algorithme est de trouver les éléments invariants par puissance q dans l'algèbre $\mathbb{F}_q[X]/<P>$ ce qui revient à calculer les sous-espace propres d'une certaine application linéaire.

2 L'algorithme de Berlekamp

Soient p un nombre premier, $q = p^s$ et $\mathbb{F}_q$ le corps fini à q éléments. On considère un polynôme $P \in \mathbb{F}_q[X]$ sans facteur carrés : on l'écrit : $P = \prod_{i=1}^{r} P_i$ où les P_i sont des polynômes irréductibles premiers deux à deux. On note $x = (X \mod P)$ dans $\mathbb{F}_q[X]/<P>$ et considérons la base $\mathcal{B} = \{1, x, \dots, x^{deg(P)-1}\}$ de $\mathbb{F}_q[X]/<P>$. L'algorithme de Berlekamp calcule le nombre r de facteurs irréductibles de P et, lorsque $r \geq 2$ donne explicitement les P_i.

Théorème. *Soit $P \in \mathbb{F}_q[X]$ un polynôme dont la décomposition en facteurs irréductibles est sans carrés. On note $x = (X \mod P)$ dans $\mathbb{F}_q[X]/<P>$ et considérons la base $\mathcal{B} = \{1, x, \dots, x^{deg(P)-1}\}$ de $\mathbb{F}_q[X]/<P>$.*

Alors, l'algorithme de Berlekamp (algorithme 1) termine et est correct (c'est-à-dire donne la décomposition en facteur irréductible de P)

Schéma du développement

1. Montrer la correction.
   (a) Montrer que l'application S_P est linéaire (lemme 1) (via la puissance).
   (b) Montrer que le nombre de polynômes irréductibles vaut $\dim \ker (S_P - Id)$ (lemme 2).
   (c) Montrer la décomposition de P sur $\mathbb{F}_q$ (lemme 3).
      i. Montrer que pour tout $i \in [\![1, r]\!]$, il existe $V \in \mathbb{F}_q[X]$ non constant et $\alpha_i \in \mathbb{F}_q$ tel que $\alpha_i = (V \mod P_i)$.
      ii. Pour tout $\alpha \in \mathbb{F}_q$, montrons que $\gcd(P, V - \alpha) = \prod_{i,\alpha_i=\alpha} P_i$.
      iii. Montrer que $P = \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V - \alpha)$.
   (d) Montrer que les facteurs de décompositions sont bien propres (lemme 4).
2. Montrer la terminaison.

Algorithm 1 Algorithme de Berlekamp

1: On considère l'application linéaire S_P définie telle que :

$$\begin{array}{rccc} S_P : & \mathbb{F}_q[X]/\langle P\rangle & \to & \mathbb{F}_q[X]/\langle P\rangle \\ & Q(X) \mod P & \mapsto & Q(X^q) \mod P \end{array}$$

On calcul la matrice $S_P - Id$ dans $\mathcal{B}$.

2: Le nombre de facteur irréductibles de P est

$$r = \dim(\ker(S_P - Id)) = \deg(P) - \operatorname{rg}(S_P - Id)$$

On calcul r avec un pivot de Gauss.

3: **if** $r = 1$ **then**

4: P est irréductible et on a fini.

5: **else**

6: On choisi V non constant de $\mathbb{F}_q[X]/\langle P\rangle$ tel que $V \in \ker(S_P - Id)$.

7: Calcul de $\gcd(P, V - \alpha)$, où $\alpha \in \mathbb{F}_q$ à l'aide de l'algorithme d'Euclide. On a alors

$$P = \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V - \alpha)$$

.

8: On applique l'algorithme (à partir de 1) aux facteurs non triviaux de ce produit s'ils existent.

9: **end if**

Démonstration. Soit $P \in \mathbb{F}_q[X]$ un polynôme dont la décomposition en facteurs irréductibles est sans carrés. On note $x = (X \mod P)$ dans $\mathbb{F}_q[X]/<P>$ et considérons la base $\mathcal{B} = \{1, x, \ldots, x^{deg(P)-1}\}$ de $\mathbb{F}_q[X]/<P>$. Montrons que l'algorithme de Berlekamp (algorithme 1) termine et est correct.

Étape 1 : preuve de la correction La preuve de la correction de l'algorithme se fait par induction sur les facteurs irréductibles (on a un algorithme récursif). Avant de commencer l'induction, on va monter deux lemmes qui montre la correction des deux premières étapes de notre algorithme (algorithme 1). On va alors s'appuyer sur deux lemmes permettant de montrer que les deux premières étapes de l'algorithme sont correctes. L'induction intervient pour montrer la correction de la boucle IF.

Lemme 1. *L'application S_P est bien définie, linéaire.*

Démonstration. D'après la proposition universelle des polynômes,

$$\begin{array}{rccc} \delta_1 : & \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ & Q(X) & \mapsto & Q(X^q) \end{array}$$

est l'unique morphisme tel que $\delta_1(a) = a$ pour tout $a \in \mathbb{F}_q$ et $\delta_1(X) = X^q$. De plus, on remarque que pour tout $Q \in \mathbb{F}_q[X]$,

$$\delta_1(Q) \underbrace{=}_{\text{définition}} Q(X^q) \underbrace{=}_{\forall a \in \mathbb{F}_q, a^q = a} Q^q$$

Soient $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/<P>$ la surjection cannonique et $\delta = \pi \circ \delta_1$. Comme π est un morphisme d'anneaux (à monter), on a

$$\delta(P) \underbrace{=}_{\text{définition}} \pi(\delta_1(P)) \underbrace{=}_{\text{Remarque précédente}} \pi(P^q) \underbrace{=}_{\pi \text{ morphisme}} \pi(P)^q \underbrace{=}_{P \mod P=0} 0$$

Le théorème de l'anneau quotient implique alors que δ passe au quotient par $<P>$ pour donner S_P, elle est donc bien définie.

Montrons maintenant que S_P correspond à l'élévation à la puissance q :

$$\begin{array}{rcll} S_P\left(Q \mod P\right) & = & S_P(\pi(Q)) & \text{(Définition de } \pi\text{)} \\ & = & \pi\left(Q\left(X^q\right)\right) & \left(\pi(Q) = Q \mod P\right) \\ & = & \pi\left(Q^q\right) & \left(a^q = a, \forall a \in \mathbb{F}_q\right) \\ & = & \pi\left(Q\right)^q & \text{(π est un morphisme d'anneau)} \\ & = & Q^q \mod P & \text{(Définition de } \pi\text{)} \end{array}$$

Comme l'élévation à la puissance est linéaire, on obtient le résultat. □

Remarque : La preuve de ce lemme est analogue à la preuve qui permet de montrer que le morphisme de Frobenius est linéaire.

Lemme 2. *Soit $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréductibles et premiers deux-à-deux, r est alors le nombre de polynômes irréductibles de P. Alors, $r = \dim\left(\ker\left(S_P - Id\right)\right)$.*

Démonstration. Comme les P_i sont irréductibles, les $\mathbb{F}_q-$espaces vectoriels de dimension fini $K_i = \mathbb{F}_q[X]/<P_i>$ sont des corps de caractéristique p et de cardinal $p^{\deg(P_i)}$. De plus, les P_i sont deux-à-deux premiers entre eux, on peut donc appliquer le théorème chinois : il existe φ un isomorphisme de $\mathbb{F}_q-$algèbre :

$$\begin{array}{rccc} \varphi: & \mathbb{F}_q[X]/<P> & \to & K_1 \times \cdots \times K_r \\ & Q \mod P & \mapsto & \left(Q \mod P_1, \ldots, Q \mod P_r\right) \end{array}$$

Dans la suite si $Q \in \mathbb{F}_q[X]/<P>$, on notera $Q_i = Q \mod P$.

On pose $\tilde{S_P} = \varphi \circ S_P \circ \varphi^{-1} : K_1 \times \cdots \times K_r \to K_1 \times \cdots \times K_r$ correspondant à l'élévation à la puissance q dans l'anneau produit $K_1 \times \cdots \times K_r$. En effet, soit $Q \in \mathbb{F}_q[X]/ < P >$,

$$\begin{array}{rcll} \tilde{S_P}(Q_1, \ldots, Q_r) & = & \varphi \circ S_P \circ \varphi^{-1}(Q_1, \ldots, Q_r) & \text{(Définition de } \tilde{S_P}\text{)} \\ & = & \varphi \circ S_P(Q) & \text{(Définition de } \varphi \text{ qui est un isomorphisme)} \\ & = & \varphi\left(Q^q\right) & \text{(comme dans le lemme 1)} \\ & = & \left(Q_1^q, \ldots, Q_r^q\right) & \text{(Définition de } \varphi\text{)} \end{array}$$

Ainsi,

$$\begin{array}{rcll} (Q_1, \ldots, Q_r) \in \ker\left(\tilde{S_P} - Id\right) & \Leftrightarrow & \left(Q_1^q, \ldots, Q_r^q\right) = (Q_1, \ldots, Q_r) & \text{(Définition de ker } \left(\tilde{S_P} - Id\right)\text{)} \\ & \Leftrightarrow & \forall i \in [\![1, r]\!], Q_i^q - Q_i = 0 \mod P_i & \left(Q_i \in K_i \text{ et } S_P \in \mathbb{F}_q[X]/<P>\right) \\ & \Leftrightarrow & \forall i \in [\![1, r]\!], Q_i^q = Q_i \text{ dans } K_i & \text{(Définition de } K_i\text{)} \end{array}$$

Comme $\forall i \in [\![1, i]\!]$, K_i est une extension de corps de $\mathbb{F}_q$ ($\mathbb{F}_q \hookrightarrow K_i$) : l'image de $\mathbb{F}_q$ dans K_i est l'ensemble des éléments de K_i vérifiant $x^q = x$. En effet, si $x \in \mathbb{F}_q^{\times}$, le théorème de Lagrange sur $\mathbb{F}_q$ nous assure que $x^{q-1} = 1$, soit en multipliant par x, on obtient $x^q = x$. De plus, 0 vérifie l'équation. Donc $\mathbb{F}_q \subset \{x | x^q = x, x \in K_i\}$. Réciproquement, on remarque que le polyne $X^q - X \in K_i[X]$ admet au plus q racines ($\deg = q$ et K_i est un corps) et on a déjà q racines (les éléments de $\mathbb{F}_q$ sont racines). Donc il n'existe pas d'autre racines dans $K_i \setminus \mathbb{F}_q$. On en déduit que l'image de $\mathbb{F}_q$ dans K_i est l'ensemble des éléments de K_i vérifiant $x^q = x$.

On en déduit donc que

$$(Q_1, \ldots, Q_r) \in \ker\left(\tilde{S_P} - Id\right) \Leftrightarrow \forall i \in [\![i, r]\!], x_i \in \mathbb{F}_q \hookrightarrow K_i$$

et donc $\ker\left(\tilde{S_P} - Id\right) = \left(\mathbb{F}_q\right)^r$. Or $\ker\left(\tilde{S_P} - Id\right) = \varphi\left(\ker\left(S_P - Id\right)\right) = \left(\mathbb{F}_q\right)^r$. Comme φ est un isomorphisme de $\mathbb{F}_q-$espaces vectoriels, on en conclut que

$$\dim_{\mathbb{F}_q}\left(\ker\left(S_P - Id\right)\right) = \dim_{\mathbb{F}_q}\left(\mathbb{F}_q^r\right) = r$$

□

Lemme 3. *Soit $P = \prod_{i=1}^{r} P_i$ tel que les P_i sont irréductibles et premiers deux-à-deux et $r > 1$. Montrons que $P = \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V - \alpha)$.*

Remarque : L'ensemble des $U \mod P$ tels que U est constant modulo P est la droite vectoriel de $\mathbb{F}_q[X]/<P>$.

Démonstration. Soit $P = \prod_{i=1}^{r} P_i$ tel que les P_i sont irréductibles et premiers deux-à-deux et $r > 1$.

Étape 1 : montrons que pour tout $i \in [\![1,r]\!]$, il existe $V \in \mathbb{F}_q[X]$ non constant et $\alpha_i \in \mathbb{F}_q$ tel que $\alpha_i = (V \mod P_i)$. Comme $r > 1$, par le lemme 2, on a $r = \dim_{\mathbb{F}_q}(\ker(S_P - Id)) > 1$. Donc, il existe (voir la remarque précédente) $V \in \mathbb{F}_q[X]$ non contant tel que $(V \mod P) \in \ker(S_P - Id)$. Or, comme φ est un isomorphisme, on a (par le lemme 2) :

$$(V \mod P) \in \ker(S_P - Id) \Leftrightarrow (V \mod P_1, \dots, V \mod P_r) \in \mathbb{F}_q^r$$

Autrement dit,

$$\forall i \in [\![1,i]\!], \alpha_i = (V \mod P_i) \in F_q \subset K_i$$

Etape b : pour tout $\alpha \in \mathbb{F}_q$, montrons que $\gcd(P, V-\alpha) = \prod_{i,\alpha_i=\alpha} P_i$. Soit $\alpha \in \mathbb{F}_q$. Comme $\gcd(P, V-\alpha)$ divise P et que les P_i sont irréductible, alors il existe $I_\alpha \subset [\![1,r]\!]$ tel que $\gcd(P, V-\alpha) = \prod_{i \in I_\alpha} P_i$. Or les P_i sont premiers deux à deux, donc par le lemme de Gauss, $I_\alpha = \{i \in [\![1,r]\!], P_i | V-\alpha\}$.

On remarque que pour tout $i \in llbracket 1, r]\!]$:

$$\alpha_i = \alpha \underbrace{\Leftrightarrow}_{\substack{V-\alpha = V-\alpha_i = 0 \mod P_i \\ \text{(hypothèse)}}} V - \alpha = 0 \mod P_i \underbrace{\Leftrightarrow}_{\text{Définition du modulo}} P_i | (V-\alpha)$$

Donc par ce qui précède, $I_\alpha = \{i | \alpha = \alpha_i\}$. Donc, $\gcd(P, V-\alpha) = \prod_{i,\alpha_i=\alpha} P_i$.

Étape c : montrons que $P = \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V-\alpha)$. On a

$$P = \prod_{i=1}^{r} P_i \underbrace{=}_{\substack{\alpha_i = \alpha \wedge \alpha_i = \beta \Rightarrow \alpha = \beta \\ V \mod P_i \in \mathbb{F}_q}} \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\{i, \alpha = \alpha_i\}} P_i \right) \underbrace{=}_{\text{précédent}} \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V-\alpha)$$

D'où le résultat. □

Lemme 4. *Soit $P = \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V-\alpha)$ avec V choisi comme dans le lemme 3, alors il existe $\alpha \in \mathbb{F}_q$ tel que $\gcd(P, V-\alpha)$ soit un facteur strict de P.*

Démonstration. Le choix de V nous assure qu'il existe $(i,j) \in [\![1,r]\!]^2$ tel que $\alpha_i \neq \alpha_j$. En effet, sinon, $\forall i \in [\![1,r]\!], \alpha_i = \alpha \in \mathbb{F}_q$ et

$$\begin{aligned} \forall i,\ P_i | V-\alpha &\Rightarrow \prod_{i=1}^{r} P_i | V-\alpha && \text{(Les } P_i \text{ sont premiers deux à deux)} \\ &\Rightarrow V = \alpha = cst \mod P && \text{(Définition du modulo)} \end{aligned}$$

Contradiction car V serait constant modulo P.

On en déduit que $P_i | \gcd(P, V-\alpha_i)$ donc $\deg(\gcd(P, V-\alpha_i)) > 0$. De même $P_j \nmid \gcd(P, V-\alpha_i)$ donc $\deg(\gcd(P, V-\alpha_i)) < \deg(P)$. Donc $\gcd(P, V-\alpha_i)$ est un facteur strict de la décomposition de P. □

Montrons maintenant la correction de l'algorithme. Pour cela, nous allons raisonner par induction sur la décomposition en facteur irréductible de P. Nous allons donc raisonner par récurrence sur r. Montrons pour tout $r \in \mathbb{N}^*$ la propriété $\mathcal{P}_r$: " Si $P = \prod_{i=1}^{r} P_i$ avec les P_i irréductible et deux à deux distincts, alors l'algorithme de Berlekamp (algorithme 1) renvoie la décomposition de P en facteur irréductible soit $\prod_{i=1}^{r} P_i$."

Cas $r = 1$ Si $r = 1$ alors le nombre de polynôme irréductible de P est 1, donc P est irréductible et l'algorithme est correct.

Cas $\mathcal{P}_r$ Soit r tel que pour tout $1 \leq i \leq r-1$ la propriété $\mathcal{P}_i$ soit vérifiée Montrons la propriété dans le cas r. Soit $p = \prod_{i=1}^{r} P_i$ Par les lemmes 1 et 2, l'algorithme de Berlekamp calcul un r correct. En particulier $r > 1$, on applique donc le lemme3 qui nous assure que $\prod_{\alpha \in \mathbb{F}_q} \gcd(P, V-\alpha)$. Par le lemme 4, il existe $\alpha \in \mathbb{F}_q$ tel que $\gcd(P, V-\alpha)$ soit un facteur strict de P. Comme $\gcd(P, V-\alpha)$ divise P, il est sans facteur carré et possède moins de facteurs irréductibles. De plus comme p est sans facteur carré, $\forall \alpha \in \mathbb{F}_q$, $\gcd(P, V-\alpha)$ possède moins de facteurs irréductibles (sinon, contradiction avec l'hypothèse sur les facteurs carrés). Donc, on peut appliquer l'algorithme de Berlekamp à $\gcd(P, V-\alpha)$, pour tout $\alpha \in \mathbb{F}_q$. De plus, par hypothèse de récurrence, l'algorithme de Berlekamp est correct sur ces polynôme d'où la correction pour P. Donc $\mathcal{P}_r$ est vraie.

On a alors monter la correction de cet algorithme.

Preuve de la terminaison Pour montrer que l'algorithme termine, il faut montrer que r, le nombre de polynômes irréductibles de l'entrée décrois strictement (ils forment un ordre bien formé). Par le lemme 4, on a l'existence de $\alpha \in \mathbb{F}_q$ tel que $\gcd(P, V - \alpha)$ soit un facteur strict dans la décomposition de P, donc il possède moins de facteur irréductible. De plus, F est sans facteurs carrés, donc pour tout $\alpha \in \mathbb{F}_q$, $\gcd(P, V - \alpha)$ est soit un facteur stricte de la décomposition de P soit une constante. Comme on applique l'algorithme àgcd $(P, V - \alpha)$, pour tout $\alpha \in \mathbb{F}_q$, alors r décrois strictement à chaque itération. D'où la terminaison. □

3 Compléments autours de cet algorithme

Complexité de l'algorithme de Berlekamp

En pratique, l'algorithme de Berlekamp nécessite le calcul de pgcd (via l'algorithme d'Euclide) et de rang de matrice (via le pivot de Gauss). On a alors, la complexité du pivot de Gauss en $O\left(\deg(P)^3\right)$ puisque la taille de la matrice de $S_P - Id$ dans la base $\mathcal{B}$ est de $\deg(P)$. De plus, on effectue q calcul de pgcd dans l'algorithme de d'Euclide car on a $\deg(P)$ étapes de calcul de l'algorithme d'Euclide et une division par x en $\deg(P)$. On en déduit que la factorisation de P se fait en $O\left(q \deg(P)^2\right)$. Donc un appel de l'algorithme de Berlekamp se fait en $O\left(\deg(P)^3 + q \deg(P)^2\right)$.

Application pratique de cet algorithme [1, p.248]

Une application première de cet algorithme est la factorisation des polynômes sur un corps finis. On donne ici un algorithme basé sur l'algorithme de Berlekamp permettant de réaliser cette factorisation (algorithme 2). Comme, on ne peut pas appliquer l'algorithme de Berlekamp à un polynôme à facteur multiples, il nous faut un test pour savoir comment appliqué cet algorithme. Un outil intéressant dans ce cas est le polynôme dérivée car on détecte les facteurs multiple dans P en calculant $\gcd(P, P')$ (car les facteurs multiples restent lors de la dérivation).

Algorithm 2 Algorithme factorisant les polynômes dans un corps fini k de caractéristique q.

if P constant **then**
    On a fini
else
    On calcul $\gcd(P, P')$
    if $\gcd(P, P') = 1$ **then**
        On applique Berlekamp (algorithme 1) à P.
    else
        if $\gcd(P, P') = P$ **then**
            On calcul R tel que $R^q = P$.
            On s'appelle récursivement sur R
        else
            $P_1 = \gcd(P, P')$ et $P_2 = \frac{P}{\gcd(P, P')}$ sont deux facteurs non triviaux de P.
            On s'appelle alors récursivement sur P_1 et P_2.
        end if
    end if
end if

Quelques résultats sur les anneaux nécessaires à la démonstration.

Nous allons rappeler les résultats majeurs pour l'études des anneaux commutatifs [1, p.236] (comme la construction de morphismes d'anneaux, les propriétés de divisibilités, les anneaux euclidiens, ...).

Morphismes d'anneaux Nous commençons par donner quelques énoncés permettant de construire des morphismes d'anneaux.

Proposition (Propriété universelle de $\mathbb{Z}$)**.** *Soit A un anneau unitaire (non nécessairement commutatif) ; il existe un unique morphisme d'anneau unitaires de $\mathbb{Z}$ dans A. Ce morphisme φ est donné par :*

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & A \\ & n & \mapsto & n1_A \end{array}$$

Ce résultat permet de définir la caractéristique d'un anneau unitaire : c'est l'unique entier $n \in \mathbb{N}$ tel que $\ker \phi = n\mathbb{Z}$. Nous allons maintenant étudier les morphismes issues de quotient.

Théorème (Anneau quotient)**.** *Soient A un anneau commutatif unitaire et I un idéal de A. Il existe sur A/I une unique structure d'anneau (unitaire) qui fasse de π un morphisme d'anneaux (unitaires).*

Par ailleurs, pour tout anneaux B et tout morphisme d'anneaux $\varphi : A \to B$ tel que $\phi(I) = \{0\}$ ($I \subset \ker \phi$), il existe un unique morphisme d'anneaux $\tilde{\varphi} : A/I \to B$ tel que $\varphi = \tilde{\varphi} \circ \pi$. Ajoutons que $Im\tilde{\varphi} = Im\varphi$ et $\ker \tilde{\varphi} = (\ker \varphi)/I$. En particulier, si $I = \ker \varphi$ alors $\tilde{\varphi}$ réalise un isomorphisme entre A/I et $Im\varphi$.

Remarque : L'anneau B (contrairement à l'anneau A) n'est pas supposé commutatif.

Pour construire un morphisme d'anneaux issu d'un anneau quotient A/I, il suffit de "faire passer au quotient" un morphisme ϕ issue de A vérifiant $\phi(I) = \{0\}$. Définissons maintenant des morphismes d'anneaux sur les anneaux de polynômes.

Théorème (Propriété universelle des polynômes)**.** *Soient A et B deux anneaux commutatifs, $\varphi : A \to B$ un morphisme d'anneaux et $i : A \to A[X_1, \ldots, X_n]$ l'inclusion canonique. Pour tout $(b_1, \ldots, b_n) \in B^n$, il existe un unique morphisme d'anneau $\phi : A[X_1, \ldots, X_n]$ vérifiant les propriétés suivantes :*

— *$\phi(i(a)) = \varphi(a)$ pour tout $a \in A$, c'est-à-dire $\phi \circ i = \varphi$;*

— *$\phi(X_j) = b_j$, pour tout $j \in [\![1, n]\!]$.*

Remarque : Le cas où B n'est pas commutatif est plus délicat mais le résultat (du moins son esprit) reste vrai.

Pour construire un morphisme d'anneaux issu d'anneau de polynômes, il suffit de le définir sur l'anneau sous-jacent et ses indéterminées.

Anneaux euclidien Nous allons donner la définition des anneaux euclidien ainsi que quelques exemples de tels anneaux.

Définition (Anneau euclidien)**.** Un anneau A est dit euclidien si A est intègre, et s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ vérifiant

$$\forall (a, b) \in A \times A \setminus \{0\}, \exists q, r \in A, a = bq + r \text{ et } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

L'application ϕ s'appelle un stathme euclidien.

Les anneaux $k[X]$ où k est un corps muni de l'application degré et $\mathbb{Z}$ muni de la valeur absolue sont des anneaux euclidien. Il est également important de noté que les anneaux euclidiens sont des anneaux principaux (mais la réciproque est fausse). Cependant les anneaux euclidien apporte des algorithmes (par exemple pour les coefficients de Bézout), le calcul explicite de ces notions, qui n'existe pas dans les anneaux principaux.

Divisibilité Soit A un anneau commutatif. Pour $a \in A$, on associe l'idéal principal $I = <a>$. Notons qu'un idéal principal à quant-à-lui plusieurs générateurs, il nous faut alors en choisir un ce qui revient à choisir les représentant des classes d'équivalence pour a relation de divisibilité.

Définition (Éléments premiers et irréductibles)**.** Soit A un anneau commutatif ; un élément $a \in A \setminus \{0\}$ est dit *premier* s'il vérifié l'une des deux propositions équivalentes suivantes :

— $a \notin A^\times$ et si pour $b, c \in A$, on a $a|bc$, alors $a|b$ ou $a|c$;

— l'idéal $<a>$ est un idéal premier.

Un élément $a \in A \setminus \{0\}$ est dit *irréductible* s'il vérifié l'une des deux propositions équivalente suivantes :

— $a \notin A^\times$ et si pour $b, c \in A$, on a $a = bc$, alors $a \in A^\times$ ou $a \in A^\times$;

— l'idéal $<a>$ est maximal parmi les idéaux principaux de A distincts de $A/$.

Les nuances de ces définitions dépendent de l'anneau que l'on considère.

Si l'anneau est intègre Un élément premier est nécessairement irréductible.

Si l'anneau est factoriel Un anneau factoriel est intègre, donc par la remarque précédente, on a qu'un élément premier est irréductible. Cette notion donne une caractérisation des anneaux factoriels par ces éléments premiers et irréductibles.

Définition (Anneau factoriel)**.** Un anneau A est factoriel si et seulement si A est intègre, tout éléments de A se décompose en produit d'éléments irréductibles dans A et tout élément irréductibles dans A est aussi premier dans A.

Si l'anneau est principal Les éléments irréductibles et premiers coïncident. C'est la première étape pour montrer que les anneaux principaux sont factoriels.

Lorsque l'anneau que l'on étudie est factoriel, on sait que ces éléments admettent une décomposition en éléments irréductibles. La question naturelle est alors comment calculer cette décomposition : cette action est appelée factorisation.

Théorème chinois

Le théorème chinois est un résultat fondamental dans l'étude de système de congruence [1, p.241]. Il possède de multiples applications notamment en cryptographie avec RSA ou pour l'algorithme de Berlekamp.

Soient A un anneau commutatif et unitaire et I, J deux idéaux de A. On note $\pi_I : A \to A/I$ et $\pi_J : A \to A/J$ les surjections canoniques. Comme π_I et π_J sont des morphismes d'anneaux unitaires, l'application : $\begin{array}{rccc} \varphi : & A & \to & A/I \times A/J \\ & x & \mapsto & \big(\pi_I(x), \pi_J(x)\big) \end{array}$ est un morphisme d'anneaux unitaires. Comme

$$\varphi(x) = 0 \Leftrightarrow \big(\pi_I(x) = 0 \text{ et } \pi_J(x) = 0\big) \Leftrightarrow x \in I \cap J$$

le noyau de φ est alors $I \cap J$. Le théorème chinois assure que φ est surjectif lorsque les idéaux I et J sont étrangers, c'est-à-dire s'ils vérifient $I + J = \langle 1_A \rangle = A$.

Théorème (Théorème chinois)**.** *Soient A un anneau commutatif unitaire et I, J deux idéaux étrangers de A. Alors l'application φ définie précédemment est un morphisme surjectif unitaire d'anneaux (et de $A-$modules). De plus, son noyau est* $\ker \varphi = I \cap J = IJ$.

En passant au quotient, on obtient l'isomorphisme d'anneaux unitaires (et de $A-$modules) :

$\begin{array}{rccc} \tilde{\varphi} : & A/IJ & \to & A/I \times A/J \\ & y = \pi_{IJ}(x) & \mapsto & \big(\pi_I(x), \pi_J(x)\big) \end{array}$ *où π_{IJ} est la surjection canonique.*

Remarque : Le théorème s'étend à un nombre fini d'idéaux

Une spécialisation essentielle de ce théorème est son application au cas particulier des anneaux $\mathbb{Z}/n\mathbb{Z}$ dont nous allons rappeler l'énoncer et la preuve (sans être conséquence du précédent théorème).

Théorème (Théorème chinois [3, p.31])**.** *Soient n et m deux entiers naturels non nuls premiers entre eux. Les anneaux $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ et $(\mathbb{Z}/nm\mathbb{Z})$ sont isomorphes.*

Démonstration. On considère l'application $f : \mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ définie telle que $f(x) = (\dot{x}, \overline{x})$. C'est un morphisme d'anneaux, de noyau $\ker f = \{x \in \mathbb{Z}, m|x \text{ et } n|x\}$. Comme $m \wedge n = 1$, on a aussi $\ker f = \{x \in \mathbb{Z}, mn|x\} = mn\mathbb{Z}$. Donc $f(\mathbb{Z})$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes. En particulier, $Card\,(f(\mathbb{Z})) = Card\,(\mathbb{Z}/mn\mathbb{Z}) = mn$ et donc $f(\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. D'où le résultat. □

Remarque : En raisonnant par récurrence, nous pouvons étendre ce résultat à un nombre fini d'entier deux à deux premiers entre eux. Par le théorème fondamental de l'arithmétique, on en déduit que $\mathbb{Z}/n\mathbb{Z}$ peut être décomposé en un produit de $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Remarque : L'isomorphisme de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est donné par $f(k \mod mn) = (k \mod n, k \mod m)$. L'application réciproque peut être calculer en utilisant une relation de Bézout entre m et n.

Algorithmes en jeux ici.

Dans ce développement, nous utilisons deux algorithmes important : l'algorithme d'Euclide (algorithme 3) qui nous permet d'obtenir le pgcd entre deux polynôme et le pivot de Gauss (algorithme 4) qui nous donne le rang d'une matrice.

Algorithm 3 Algorithme d'Euclide permettant de calculer le pgcd deux éléments d'un anneau euclidien.

function (Euclide)(a, b) avec $a > b$ et a, b non nuls
    $r \leftarrow a \mod b$
    while $r \neq 0$ **do**
        $a \leftarrow b$
        $b \leftarrow r$
        $r \leftarrow a \mod b$
    end while
    Renvoie b
end function

La méthode du pivot de Gauss permet d'obtenir des résultats sur des matrices en répétant plusieurs fois une opération simple (on voit apparaître le côté algorithmique) [2, p.205]. Cette méthode permet de répondre à quelques questions ou problèmes sur les matrices comme :

1. Un élément de $\mathcal{M}_n(K)$ est-il dans $GL_n(K)$? (Trouver une matrice triangulaire équivalente à la matrice de départ et vérifier la présence de coefficients nuls sur la diagonale.)
2. Quel est le rang d'une matrice de $\mathcal{M}_n(K)$? (Trouver une matrice diagonale équivalente à la matrice de départ dont on compte le nombre de coefficients non nuls.)
3. Calcul d'une matrice inversible de $GL_n(K)$. (Appliquer les transformations pour trouver l'identité de la matrice de départ à l'identité.)
4. Résoudre un système linéaire. (Mettre le système sous forme triangulaire.)
5. Trouver les générateurs de $GL_n(K)$.

Définitions et notations Soit $M \in \mathcal{M}_n(K)$, on note L_i sa $i^{\text{ième}}$ ligne et C_j sa $j^{\text{ième}}$ colonne. On note $E_{i,j}(n)$ la matrice élémentaire dont le seul coefficient non nul, 1, est à la $i^{\text{ième}}$ ligne et $j^{\text{ième}}$ colonne.

Définition. On appelle matrice de transvection de $\mathcal{M}_n(K)$ toute matrice de la forme $I_n + \lambda E_{i,j}(n)$ où $\lambda \in K$ et $i \neq j$. On la notera $T_{i,j}(\lambda, n)$.

Remarque : La matrice $T_{i,j}(\lambda, n)$ est inversible d'inverse $T_{i,j}(-\lambda, n)$.

Définition. On appelle matrice de dilation de $\mathcal{M}_n(K)$ toute matrice de la forme $I_n + (\lambda - 1)E_{j,j}(n)$ où $\lambda \in K^\times$. On la notera $D_j(\lambda, n)$.

Remarque : La matrice $D_j(\lambda, n)$ est inversible d'inverse $D_j(\frac{1}{\lambda}, n)$.

Définition. On appelle matrice de permutation de $\mathcal{M}_n(K)$ toute matrice $P = (p_{i,j})_{1 \leq i,j \leq n}$ tel qu'il existe un élément $\sigma \in \mathfrak{S}_n$ tel que $\forall 1 \leq i, j \leq n$, $p_{i,j} = \delta_{i,\sigma(j)}$ où $\delta_{i,j}$ est nul si $i \neq j$ et vaut 1 sinon.

Remarque : La matrice $P(\sigma, n)$ est inversible d'inverse $P(\sigma^{-1}, n) = {}^t P(\sigma, n)$.

La méthode de Gauss pour les coefficients dans un corps Soit $M \in \mathcal{M}_{p,n}(K)$. Commençons par donner une intuition de l'action de ces matrices sur une matrice par la multiplication à gauche ou à droite.

— Multiplier à gauche (respectivement à droite) la matrice M par $T_{i,i'}(\lambda, p)$ (respectivement par $T_{j,j}(\lambda, n)$) revient à ajouter à la ligne $L_i(M)$ (respectivement à la colonne $C_{j'}(M)$) λ fois la ligne $L_{i'}(M)$ (respectivement à la colonne $C_j(M)$).

— Multiplier à gauche (respectivement à droite) la matrice M par $D_i(\mu, p)$ (respectivement par $D_j(\mu, n)$) revient à multiplier la ligne $L_i(M)$ (respectivement à la colonne $C_{j'}(M)$) par μ.

— Multiplier à gauche (respectivement à droite) la matrice M par $P(\sigma, p)$ (respectivement par $P(\sigma, n)$) revient à échanger les lignes (respectivement les colonnes) des M.

Comme on peut toujours se ramener à une matrice carrée en rajoutant des lignes (ou des colonnes) qui manquent, on considère $M \in \mathcal{M}_n(K)$. Énonçons le principe de cet algorithme.

1. Mettre M sous forme triangulaire supérieure : on utilise les permutations et le transvections des lignes. Cette étape consiste à nettoyer tous les coefficients inférieurs au coefficient diagonal (la permutation permet d'obtenir le triangle).
2. Mettre une matrice triangulaire supérieure sous forme diagonale : permutation et transvections des colonnes. Cette étape nous permet alors de nettoyer les coefficients à droite des coefficients diagonaux.
3. Obtenir l'identité d'une matrice diagonale (si c'est possible : $M \in GL_n(K)$: dilatation des coefficients.

L'algorithme 4 met en place cet algorithme : il cherche les forme échelonnée réduite de matrice. Pour chacun des coefficients, il traite les trois étapes en même temps. Sa complexité est en $O(n^3)$.

Proposition. *1. Le groupe $SL_n(K)$ est engendré par les matrices de transvections. Le groupe $GL_n(K)$ est engendré par les transvections et les dilatations.*

2. Si $A \in GL_n(K)$, il existe un unique élément $M \in SL_n(K)$ et un unique élément $\mu \in K^\times$ tel que $A = MD_n(\mu)$. L'élément μ est le déterminant de la matrice A.

Démonstration. 1. D'après la décomposition obtenu par l'algorithme de Gauss, si $\det A = 1$, alors la matrice obtenue sans les dilatations est déjà I_n. Comme on l'obtient uniquement en multipliant des matrices de transvection ou leur inverse (qui est aussi une matrice de transvection), on en déduit le système de générateurs.
La troisième étape de la décomposition consiste à rajouter des dilatations : d'où le résultat.

2. Reformulation classique de la méthode de Gauss dans la troisième étape.

□

Algorithm 4 Algorithme de Gauss–Jordan (ou pivot de Gauss).

```
1:  function (Gauss-Jordan)
2:      r ← 0                                   ▷ (r est l'indice de ligne du dernier pivot trouvé)
3:      for j = 1 à m do                        ▷ (j décrit tous les indices de colonnes)
4:          Rechercher k = max(|A[i,j]|, r+1 ≤ i ≤ n)        ▷ (A[k,j] est le pivot)
5:          if A[k,j] ≠ 0 then                  ▷ (A[k,j] désigne la valeur de la ligne k et de la colonne j)
6:              r ← r + 1                       ▷ (r désigne l'indice de la future ligne servant de pivot)
7:              Diviser la ligne k par A[k,j]   ▷ (On normalise la ligne de pivot de façon que le pivot
    prenne la valeur 1)
8:              Échanger les lignes k et r      ▷ (On place la ligne du pivot en position r)
9:              for i = 1 à n do                ▷ (On simplifie les autres lignes)
10:                 if i ≠ r then
11:                     Soustraire à la ligne i la ligne r multipliée par A[i,j]   ▷ (de façon à annuler A[i,j])
12:                 end if
13:             end for
14:         end if
15:     end for
16: end function
```

Pivot de Gauss pour les matrices à coefficients dans $\mathbb{Z}$ Le pivot de Gauss peut s'étendre aux matrices de $\mathcal{M}_{m,n}(\mathbb{Z})$ et nous permet de connaître les générateurs de $GL_n(\mathbb{Z})$ (qui est l'ensemble des matrices de coefficients dans $\mathbb{Z}$ dont le déterminant vaut -1 ou 1) et de classifier (à équivalence près) les matrices de $\mathcal{M}_{m,n}(\mathbb{Z})$. Comme nous ne sommes plus dans un corps, il nous faut faire attention à la division...

Nous allons considérés les même matrices élémentaires que pour un corps, mais elles seront définies de manière à rester dans $GL_n(\mathbb{Z})$. Ainsi, on utilisera $T_{i,j}(\epsilon, n)$ avec $\epsilon \in \{1, -1\}$ (la multiplication à gauche d'une telle matrice revient à ajouter ou retrancher une ligne i à la ligne j). De même, on considère

les matrices de permutation qui appartiennent à $GL_n(\mathbb{Z})$ qui permettent d'échanger deux lignes ou deux colonnes. On considère enfin les matrices de dilatation $D_i(-1,n)$ telle que multiplier à gauche par cette matrice revient à prendre l'opposée de la ligne i.

On peut alors définir une action de $GL_n(\mathbb{Z})$ sur $\mathcal{M}_{n,1}(\mathbb{Z})$ en associant à tout couple (P,X) le vecteur colonne PX. La méthode de Gauss permet de paramétrer les orbites de cette action par le pgcd des coefficients constituant la colonne de X, on peut alors en trouver un représentant.

Proposition. *Soit X un élément de $\mathcal{M}_{n,1}(\mathbb{Z})$.*

1. *L'élément X' de $\mathcal{M}_{n,1}(\mathbb{Z})$ appartient à l'orbite ω_X si et seulement si le pgcd des coefficients de X' est égal au pgcd des coefficients de X.*
2. *Si a_X est le pgcd des coefficients de X, $\omega_X = \omega_{C_{a_X}}$. La famille $(C_a)_{a\in\mathbb{N}}$ est un système de représentant de la relation d'équivalence induite par l'action.*

Démonstration. 1. Si $X = 0$, ok. Supposons $X \neq 0$, donc $X' \neq 0$. Si $X' \in \omega_X$, il existe $P \in GL_n(\mathbb{Z})$ tel que $X' = PX$ et en écrivant les coefficients de X' en fonction de P et de X, on obtient le résultat. Réciproquement, il faut montrer que pour toute colonne X', il existe $P \in GL_n(\mathbb{Z})$ tel que PX' est la colonne $C_{a'_X}$ (se montre par récurrence).

2. Application de ce qui précède.

□

Corollaire. *Le groupe $GL_n\mathbb{Z}$ est engendré par les matrices élémentaire $(T_{i,j}(\epsilon,n)$, $D_i(-1,n)$ et $P(\sigma,n)$ où $\epsilon \in \{-1,1\})$.*

Démonstration. On raisonne par récurrence. □

Application ici [4]

Références

[1] V. Beck, J. Malik, and G. Peyré. *Objectif Agrégation*. H et K, 2004.

[2] M. Cognet. *Algèbre linéaire*. Bréal, 2000.

[3] X. Gourdon. *Algèbre*. Les maths en tête. Ellipses, 2009.

[4] A. Szpirglas. *Mathématiques Algèbre L3*. Pearson Education, 2009.