Université de Paris
M2 Mathématiques Fondamentales

Mémoire de Master
du 06/04/2020 au 30/06/2020

Étude d'algèbres d'opérateurs différentiels, techniques de calcul rapide de factorielles et applications au calcul de la p-courbure

Étudiant :
Raphaël Pagès

Encadrants :
Alin Bostan
Xavier Caruso

Institut de Mathématiques de Bordeaux
Équipe Théorie des Nombres — CNRS UMR 5251
351, cours de la Libération
F 33 405 TALENCE

INRIA Saclay Île-de-France
Équipe SpecFun
Bâtiment Alan Turing, 1 rue Honoré d'Estienne d'Orves
91120 Palaiseau

Résumé

L'étude des équations différentielles est un vaste pan des mathématiques qui trouve des applications dans de nombreux domaines notamment issus des sciences physiques. Bien que l'étude classique des équations différentielles concerne essentiellement des fonctions de variables réelles ou complexes, il existe un pendant algébrique à ce domaine. Les fonctions de l'analyse sont ici remplacées par les éléments d'un anneau dit *différentiel*, et l'« ensemble des équations différentielles » est muni d'une structure d'anneau. Le formalisme plus souple que celui de l'analyse permet de s'affranchir de la nécessité d'évoluer en caractéristique nulle, et permet d'étudier des problèmes en caractéristique strictement positive.

Ce mémoire propose une introduction à ce formalisme, et s'intéresse à l'aspect effectif des manipulations de ces nouveaux objets. Spécifiquement, après avoir travaillé à définir l'algèbre des opérateurs différentiels dans la seconde partie de ce document, nous introduisons un invariant important de ces opérateurs en caractéristique $p > 0$: la *p-courbure* [Clu03]. L'étude théorique réalisée dans la suite de cette partie permettra de ramener le calcul du polynôme caractéristique de cet invariant au calcul d'une *factorielle de matrices* [BCS14].

Ce travail permettra dans la dernière section de ce mémoire de réutiliser les techniques de calcul de factorielles développées dans la première partie, et de passer d'un algorithme naïf quasi-quadratique pour le calcul d'une seule p-courbure, à un algorithme quasi-linéaire pour le calcul d'un grand nombre de p-courbures, ce qui est un résultat nouveau et sera l'aboutissement de ce mémoire.

Dans un premier temps nous étudierons donc des techniques de calcul de factorielles. Si le problème que nous étudierons concernera le calcul des $(p-1)! \bmod p^2$, pour un seul ou un grand nombre de premiers p, les techniques vues dans cette section seront adaptables au calcul de *factorielles de matrices* ce qui, en plus de servir notre but, a également des applications au comptage des points sur une courbe sur un corps fini [Har14]. Dans le souci de produire un document complet nous passerons en revue des méthodes de calcul efficace, des opérations élémentaires d'une part, puis de $(p-1)! \bmod p^2$ (pour un p unique) d'une autre, en nous appuyant sur [BCG+17]. Nous présenterons ensuite un algorithme de calcul simultané de tous les restes $(p-1)! \bmod p^2$, pour tous les nombres premiers $p \leqslant N$, avec $N \in \mathbb{N}$, en complexité binaire quasi-linéaire en N [CGH14].

Ceci fait, nous introduirons dans une deuxième partie les algèbres d'opérateurs différentiels et leur p-courbure en caractéristique $p > 0$, en nous appuyant notamment sur le livre [vdPS03]. La suite de cette section se basera sur l'article [BCS14], afin de ramener le calcul du polynôme caractéristique de cette p-courbure à celui d'une *factorielle de matrices*.

Nous pourrons alors présenter un algorithme effectuant ce calcul en $\tilde{O}(\sqrt{p})$ opérations binaires [BCS14], avant d'adapter le travail de la section 1 pour en déduire un *nouvel algorithme* permettant d'effectuer, pour un opérateur différentiel en caractéristique 0 donné, le calcul de (presque) tous les polynômes caractéristiques de ses p-courbures, pour tous les premiers $p \leqslant N$, avec $N \in \mathbb{N}$, en complexité binaire quasi-linéaire en N.

Table des matières

1 Techniques de calcul rapide de $(p-1)! \bmod p^2$ pour plusieurs premiers p

Dans cette section nous passons en revue plusieurs techniques de calcul des factorielles, d'entiers ou de matrices. L'algorithme final de cette partie donnera un moyen efficace de calculer $(p-1)! \bmod p^2$ pour un grand nombre de premiers p, dont nous pourrons transposer le principe à des cas plus variés. Le calcul de $(p-1)! \bmod p^2$ pour un grand nombre de premiers p, est motivé par la recherche des entiers premiers de Wilson, des nombres premiers vérifiant non seulement $(p-1)! \equiv -1 \bmod p$ comme tout nombre premier, mais $(p-1)! \equiv -1 \bmod p^2$. La résolution de ce type de problèmes a également des applications au comptage des points sur une courbe sur un corps fini [Har14], même si nous n'aborderons pas ces questions dans ce mémoire.

1.1 Calcul efficace des opérations de base

1.1.1 Algorithmes naïfs et algorithmes élémentaires

Avant de s'intéresser au calcul efficace des factorielles, il est bon de connaître le coût des opérations basiques (additions et multiplications). Nous aborderons en priorité la question de la multiplication dans $\mathbb{Z}$, mais commençons par résoudre celle de l'addition. Avant tout, nous mettons une chose au clair.

Définition 1.1.1.1. — *Dans la suite de ce document la « taille » d'un entier sera la longueur de son écriture binaire. Ainsi $a \in \mathbb{N}$ est dit de taille $\lceil \log_2(a+1) \rceil$.*

Soient a et b dans $\mathbb{N}$. L'algorithme le plus naïf d'addition de a et b est celui que l'on nommera affectueusement « compter sur ses doigts ».

Données : $a, b \in \mathbb{N}$
Résultat : $a + b$

$res \leftarrow a$;
pour i *allant de* 1 *à* b **faire**
  incrémenter res
retourner res

Algorithme 0 : Compter sur ses doigts

Incrémenter un nombre a est une opération qui prend $\log(a)$ opérations binaires. On l'illustre par l'algorithme suivant :

Données : $a \in \mathbb{N}$ écrit en base binaire
Résultat : $a + 1$

$res \leftarrow$ le mot vide ;
$i \leftarrow$ le chiffre des unités de a ;
tant que $i \neq 0$ **faire**
  écrire 0 devant res ;
  $i \leftarrow$ le chiffre suivant de a
écrire 1 devant res ;
écrire le reste des chiffres de a devant res ;
retourner res

Algorithme 1 : Incrémenter

Il suit que l'algorithme consistant à compter sur ses doigts termine en $O(b \log(\max(a,b)))$. Comme $a+b$ peut s'écrire sur $O(\log(\max(a,b)))$ chiffres, on voit que cet algorithme est loin d'être optimal. Ce que n'importe qui ayant passé le CE1 aurait pu nous dire d'ailleurs. L'algorithme appris dans cette classe est optimal :

```
Données : a, b ∈ ℕ écrits en base binaire sur le même nombre de bits (quitte à rajouter
          des zéros)
Résultat : a + b

res ← le mot vide ;
retenue ← Faux ;
pour i et j parcourant les chiffres de a et b faire
    si i = 0 alors
        si retenue alors
            si j = 1 alors
                écrire 0 devant res
            sinon
                écrire 1 devant res ;
                retenue ← Faux
        sinon
            écrire j devant res
    sinon
        si j = 1 alors
            si retenue alors
                écrire 1 devant res
            sinon
                écrire 0 devant res ;
                retenue ← Vrai
        sinon
            si retenue alors
                écrire 0 devant res
            sinon
                écrire 1 devant res
si retenue alors écrire 1 devant res ;
retourner (res)
```

Algorithme 2 : Addition efficace

Cet algorithme termine bien en $O(\log(\max(a,b)))$, il est donc optimal. Les seules améliorations que l'on pourrait lui apporter consisteraient à faire baisser la constante dans le $O(\cdot)$.

Nous nous attaquons maintenant au problème de la multiplication de deux entiers a et $b \in \mathbb{N}$. Dans la lignée de l'algorithme « compter sur ses doigts », l'algorithme le plus naïf que l'on puisse donner consiste à additionner b fois a avec lui-même. Nous savons alors qu'à l'étape k nous faisons le calcul $ka+a$ dont nous savons que le coût est $O(\log(a)+\log(k))$. On peut donc en déduire que cet algorithme a pour coût total $O(b(\log(a)+\log(b)))$. La sortie ab pouvant s'écrire sur $O(\log(a)+\log(b))$ bits, cet algorithme est loin d'être optimal.
Une première amélioration vient en reprenant l'algorithme d'exponentiation rapide :

```
Données : a, b ∈ ℕ
Résultat : ab

si b = 1 alors
    retourner a
sinon
    calculer res = a ⌊b/2⌋ ;
    si b est pair alors
        retourner res + res
    sinon
        retourner res + res + a
```

Cet algorithme termine lui en $O(\log(b)\log(a)+\log^2(b))$. En effet on peut supposer le coût de cet algorithme croissant avec b. Prenons alors $2^{n-1} < b \leqslant 2^n$. Le coût est alors majoré par :

$$\sum_{k=0}^{n-1} O(\log(2^k a)) = O\left(\log(a)n + \log(2)\frac{n(n-1)}{2}\right).$$

Le gain de temps est significatif, mais on peut encore faire mieux. On rappelle que la multiplication par 2 en binaire (au même titre que la multiplication par 10 en base 10) peut-être vue comme faisable en temps constant, même si en réalité il y a toujours le coût de l'écriture de la sortie.

Données : $a, b \in \mathbb{N}$ avec b écrit en base 2.
Résultat : ab

$res \leftarrow 0$;
$aj \leftarrow a$;
pour i *parcourant les chiffres de* b **faire**
  si $i = 1$ **alors** $res \leftarrow res + aj$;
  $aj \leftarrow 2 * aj$
retourner res

Algorithme 3 : Multiplication à l'école primaire

La complexité de cet algorithme est en $O(\log(a)\log(b))$ (en s'y prenant bien, on peut voir qu'à l'étape $res \leftarrow res + aj$ on n'a à modifier que les « a premiers chiffres de res »). En supposant que $b \leqslant a$, cela donne la même complexité que l'algorithme précédent, même si la constante dans le O n'est pas la même).

D'autres moyens d'améliorer la complexité existent, dont l'algorithme de Karatsuba [BCG+17]. Cependant l'objet de ce mémoire n'est pas de faire un historique de la multiplication des entiers. Nous nous penchons donc directement sur un algorithme utilisant la multiplication des polynômes.

1.1.2 Multiplication des entiers par multiplication des polynômes

Nous présentons ci-dessous un algorithme rapide de multiplication des polynômes faisant intervenir la transformée de Fourier rapide.
D'ailleurs, puisque le but est d'en déduire un algorithme de multiplication rapide d'entiers, il serait bon que notre algorithme n'utilise pas, ou peu, ces multiplications.
Soient A un anneau intègre et $P, Q \in A[X]$ deux polynômes de degré au plus $d \in \mathbb{N}$. Supposons que A contienne au moins $d+1$ éléments. On sait que $P = Q$ si et seulement s'il existe $x_0, \dots, x_d \in A^{d+1}$ deux à deux distincts, tels que $P(x_i) = Q(x_i)$ pour $i \in [\![0, d]\!]$.
Ce constat est le point de départ de l'algorithme de multiplication rapide des polynômes dont l'idée est résumée ci-dessous :

Données : $P, Q \in A[X]$ de degré au plus d ;
$x_0, \dots, x_{2d} \in A$ deux à deux distincts
Résultat : PQ

Calculer $(P(x_0, \dots, P(x_{2d}))$;
Calculer $(Q(x_0), \dots, Q(x_{2d}))$;
Calculer $(P(x_0)Q(x_0), \dots, P(x_{2d})Q(x_{2d}))$;
retourner $R \in A[X]$ *tel que* $(R(x_0), \dots, R(x_{2d})) = (P(x_0)Q(x_0), \dots, P(x_{2d})Q(x_{2d}))$

L'idée est qu'il est facile de connaître la valeur de PQ en un point à partir de celles de P et Q en ce point, sans connaître les coefficients de PQ. Comme PQ est entièrement déterminé par ses valeurs en $2d+1$ points, il suffit de trouver l'unique polynôme ayant ces valeurs en ces points.

Trois questions se posent alors :

1. Comment choisir les points en lesquels évaluer P et Q ?
2. Comment évaluer rapidement P et Q en ces points ?
3. Comment interpoler rapidement en $2d+1$ points ?

DÉFINITION 1.1.2.1. — *Soit $n \in \mathbb{N}$. On dit que $\omega \in A$ est une racine primitive n-ième de l'unité si $\omega^n = 1$ et si pour tout $k < n$, $\omega^k \neq 1$.*

On suppose désormais que A contient une racine primitive n-ième de l'unité ω, avec n pair. On choisit les points d'évaluation comme étant $(1, \omega, \omega^2, \ldots, \omega^{n-1})$.
On cherche à présent à résoudre la question de l'évaluation. Comme n est pair $X^n - 1 = (X^{n/2} - 1)(X^{n/2} + 1)$. De plus on voit que si k est pair alors ω^k est racine de $X^{n/2} - 1$, et que s'il est impair alors il est racine de $X^{n/2} + 1$. Écrivons

$$P = Q_0 \cdot (X^{n/2} - 1) + R_0 \text{ avec } \deg(R_0) < n/2$$

et

$$P = Q_1 \cdot (X^{n/2} + 1) + R_1 \text{ avec } \deg(R_1) < n/2.$$

Évaluer P en les puissances paires de ω revient à évaluer R_0 en les puissances paires de ω, et évaluer P en les puissances impaires de ω revient à évaluer R_1 en les puissances impaires de ω.
De plus pour tout $k \leqslant d$, $R_1(\omega^{2k+1}) = R_1(\omega\omega^{2k})$.
On peut donc calculer $\overline{R_1}(X) = R_1(\omega X)$ et l'évaluer en les puissances paires de ω.
Il se trouve que R_0 et $\overline{R_1}$ sont calculables en $O(d)$ opérations dans A.
On peut supposer que P est de degré strictement plus petit que n. On écrit alors $P = \sum_{k=0}^{n-1} p_k X^k$.
Il vient alors que $P(\omega^{2k}) = \sum_{i=0}^{n/2-1} (p_i + p_{i+n/2})\omega^{2ki}$ et donc $R_0 = \sum_{i=0}^{n/2-1} (p_i + p_{i+n/2}) X^i$ puisque R_0 est déterminé par ses valeurs en $n/2$ points.
Similairement $P(\omega^{2k+1}) = \sum_{i=0}^{n/2-1} (p_i - p_{i+n/2})\omega^{i(2k+1)}$ et donc $\overline{R_1} = \sum_{i=0}^{n/2-1} (p_i - p_{i+n/2})\omega X^i$.
Comme ω^2 est une racine $n/2$-ième primitive de l'unité, si n est bien choisi on peut évaluer R_0 et $\overline{R_1}$ récursivement.

Données : $P = \sum_{k=0}^{\deg(P)} p_k X^k \in A[X]$, $n \in \mathbb{N}$ tel que $\deg(P) < 2^n$;
ω une racine primitive 2^n-ième de l'unité dans A
Résultat : $P(1), P(\omega), \ldots, P(\omega^{2^n-1})$

si $n = 0$ **alors**
  retourner $P(0)$
sinon
  $R_0 \leftarrow \sum_{k=0}^{2^{n-1}} (p_k + p_{k+2^{n-1}}) X^k$;
  $\overline{R_1} \leftarrow \sum_{k=0}^{2^{n-1}} (p_k - p_{k+2^{n-1}}) \omega X^k$;
  calculer récursivement $R_0(1), R_0(\omega^2), \ldots, R_0(\omega^{2^{n-1}-1})$ et $\overline{R_1}(1), \overline{R_1}(\omega^2), \ldots, \overline{R_1}(\omega^{2^{n-1}-1})$;
  retourner $R_0(1), \overline{R_1}(1), R_0(\omega), \ldots, R_0(\omega^{2^{n-1}-1}), \overline{R_1}(\omega^{2^{n-1}-1})$

Algorithme 4 : Evaluation rapide en les racines de l'unité

On peut, pour les utilisations qui nous intéressent, supposer que $\deg(P) \sim 2^n$. On note $C(n)$ la complexité de cet algorithme pour $\deg(P) \sim 2^n$.
On a alors

$$C(n) = O(2^n) + 2C(n-1).$$

Il en vient immédiatement :

$$C(n) = \sum_{k=0}^{n} O(2^{n-k}.2^k) = O(n2^n)$$

Cet algorithme termine donc en $O(\deg(P)\log(\deg(P)))$.
La question de l'évaluation étant réglée il reste à savoir comment réaliser l'interpolation.

Définition 1.1.2.2. — *Soit ω une racine n-ième de l'unité n-ième de l'unité avec $n \geqslant d+1$. L'application $\mathcal{F}_\omega : P \in A[X]_{n-1} \mapsto \sum_{k=0}^{n-1} P(\omega^k)X^k \in A[X]_{n-1}$ est appelée transformée de Fourier discrète.*

Proposition 1.1.2.3. — *On a la relation suivante :*

$$\mathcal{F}_{\omega^{-1}} \circ \mathcal{F}_\omega = n \cdot \mathrm{Id}.$$

Preuve. Soit $P = \sum_{k=0}^{n-1} p_k X^k \in A[X]_{n-1}$.

$$\begin{aligned}
\mathcal{F}_{\omega^{-1}} \circ \mathcal{F}_\omega(P) &= \sum_{k=0}^{n-1} \mathcal{F}_\omega(P)(\omega^{-k})X^k \\
&= \sum_{k=0}^{n-1} \left(\sum_{l=0}^{n-1} \left(\sum_{m=0}^{n-1} p_m \omega^{lm} \right) \omega^{-kl} \right) X^k \\
&= \sum_{k=0}^{n-1} \left(\sum_{m=0}^{n-1} p_m \left(\sum_{l=0}^{n-1} \omega^{l(m-k)} \right) \right)
\end{aligned}$$

Or $\sum_{l=0}^{n-1} \omega^{l(m-k)} = n\delta_{m,k}$, donc

$$\mathcal{F}_{\omega^{-1}} \circ \mathcal{F}_\omega(P) = \sum_{k=0}^{n-1} np_k X^k = nP$$

□

On a donc ramené le problème d'interpolation à une évaluation ce qui amène le résultat final :

Théorème 1.1.2.4. — *Soit A un anneau intègre tel que 2 soit inversible dans A. Soit P, Q deux polynômes de degré au plus d, et $n \in \mathbb{N}$ tel que $2^n \geqslant 2d+1 > 2^{n-1}$. On suppose qu'il existe $\omega \in A$ une racine primitive 2^n-ième de l'unité.*
On peut alors calculer PQ en $O(d\log(d))$ opérations arithmétiques dans A via l'algorithme suivant :

Données : $P, Q \in A[X]_d$;
ω *une racine primitive* 2^n*-ième de l'unité.*
Résultat : PQ
Calculer $P(1), P(\omega), \ldots, P(\omega^{2^n-1})$;
Calculer $Q(1), Q(\omega), \ldots, Q(\omega^{2^n-1})$;
Calculer les produits $P(1)Q(1), P(\omega)R(\omega), \ldots, P(\omega^{2^n-1})Q(\omega^{2^n-1})$. ;
retourner $2^{-n}\mathcal{F}_{\omega^{-1}}(P(\omega^{2^n-1})R(\omega^{2^n-1})X^{2^n-1} + \ldots + P(1)R(1))$

Algorithme 5 : Multiplication rapide de polynômes par FFT dans un bon anneau

Le problème de cet algorithme est qu'il nécessite d'avoir suffisamment de racines de l'unité. Bien sûr comme A est intègre on peut en général étendre l'anneau pour les introduire, mais cela fait croître le coût des opérations arithmétiques dans l'anneau de base. C'est pourquoi on introduit une variante de cette algorithme qui aura l'avantage de fonctionner dans n'importe quel anneau de base A intègre dans lequel 2 est inversible.

L'idée peut-être vue de la façon suivante : les combinaisons linéaires de puissances de ω qui apparaissent dans l'algorithme de FFT peuvent être vues comme des écritures formelles ne devant vérifier que $\omega^{2n} = 1$ pour un n bien choisi, et encore $\omega^n + 1 = 0$. De telles écritures formelles sont très bien représentées par l'anneau $A[X]/(X^n+1)$, où X est alors une racine primitive $2n$-ième de l'unité.
Malheureusement cet anneau n'est en général pas intègre, l'algorithme précédent ne peut donc pas s'appliquer aussi facilement.
Pour surmonter cette difficulté nous aurons pour commencer besoin de renforcer la notion de racine primitive.

Définition 1.1.2.5. — *Soit A un anneau commutatif (pour nécessairement intègre) et ω une racine n-ième de l'unité. On dit que ω est principale si pour tout $t < n$, $(\omega^t - 1)$ n'est pas diviseur de zéro.*

Remarque 1.1.2.6. — *Sur un anneau intègre les notions de racines primitives et principales coïncident.*

L'intérêt de cette définition vient de la proposition suivante :

Proposition 1.1.2.7. — *Soit ω une racine principale n-ième de l'unité et $P \in A[X]$. Si $P(1) = P(\omega) = \ldots = P(\omega^{n-1}) = 0$ alors $X^n + 1 | P$.*

Preuve. Comme $P(1) = 0$ on a $P = (X-1)P_1$. Supposons que l'on ait montré que $P = (X-1)(X-\omega)\ldots(X-\omega^k)P_{k+1}$ pour un certain k.
On a encore $P(\omega^{k+1}) = P_{k+1}(\omega^{k+1})\prod_{i=0}^{k}(\omega^{k+1} - \omega^i) = 0$. Si $P_{k+1}(\omega_{k+1}) \neq 0$ alors au moins l'un des $\omega^{k+1} - \omega^i = \omega^i(\omega^{k+1-i} - 1)$ est un diviseur de 0 ce qui est absurde par hypothèse. Donc $P_{k+1}(\omega^{k+1}) = 0$. On conclut par récurrence. □

Proposition 1.1.2.8. — *Une racine n-ième de l'unité $\omega \in A$ est principale si et seulement si pour tout $t|n$, $\omega^t - 1$ n'est pas un diviseur de zéro.*

Preuve. On a un sens trivial. Supposons que pour tout $t|n$, $\omega^t - 1$ ne soit pas un diviseur de 0. Soit t ne divisant pas n. On considère $d := \text{pgcd}(t, n)$. Par le théorème de Bezout il existe $u, v \in \mathbb{Z}$ tels que $ut + vn = d$. Mais alors $(\omega^t - 1)(1 + \omega^t + \ldots + \omega^{t(u-1)}) = \omega^{tu} - 1 = \omega^{d-vn} - 1 = \omega^d - 1$. Ainsi si $\omega^t - 1$ est un diviseur de zéro, c'est aussi le cas de d, ce qui n'est pas le cas par hypothèse. □

Il en découle que, dès lors 2 est inversible dans A, X est une racine principale $2n$-ième de l'unité dans ${}^{A[X]}/_{X^n+1}$ lorsque n est une puissance de 2. En effet par ce qui précède, il suffit de montrer $X^k - 1$ n'est pas un diviseur de 0 pour $k|n$ soit k une puissance de 2 inférieure à $2n$. Mais $\omega^k - 1 | \omega^n - 1 = -2$ inversible dans A. Ainsi X est une racine principale $2n$-ième de l'unité.

Remarque 1.1.2.9. — *Il suit immédiatement des définitions que si ω est une racine principale n-ième de l'unité alors ω^k est une racine principale* $\text{pgcd}(k, n)$*-ième de l'unité.*

Nous avons maintenant les cartes en mains pour écrire l'algorithme final de multiplication rapide des polynômes.
Nous ne pouvons pas nous contenter d'introduire une racine principale de l'unité de degré suffisamment grand. En effet, nous pourrions effectuer la multiplication dans $B[Y] = {}^{A[X]}/_{(X^n+1)}[Y]$ pour n assez grand en $O(d\log(d))$ opérations arithmétiques dans B, mais nous n'aurions rien gagné puisque le coût de ces opérations augmente avec n (de la même façon…que le coût d'une multiplication de polynômes). On opte donc plutôt pour un algorithme récursif.
Soient $P, Q \in A[X]$ de degré strictement inférieurs à $n = 2^k$. Le but est de calculer $PQ \bmod X^n + 1$. L'idée est la suivante : nous allons partager équitablement la difficulté du calcul entre d'une part le calcul des opérations arithmétiques dans l'anneau de base, et le calcul d'une multiplication de polynômes de plus petits degrés d'autre part.

On pose $d = 2^{\lfloor \frac{k}{2} \rfloor}$ et $\delta = n/d$. On peut réécrire F et G sous la forme :

$$\overline{P}(X, Y) = P_0(X) + P_1(X)Y + \ldots + P_{\delta-1}Y^{\delta-1}$$

et

$$\overline{Q}(X, Y) = Q_0(X) + Q_1(X)Y + \ldots + Q_{\delta-1}Y^{\delta-1}$$

avec les P_i et les Q_i de degré strictement inférieur à d de sorte que $P = \overline{P}(X, X^d)$ et $Q = \overline{Q}(X, X^d)$. Il ne reste plus qu'à faire le calcul de $\overline{H} = \overline{P}\overline{Q} \in A[X][Y]$. Comme on sait que les P_i et Q_i sont de degré strictement inférieur à d, on déduit que $\overline{H}$ a des coefficients de degré strictement plus petit que $2d$. Ainsi nous pouvons calculer ces coefficients dans $B = {}^{A[X]}/_{(X^{2d}+1)}$. De plus B est muni d'une racine principale $4d$-ième de l'unité. Le calcul des produits dans B peut se faire récursivement dès que $2d < n$ soit $k \geqslant 3$.
Comme de plus $\delta | 4d$ on peut trouver une racine δ-ième de l'unité dans B et calculer $\overline{H} \bmod Y^\delta - 1$.

Comme on veut connaître $\overline{H}$ mod $Y^\delta + 1$, on a l'idée de calculer $\overline{H}(X, X^i Y)$ mod $Y^\delta - 1$ par FFT de sorte que $X^{-i\delta} = -1$.
On a alors une disjonction de cas pour déterminer i :
Si $2|k$ alors $\delta = d$ et X^4 est une racine δ-ième de l'unité dans B.
De plus $X^{-i} = -X^{2d-i}$, et $X^{-i\delta} = (-1)^\delta X^{2d^2-id} X^{2d^2-id}$. On veut que $X^{2d^2-id} = -1$. Pour $i = 2$ on a $X^{2d^2-2d} = X^{2d(d-1)} = (-1)^{d-1}$. Comme d est pair on trouve bien -1.

Si 2 ne divise pas k, alors $\delta = 2d$ et X^2 est une racine principale δ-ième de l'unité. On trouve $X^{-i\delta} = (-1)^\delta X^{2d^2-2id}$. Pour $i = 1$ on retrouve $X^{-\delta} = -1$.

On en déduit enfin l'algorithme :

Données : $P, Q \in A[X]_{n-1}$ avec $n = 2^k$
Résultat : PQ mod $X^n + 1$

si $k \leqslant 2$ **alors**
  Faire le calcul naïf de PQ mod $X^n + 1$
sinon
  $d \leftarrow 2^{\lfloor k/2 \rfloor}$;
  $\delta \leftarrow n/d$;
  calculer ;
  $\overline{P} = P_0(X) + P_1(X)Y + \ldots + P_{\delta-1}(X)Y^{\delta-1}$;
  $\overline{Q} = Q_0(X) + Q_1(X)Y + \ldots + Q_{\delta-1}(X)Y^{\delta-1}$;
  de sorte que les P_i et les Q_i aient dégré maximal $d-1$ et $\overline{P}(X, X^d) = P$ et $\overline{Q}(X, X^d) = Q$;
  $B \leftarrow A[X]/(X^{2d} + 1)$;
  si $2|k$ **alors**
    Calculer $\mathcal{F}_{X^4}(\overline{P}(X, X^2Y))$ dans $B[Y]$;
    Calculer $\mathcal{F}_{X^4}(\overline{Q}(X, X^2Y))$ dans $B[Y]$;
    pour *i allant de* 0 *à* $\delta - 1$ **faire**
      Calculer récursivement$\overline{P}(X, X^{2+4i})\overline{Q}(X, X^{2+4i})$ mod $X^{2d} + 1$
    Ecrire le polynôme associé $\tilde{H}$;
    $\overline{H}(X, Y) \leftarrow \mathcal{F}_{X^{-4}}(\tilde{H})$ mod $Y^\delta - 1$;
    retourner $\overline{H}(X, X^{d-2}) = PQ$ mod $X^n + 1$
  sinon
    Calculer $\mathcal{F}_{X^2}(\overline{P}(X, XY))$ dans $B[Y]$;
    Calculer $\mathcal{F}_{X^2}(\overline{Q}(X, XY))$ dans $B[Y]$;
    pour *i allant de* 0 *à* $\delta - 1$ **faire**
      Calculer récursivement$\overline{P}(X, X^{1+2i})\overline{Q}(X, X^{1+2i})$ mod $X^{2d} + 1$
    Ecrire le polynôme associé $\tilde{H}$;
    $\overline{H}(X, Y) \leftarrow \mathcal{F}_{X^{-2}}(\tilde{H})$ mod $Y^\delta - 1$;
    retourner $\overline{H}(X, X^{d-1}) = PQ$ mod $X^n + 1$

Algorithme 6 : Algorithme de Schönhage-Strassen

On voit qu'à l'étape n, le calcul nécessite $O(d \log(d))$ opérations arithmétiques dans B en $O(d)$ opérations dans A chacune (les multiplications par une puissance de X aussi puisqu'elles consistent à décaler les indices), et δ appels récursifs. Notons $C(n)$ le coût de cet algorithme pour n. On a :

$$C(n) \leqslant Kd^2 \log d + \delta C(2d).$$

avec K une constante ne dépendant pas de n. On peut diviser par n :

$$\frac{C(n)}{n} \leqslant K' \log(d) + 2\frac{C(2d)}{2d}$$

On se souvient que $\lfloor (k+1)/2 \rfloor = \lceil k/2 \rceil$ et on en déduit :

$$\frac{C(2n)}{2n} \leqslant K' \log(n) + 2\frac{C(2^{\lceil k/2 \rceil + 1})}{2^{\lceil k/2 \rceil}}$$

En posant $c(k) = \frac{C(2^{k+1})}{2^{k+1}}$ on en déduit $c(k) \leqslant K''k + 2c(\lceil k/2 \rceil)$ et encore $c(k) = O(k \log(k))$. Cela se traduit par $C(n) = O(n \log(n) \log\log(n))$.

L'idée principale à présent pour multiplier des entiers revient à représenter un entier $a = \sum_{i=0}^{d} a_i 2^i$ avec $a_i \in \{0, 1\}$ par le polynôme $\sum_{i=0}^{d} a_i X^i$. On ramène donc la multiplication de deux entiers à celle de deux polynômes dans un anneau bien choisi. Il suffit ensuite d'évaluer le polynôme en 2. Les coefficients de ce produit valant au maximal d où les deux entiers a et b sont de taille maximale d, l'évaluation en d peut se faire en $O(d \log(d))$ opérations binaires ne correspondant qu'à des additions.
On peut effectuer la multiplication des polynômes dans un $\mathbb{Z}/p\mathbb{Z}$ avec $p \geqslant 2d$. Le coût d'une multiplication dans cet anneau est celui de la multiplication « naïve » d'entiers valant au plus $2d$, soit $O(\log^2(d))$. Cela conduit à un algorithme de coût $O(d \log^3(d) \log(\log(d)))$. D'autres amélioration sont possibles, mais nous ne les évoquerons pas ici. On se contentera d'admettre le résultat suivant :

THÉORÈME 1.1.2.10. — *Il est possible de multiplier deux entiers de taille d en $O(d \log(d) \log\log(d))$ opérations binaires.*

REMARQUE 1.1.2.11. — *Un article de 2019 dû à DAVID HARVEY et JORIS VAN DER HOEVEN a montré que la multiplication de deux polynômes à coefficients dans $\mathbb{F}_q$ de degré au plus n peut théoriquement s'effectuer en $O(n \log(q) \log(n \log(q)))$ opérations binaires, uniformément en q, et que la multiplication de deux entiers de taille n peut théoriquement s'effectuer en $O(n \log(n))$ opérations binaires.*
Nous n'utiliserons pas ce résultat.

1.2 Techniques de calcul des factorielles

Dans cette sous-section, nous attaquons la question du calcul des factorielles. Nous aborderons cette question en essayant de résoudre le problème du calcul de $(p-1)! \bmod p^2$ pour tous les p premiers inférieurs à un certain N.

L'algorithme le plus naïf imaginable consiste simplement à calculer chaque $(p-1)!$ et à le réduire modulo p^2. Un algorithme de calcul de la division euclidienne de a par b est donné par

Données : $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ écrits en base binaire
Résultat : $q, r \in \mathbb{N}$ tels que $a = qb + r$ avec $r < b$

$q \leftarrow$ le mot vide ;
$r \leftarrow$ le mot vide ;
pour *i parcourant les chiffres de a* **faire**
    écrire i à la fin de r
    si $r \geqslant b$ **alors**
        écrire 1 à la fin de q ;
        $r \leftarrow r - b$
    sinon
        écrire 0 à la fin de q
retourner q, r

Le coup de chaque étape de l'algorithme est en $O(\log(b))$ opérations binaires lorsque $r \geqslant b$ car $r < 2b$ à chaque étape de l'algorithme. Lorsque $r < b$, cette étape a coût constant. Si a est écrit sur d_a bits et b sur d_b bit, cela est le cas sur les d_b premières étapes. On conclut que le coût de cet algorithme est $O(\log(b)(\log(a) - \log(b)))$ opérations binaires.

Rappelons que la taille binaire de $(p-1)!$ est linéaire en $p \log(p)$. La division euclidienne naïve de $(p-1)!$ par p^2 s'effectue donc en $O(p \log^2(p))$ opérations binaires. On peut améliorer ce temps de calcul comme nous le verrons plus tard (voir A.7), mais le gain de temps vaudra surtout lorsque

le dividende est d'une taille similaire au diviseur, ce qui n'est pas le cas ici.
Il reste à déterminer le coût du calcul de $(p-1)!$ dans $\mathbb{N}$. Voyons cela dans le cas de l'algorithme donné par la formule de récurrence :

Données : $n \in \mathbb{N}$
Résultat : $n!$

si $n \leqslant 1$ **alors**
  retourner 1
sinon
  Calculer récursivement $f := (n-1)!$;
  retourner $n \cdot f$

Algorithme 7 : Calcul naïf de la factorielle

Cet algorithme coûte le prix de la multiplication de n par $(n-1)!$ soit $O(\log((n-1)!)\log\log((n-1)!)\log\log\log((n-1)!))$ opérations binaires, et d'un appel récursif. On peut donc écrire, en appelant $C(n)$ le coût de l'algorithme :

$$C(n) = O(n\log^2(n)\log\log(n)) + C(n-1)$$

et donc $C(n) = O(n^2\log^2(n)\log\log(n))$.

Le calcul naïf de la factorielle $(p-1)!$ a donc un coût quasi-quadratique en p. Nous allons voir au cours de cette sous-section que le calcul de $(p-1)! \in \mathbb{Z}$ peut être ramené à un coût binaire quasi-linéaire en p, que le calcul de $(p-1)! \bmod p^2$ peut être réalisé en $\tilde{O}(\sqrt{p})$ opérations binaires, et qu'enfin, notre problème initial (calcul simultané des restes $(p-1)! \bmod p^2$, pour tous les p premiers inférieurs à N) peut-être résolu en temps quasi-linéaire en N.
Cela représente un gain significatif. En effet, même en considérant que dans notre problème nous pouvons calculer les $(p-1)! \bmod p^2$ en gardant en mémoire la valeur de $(p-1)!$, de sorte à ne faire qu'un seul calcul de factorielle, le coût reste au moins quadratique.

1.2.1 Calcul efficace d'une seule factorielle

La première amélioration du calcul de la factorielle consiste à équilibrer les facteurs dans les multiplications. Cela se présente sous la forme d'un algorithme de type diviser pour régner :

Données : $a_1, \ldots, a_n \in \mathbb{N}$
Résultat : $\prod_{i=1}^{n} a_i$

si $n = 1$ **alors**
  retourner a_1
sinon
  Calculer récursivement $a = \prod_{i=1}^{\lfloor n/2 \rfloor} a_i$;
  Calculer récursivement $b = \prod_{i=\lfloor n/2 \rfloor + 1}^{n} a_i$;
  retourner ab

Algorithme 8 : Calcul de la factorielle par scindage binaire

Cet algorithme appliqué à des $a_i \leqslant n$ a pour coût celui d'une multiplication d'entiers s'écrivant sur $O(n\log(n))$ bits, et 2 appels récursifs. Son coût vérifie donc :

$$C(n) = O(n\log^2(n)\log\log(n)) + 2C(n/2).$$

On en déduit donc

$$C(n) = O(n\log^3(n)\log\log(n)).$$

Il y a là un progrès significatif.

On peut encore faire mieux en se souvenant que nous voulons calculer les factorielles dans $\mathbb{Z}/p^2\mathbb{Z}$. Dans cet anneau les éléments « valent au plus » p^2 (et même $(p^2-1)/2$ en valeur absolue). Cela nous permet d'effectuer des opérations arithmétiques en temps constant (en fait dépendant de p,

mais pas de la taille des objets multipliés). Pour simplifier, on suppose que n est un carré parfait. On peut écrire :

$$n! = \prod_{i=1}^{n} i = \prod_{i=0}^{\sqrt{n}-1} \prod_{j=1}^{\sqrt{n}} (i\sqrt{n} + j)$$

Ainsi si on note $P = (X+1)(X+2)\dots(X+\sqrt{N})$, on peut écrire :

$$n! = \prod_{i=1}^{n} P(i\sqrt{n}).$$

Données : $p \in \mathbb{N}$ premier
Résultat : $(p-1)! \bmod p^2$

Calculer $a = \prod_{i=\lfloor\sqrt{p-1}\rfloor^2+1}^{p-1} i \bmod p^2$;
Calculer $P = (X+1)(X+2)\dots(X+\lfloor\sqrt{p-1}\rfloor)$;
Calculer $P(0), P(\lfloor\sqrt{p-1}\rfloor), \dots, P((\lfloor\sqrt{p-1}\rfloor - 1)\lfloor\sqrt{p-1}\rfloor)$;
retourner $a \prod_{i=0}^{\lfloor\sqrt{p-1}\rfloor-1} P(i\lfloor\sqrt{p-1}\rfloor)$

Algorithme 9 : Calcul efficace d'une factorielle

Le calcul de P s'effectue récursivement en scindant les produits comme pour le calcul de la factorielle par scindage binaire. On notant $C(n)$ le coût du calcul d'un produit de n polynômes de degré 1 par cet algorithme, en opérations dans $\mathbb{Z}/p^2\mathbb{Z}$, on trouve

$$C(n) = O(n \log(n) \log\log(n)) + 2C(\lceil n/2 \rceil)$$

et donc

$$C(\lfloor\sqrt{p-1}\rfloor) = O(\sqrt{p} \log^2(p) \log\log(p)).$$

Il reste à savoir comment faire efficacement les évaluations de P. Cela peut-être fait en $O(\sqrt{p} \log^2(p) \log\log(p))$ opérations arithmétiques dans $\mathbb{Z}/p^2\mathbb{Z}$ (voir A.2), soit $O(\sqrt{p} \log^3(p) \log\log(p)^2 \log\log\log(p))$ opérations binaires. On en déduit que le coût total de cet algorithme est $O(\sqrt{p} \log^3(p) \log\log(p)^2 \log\log\log(p))$ opérations binaires.
Cette technique est communément nommée « pas de bébés, pas de géants ».

On note p_k le k-ième nombre premier. On sait par le théorème des nombres premiers que

$$p_k \sim k \log(k).$$

L'utilisation de cet algorithme pour le calcul de tout les $(p-1)! \bmod p^2$ pour $p \leqslant n$ premier aurait donc un coût

$$C(n) \sim \sum_{k=0}^{\frac{n}{\log(n)}} O(\sqrt{k} \log^{3+1/2}(k) \log\log(k)^2 \log\log\log(k)) = O(n^{3/2} \log^2(n) \log\log(n)^2 \log\log\log(n)).$$

Nous avons fait des progrès, mais on peut encore mieux faire.

1.2.2 Calcul efficace d'un grand nombre de factorielles

L'idée principale derrière l'algorithme que nous allons présenter est en fait similaire à celle que nous avions eue lors du calcul naïf de la factorielle, qui est de garder en mémoire les calculs intermédiaires de $n!$. Plus précisément on voit que $(p-1)!$ apparait dans le calcul de tous les $(p'-1)! \bmod p'^2$ pour $p \leqslant p' \leqslant N$.
On veut donc conserver $(p-1)!$ sous une forme utilisable pour son calcul modulo p'^2.
Nous allons donc garder en mémoire $(p-1)! \bmod \prod_{\substack{p \leqslant p' \leqslant N \\ p' \text{ premier}}} p'^2$.
Ceci est l'idée fondamentale derrière cet algorithme. Nous voulons pouvoir effectuer ce calcul de manière récursive. Il est facile de calculer

$$(p-1)! \bmod \prod_{\substack{p \leqslant p' \leqslant N \\ p' \text{ premier}}} p'^2$$

connaissant

$$\left(\frac{p-1}{2}\right)! \bmod \prod_{\substack{\frac{p-1}{2}+1 \leqslant p' \leqslant N \\ p' \text{ premier}}} p'^2$$

et

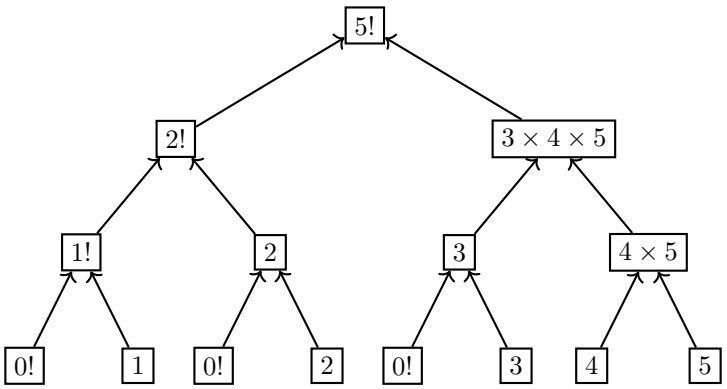
$$\prod_{i=\frac{p-1}{2}+1}^{p-1} i \bmod \prod_{\substack{p \leqslant p' \leqslant N \\ p' \text{ premier}}} p'^2.$$

Nous allons donc calculer $(N-1)!$ par scindage binaire, mais en conservant l'arbre des sous-produits.
Pour la suite de l'algorithme on fera en sorte que cet arbre soit plein.

Définition 1.2.2.1. — *On dira qu'un arbre binaire est plein si ses deux sous-arbres sont pleins et de même profondeur, ou bien si c'est une feuille.*

Cela implique que certaines feuilles contiendront éventuellement des produits vides.

Exemple 1.2.2.2. — *Voici l'arbre en question pour le calcul de* 5! *:*



Notons $d = \lceil \log_2(N) \rceil$. Pour tout $0 \leqslant i \leqslant d$ et $0 \leqslant j < 2^i$ on note

$$U_{i,j} := \left\{ k \in \mathbb{N} \;\middle|\; j\frac{N}{2^i} < k \leqslant (j+1)\frac{N}{2^i} \right\}.$$

On a la relation suivante pour tout $0 \leqslant i < d$ et $0 \leqslant j < 2^i$:

$$U_{i,j} = U_{i+1,2j} \sqcup U_{i+1,2j+1}.$$

Pour un N quelconque, on écrit l'arbre des sous-produits du calcul de $N!$ de la figure 2.

On note $A_{i,j} = \prod_{k \in U_{i,j}} k$. Similairement on peut écrire l'arbre binaire des diviseurs successifs en définissant $S_{i,j} = \prod_{\substack{p \in U_{i,j} \\ p \text{ premier}}} p^2$. On a évidemment $S_{i,j} = S_{i+1,2j} S_{i+1,2j+1}$ ce qui permet de définir un arbre similaire.

Notre but est de connaitre $(p-1)! \bmod p^2$ ce qui, en supposant que $p^2 \in U_{d,j}$, peut encore s'écrire $\prod_{l=0}^{j-1} A_{d,l} \bmod S_{d,j}$. On a donc l'idée d'introduire :

$$W_{i,j} := \prod_{l=0}^{j-1} A_{i,l} \bmod S_{i,j} = \left\lfloor j\frac{N}{2^i} \right\rfloor ! \bmod S_{i,j}$$

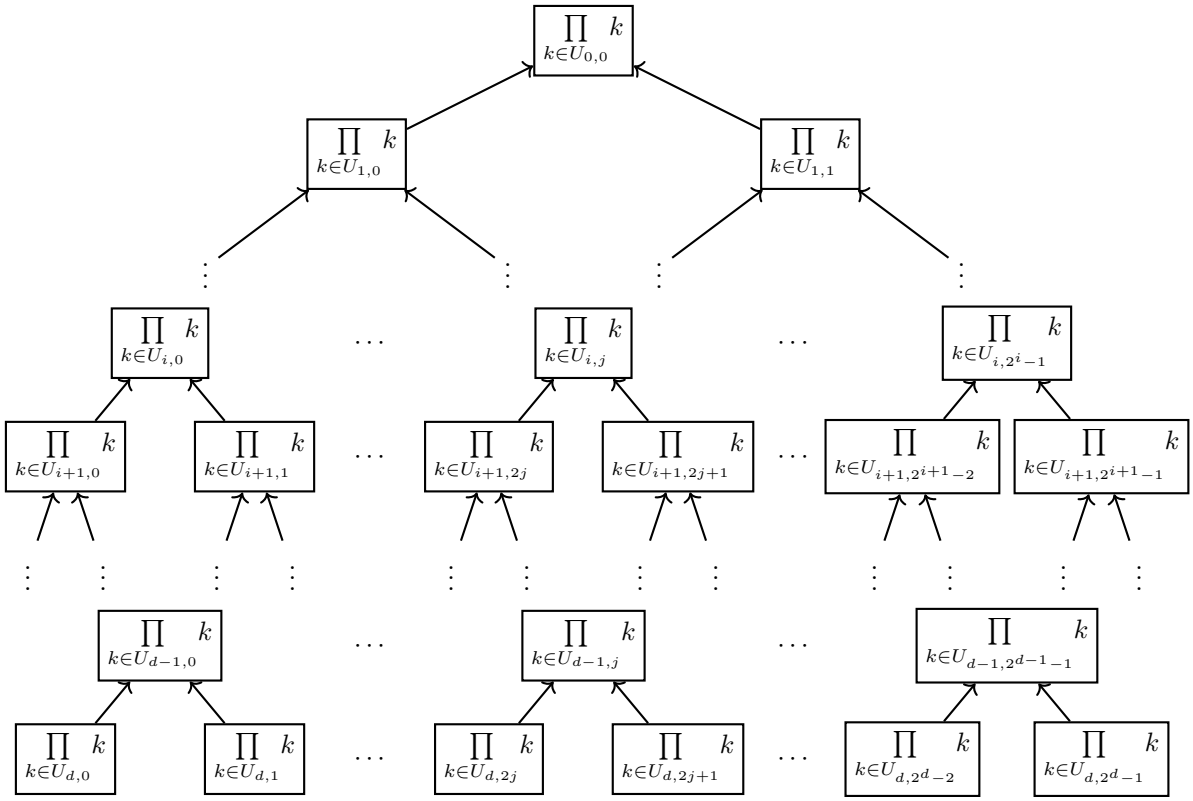


FIG. 2 : Arbre des sous-produits

pour $0 \leqslant i \leqslant d$ et $0 \leqslant j < 2^i$. On va construire un nouvel arbre binaire en partant de $W_{0,0} = 1$ et en se servant des relations de récurrence :

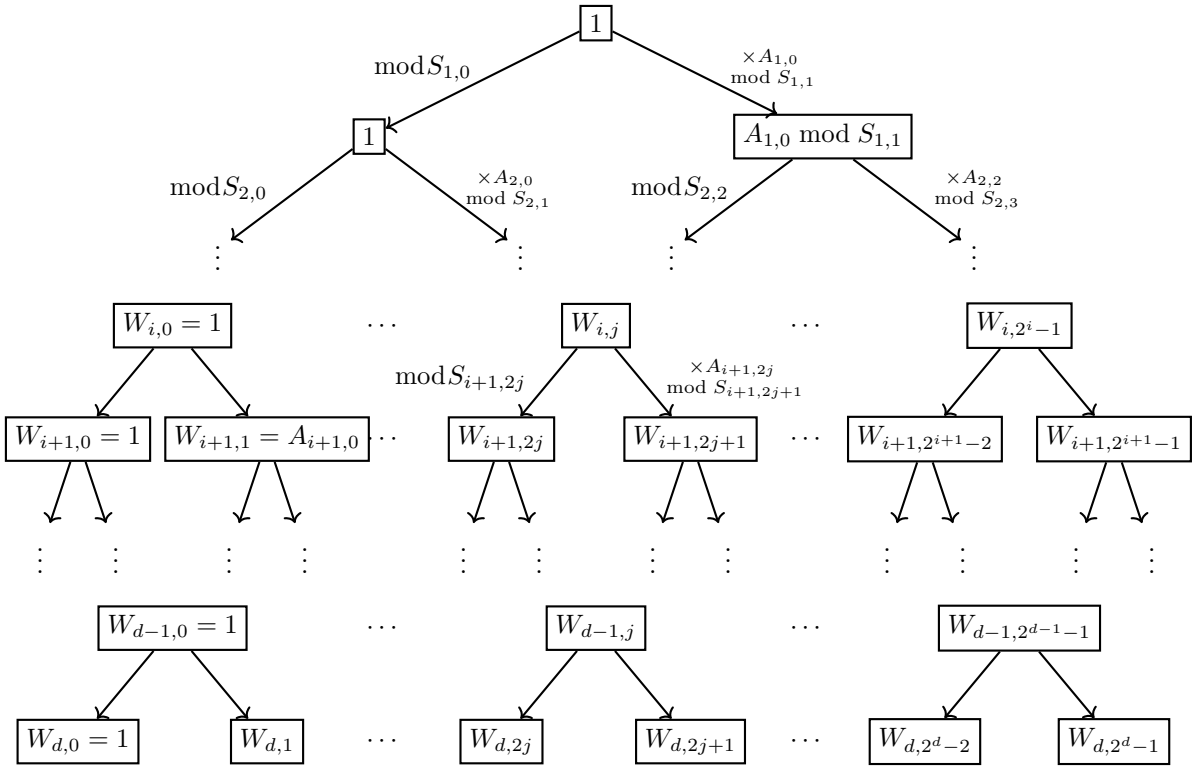
$$\begin{aligned} W_{i+1,2j} &= \prod_{l=0}^{2j-1} A_{i+1,l} \bmod S_{i+1,2j} \\ &= \prod_{l=0}^{j-1} A_{i+1,2l} A_{i+1,2l+1} \bmod S_{i+1,2j} \\ &= \prod_{l=0}^{j-1} A_{i,l} \bmod S_{i+1,2j} \\ &= W_{i,j} \bmod S_{i+1,2j} \end{aligned}$$

et

$$\begin{aligned} W_{i+1,2j+1} &= \prod_{l=0}^{2j} A_{i+1,l} \bmod S_{i+1,2j+1} \\ &= A_{i+1,2j} \prod_{l=0}^{j-1} A_{i+1,2l} A_{i+1,2l+1} \bmod S_{i+1,2j+1} \\ &= A_{i+1,2j} \prod_{l=0}^{j-1} A_{i,l} \bmod S_{i+1,2j+1} \\ &= A_{i+1,2j} W_{i,j} \bmod S_{i+1,2j} \end{aligned}$$

On construit enfin l'arbre suivant :

En récupérant les $W_{d,j}$ qui nous intéressent on obtient le résultat.



Avant de mettre en place cet algorithme, il convient d'établir la liste des entiers premiers plus petits que N. On utilise pour cela un crible de Eratosthène :

Données : $N \in \mathbb{N}$
Résultat : La liste des entiers premiers inférieurs à N, dans l'ordre croissant

$L \leftarrow [\![2; N]\!]$;
$res \leftarrow []$ la liste vide ;
$d \leftarrow \lfloor \sqrt{N} \rfloor$;
$a \leftarrow 2$;
tant que $a \leqslant d$ **faire**
  Ajouter a à la fin de res ;
  $b \leftarrow 0$;
  pour i *allant de* 1 *à* $\lfloor N/a \rfloor$ **faire**
    $b \leftarrow b + a$;
    Retirer b de L
  $a \leftarrow$ le plus petit élément de L.
Ajouter L à la fin de res. **retourner** res

Algorithme 10 : crible d'Eratosthène

Remarque 1.2.2.3. — *En pratique si on enlève un élément de L codée par exemple par un tableau python, on doit effectuer une recherche de b à chaque fois que l'on veut l'enlever puisque sa place dans L varie. On préférera associer à chaque élément de la liste un booléen qui vaudra « Faux » dès qu'un élément aura déjà été regardé (soit parce qu'on sait qu'il est premier, soit parce qu'on sait qu'il ne l'est pas). Afin d'accéder au « plus petit élément de L », on cherchera simplement le premier dont le booléen vaut vrai. On retiendra l'indice de cet élément pour ne pas avoir à consulter le début de la liste à chaque étape. Comme on ne parcourra la liste à la recherche des booléens « Vrai » qu'une seule fois, cela aura un coût en $O(N)$ qui sera négligeable.*
On supposera donc dans l'algorithme précédent qu'enlever un élément de L et prendre son plus petit élément à un coût constant.
Une remarque similaire peut-être faite si res a une structure de liste (ie un objet dont on connait

la tête, et un pointeur vers le reste de la liste ; c'est la structure privilégiée lorsque comme ici on ne connait pas la taille précise des données) puisqu'on ne peut pas alors alors ajouter d'élément à la fin de la liste en temps constant. On peut en revanche le faire au début de la liste. Il suffira à la fin de renverser la liste ce qui peut être fait en $O(N)$ opérations également.

Cet algorithme effectue une étape pour chaque p premier plus petit que $\sqrt{N}$, dont le coût est N/p addition d'entiers écrits sur au plus $O(\log(N))$ bits. En reprenant les équivalents donnés par le théorème des nombres premiers on voit que cet algorithme termine en $O(\sum_{k=1}^{\sqrt{N}/\log(N)} \frac{N}{k\log(k)})$ addition d'entiers écrits sur $\log(N)$ bits, soit encore $O(N\log(N)\log\log(N))$ opérations binaires.

On peut passer au cœur de l'algorithme :

Données : $N \in \mathbb{N}$
Résultat : $(p-1)! \bmod p^2$ pour $p \leqslant N$ premier

$d \leftarrow \lceil \log_2(N) \rceil$;
Calculer L la liste de nombres premiers inférieurs à N ;
Calculer récursivement l'arbre des sous-produits ;
Calculer récursivement l'arbre binaire des diviseurs successifs ;
Calculer les emplacements des p premiers parmi les feuilles de l'arbre des diviseurs ;
Calculer récursivement l'arbre des $W_{i,j}$;
retourner *les feuilles de cet arbre qui nous intéressent*

Algorithme 11 : Algorithme efficace de calcul de plusieurs factorielles

Remarque 1.2.2.4. — *En pratique on calcule l'arbre des sous-produits et l'arbre des diviseurs en même temps que l'on calcule l'emplacement des nombres premiers parmi les feuilles de l'arbre des diviseurs. On peut faire ceci en ajoutant par exemple à la fonction récursive qui effectuerait le calcul, un « compteur » qui indiquerait notre position dans l'arbre.*

Cela justifie le fait de considérer que le calcul des emplacements des p premiers parmi les feuilles de l'arbre des diviseurs soit considéré comme d'un coût négligeable.

On note $C(n)$ le coût en opérations binaires du calcul de l'arbre des sous-produits, d'un produit de n entiers écrits sur au plus $\log(N)$ bits. On effectue $O(1)$ multiplications d'entiers de taille au plus $N/2\log_2(N/2)$, et 2 appels récursifs ce qui conduit à :

$$C(n) = O(n\log^2(n)\log\log(n)) + 2C(\lceil n/2 \rceil)$$

et enfin

$$C(n) = O(n\log^3(n)\log\log(n)).$$

Le calcul de l'arbre des diviseurs a un coût similaire (En fait puisqu'on ne fait des multiplications que sur des nombres premiers, on peut montrer que ce coût n'est qu'en $O(n\log^2(n)\log\log(n))$, mais cela n'a pas d'importance).
Comme le calcul d'une division euclidienne dans $\mathbb{N}$ est peu ou prou le même que celui d'une multiplication dans $\mathbb{Z}$ (voir A.7), on en déduit un coût du même ordre de grandeur pour le calcul de l'arbre des $W_{i,j}$ ce qui donne le résultat.

Théorème 1.2.2.5. — *Le calcul des $(p-1)! \bmod p^2$ pour tous les p premiers inférieurs ou égaux à N peut s'effectuer en $O(N\log^3(N)\log\log(N))$, soit en temps quasi-linéaire.*

2 Opérateurs différentiels en caractéristique positive

Cette section est consacrée à l'étude des algèbres d'opérateurs différentiels en caractéristique p et de la p-courbure, et particulier de son polynôme caractéristique.
Ces algèbres peuvent être vues comme un ensemble de polynômes en une variable ∂ à coefficients dans un anneau commutatif A différentiel (c'est à dire munie d'une dérivation), non commutatifs, où la multiplication vérifie la règle de commutation suivante :

$$\forall a \in A, \partial a = a\partial + a'.$$

Cette règle de commutation découle de l'action de l'algèbre des opérateurs différentiels sur A et de la règle de Leibniz :

$$\forall a, b \in A, (ab)' = ab' + a'b.$$

La première partie de cette section sera consacrée à l'étude superficielle d'algèbres de "polynômes non commutatifs" plus générales : les algèbres de polynômes de Ore, dont l'objet qui nous intéresse sera un cas particulier.
Ce travail accompli, nous restreindrons notre étude à une classe particulière d'algèbres d'opérateurs différentiels définis sur des anneaux de caractéristique p et définirons la p-courbure d'un opérateur différentiel. Nous étudierons également son rôle dans la résolution d'équations différentielles linéaires, en évoquant en particulier les conséquences de sa nullité, ou de sa nilpotence. L'objet principal de cette partie sera d'introduire les objets théoriques nécessaires à l'élaboration d'un algorithme de calcul rapide du polynôme caractéristique de cette p-courbure, lequel sera présenté en section 3.

2.1 Algèbres de polynômes de Ore

2.1.1 Construction classique

Définition 2.1.1.1. — *Soit $\mathfrak{A}$ un anneau commutatif et $\theta : \mathfrak{A} \to \mathfrak{A}$ un endomorphisme. On définit une θ-dérivation sur $\mathfrak{A}$ comme étant une application $\partial : \mathfrak{A} \to \mathfrak{A}$ additive vérifiant la règle de Leibniz tordue :*

$$\forall a, b \in \mathfrak{A}, \partial(ab) = \theta(a)\partial(b) + \partial(a)b$$

Remarque 2.1.1.2. — *Dans le cas où $\theta = \mathrm{Id}_{\mathfrak{A}}$, il ne s'agit de rien d'autre que de la règle de Leibniz classique. On parlera alors simplement de dérivation.*

On suppose désormais que $\mathfrak{A}$ est fixé, ainsi que $\theta : \mathfrak{A} \to \mathfrak{A}$ et $\partial : \mathfrak{A} \to \mathfrak{A}$ une θ-dérivation. On va définir une structure d'anneau particulière sur le $\mathfrak{A}$-module à gauche $\mathfrak{A}[X]$. On notera $\mathfrak{A}[X]$ muni de cette structure $\mathfrak{A}[X;\theta,\partial]$. On veut que cette structure soit munie d'un morphisme d'anneau $\mathfrak{A} \to \mathfrak{A}[X;\theta,\partial]$ induisant sa structure de $\mathfrak{A}$-module à gauche.
On désire de plus que $\mathfrak{A}$ puisse être vu comme un $\mathfrak{A}[X;\theta,\partial]$-module à gauche vérifiant :

$$\forall a \in \mathfrak{A}, X.a = \partial(a).$$

On veut donc naturellement que la multiplication sur $\mathfrak{A}[X;\theta,\partial]$ vérifie :

$$\forall a \in \mathfrak{A}, Xa = \theta(a)X + \partial(a).$$

Proposition 2.1.1.3. — *Il existe une unique loi de composition sur $\mathfrak{A}[X;\theta,\partial]$ le munissant d'un morphisme $\mathfrak{A} \to \mathfrak{A}[X;\theta,\partial]$ induisant sa structure de $\mathfrak{A}$-module à gauche, et vérifiant de plus*

$$\forall a \in \mathfrak{A}, Xa = \theta(a)X + \partial(a)$$

et

$$\forall i \in \mathbb{N}, X.X^i = X^{i+1}$$

Preuve. **Unicité :** Si une telle loi existe, elle est obligatoirement $\mathfrak{A}$-linéaire, ie $\forall a \in \mathfrak{A}, \forall P, Q, R \in \mathfrak{A}[X;\theta,\partial]$, $(aP+R).Q = a(P.Q) + R.Q$.

Lemme 2.1.1.4. — *Si une telle loi existe alors elle vérifie $X^i.X^j = X^{i+j}$ pour tout $i, j \in \mathbb{N}$*

Cela se fait immédiatement par récurrence sur $i+j$. Par $\mathfrak{A}$-linéarité, on en déduit que pour tout $P(X)=\sum_i a_iX^i$ on a

$$P(X)X^j=\sum_i a_iX^{i+j}. \tag{2.1.1.1}$$

LEMME 2.1.1.5. — *Si deux telles lois $\cdot_1$ et $\cdot_2$ existent alors elles coïncident sur $\{X^i|i\in\mathbb{N}\}\times\mathfrak{A}$.*

Preuve. La preuve s'effectue encore par récurrence sur i. On sait déjà que le résultat est vrai pour $i=0,1$. Supposons à présent qu'il soit vrai pour $i\in\mathbb{N}$. Alors $X^i\cdot_1 a=P(X)=X^i\cdot_2 a$ et

$$\begin{aligned}
X^{i+1}\cdot_1 a &= X^i\cdot_1(X\cdot_1 a)\\
&= X^i\cdot_1(aX+a')\\
&= X^i\cdot_1(a\cdot_1 X)+X^i\cdot_1 a'\\
&= (X^i\cdot_1 a)\cdot_1 X+X^i\cdot_1 a'\\
&= (X^i\cdot_2 a)\cdot_1 X+X^i\cdot_2 a'\\
&= (X^i\cdot_2 a)\cdot_2 X+X^i\cdot_2 a' \text{ par (2.1.1.1)}\\
&= X^i\cdot_2(aX+a')\\
&= X^i\cdot_2(X\cdot_2 a)\\
&= X^{i+1}\cdot_2 a
\end{aligned}$$

□

On en déduit encore par $\mathfrak{A}$-linéarité pour tout $P(X)\in\mathfrak{A}[\theta,\partial,X]$ que deux telles lois $\cdot_1$ et $\cdot_2$ vérifient

$$P(X)\cdot_1 a=P(X)\cdot_2 a \tag{2.1.1.2}$$

et encore en combinant (2.1.1.1) et (2.1.1.2)

$$P(X)\cdot_1(aX^j)=(P(X)\cdot_1 a)X^j=(P(X)\cdot_2 a)X^j=P(X)\cdot_2(aX^j) \tag{2.1.1.3}$$

et enfin l'unicité par distributivité.

Existence.
Le travail effectué lors de la preuve de l'unicité fournit une unique loi de composition dont il reste à voir qu'elle vérifie les bonnes propriétés (distributivité et associativité). Par construction, elle vérifie pour tout $a,b\in\mathfrak{A}$:

$$X^{i+1}a=X^i(Xa) \tag{2.1.1.4}$$

$$(aX^i)(bX^j)=a(X^ib)X^j \tag{2.1.1.5}$$

$$(\sum_i a_iX^i)(\sum_j b_jX^j)=\sum_{i,j}(a_iX^i)(b_jX^j) \tag{2.1.1.6}$$

et par ailleurs

$$X(a+b)=\theta(a+b)X+\partial(a+b)=\theta(a)X+\theta(b)X+\partial(a)+\partial(b)=Xa+Xb. \tag{2.1.1.7}$$

et

$$\begin{aligned}
X(ab) &= \theta(ab)X+\partial(ab)\\
&= \theta(a)\theta(b)X+\theta(b)X+\theta(a)\partial(b)+\partial(a)b\\
&= \theta(a)(\theta(b)X+\partial(b))+\partial(a)b\\
&= \theta(a)(Xb)+\partial(a)b
\end{aligned}$$

soit

$$X(ab)=(Xa)b. \tag{2.1.1.8}$$

Par récurrence en combinant (2.1.1.4),(2.1.1.5) et (2.1.1.7) on en déduit

$$X^i(a+b) = X^i a + X^i b \tag{2.1.1.9}$$

ce qui combiné à (2.1.1.6) donne la distributivité. Pour l'associativité on voit par (2.1.1.5) et (2.1.1.6) que l'on a pour tout $a \in \mathfrak{A}$ et tout $P(X), Q(X) \in \mathfrak{A}[X;\theta,\partial]$:

$$(aP(X))Q(X) = a(P(X)Q(X)) \tag{2.1.1.10}$$

et

$$P(X)(Q(X)X^n) = (P(X)Q(X))X^n. \tag{2.1.1.11}$$

Les égalités (2.1.1.11) et (2.1.1.5) ensemble montrent que pour tout $i \in \mathbb{N}$, tout $a \in \mathfrak{A}$ et tout $n \in \mathbb{N}$:

$$\begin{aligned}(X^{i+1}).(aX^n) &= (X^{i+1}a)X^n \\ &= (X^i(Xa))X^n \\ &= X^i(XaX^n)\end{aligned}$$

Et encore par distributivité, pour tout $P \in \mathfrak{A}[X;\theta,\partial]$:

$$X^{i+1}P(X) = X^i(XP(X))$$

et enfin par récurrence, pour tout $n, m \in \mathbb{N}$:

$$X^{n+m}P(X) = X^n(X^mP(X)). \tag{2.1.1.12}$$

D'autre part, (2.1.1.10) et (2.1.1.12) donnent pour $P = X^{n+m}$:

$$\begin{aligned}(aX^{n+m})Q(X) &= (a(X^nX^m))Q(X) \\ &= a(X^n(X^mQ(X))) \\ &= (aX^n)(X^mQ(X))\end{aligned}$$

soit :

$$((aX^n)X^m)Q(X) = (aX^n)(X^mQ(X))$$

et encore par distributivité :

$$(P(X)X^m)Q(X) = P(X)(X^mQ(X)) \tag{2.1.1.13}$$

pour tout $P(X)$ et $Q(X) \in \mathfrak{A}[X;\theta,\partial]$.
De plus en multipliant (2.1.1.8) par X^n on obtient par (2.1.1.11) :

$$\begin{aligned}(X(ab))X^n &= X(a(bX^n)) \\ &= ((Xa)b)X^n \\ &= (Xa)(bX^n)\end{aligned}$$

et donc par linéarité pour tout $Q(X) \in \mathfrak{A}[X;\theta,\partial]$:

$$X(aQ(X)) = (Xa)Q(X) \tag{2.1.1.14}$$

On applique (2.1.1.14) à $P(X) = (X^nb)$:

$$\begin{aligned}X((aX^n)b)) &= X(a(X^nb)) \text{ par (2.1.1.5)} \\ &= (Xa)(X^nb) \text{ par (2.1.1.14)} \\ &= ((Xa)X^n)b \text{ par (2.1.1.13)} \\ &= (X(aX^n))b \text{ par (2.1.1.5)}\end{aligned}$$

Et encore par linéarité pour tout $P(X) \in \mathfrak{A}[X;\theta,\partial]$ et tout $b \in \mathfrak{A}$:

$$X(P(X)b) = (XP(X))b.$$

On peut multiplier cette équation par X^n ce qui donne par (2.1.1.11), pour tout $P(X) \in \mathfrak{A}[X;\theta,\partial]$, tout $b \in \mathfrak{A}$ et tout $n \in \mathbb{N}$:

$$X(P(X)(bX^n)) = (XP(X))(bX^n)$$

et encore par linéarité pour tout $P(X), Q(X) \in \mathfrak{A}[X;\theta,\partial]$:

$$X(P(X)Q(X)) = (XP(X))Q(X) \tag{2.1.1.15}$$

Supposons alors que l'on ait $X^i(P(X)Q(X)) = (X^iP(X))Q(X)$ pour tout P et Q. On a alors :

$$\begin{aligned} X^{i+1}(P(X)Q(X)) &= (X^iX)(P(X)Q(X)) \\ &= X^i(X(P(X)Q(X))) \text{ par (2.1.1.13)} \\ &= X^i((XP(X))Q(X)) \text{ par (2.1.1.15)} \\ &= (X^i(XP(X)))Q(X) \text{ par hypothèse} \\ &= ((X^iX)P(X))Q(X) \text{ par (2.1.1.13)} \\ &= (X^{i+1}P(X))Q(X) \end{aligned}$$

Par récurrence et par $\mathfrak{A}$-linéarité on a donc enfin montrer l'associativité de cette loi de composition, et donc l'existence d'une structure de $\mathfrak{A}$-algèbre à gauche sur $\mathfrak{A}[X;\theta,\partial]$ vérifiant nos hypothèses. □

Quoique d'apparence peu élégante par la lourdeur des vérifications, cette construction présente de nombreux avantages, dont celui de connaître explicitement tous les éléments de $\mathfrak{A}[X;\theta,\partial]$ et sa structure de $\mathfrak{A}$-module à gauche.
En revanche cette construction ne rend pas compte des morphismes de $\mathfrak{A}[X;\theta,\partial]$ vers les objets de la catégorie des anneaux. C'est pourquoi on présente une autre construction de cette algèbre par des algèbres de « polynômes non commutatifs ». Cette autre construction rend ardus les tests d'égalité, mais donne un certain nombre de propriétés universelles (une seule en fait, mais c'est déjà bien) qui nous seront utiles par la suite.
Pareillement on étudiera au cours de ce document de nombreux objets que l'on verra comme des $\mathfrak{A}[X;\theta,\partial]$-modules à gauche. La seconde construction permettra de voir facilement que de tels modules ne sont rien d'autre qu'un $\mathfrak{A}$-module à gauche munie d'une θ-connexion (ce que l'on définira en temps voulu).
Bien sûr on montrera que les deux constructions sont équivalentes.

2.1.2 Construction par des algèbres de « polynômes »

Le but de cette sous-section est d'introduire des algèbres possédant des propriétés similaires aux algèbres de polynômes dans le cas commutatifs, notamment un équivalent du morphisme d'évaluation. La principale difficulté vient de la nécessité de rendre compte de l'absence de commutativité entre les variables et les coefficients.

Définition 2.1.2.1. — *Soit R un anneau commutatif et M un R-module. On définit la R-algèbre libre associée à M :*

$$\mathcal{A}_R(M) = \bigoplus_{n\in\mathbb{N}} M^{\otimes n}$$

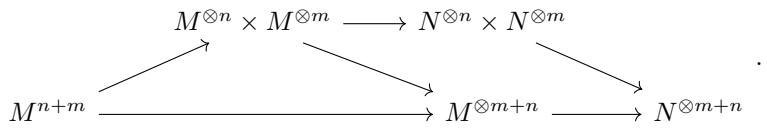
avec par convention $M^{\otimes 0} = R$.
On a

$$\begin{array}{rcl} M^{\otimes n} \times M^{\otimes m} & \to & M^{\otimes m+n} \\ (m_{0,1} \otimes \cdots \otimes m_{0,n}, m_{1,1} \otimes \cdots \otimes m_{1,m}) & \mapsto & m_{0,1} \otimes \cdots \otimes m_{0,n} \otimes m_{1,1} \otimes \cdots \otimes m_{1,m} \end{array}$$

Et par linéarité on en déduit le produit sur $\mathcal{A}_R(M)$

Proposition 2.1.2.2. — $\mathcal{A}_R : R\text{-}\mathbf{mod} \to R\text{-}\mathbf{Alg}$ *est un foncteur, adjoint à gauche du foncteur d'oubli* $U : R\text{-}\mathbf{Alg} \to R\text{-}\mathbf{mod}$.

Preuve. Soient M et N deux R-modules. Soit $\varphi : M \to N$ un morphisme de R-modules.
φ induit une application n-linéaire de $M^n \to N^{\otimes n}$ pour tout n et donc $M^{\otimes n} \to N^{\otimes n}$. On en déduit $\mathcal{A}_R(\varphi) : \mathcal{A}_R(M) \to \mathcal{A}_R(N)$ par linéarité.
Il faut voir qu'il s'agit bien d'un morphisme d'anneaux, mais cela vient de la commutativité du diagramme suivant :



La fonctorialité est immédiate.
Soient M un R-module et A une R-algèbre. Comme $M \subset \mathcal{A}_R(M)$ on en déduit par restriction :

$$\eta_{M,A} : \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(\mathcal{A}_R(M), A) \hookrightarrow \mathrm{Hom}_{R\text{-}\mathbf{mod}}(\mathcal{A}_R(M), A) \to \mathrm{Hom}_{R\text{-}\mathbf{mod}}(M, A)$$

On vérifie immédiatement que les $\eta_{M,A}$ induisent une transformation naturelle

$$\eta : \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(\mathcal{A}_R(-), -) \Rightarrow \mathrm{Hom}_{R\text{-}\mathbf{mod}}(-, -).$$

Il reste à voir que c'est un isomorphisme.
L'injectivité est évidente : si $\varphi, \psi : \mathcal{A}_R(M) \to A$ coïncident sur M, alors ils coïncident sur tous les tenseurs purs (par multiplicativité), donc sur $\mathcal{A}_R(M)$.
Si, d'autre part, $\varphi : M \to A$ est un morphisme de R-modules, on en déduit que $M^n \to A$ est multilinéaire et donc induit une application $M^{\otimes n} \to A$ qui, à son tour, induit $\overline{\varphi} : \mathcal{A}_R(M) \to A$. C'est de plus un morphisme d'algèbres. Cela se voit car l'application

$$\begin{array}{rcl} M^{\otimes n} \times M^{\otimes m} & \to & A \\ (a, b) & \mapsto & \overline{\varphi}(a)\overline{\varphi}(b) \end{array}$$

est bilinéaire et donc se factorise en $M^{\otimes(n+m)} \to A$.
$\eta_{M,A}$ est donc surjective ce qui achève la démonstration. □

Par la suite nous ne noterons pas le foncteur d'oubli. Le contexte dira si les objets doivent être considérés comme des R-algèbres ou des R-modules.

Définition 2.1.2.3 (**Anneau de « polynômes » non commutatifs**). — *Soit A une R-algèbre. On pose :*

$$A_R\langle X\rangle := {}^{\mathcal{A}_R(A[X])}/_I$$

où I est l'idéal bilatère de $\mathcal{A}_R(A[X])$ engendré par :

$$\{ab - a \otimes b | a, b \in A\} \cup \{X^{n+m} - X^n \otimes X^m | n, m \in \mathbb{N}\} \cup \{aX^n - a \otimes X^n | a \in A, n \in \mathbb{N}\}.$$

Remarque 2.1.2.4. — *On remarque que cette construction dépend de l'anneau de base R. Cela permet par exemple dans le cas où A est commutatif de construire des anneaux de polynômes en plusieurs variables ne commutant pas entre elles, mais commutant avec les coefficients, ou non selon les besoins. Dans la suite de cette sous-section lorsque R sera sous-entendu on notera simplement $A\langle X\rangle$.*

Proposition 2.1.2.5. — *Il existe un morphisme $i : A \to A\langle X\rangle$.*

Preuve. On a une injection $\tilde{i} : A \to A[X] \to \mathcal{A}_R(A[X])$ en tant que R-modules. On en déduit donc un morphisme de R-modules $i : A \to A\langle X\rangle$. Il suffit de montrer qu'il est multiplicatif. Or c'est le cas car $ab = a \otimes b$ pour tout $a, b \in A$ dans $A\langle X\rangle$. □

Proposition 2.1.2.6. — *Soit B une R-algèbre. On a une bijection*

$$\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A\langle X\rangle, B) \to \left\{ \varphi \in \mathrm{Hom}_{R\text{-}\mathbf{mod}}(A[X], B) \;\middle|\; \begin{cases} \forall a, b \in A, \varphi(ab) = \varphi(a)\varphi(b) \\ \forall n, m \in \mathbb{N}, \varphi(X^{n+m}) = \varphi(X^n)\varphi(X^m) \\ \forall (n, a) \in \mathbb{N} \times A, \varphi(aX^n) = \varphi(a)\varphi(X^n) \end{cases} \right\}$$

Preuve. Soit $\varphi \in \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A\langle X\rangle, B)$. On en déduit $\varphi' : \mathcal{A}_R(A[X]) \twoheadrightarrow A\langle X\rangle \to B$ puis par oubli de la structure d'algèbre et restriction (par adjonction donc), un morphisme $\Psi(\varphi) : A[X] \to B$. D'autre part puisque φ' passe au quotient, on a :

$$\begin{aligned}
&\forall a, b \in A, && \Psi(\varphi)(ab) = \varphi'(ab) = \varphi'(a \otimes b) = \varphi'(a)\varphi'(b) = \Psi(\varphi)(a)\Psi\varphi(b)\\
&\forall n, m \in \mathbb{N}, && \Psi(\varphi)(X^{n+m}) = \varphi'(X^{n+m}) = \varphi'(X^n \otimes X^m) = \varphi'(X^n)\varphi'(X^m) = \Psi(\varphi)(X^n)\Psi(\varphi)(X^m)\\
&\forall (n, a) \in \mathbb{N} \times A, && \Psi(\varphi)(aX^n) = \varphi'(aX^n) = \varphi'(a \otimes X^n) = \varphi'(a)\varphi'(X^n) = \Psi(\varphi)(a)\Psi(\varphi)(X^n)
\end{aligned}$$

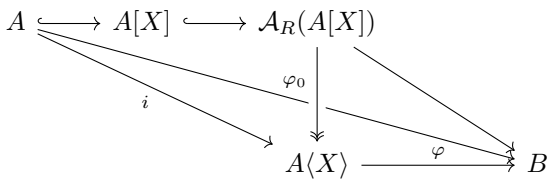
Réciproquement, de tout morphisme ψ de R-modules de $A[X]$ vers B on déduit (par adjonction) un morphisme d'algèbre de $\psi' : \mathcal{A}_R(A[X]) \to B$. De plus, par construction, on a :

$$\begin{aligned}
&\forall a, b \in A, && \psi'(ab - a \otimes b) = \psi'(ab) - \psi'(a \otimes b) = \psi(ab) - \psi(a)\psi(b) = 0\\
&\forall n, m \in \mathbb{N}, && \psi'(X^{n+m} - X^n \otimes X^m) = \psi(X^{n+m}) - \psi(X^n)\psi(X^m) = 0\\
&\forall (n, a) \in \mathbb{N} \times A, && \psi'(aX^n - a \otimes X^n) = \psi(aX^n) - \psi(a)\psi(X^n) = 0
\end{aligned}$$

Par passage au quotient on en déduit $\Phi(\psi) : A\langle X\rangle \to B$ vérifiant de plus $\Psi(\Phi(\psi)) = \psi$, d'où la surjectivité de Φ.
L'injectivité vient de ce que deux morphismes ayant même image par Ψ on forcément même morphisme induit de $\mathcal{A}_R(A[X]) \to B$ par adjonction et donc sont égaux. □

Corollaire 2.1.2.7 (**Morphisme d'évaluation**). — *Soit $\varphi_0 : A \to B$ un morphisme de R-algèbres. Pour tout $\xi \in B$ il existe un unique morphisme $\varphi : A\langle X\rangle \to B$ tel que $\varphi \circ i = \varphi_0$ et $\varphi(X) = \xi$.*

Preuve. Supposons l'existence d'un tel morphisme φ. Le diagramme suivant est commutatif dans la catégorie des R-modules



Si un tel morphisme existe, il induit alors un morphisme $\psi : A[X] \to B$ vérifiant les conditions de la proposition précédente. De plus les applications $A \hookrightarrow A[X] \xrightarrow{\psi} B$ et $A \xrightarrow{\varphi_0} B$ coïncident.
Or, on vérifie immédiatement qu'il existe un unique morphisme de R-modules de $A[X] \to B$ vérifiant les conditions de la proposition précédente et ce qui précède.
Par la proposition précédente il existe un unique $\varphi : A\langle X\rangle \to B$ correspondant. En outre, le diagramme ci-dessus commute par construction, ce qui achève la preuve. □

Corollaire 2.1.2.8. — *$i : A \to A\langle X\rangle$ est injectif.*

Preuve. Il suffit d'appliquer le corollaire précédent à $\varphi_0 = \mathrm{Id}_A$ et $\xi = 0$. □

Corollaire 2.1.2.9. — *Le morphisme de R-modules $A[X] \to A\langle X\rangle$ est injectif.*

Preuve. En reprenant la preuve du Corollaire 2.1.2.7 avec $B = A[X]$ et $\varphi_0 = A \hookrightarrow A[X]$ et $\xi = X$ on voit que $\psi = \mathrm{Id}_{A[X]}$ (même notation que dans la preuve) et on en déduit le résultat en regardant le diagramme. □

On termine ce point sur les « polynômes » non commutatifs par un lemme qui nous servira plus tard.

Proposition 2.1.2.10. — *Soit M un A-module. M est muni d'une structure de $A_R\langle X\rangle$-module à gauche si et seulement si M est muni d'un endomorphisme f R-linéaire. Il existe alors une unique structure de $A_R\langle X\rangle$-module à gauche sur M tel que $X.m = f(m)$ pour tout $m \in M$.*

Preuve. Si M est muni d'une structure de $A_R\langle X\rangle$-module à gauche, alors la multiplication par X est un endomorphisme R-linéaire.
Supposons maintenant que f soit un endomorphisme R-linéaire. Si M est muni d'une structure de $A\langle X\rangle$-module à gauche, alors cette structure est entièrement déterminée par le morphisme de R-algèbres suivant :

$$\begin{array}{ccc} A_R\langle X\rangle & \to & \mathrm{End}_{R\textbf{-mod}}(M) \\ P & \mapsto & (m \mapsto P.m) \end{array}$$

De plus, tout morphisme de $A_R\langle X\rangle \to \mathrm{End}_{R\textbf{-mod}}(M)$ définit une structure de $A_R\langle X\rangle$-module à gauche sur M. Or, on sait qu'il existe un unique tel morphisme de R-algèbres prolongeant $A \to \mathrm{End}_{R\textbf{-mod}}(M)$ dont l'image de X est f. □

Définition 2.1.2.11. — *Soit $\mathfrak{A}$ un anneau commutatif, $\theta : \mathfrak{A} \to \mathfrak{A}$ un endomorphisme et ∂ une θ-dérivation. On note*

$$\mathcal{D} := {}^{\mathfrak{A}_{\mathbb{Z}}\langle X\rangle}\!/_{J}$$

où J est l'idéal bilatère engendré par $\{Xa - \theta(a)X - \partial(a) | a \in \mathfrak{A}\}$.

Remarque 2.1.2.12. — *Nous venons de terminer la deuxième construction. Au vu de ce qui précède, il est aisé de voir pourquoi cette deuxième construction est « riche en propriété universelle ». L'idée de cette construction est de plus assez naturelle : au vu des propriétés d'évaluation de l'algèbre de polynômes, on se convainc assez naturellement que si une algèbre vérifie la règle de commutation des polynômes de Ore, alors il existe un morphisme de $\mathfrak{A}_{\mathbb{Z}}\langle X\rangle$ associant X à X, et alors J appartient à son noyau. Malheureusement cette construction rend les tests d'égalité extrêmement compliqué (il est difficile de voir quand un élément appartient à un idéal bilatère engendré par une famille d'éléments).*
La morale est qu'il n'existe pas de moyen d'échapper aux calculs effectués dans la première sous-section.

On reconnait la règle de commutation introduit auparavant lors de la définition de $\mathfrak{A}[X;\theta,\partial]$. On en déduit en particulier que le morphisme $\mathfrak{A}[X] \to \mathcal{D}$ est surjectif. Il reste à voir qu'il est injectif (en fait que les deux constructions coïncident).

Proposition 2.1.2.13. — $\mathcal{D} \simeq \mathfrak{A}[X;\theta,\partial]$.

Preuve. Par le Corollaire 2.1.2.7, il existe un unique morphisme φ de $\mathfrak{A}_{\mathbb{Z}}\langle X\rangle$ vers $\mathfrak{A}[X;\theta,\partial]$ tel que sa restriction à $\mathfrak{A}$ soit l'inclusion de $\mathfrak{A}$ dans $\mathfrak{A}[X;\theta,\partial]$ et tel que l'image de X soit X.
L'unique morphisme de $\mathbb{Z}$-modules qui s'en déduit de $\mathfrak{A}[X] \to \mathfrak{A}[X;\theta,\partial]$ est l'identité (on rappelle que $\mathfrak{A}[X;\theta,\partial]$ s'identifie à $\mathfrak{A}[X]$ en tant que $\mathfrak{A}$ module).
De plus, on a nécessairement $\varphi(Xa) = \varphi(\theta(a)X - \partial(a))$ pour tout $a \in \mathfrak{A}$, ce qui induit $\mathcal{D} \to \mathfrak{A}[X;\theta,\partial]$ et rend nécessairement injectif, donc bijectif, $\mathfrak{A}[X] \to \mathcal{D}$. On en déduit dès lors que le morphisme $\mathcal{D} \to \mathfrak{A}[X;\theta,\partial]$ est bijectif. □

L'équivalence des deux constructions étant établie, énonçons directement les propriétés qui avaient motivé ce travail

Définition 2.1.2.14. — *Soit M un $\mathfrak{A}$-module. On dit que M est un $\mathfrak{A}$-module θ-différentiel s'il est muni d'une application additive $f : M \to M$ vérifiant pour tout $a \in \mathfrak{A}$ et tout $m \in M$:*

$$f(am) = \theta(a)f(m) + \partial(a)m.$$

Une telle application est appelée θ-connexion.

Théorème 2.1.2.15. —

- *Soit $\varphi : \mathfrak{A} \to B$ un morphisme d'anneau. Pour tout $\xi \in B$ vérifiant pour tout $a \in \mathfrak{A}$, $\xi\varphi(a) = \varphi(\theta(a))\xi + \varphi(\partial(a))$ il existe un unique morphisme $\overline{\varphi} : \mathfrak{A}[X;\theta,\partial] \to B$ prolongeant φ tel que X ait pour image ξ. Par ailleurs cette propriété caractérise entièrement les morphismes d'anneaux ayant $\mathfrak{A}[X;\theta,\partial]$ pour domaine.*

- *Soit M un $\mathfrak{A}$-module. La donnée d'une structure de $\mathfrak{A}[X;\theta,\partial]$-module à gauche sur M est équivalente à celle d'une θ-connexion f sur M, la correspondance étant donnée par $X.m = f(m)$ pour tout $m \in M$.*

Preuve. Le premier point est évident.

Si M est muni d'une structure de $\mathfrak{A}[X;\theta,\partial]$-module à gauche alors la multiplication par X est une θ-connexion sur M.
Réciproquement, si M est muni d'une θ-connexion, on procède de la même manière que dans la preuve de la Proposition 2.1.2.10 : une structure de $\mathfrak{A}[X;\theta,\partial]$-module à gauche est entièrement déterminée par le morphisme d'anneaux :

$$\begin{array}{rcl} \mathfrak{A}[X;\theta,\partial] & \to & \mathrm{End}_{\mathbb{Z}\textbf{-mod}}(M) \\ P & \mapsto & (m \mapsto P.m) \end{array}$$

De plus tout tel morphisme d'anneaux définit une telle structure.
On note $\varphi : \mathfrak{A} \to \mathrm{End}_{\mathbb{Z}\textbf{-mod}}(M)$ le morphisme donné par la structure de $\mathfrak{A}$-module sur M.
Alors pour tout $m \in M$ et tout $a \in \mathfrak{A}$ on a :

$$\begin{aligned} f \circ \varphi(a)(m) &= f(am) \\ &= \theta(a)f(m) + \partial(a)m \\ &= \varphi(\theta(a)) \circ f(m) + \varphi(\partial(a))(m). \end{aligned}$$

D'après le premier point il existe un unique morphisme d'anneaux de $\mathfrak{A}[X;\theta,\partial] \to \mathrm{End}_{\mathbb{Z}\textbf{-mod}}(M)$ prolongeant φ et valant f en X. □

2.1.3 Propriétés des algèbres de polynômes de Ore et de leur modules cycliques

Nous allons maintenant énoncer un certain nombre de propriétés de $\mathfrak{A}[X;\theta,\partial]$ qui découlent plus de la première construction que l'on en a donnée.

On sait que $\mathfrak{A}[X;\theta,\partial] \simeq \mathfrak{A}[X]$ en tant que $\mathfrak{A}$-module à gauche. Il est donc possible de munir $\mathfrak{A}[X;\theta,\partial]$ d'une notion de degré.

Définition 2.1.3.1. — *Le degré d'un élément $L \in \mathfrak{A}[X;\theta,\partial]$ est le degré de son image par l'isomorphisme précédent. Dit autrement si $L = \sum_{i=0}^{d} l_i X^i$, alors son degré est le plus grand i pour lequel $l_i \neq 0$ (où les l_i sont des éléments de $\mathfrak{A}$).*

Proposition 2.1.3.2. — *Soit $P, Q \in \mathfrak{A}[X;\theta,\partial]$ et $a \in \mathfrak{A}$.*

$$\deg(aP) \leqslant \deg(P) \tag{2.1.3.1}$$
$$\deg(Pa) \leqslant \deg(P) \tag{2.1.3.2}$$
$$\deg(P+Q) \leqslant \max(\deg(P), \deg(Q) \tag{2.1.3.3}$$
$$\deg(PQ) \leqslant \deg(P) + \deg(Q) \tag{2.1.3.4}$$

Si, de plus, $\mathfrak{A}$ est intègre alors (2.1.3.1) est une égalité. Si, de plus, θ est injectif alors (2.1.3.2) et (2.1.3.4) sont des égalités. En ce cas, (2.1.3.4) montre que $\mathfrak{A}[X;\theta,\partial]$ est « intègre » (au sens où il n'a pas de diviseur non trivial de 0).
Si d'autre part $\deg(P) \neq \deg(Q)$ alors (2.1.3.3) est une égalité.

Preuve. La preuve de (2.1.3.3) et de (2.1.3.1) et de leur cas d'égalité respectifs sont les mêmes que dans le cas commutatif (puisqu'il ne s'agit que du comportement du degré vis-à-vis de la structure de $\mathfrak{A}$-module à gauche de $\mathfrak{A}[X;\theta,\partial]$).
On remarque avant de continuer la preuve qu'il est évident pour n'importe quel $P \in \mathfrak{A}[X;\theta,\partial]$ et n'importe quel $i \in \mathbb{N}$ que

$$\deg(PX^i) = \deg(P) + i.$$

Pour (2.1.3.2) on le voit par récurrence sur le degré de P. Supposons que le résultat soit vrai pour les polynômes de degré i. Alors

$$X^{i+1}a = X^i\theta(a)X + X^i\partial(a)$$

et donc par (2.1.3.3),

$$\deg(X^{i+1}a) \leqslant \max(X^i\theta(X)X, X^i\partial(a))$$

Par hypothèse de récurrence on a $\deg(X^i\theta(a)X) = \deg(X^i\theta(a)) + 1 \leqslant i+1$ (On remarque que si l'on est dans le cas d'égalité, l'inégalité se transforme en égalité) et $\deg(X^i\partial(a)) \leqslant i$ ce qui donne le résultat pour X^{i+1} puis établi la récurrence par linéarité (en utilisant (2.1.3.1) et (2.1.3.3)).
Pour (2.1.3.4) on écrit $P = \sum_{i=0}^{d_1} p_i X^i$ et $Q = \sum_{j=0}^{d_2} q_j X^j$ avec $p_{d_1} \neq 0$ et $q_{d_2} \neq 0$. On a alors :

$$\begin{aligned}\deg(PQ) &= \deg\left(\sum_{i,j} p_i X^j q_j X^j\right)\\ &\leqslant \max_{i,j}(\deg(p_i X^i q_j X^j))\\ &\leqslant \max_{i,j}(\deg(X^i q^j) + j)\\ &\leqslant \max_{i,j}(i+j)\\ &\leqslant d_1 + d_2\end{aligned}$$

De plus, toutes les inégalités se transforment en égalités dans le cas d'égalité (la première aussi, même si rétrospectivement). □

Remarque 2.1.3.3. — *Dans le cas où $\mathfrak{A}$ est intègre et θ est injectif, on constate que le coefficient dominant de PQ (en reprenant les notations de la preuve précédente) est $p_{d_1}\theta^{d_1}(q_{d_2})$.*
En effet son coefficient dominant est donné par celui de $p_{d_1}X^{d_1}q_{d_2}X^{d_2}$. On peut procéder par récurrence sur d_1 pour voir qu'il s'agit bien de $p_{d_1}\theta^{d_1}(q_{d_2})$.

On suppose désormais que $\mathfrak{A}$ est un corps K. Dans ce cas là, θ est injectif et $\mathfrak{A}$ est intègre, nous sommes donc dans le cas d'égalité de (2.1.3.4). On en déduit directement que $K[X;\theta,\partial]$ est « intègre » (même s'il n'est pas commutatif).
On a en fait mieux que ça car $K[X;\theta,\partial]$ est muni d'un équivalent de la division euclidienne des polynômes.

Proposition 2.1.3.4 (Division euclidienne à droite). — *Soient $A, B \in K[X;\theta,\partial]$ avec $B \neq 0$. Il existe un unique couple $(Q,R) \in K[X;\theta,\partial]$ avec $\deg(R) < \deg(B)$ tel que*

$$A = QB + R$$

Preuve. La preuve est essentiellement la même que dans le cas commutatif.
La preuve de l'unicité est exactement la même que dans le cas commutatif.
Montrons donc l'existence d'un tel couple. On suppose que B n'est pas de degré 0, car s'il l'était, B serait central et inversible et donc l'énoncé serait trivial.
Nous allons procéder par récurrence sur le degré de A. Pour tout A vérifiant $\deg(A) \leqslant \deg(B)$ on peut prendre $(Q,R) = (0,A)$.
Un suppose qu'un tel couple (Q,R) existe pour tout A de degré au plus $k \geqslant \deg(B) - 1$. Soit A de degré $k+1$. On peut écrire $A = a_{k+1}X^{k+1} + A'$ où A' est de degré au plus k (à ne pas confondre avec le polynôme dérivé de A). Notons b_r le coefficient dominant de B. On pose

$$\rho := \frac{a_{k+1}}{\theta^{k+1-\deg(B)}(b_r)}.$$

Alors $\rho X^{k+1-\deg(B)}B$ est de degré $k+1$ de coefficient dominant a_{k+1}. On en déduit que

$$A_1 = A - \rho X^{k+1-\deg(B)}B$$

et de degré au plus k. Par hypothèse de récurrence, il existe donc $(Q_1,R) \in K[X;\theta,\partial]$ avec $\deg(R) < \deg(B)$ tel que

$$A_1 = Q_1 B + R$$

et encore

$$A = \left(\frac{a_{k+1}}{\theta^{k+1-\deg(B)}(b_r)}X^{k+1-\deg(B)} + Q_1\right)B + R.$$

La récurrence est donc établie. □

Remarque 2.1.3.5 (Division euclidienne à gauche). — *Une question naturelle après avoir fait cela est de se demander si l'on peut effectuer des divisions euclidiennes à gauche, c'est-à-dire s'il existe un unique couple* (Q_1, R_1) *avec* $\deg(R_1) < \deg(B)$ *tel que*

$$A = BQ_1 + R_1.$$

Si la preuve de l'unicité d'un tel couple reste inchangée, l'existence n'est pas vraie en général. Elle l'est si θ *est surjectif, c'est-à-dire si c'est un automorphisme de* K*. Dans ce cas on peut remplacer la définition de* ρ *dans la preuve de l'existence par*

$$\rho := \frac{\theta^{-\deg(B)}(a_{k+1})}{b_r}$$

(et mettre les multiplications par B *à gauche), ce qui donne le résultat.*

Remarque 2.1.3.6. — *On constate immédiatement que le quotient de la division euclidienne de* A *par* B *(à droite ou à gauche) est de degré* $\deg(A) - \deg(B)$ *(si* $\deg(A) \geqslant \deg(B)$*).*

Corollaire 2.1.3.7. — $K[X;\theta,\partial]$ *est « principal à gauche » ie tous ses idéaux à gauche sont de la forme* $K[X;\theta,\partial]L$ *pour un certain* L *dans* $K[X;\theta,\partial]$*. Ce* L *est de plus unique à multiplication par un élément de* K *près. La preuve est la même que celle de « euclidien⇒ principal » dans le cas commutatif.*
Pareillement si θ *est surjectif, alors* $K[X;\theta,\partial]$ *est « principal à droite ».*

De même que dans le cas commutatif on peut alors définir des notions de pgcd et ppcm. Cependant tout comme la division euclidienne, la notion de divisibilité dépend du choix de la faire à gauche ou à droite. Pour A et $B \in K[X;\theta,\partial]$ on dira que B est un diviseur à droite de A, et A un multiple à gauche de B s'il existe $Q \in K[X;\theta,\partial]$ tel que $A = QB$.
Symétriquement on peut définir la notion de diviseur à gauche et de multiple à droite.

Définition 2.1.3.8. — *Soient* A *et* $B \in K[X;\theta,\partial]$*. On définit le plus grand diviseur commun à droite de* A *et* B*, que l'on note* $\mathrm{rgcd}(A,B)$ *l'unique polynôme de Ore* D *(à multiplication par un élément de* K *près) vérifiant :*

$$K[X;\theta,\partial]D = K[X;\theta,\partial]A + K[X;\theta,\partial]B.$$

On définit également leur plus petit multiple commun à gauche, noté $\mathrm{llcm(A,B)}$*, l'unique polynôme de Ore* M *(encore une fois à multiplication par un élément de* K *près) vérifiant :*

$$K[X;\theta,\partial]M = K[X;\theta,\partial]A \cap K[X;\theta,\partial]B.$$

Remarque 2.1.3.9. — *Si* $K[X;\theta,\partial]$ *est muni d'une division euclidienne à gauche, on définit similairement les notions de plus grand diviseur commun à gauche, noté* lgcd*, et de plus petit multiple commun à droite, noté* rlcm*, en considérant des idéaux à droite.*

Proposition 2.1.3.10. — *Comme dans le cas commutatif on voit que tout diviseur commun à droite (resp. à gauche) de* A *et* B *est un diviseur à droite de* $\mathrm{rgcd}(A,B)$ *(resp. à gauche de* $\mathrm{lgcd}(A,B)$*).*
De même tout multiple commun à gauche (resp. à droite) de A *et* B *et un multiple à gauche de* $\mathrm{llcm}(A,B)$ *(resp. à droite de* $\mathrm{rlcm}(A,B)$*).*
L'algorithme d'Euclide s'adapte par ailleurs très bien à ce cadre pour calculer $\mathrm{rgcd}(A,B)$ *(ou* $\mathrm{lgcd}(A,B)$ *selon les besoins), ainsi que les coefficients de Bézout.*

Nous allons maintenant nous intéresser à quelques propriétés des modules cycliques sur $K[X;\theta,\partial]$.

Définition 2.1.3.11. — *Un* $K[X;\theta,\partial]$*-module à gauche est dit cyclique s'il est engendré par un unique élément* x*.*

Soit M un $K[X;\theta,\partial]$-module à gauche cyclique et x un élément générateur. Alors le morphisme de $K[X;\theta,\partial]$-modules à gauche

$$\begin{array}{ccc} K[X;\theta,\partial] & \to & M \\ P & \mapsto & P.x \end{array}$$

est surjectif et son noyau est un idéal à gauche de $K[X;\theta,\partial]$, donc de la forme $K[X;\theta,\partial]P$ pour un certain P.
On en déduit que M est de la forme

$$M_P := {}^{K[X;\theta,\partial]}\!/_{K[X;\theta,\partial]P}.$$

PROPOSITION 2.1.3.12. — *L'application $A \mapsto M_A$ réalise une bijection de l'ensemble des diviseurs à droite unitaires de P (pour $P \in K[X;\theta,\partial]$) et l'ensemble des quotients de M_P.*

Preuve. Soit M un tel quotient. Alors la composée des surjections $k[X;\theta,\partial] \to M_P \to M$ a pour noyau un certain $K[X;\theta,\partial]A$ donc $M \simeq M_A$. Ce A est unique si on exige de plus qu'il soit unitaire. D'autre part P est dans le noyau de cette application donc A est un diviseur de P à droite. Réciproquement M_A, où A divise P à droite, peut être vu comme un quotient de M_P puisque l'on a un morphisme surjectif $M_P \twoheadrightarrow M_A$ obtenue par factorisation canonique. □

REMARQUE 2.1.3.13. — *On a une bijection au sens où tous les quotients de M_P sont de cette forme, et tout diviseur à droite de P définit un quotient de M_P. En revanche il n'est pas vrai en général qu'une classe de quotients de M_P à isomorphisme près soit définie par un unique diviseur à droite de P.*

PROPOSITION 2.1.3.14. — *Soit $P, A, B \in K[X;\theta,\partial]$ tels que $P = BA$. Il existe alors une suite exacte de $K[X;\theta,\partial]$-modules à gauche :*

$$0 \to M_B \xrightarrow{f_1} M_P \xrightarrow{f_2} M_A \to 0$$

où f_1 est donnée par la multiplication à droite par A et f_2 est induite par factorisation canonique.

Preuve. Montrons d'abord que f_1 et f_2 sont bien définies.
On a un morphisme de $K[X;\theta,\partial]$-modules à gauche

$$\begin{array}{rccc} \tilde{f_1} : & K[X;\theta,\partial] & \to & M_P \\ & Q & \mapsto & QA \end{array}$$

et B fait partie de son noyau. f_1 est donc bien définie par factorisation canonique. Par ailleurs f_1 est injective. En effet, si $Q \in \ker(\tilde{f}_1))$ alors il existe $L \in K[X;\theta,\partial]$ tel que $QA = LP = LBA$ et, par intégrité de $K[X;\theta,\partial]$, on en déduit que Q est un multiple à gauche de B.
Par ailleurs, P est évidemment dans le noyau de la projection canonique de $K[X;\theta,\partial]$ sur M_A. L'application f_1 est donc bien définie et surjective.
Il est évident que $\mathrm{Im}\,(f_1) \subset \ker(f_2)$. Réciproquement supposons $\overline{Q} \in \ker(f_2)$ et Q un rélèvement de $\overline{Q}$ dans $K[X;\theta,\partial]$. Alors il existe L tel que $Q = LA$ et donc $\overline{Q} = f_1(\overline{L})$. □

PROPOSITION 2.1.3.15. — *Soient $A, B \in K[X;\theta,\partial]$. On a une suite exacte :*

$$0 \to M_{\mathrm{llcm}(A,B)} \xrightarrow{f_1} M_A \oplus M_B \xrightarrow{f_2} M_{\mathrm{rgcd}(A,B)} \to 0$$

où f_1 est induite par les surjections canoniques, et f_2 provient de

$$\begin{array}{rccc} K[X;\theta,\partial]^2 & \to & M_{\mathrm{rgcd}(A,B)} \\ (S,T) & \mapsto & S - T \end{array}$$

Preuve. f_2 est évidemment bien définie. Elle est de plus surjective car sa restriction à $M_A \oplus \{0\}$ l'est.
f_1 est par ailleurs injective. En effet le noyau des projections canoniques est $K[X;\theta,\partial]A \cap K[X;\theta,\partial]B$.
On voit d'autre part que $f_2 \circ f_1 = 0$. En effet si un élément (Q, L) est dans l'image de f_1 alors Q et L on un même relèvement dans $K[X;\theta,\partial]$.
Soit maintenant $(\overline{S}, \overline{T}) \in \ker(f_2)$, et donnons-nous en (S,T) des relèvements respectifs.
Il existe $Q \in K[X;\theta,\partial]$ tel que $T = S + Q\mathrm{rgcd}(A,B)$. On sait qu'il existe U, V des polynômes de ORE tels que $UA + VB = \mathrm{rgcd}(A,B)$ et donc

$$T - QVB = S + QUA$$

Or $T - QVB$ et $S + QUA$ sont des relèvements respectifs de $\overline{T}$ et $\overline{S}$, et $(\overline{S}, \overline{T}) = f_1(\overline{T - QVB})$. □

Corollaire 2.1.3.16. — *On en déduit en particulier que* $\deg(\mathrm{rgcd}(A,B)) + \deg(\mathrm{llcm}(A,B)) = \deg(A) + \deg(B)$*, ce qui n'est pas évident de prime abord.*

Une question qui se pose maintenant naturellement est celle des morphismes entre modules cycliques. Supposons P et P' des polynômes de Ore. Si un morphisme $\varphi : M_P \to M_{P'}$ existe, alors il vérifie pour tout $\overline{S} \in M_P$, en notant $Q := \varphi(\overline{1}))$:

$$\varphi(\overline{S}) = \varphi(S.\overline{1}) = SQ.$$

De plus, P serait dans le noyau de l'application composée $K[X;\theta,\partial] \twoheadrightarrow M_P \xrightarrow{\varphi} M_{P'}$, donc P' serait un diviseur à droite de PQ. Une condition nécessaire à l'existence d'un morphisme entre M_P et M'_P est donc l'existence de Q tel que

$$\exists Q' \in K[X;\theta,\partial], PQ = Q'P'. \tag{2.1.3.5}$$

Proposition 2.1.3.17. — *C'est une condition suffisante.*

En effet si cette condition est respectée on a alors un morphisme $K[X;\theta,\partial] \to M'_P$ qui à S associe SQ et P est dans son noyau.
On voit par ailleurs que l'ensemble ${}^{\{Q\in K[X;\theta,\partial]\,|\,\exists Q',PQ=Q'P'\}}/_{K[X;\theta,\partial]P'}$ est en bijection avec l'ensemble des morphismes de M_P vers M'_P.

Proposition 2.1.3.18. — *Soit Q vérifiant (2.1.3.5) et f le morphisme qui lui est associé.*

(i) f est surjectif si et seulement si $\mathrm{rgcd}(P',Q) = 1$.

(ii) f est bijectif si et seulement si, de plus, $\deg(P) = \deg(P')$.

Preuve. (ii) se déduit directement de (i) par égalité des dimensions en tant que K-espaces vectoriels.
Supposons f surjectif. Alors il existe $U \in K[X;\theta,\partial]$ tel que $UQ = 1 \mod P'$ donc il existe $V \in K[X;\theta,\partial]$ tel que $UQ + VP' = 1$ et donc $\mathrm{rgcd}(P',Q) = 1$.
Réciproquement si $\mathrm{rgcd}(P',Q) = 1$ alors pour tout $S \in K[X;\theta,\partial]$ il existe des polynômes de Ore U_S et V_S tels que $U_SQ + V_SP' = S$. On en déduit $f(U_S) = \overline{S}$ et donc que f est surjective. □

Le sujet est vaste et il y aurait encore beaucoup à dire au sujet des polynômes de Ore, par exemple un analogue de factorialité non commutative de ces anneaux, mais ce coup d'oeil superficiel nous suffira pour le reste de ce mémoire, dont le sujet n'est pas l'étude des polynômes de Ore dans leur plus grande généralité.

2.2 Algèbres des opérateurs différentiels et p-courbure

Dans cette sous-section nous restreignons notre étude au cas où $\theta = \mathrm{Id}$. Dans ce cadre nous allons pouvoir étudier des problèmes venant de l'analyse (résolutions d'équations différentielles linéaires) dans un cadre algébrique. Nous restreindrons très vite notre étude à la caractéristique $p > 0$, ce qui permettra l'introduction et l'étude d'un invariant très utile : la p-courbure. La suite de ce mémoire tournera autour du calcul efficace de son polynôme caractéristique.

Les paragraphes 2.2.1 et 2.2.2 suivent la présentation de [vdPS03], tandis que les résultats des paragraphes suivants sont issus de [BCS14].

2.2.1 Motivation

Définition 2.2.1.1. — *Soit A un anneau commutatif muni d'une dérivation $\frac{d}{dz} : a \mapsto a'$, c'est-à-dire d'une θ-dérivation avec $\theta = \mathrm{Id}_A$. On note $A\langle\partial\rangle := A\left[X;\mathrm{Id}_A,\frac{d}{dz}\right]$. Pour éviter la confusion dans la suite de ce document, les éléments de $A\langle\partial\rangle$ seront des polynômes en la variable ∂ et vérifieront la règle de commutation suivante :*

$$\partial a = a\partial + a', \quad \textit{pour tout } a \in A.$$

Remarque 2.2.1.2. — *Dans toute la suite de ce document, on pourra supposer A intègre, ce qui nous placera dans le cadre d'égalité de la proposition 2.1.3.2.*

Soit K un corps différentiel (i.e., muni d'une dérivation). Dans la suite de ce document nous étudierons des opérateurs différentiels $L \in K\langle\partial\rangle$. Cette étude passe par celle du K-module différentiel cyclique ${}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$ associé à un tel opérateur. Cependant l'intérêt de l'étude de ce K-module différentiel se comprend mieux en considérant d'abord des systèmes de la forme

$$Y' = AY \tag{$\mathcal{E}$}$$

où $Y \in K^n$ et $A \in M_n(K)$. Si nous spécifiions des conditions initiales et si K était un anneau de fonctions régulières issues de l'analyse, nous reconnaitrions ici un problème de Cauchy linéaire. L'analogue de ces problèmes dans le cadre qui est le notre est de savoir si ce système admet une base de solutions dans K^n.
On peut munir K^n de la connexion suivante :

$$\partial_A(Y) = Y' - AY.$$

Il s'agit bien d'une connexion :

$$\partial_A(aY) = (aY') - aAY = a'Y + aY' - aAY = a'Y + a\partial_A(Y).$$

K^n peut donc être muni d'une structure de $K\langle\partial\rangle$-module différentiel à gauche. L'existence d'une base de solutions à ($\mathcal{E}$) se ramène au problème suivant : existe-t-il une base de « vecteurs horizontaux » de K^n, i.e., annulés par la connexion ∂_A ?

On voit donc apparaître une nouvelle classe de problèmes : étant donné un K-module différentiel (M, ∂) de dimension finie sur K, existe-t-il, éventuellement dans une extension de corps L de K, une base de vecteurs horizontaux de M (ou de $L \otimes_K M$) ? Dans la suite de ce document, nous ne nous intéresserons pas à la question des extensions de corps de K.

L'intérêt de l'étude de ${}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$ devient plus évident : l'existence de solutions à

$$L.y = 0 \tag{$\mathcal{E}'$}$$

se ramène au problème

$$Y' = A_L Y \tag{$\mathcal{E}''$}$$

dans K^n avec

$$A_L := \begin{pmatrix} & & -l_0 \\ 1 & & -l_1 \\ & \ddots & \vdots \\ & 1 & -l_{n-1} \end{pmatrix}$$

où $L = l_n(\partial^n + l_{n-1}\partial^{n-1} + \cdots + l_1\partial + l_0)$. Le diagramme suivant est commutatif

$$\begin{array}{ccc} {}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L} & \xrightarrow{\sim} & K^n \\ \downarrow{\scriptstyle\partial} & & \downarrow{\scriptstyle\partial_{A_L}} \\ {}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L} & \xrightarrow{\sim} & K^n \end{array}$$

où l'isomorphisme est celui envoyant la base canonique de l'un sur celle de l'autre.

Avant de conclure cette introduction au problème, nous définissons une dernière notion qui nous sera utile.

Définition-Proposition 2.2.1.3. — *Soit A un anneau différentiel. On peut définir son sous-anneau des constantes comme étant le sous-anneau des éléments $a \in A$ vérifiant $a' = 0$. Si de plus A est un corps, alors ce sous-anneau est un sous-corps de A que l'on appelle alors son corps des constantes.*

Preuve.
- $1'_A = 0$. En effet $1'_A = (1_A.1_A)' = 1'_A.1_A + 1_A1'_A = 1'_A + 1'_A$ et donc $1'_A = 0$.
- $0'_A = 0_A$, car la dérivation est additive.
- Soient $a, b \in A$ tels que $a' = b' = 0$. Alors $(a+b)' = a' + b' = 0$. De plus $(ab)' = a'b + ab' = 0$.

Le sous-anneau des constantes de A est donc bien un sous-anneau. Si de plus A est un corps alors pour tout $a \in A^\times$ tel que $a' = 0$ on a $(aa^{-1})' = 0 = a'a^{-1} + a(a^{-1})' = a(a^{-1})'$. Donc $(a^{-1})' = 0$.
Le sous-anneau des constantes de A est donc bien un sous-corps de A. □

2.2.2 Caractéristique $p > 0$ et p-courbure

On suppose à présent que K est un corps de caractéristique p, avec p premier, vérifiant $[K : K^p] = p$. On suppose de plus que la dérivation n'est pas triviale sur K. Il suit que K^p est exactement le corps des constantes de K. En effet tous les éléments de K^p sont constants puisque pour tout $a \in K$,

$$(a^p)' = pa'a^{p-1} = 0.$$

Notons alors K_c le corps des constantes de K. On a $[K : K_c][K_c : K^p] = [K : K^p] = p$. Il suit que $[K : K_c] = p$ et $[K_c : K^p] = 1$.

EXEMPLE 2.2.2.1. — *Soit k un corps fini de caractéristique p. Alors $k(x)$ et $k((x))$ (le corps des séries de LAURENT à coefficients dans k) sont deux tels corps.*

Preuve. On a $k(x)^p = k(x^p)$. La famille $(1, x, \dots, x^{p-1})$ est une base de $k(x)$ en tant que $k(x^p)$-espace vectoriel.
En effet si on a

$$\sum_{l=0}^{p-1} \frac{P_l(x^p)}{Q_l(x^p)} x^l = 0$$

on peut alors se ramener à une équation du type

$$\sum_{l=0}^{p-1} P_l(x^p) x^l = 0.$$

Tous les termes de la somme sont de degrés différents car

$$\deg(P_l(x^p)x^l) \equiv l \bmod p$$

et ainsi

$$\max_{l=0}^{p-1}(p \deg(P_l) + l) = -\infty \quad \Longrightarrow \quad \forall 0 \leqslant l \leqslant p-1, P_l = 0.$$

Ainsi cette famille est libre.

De plus pour tout $P := \sum_{l=0}^{d} a_d x^d$ avec $d = qp + r$ (la division euclidienne de d par p) on a :

$$P = \left(\sum_{i=0}^{q-1} x^{ip} \sum_{j=0}^{p-1} a_{ip+j} x^j \right) + x^{qp} \sum_{i=0}^{r} a_{qp+i} x^i.$$

Enfin pour tout $F = \frac{P}{Q} \in k(x)$ on a

$$F = \frac{PQ^{p-1}}{Q^p}$$

et ainsi $(1, x, \dots, x^{p-1})$ est génératrice, et libre, c'est donc bien une base.

On montre similairement que $k((x))$ est un tel corps (même base). □

On fait maintenant l'hypothèse supplémentaire qu'il existe $z \in K$ tel que z' soit une constante. Quitte à diviser par une constante, on peut supposer qu'il existe $z \in K$ tel que $z' = 1$. K est alors engendré par la famille $(1, z, z^2, \dots, z^{p-1})$ en tant que K^p-espace vectoriel. En effet $K^p[z]$ est un sous-corps de K vérifiant $K^p \subsetneq K^p[z]$. Il vient alors $[K : K^p[z]][K^p[z] : K^p] = p$ et encore $[K : K^p[z]] = 1$.

PROPOSITION 2.2.2.2. — *Sous cette hypothèse, pour tout $a \in K$, $\partial^p a = a\partial^p$, ce qui revient à dire que $a^{(p)} = 0$ pour tout $a \in K$.*

Preuve. Soit $a \in K$. Pour tout $n \in \mathbb{N}$ on a

$$\partial^n a = \sum_{k=0}^{n} \binom{n}{k} a^{(n-k)} \partial^k.$$

Cela se prouve facilement par récurrence. En particulier pour $n = p$ on trouve

$$\partial^p a = a\partial^p + a^{(p)}. \tag{2.2.2.1}$$

D'autre part il existe $P \in K^p[X]$ de degré au plus $p-1$ tel que $a = P(z)$.
On en déduit :

$$a' = z'P'(z) = P'(z).$$

Par récurrence immédiate il vient

$$a^{(p)} = P^{(p)}(z).$$

Or P est de degré au plus $p-1$ donc $P^{(p)} = 0$ ce qui achève la démonstration. □

Remarque 2.2.2.3. — *La formule (2.2.2.1) montre que même lorsque l'existence de z vérifiant $z' = 1$ n'est pas vérifiée, la « dérivée p-ième » définit une dérivation sur K.*

Remarque 2.2.2.4. — *L'existence d'un z tel que $z' = 1$ n'est pas garantie. En effet on peut supposer par exemple que $K^p = k(x^p)$ où k est un corps fini de caractéristique p. Le polynôme $X^p - x^p$ est irréductible sur $k(x^p)$. En effet x est une racine de $X^p - x^p$ dans $k(x)$. Or x engendre $k(x)$ de dimension p sur $k(x^p)$. Ainsi le polynôme minimal de x sur $k(x^p)$ est de degré p et divise $X^p - x^p$.*
On peut donc considérer l'extension de corps $K = {}^{k(x^p)[X]}/_{(X^p - x^p)}$. On note z l'image de X par le passage au quotient. Pour tout choix de $P \in k(x^p)[X]$ on peut définir une dérivation sur K :

$$P\frac{d}{dz} : Q(z) \mapsto P(z)Q'(z).$$

Une telle application est bien définie :

$$P\frac{d}{dz}((Q + R(X^p - x^p))(z)) = P(z)(Q' + R'(X^p - x^p))(z) \equiv P(z)Q'(z) \bmod X^p - x^p$$

et vérifie bien la règle de Leibniz.
En particulier pour $P = X$, $z^{(p)} = z$. Par la proposition qui précède, on en déduit qu'il n'existe pas de $a \in K$ de sorte que $a' = 1$.

Définition 2.2.2.5. — *Soit (M, ∂_M) un K-module différentiel de dimension finie. Il est évident que :*

$$\begin{array}{rccc} \partial_M : & M & \to & M \\ & m & \mapsto & \partial.m \end{array}$$

est un endomorphisme K^p-linéaire de M. C'est donc aussi le cas de sa composée p-ième ∂_M^p. De ce qui précède, on voit qu'il s'agit en fait d'un endomorphisme K-linéaire.
On appelle cet endomorphisme la p-courbure de (M, ∂_M).
Dans le cas où $M = {}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$ on dira par abus de langage la p-courbure de L.

Dans le cas où $M = K^n$ et $\partial_M = \partial_A$ avec $A \in M_n(K)$, la p-courbure de M peut se calculer de manière récursive de la manière suivante : on pose $A_0 = I_n$ et pour tout $k \leqslant p$, $A_k = A'_{k-1} - AA_{k-1}$. Alors A_p est la matrice de la p-courbure dans la base canonique de K^n. Il en vient immédiatement le résultat suivant :

Lemme 2.2.2.6. — *Si A est à coefficients dans $\mathfrak{A} \subset K$ un sous-anneau différentiel (i.e., stable pour la dérivation de K), alors la matrice de sa p-courbure dans la base canonique de K^n est à coefficients dans $\mathfrak{A}$.*

L'utilité de la p-courbure provient en partie du résultat suivant :

Proposition 2.2.2.7. — *Soit (M, ∂_M) un K-module différentiel de dimension finie d sur K. M admet une base de vecteurs horizontaux pour ∂_M si et seulement si $\partial_M^p = 0$.*

Preuve. Supposons que $\partial_M^p = 0$. Alors l'application K^p-linéaire ∂_M est nilpotente. En particulier il existe $e_1 \in M$ tel que $\partial_M(e_1) = 0$.
On peut alors considérer le K-module différentiel $M' = {}^M\!/_{Ke_1}$ munie de la connexion $\partial_{M'}(\overline{m}) = \overline{\partial_M(m)}$. Cela définit bien une connexion car $\partial_M(e_1) = 0$. De plus par définition, $\partial_{M'}^p = 0$ donc par hypothèse de récurrence, M' est munie d'une base $(\overline{e_2}, \dots, \overline{e_d})$ de vecteurs horizontaux pour $\partial_{M'}$. Donnons-nous des relèvements $e_2, \dots, e_d$. La famille $(e_1, \dots, e_d)$ est alors une base de M et, de plus, pour tout $2 \leqslant i \leqslant d$, on a $\partial_M e_i = f_i e_i$ avec $f_i \in K$.
On peut écrire $f_i = P_i(z)$ où $z' = 1$ (qui existe par hypothèse sur K) et P_i est de degré au plus $p-1$.
Alors $\partial_M e_i = f_i^{(p-1)} e_1 = 0$. On en déduit $f_i^{(p-1)} = 0$.
Or $f_i^{(p-1)}$ est l'opposé du coefficient de rang $p-1$ de P_i. On en déduit que P_i est de rang au plus $p-2$.
Il vient qu'il existe $g_i \in K$ tel que $g_i' = f_i$. Alors $\partial_M(e_i - g_i e_1) = 0$ et $(e_1, e_2 - g_2 e_1, \dots, e_d - g_d e_1)$ est une base de M de vecteurs horizontaux pour ∂_M. □

Ce résultat permet de mieux comprendre l'intérêt porté à cet invariant. De manière plus générale, la p-courbure intervient dans l'énoncé de la conjecture de Grothendieck-Katz [Kat82], dans des algorithmes de factorisation d'opérateurs différentiels [Clu03], et dans le calcul de l'algèbre de Lie du groupe de Galois différentiel d'un sytème différentiel linéaire [BCWDV16]. En particulier, décider la nilpotence de la p-courbure, ou plus généralement calculer son polynôme caractéristique sont des questions intéressantes. Dans la suite de cette section nous nous employons à mettre en place des résultats théoriques et algorithmiques sur ce fameux calcul.
Avant cela, nous énonçons et démontrons le résultat suivant qui nous sera très utile dans la suite de ce document :

PROPOSITION 2.2.2.8. — *Soit (M, ∂_M) un K-module différentiel de dimension finie sur K. Le polynôme caractéristique de sa p-courbure est à coefficients dans K^p.*

Preuve. Nous allons en fait montrer le résultat plus général suivant :

LEMME 2.2.2.9. — *Soit K un corps différentiel et (M, ∂_M) un K-module différentiel de dimension finie sur K. Soit $f \in \mathcal{L}(M)$ un endomorphisme vérifiant $f \circ \partial_M = \partial_M \circ f$. Alors $\det(f)$ est une constante.*

Preuve. Soit n la dimension de M. f induit un endomorphisme Det(f) : $\Lambda^n M \to \Lambda^n M$. D'autre part ∂_M induit sur $\Lambda^n M$ une connexion $\mathrm{Det}(\partial_M)$ définie par la formule :

$$\mathrm{Det}(\partial_M)(x_1 \wedge \ldots \wedge x_n) = \sum_{i=1}^{n} x_1 \wedge \ldots \wedge x_{i-1} \wedge \partial_M(x_i) \wedge x_{i+1} \wedge \ldots \wedge x_n.$$

De la commutation de ∂_M et f on déduit la commutation de $\mathrm{Det}(f)$ et $\mathrm{Det}(\partial_M)$:

$$\begin{aligned}
\mathrm{Det}(f)(\mathrm{Det}(\partial_M)(x_1 \wedge \ldots \wedge x_n) &= \sum_{i=1}^{n} f(x_1) \wedge \ldots \wedge f(x_{i-1}) \wedge f(\partial_M(x_i)) \wedge f(x_{i+1}) \wedge \ldots \wedge f(x_n) \\
&= \sum_{i=1}^{n} f(x_1) \wedge \ldots \wedge f(x_{i-1}) \wedge \partial_M(f(x_i)) \wedge f(x_{i+1}) \wedge \ldots \wedge f(x_n) \\
&= \mathrm{Det}(\partial_M)(\mathrm{Det}(f)(x_1 \wedge \ldots \wedge x_n).
\end{aligned}$$

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de M. L'application déterminant (dans la base $\mathcal{B}$) est une forme multilinéaire alternée sur M^n. Elle induit donc une application det : $\Lambda^n M \to K$ linéaire qui permet d'identifier $\Lambda^n M$ à K.

On en déduit donc une application $\det_B(f) : K \to K$, $\lambda \mapsto \det(\mathrm{Det}(f)(\lambda.e_1 \wedge \ldots \wedge e_n))$. Il vient immédiatement que $\det_B(f)$ n'est que la multiplication par $\det(f)$.
De même, det induit $\det_B(\partial_M) : \lambda \mapsto \det(\mathrm{Det}(\partial_M)(\lambda.(e_1 \wedge \ldots \wedge e_n))$, qui est une connexion sur K :

$$\begin{aligned}
\det_B(\partial_M)(\lambda_1\lambda_2) &= \det(\mathrm{Det}(\partial_M)(\lambda_1.\lambda_2(e_1 \wedge \ldots \wedge e_n)) \\
&= \lambda_1 \det_B(\partial_M(\lambda_2)) + \lambda_1'\lambda_2.
\end{aligned}$$

Comme K est de dimension 1, $\det_B(\partial_M)$ est entièrement déterminée par $c = \det_B(\partial_M)(1)$. On a pour tout $\lambda \in K$, $\det_B(\partial_M)(\lambda) = \lambda c + \lambda'$.
Il vient de plus $\det_B(\partial_M) \circ \det_B(f) = \det_B(f) \circ \det_B(\partial_M)$. Cette égalité en 1 donne :

$$\det(f)' + c\det(f) = c\det(f),$$

ce qui donne encore $\det(f)' = 0$, ce que l'on voulait démontrer. □

On applique alors le résultat précédent au corps $K_1 = K(X)$ muni de la dérivation coefficient par coefficient (il s'agit bien d'une dérivation sur $K[X]$ et elle induit une dérivation sur son corps des fractions via la formule $\left(\frac{P}{Q}\right)' = \frac{P'Q - PQ'}{Q^2}$.). On prend $M' = K_1^n$ où n est la dimension de M en tant que K-espace vectoriel. La connexion sur M' est donnée par $\partial_{M'}(0, \dots, 0, P(X), 0, \dots, 0) = P(X)\partial_M(0, \dots, 0, 1, 0, \dots, 0) + (0, \dots, 0, P'(X), 0, \dots, 0)$. On suppose que la matrice de la p-courbure dans la base canonique de M est A. On applique le résultat précédent à $XI_n - A$. Cette application commute avec $\partial_{M'}$ ce qui donne le résultat. □

Dans toute la suite de ce mémoire nous noterons $\chi(A_p(L))$ le polynôme caractéristique de la p-courbure associé à $L \in k(x)\langle\partial\rangle$.

2.2.3 Isomorphisme entre algèbres de polynômes de Ore et application à l'étude de la p-courbure

On suppose dans cette partie que $K = k(x)$ où k est un corps fini de caractéristique p, muni de la dérivation usuelle. Pour la suite de ce document nous aurons besoin de considérer l'existence d'un « opérateur d'intégration » ∂^{-1}, et l'algèbre $k(x)\langle\partial^{\pm 1}\rangle$ des polynômes de Laurent en la variable ∂. Si une telle algèbre existe, on voit que, pour tout $f \in k(x)$, on a

$$\begin{aligned}\partial^{-1}\partial f &= f \\ &= \partial^{-1} f \partial + \partial^{-1} f'.\end{aligned}$$

Il suit que

$$\partial^{-1} f = f\partial^{-1} - \partial^{-1} f' \partial^{-1}.$$

Par récurrence on en déduit

$$\partial^{-1} f = \sum_{i=0}^{p-1} (-1)^i f^{(i)} \partial^{-i-1}$$

puisque $f^{(p)} = 0$.
L'existence d'une telle algèbre revient à construire un anneau classique de quotient à droite de $R := k(x)\langle\partial\rangle$ par $S := \{\partial^i | i \in \mathbb{N}\}$ comme défini en B.6. Pour voir qu'un tel anneau existe il suffit de voir que le couple (R, S) vérifie la condition de Ore à droite (B.10).
Soit $(r, \partial^i) \in R \times S$. Il existe un unique couple $(q, j) \in \mathbb{N}$ tel que $0 \leqslant j < i$ et $i = qp + j$. Alors $\partial^{i+p-j} = \partial^{(q+1)p}$ est un élément central de R et donc $r\partial^{(q+1)p} = \partial^i \partial^{p-j} r$.

On en déduit donc qu'un tel anneau $k(x)\langle\partial^{\pm 1}\rangle$ peut bien être défini. De plus, les résultats de l'appendice B.8 assurent qu'une telle structure est unique puisque les éléments de S commutent entre eux, et qu'elle vérifie de plus la propriété universelle de la localisation.

Proposition 2.2.3.1. — *Soit $\varphi : k(x)\langle\partial\rangle \to B$ un morphisme d'anneaux. Si $\varphi(\partial) \in B^\times$ alors il existe un unique morphisme d'anneaux faisant commuter le diagramme suivant :*

$$\begin{array}{ccc} k(x)\langle\partial\rangle & \hookrightarrow & k(x)\langle\partial^{\pm 1}\rangle \\ & \searrow^{\varphi} & \downarrow \exists! \\ & & B \end{array}$$

Similairement, on peut définir $k[x]\langle\partial^{\pm 1}\rangle$ l'algèbre des polynômes de Laurent à coefficients polynomiaux en la variable ∂ (même preuve). La structure d'anneaux classique de quotient à droite permet d'identifier $k[x]\langle\partial^{\pm 1}\rangle$ à un sous-anneau de $k(x)\langle\partial^{\pm 1}\rangle$. Il vérifie de plus la propriété universelle plus générale suivante :

PROPOSITION 2.2.3.2. — *Soient $\varphi : k \to B$ un morphisme d'anneaux, $(b, \xi) \in B \times B^\times$ de sorte que $\xi b = b\xi + 1$. Il existe un unique morphisme d'anneaux $\tilde{\varphi} : k[x]\langle\partial^{\pm 1}\rangle \to B$ prolongeant φ et vérifiant $\tilde{\varphi}(x) = b$ et $\tilde{\varphi}(\partial) = \xi$.*

Preuve. Il existe un unique $f : k[x] \to B$ prolongeant φ et vérifiant $f(x) = b$. On vérifie facilement que pour tout $P \in k[x]$ on a $\xi P(b) = P(b)\xi + P'(b)$. Par la propriété universelle des polynômes de ORE, il existe un unique morphisme $F : k(x)\langle\partial\rangle$ prolongeant f et valant ξ en ∂. On conclut avec la propriété universelle du localisé. □

On considère maintenant l'élément particulier $x\partial \in k(x)\langle\partial\rangle$. Cet élément vérifie les règles de commutation suivantes :

$$\begin{aligned}(x\partial).x &= x^2\partial + x \\ &= x(x\partial - 1)\end{aligned}$$

et

$$\begin{aligned}\partial(x\partial) &= x\partial^2 + \partial \\ &= (x\partial + 1)\partial.\end{aligned}$$

Ceci motive l'apparition de l'algèbre de polynômes de ORE $k(\theta)\langle\partial\rangle$ twisté par l'automorphisme de $k(\theta)$ donné par $F(\theta) \mapsto F(\theta + 1)$. Les éléments de cette algèbre sont donc des polynômes en la variable ∂ à coefficients dans $k(\theta)$, vérifiant la règle de commutation suivante :

$$\partial\theta = (\theta + 1)\partial$$

et donc pour tout $F \in k(\theta)$ et tout $i \in \mathbb{N}$:

$$\partial F(\theta) = F(\theta + i)\partial^i.$$

On comprend à présent la nécessité d'un « opérateur d'intégration » : dans cette nouvelle algèbre la variable θ représente $x\partial$ et offre un cadre où le calcul est (ou du moins semble) plus facile. On y perd cependant *a priori* de l'information, d'où la nécessité d'un opérateur ∂^{-1}.
De la même façon que précédemment on introduit l'algèbre $k(\theta)\langle\partial^{\pm 1}\rangle$ des polynômes de LAURENT en la variable ∂, possédant la propriété universelle du localisé de $k(\theta)\langle\theta\rangle$ en ∂.
On peut encore se restreindre aux coefficients polynomiaux en θ et considérer l'algèbre $k[\theta]\langle\partial^{\pm 1}\rangle$ qui possède la propriété universelle suivante :

PROPOSITION 2.2.3.3. — *Soit $\varphi : k \to B$ et $(b, \xi) \in B \times B^\times$ tel que $\xi b = (b + 1)\xi$. Alors il existe un unique morphisme $\tilde{\varphi} : k[\theta]\langle\partial^{\pm 1}\rangle \to B$ prolongeant φ tel que $\tilde{\varphi}(\theta) = b$ et $\tilde{\varphi}(\partial) = \xi$.*

Les inclusions des différentes algèbres sont résumées dans les diagrammes commutatifs ci-dessous :

$$\begin{array}{ccc} k[x]\langle\partial\rangle & \hookrightarrow & k[x]\langle\partial^{\pm 1}\rangle \\ \downarrow & & \downarrow \\ k(x)\langle\partial\rangle & \hookrightarrow & k(x)\langle\partial^{\pm 1}\rangle \end{array} \quad \text{et} \quad \begin{array}{ccc} k[\theta]\langle\partial\rangle & \hookrightarrow & k[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow & & \downarrow \\ k(\theta)\langle\partial\rangle & \hookrightarrow & k(\theta)\langle\partial^{\pm 1}\rangle \end{array}$$

THÉORÈME 2.2.3.4. — *On a un isomorphisme de k-algèbres donné par :*

$$\begin{array}{ccc} k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & k[\theta]\langle\partial^{\pm 1}\rangle \\ x & \mapsto & \theta\partial^{-1} \\ x\partial & \leftarrow\!\shortmid & \theta \\ \partial & \leftrightarrow & \partial \end{array}$$

Preuve. Commençons par vérifier que cela définit bien un morphisme de k-algèbres. D'après la Proposition 2.2.3.2 il suffit de vérifier que $\partial \in (k[\theta]\langle\partial^{\pm 1}\rangle)^\times$ (ce qui est le cas par hypothèse) et, de plus, que

$$\partial\theta\partial^{-1} = \theta\partial^{-1}\partial + 1 = \theta + 1.$$

Or

$$\partial\theta\partial^{-1} = (\theta+1)\partial\partial^{-1} = \theta + 1.$$

On a donc bien un morphisme $k[x]\langle\partial^{\pm 1}\rangle \to k[\theta]\langle\partial^{\pm 1}\rangle$.
De même, on vérifie par la Proposition 2.2.3.3 que le morphisme inverse est bien défini :

$$\partial x\partial = (x\partial + 1)\partial.$$

Il reste encore à voir que ces deux morphismes sont inverses l'un de l'autre. Comme on a

$$x \mapsto \theta\partial^{-1} \mapsto x\partial\partial^{-1} = x$$

et

$$\theta \mapsto x\partial \mapsto \theta\partial^{-1}\partial = \theta$$

on en déduit par les Propositions 2.2.3.2 et 2.2.3.3 que la composée de ces deux morphismes (dans un sens ou dans l'autre) est l'unique endomorphisme de $k[x]\langle\partial^{\pm 1}\rangle$ (resp. $k[\theta]\langle\partial^{\pm 1}\rangle$) associant x à x (resp. θ à θ) et ∂ à ∂, il s'agit donc de l'identité. □

Remarque 2.2.3.5. — *Cet isomorphisme ne se prolonge cependant pas en $k(x)\langle\partial^{\pm 1}\rangle \to k(\theta)\langle\partial^{\pm 1}\rangle$. En effet ces deux anneaux n'ont pas les mêmes éléments inversibles. Par exemple $(x+1)\partial$ est inversible dans $k(x)\langle\partial^{\pm 1}\rangle$ mais son image $\partial + \theta$ ne l'est pas dans $k(\theta)\langle\partial^{\pm 1}\rangle$.*

L'intérêt de cet isomorphisme est qu'il va permettre de ramener le calcul du polynôme caractéristique de la p-courbure d'un opérateur $L \in k(x)\langle\partial\rangle$, à celui d'une matrice plus simple à calculer. On introduit donc un analogue de la p-courbure pour $L \in k(\theta)\langle\partial\rangle$, dont nous comparerons les propriétés avec celle de son équivalent différentiel au fur et à mesure.

Proposition 2.2.3.6. — *Soit $L \in k(\theta)\langle\partial\rangle$. Le quotient $M = {}^{k(\theta)\langle\partial\rangle}/_{k(\theta)\langle\partial\rangle L}$ est muni d'une structure de $k(\theta)\langle\partial\rangle$-module à gauche, et d'une base $\mathcal{B} = (1, \partial, \dots, \partial^{m-1})$, où m est le degré de L. De plus, $P \mapsto \partial^p P$ est une application $k(\theta)$-linéaire et si $B_p(L)$ désigne sa matrice dans la base $\mathcal{B}$, on a :*

$$B_p(L) = B(\theta)B(\theta+1)\dots B(\theta+p-1).$$

où

$$B(\theta) = \begin{pmatrix} & & -l_0(\theta) \\ 1 & & -l_1(\theta) \\ & \ddots & \vdots \\ & 1 & -l_{m-1}(\theta) \end{pmatrix}.$$

Preuve. On nomme $(e_0, \dots, e_{m-1})$ les vecteurs de $\mathcal{B}$. Nous allons montrer par récurrence que pour tout $i \in [\![0, m-1]\!]$ et tout $n \in \mathbb{N}^*$, $\partial^n e_i$ s'écrit dans la base $\mathcal{B}$ comme

$$B(\theta)B(\theta+1)\dots B(\theta+n-1)e_i.$$

Cela est évident au rang 1. Supposons le résultat vrai au rang n. Soit $i \in [\![0, m-1]\!]$.

$$\begin{aligned}
\partial^{n+1}e_i &= \partial\partial^n(e_i) \\
&= \partial.B(\theta)B(\theta+1)\dots B(\theta+n-1)e_i \\
&= \sum_{k=0}^{m-1} \partial P_{n,i,k}(\theta)e_k \\
&= \sum_{k=0}^{m-1} P_{n,i,k}(\theta+1)\partial e_k \\
&= \sum_{k=0}^{m-1} P_{n,i,k}(\theta+1)B(\theta)e_k \\
&= B(\theta)\left(\sum_{k=0}^{m-1} P_{n,i,k}(\theta+1)e_k\right) \\
&= B(\theta).(B(\theta+1)B(\theta+2)\dots B(\theta+n))e_i.
\end{aligned}$$

□

L'objet de ce mémoire étant le calcul du polynôme caractéristique de la p-courbure, il est naturel que le polynôme caractéristique de son analogue dans $k(\theta)\langle\partial\rangle$ nous intéresse. Pour $L \in k(\theta)\langle\partial\rangle$ on le note $\chi(B_p(L))$. Avant d'aller plus loin, nous introduisons l'application suivante, qui n'est guère qu'une renormalisation de $\chi \circ A_p$:

$$\begin{array}{rccc} \Xi_{x,\partial} : & k(x)\langle\partial\rangle & \to & k(x)\langle\partial\rangle \\ & L & \mapsto & l_r(x)^p \chi(A_p(L))(\partial^p) \end{array}$$

ainsi que celle-ci qui est une renormalisation de $\chi \circ B_p$:

$$\begin{array}{rccc} \Xi_{\theta,\partial} : & k(\theta)\langle\partial\rangle & \to & k(\theta)\langle\partial\rangle \\ & G & \mapsto & g_r(\theta)g_r(\theta+1) + \cdots + g_r(\theta+p-1)\chi(B_p(G))(\partial^p) \end{array}$$

où l_r (resp. g_r) est le coefficient dominant de L (resp. G). Le but de la suite de cette sous-section est de montrer que l'on pourra passer du calcul de $\Xi_{x,\partial}$ à celui de $\Xi_{\theta,\partial}$ et vice-versa. L'idée est résumée par le diagramme ci-dessous :

$$\begin{array}{ccc} k(x)\langle\partial^{\pm 1}\rangle & \longrightarrow & k(\theta)\langle\partial^{\pm 1}\rangle \\ \downarrow{\scriptstyle \Xi_{x,\partial}} & & \downarrow{\scriptstyle \Xi_{\theta,\partial}} \\ k(x)\langle\partial^{\pm 1}\rangle & \longrightarrow & k(\theta)\langle\partial^{\pm 1}\rangle \end{array}$$

Malheureusement toutes les flèches de ce diagramme ne sont pas encore bien définies. La route est longue, et elle commence par l'étude des centres de ces algèbres, après toutefois avoir montré le résultat suivant :

PROPOSITION 2.2.3.7. — *$\Xi_{x,\partial}$ et $\Xi_{\theta,\partial}$ sont multiplicatives.*

Preuve.

- Dans $k(x)\langle\partial\rangle$, l'application qui à L associe son coefficient dominant est multiplicative.
- Soit $F, G \in k(\theta)\langle\partial\rangle$. Le coefficient dominant de FG est $f_r(\theta)g_s(\theta+i)$ où f_r, g_s sont les coefficients dominants respectifs de F et G et $i \in \mathbb{F}_p$. Alors

$$f_r(\theta)g_s(\theta+i)\dots f_r(\theta+p-1)g_s(\theta+i+p-1) = f_r(\theta)\dots f_r(\theta+p-1)g_s(\theta)\dots g_s(\theta+p-1).$$

Il suffit donc de voir que les applications $\chi \circ A_p$ et $\chi \circ B_p$ sont multiplicatives. Soient $A, B \in k(x)\langle\partial\rangle$ (resp. $A, B \in k(\theta)\langle\partial\rangle$). On note $M_A = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle A}$ (resp. $M_A = {}^{k(\theta)\langle\partial\rangle}/_{k(\theta)\langle\partial\rangle A}$), $M_B = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle B}$ (resp. $M_B = {}^{k(\theta)\langle\partial\rangle}/_{k(\theta)\langle\partial\rangle B}$) et $M_L = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle BA}$ (resp. $M_L = {}^{k(\theta)\langle\partial\rangle}/_{k(\theta)\langle\partial\rangle BA}$). On sait par la Proposition 2.1.3.14 qu'on a une suite exacte :

$$0 \to M_B \xrightarrow{f_1} M_L \xrightarrow{f_2} M_A \to 0$$

où f_1 est induite de la multiplication à droite par A et f_2 du passage au quotient. Comme l'application linéaire considérée n'est autre que la multiplication à gauche par ∂^p, on a le diagramme commutatif à lignes exactes suivant :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_B & \xrightarrow{f_1} & M_L & \xrightarrow{f_2} & M_A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \partial^p} & & \downarrow{\scriptstyle \partial^p} & & \downarrow{\scriptstyle \partial^p} & & \\ 0 & \longrightarrow & M_B & \xrightarrow{f_1} & M_L & \xrightarrow{f_2} & M_A & \longrightarrow & 0 \end{array}$$

On en déduit que, dans une bonne base, la matrice $A_p(L)$ (resp. $B_p(L)$) s'écrit :

$$A_p(L) = \begin{pmatrix} A_p(B) & \star \\ & A_p(A) \end{pmatrix} \qquad (\text{resp. } B_p(L) = \begin{pmatrix} B_p(B) & \star \\ & B_p(A) \end{pmatrix}).$$

On en déduit le résultat. □

Il est à présent temps de s'intéresser aux centres de ces algèbres.

PROPOSITION 2.2.3.8. — *$k[\theta]\langle\partial\rangle$ a pour centre $k[\theta^p-\theta][\partial^p]$.*

Preuve. Commençons par remarquer qu'un élément $L\in\mathcal{A}_\theta=k[\theta]\langle\partial\rangle$ est dans le centre de $\mathcal{A}_\theta$ si et seulement s'il commute avec ∂ et θ.

Soit

$$L=\sum_{i=0}^{d} l_i(\theta)\partial^i$$

un élément du centre. Alors

$$L\theta=\sum_{i=0}^{d} l_i(\theta)(\theta+i)\partial^i=\theta L=\sum_{i=0}^{d} l_i(\theta)\theta\partial^i.$$

On en déduit immédiatement que pour tout i, soit $l_i=0$ soit $p|i$.

Par ailleurs

$$L\partial=\sum_{i=0}^{d} l_i(\theta)\partial^{i+1}=\sum_{i=0}^{d} l_i(\theta+1)\partial^{i+1}.$$

Ainsi pour tout i, $l_i(\theta)=l_i(\theta+1)$.

Montrons que cela implique $l_i\in k[\theta^p-\theta]$. On écrit $l_i(\theta)=\sum_{k=0}^{d_i}a_k\theta^k$ avec $a_{d_i}\neq 0$. Alors

$$p_i(\theta+1)=\sum_{k=0}^{d_i}\sum_{l=k}^{d_i} a_l\binom{l}{k}\theta^k$$

et on en déduit pour tout k :

$$\sum_{l=k+1}^{d_i} a_l\binom{l}{k}=0 \tag{2.2.3.1}$$

en particulier pour $k=d_i-1$ on a $p|d_i$ car $a_{d_i}\neq 0$.
Ecrivons donc $d_i=n_ip$.
Pour $(n_i-1)p+1\leqslant k<n_ip$, on a par ailleurs que p divise $\binom{n_ip}{k}$ et on en déduit de proche en proche que $a_k=0$.
Pour $k=(n-1)p$, l'égalité (2.2.3.1) se réécrit $n_ia_{n_ip}+a_{(n_i-1)p+1}=0$.
Or pour tout $n\in\mathbb{N}^*$

$$(\theta^p-\theta)^n=\theta^{np}-n\theta^{(n-1)p+1}+f(\theta)$$

avec f de degré au plus $(n-1)p$.
On en déduit que on peut réécrire $l_i(\theta)=a_{n_ip}(\theta^p-\theta)^{n_i}+g(\theta)$ avec g de degré au plus $(n-1)p$ dans le centre de $k(\theta)\langle\partial\rangle$ et on conclut par récurrence. □

COROLLAIRE 2.2.3.9. — *(i) $k[\theta]\langle\partial^{\pm 1}\rangle$ a pour centre $k[\theta^p-\theta][\partial^{\pm p}]$.*

(ii) $k(\theta)\langle\partial\rangle$ a pour centre $k(\theta^p-\theta)[\partial^p]$.

(iii) $k(\theta)\langle\partial^{\pm 1}\rangle$ a pour centre $k(\theta^p-\theta)[\partial^{\pm p}]$.

Preuve. (i) ∂^p est un élément du centre de $k(\theta)\langle\partial\rangle$. Soit $L\in k[\theta]\langle\partial^{\pm 1}\rangle$, un élément du centre. Il existe $n\in\mathbb{N}$ tel que $\partial^{pn}L\in k[\theta]\langle\partial\rangle$. En tant que produit d'éléments du centre, $\partial^{pn}L$ est un élément du centre, en particulier c'est un élément du centre de $k[\theta]\langle\partial\rangle$. Ainsi $\partial^{pn}L\in k[\theta^p-\theta][\partial^p]$ et donc $L\in k[\theta^p-\theta][\partial^{\pm p}]$.
L'inclusion réciproque est évidente.

(ii) Soit $L\in k(\theta)\langle\partial\rangle$. Il existe $P\in k[\theta]$ tel que $P.L\in k[\theta]\langle\partial\rangle$. Alors $P(\theta)P(\theta+1)\dots P(\theta+p-1).L$ est dans le centre de $k[\theta]\langle\partial\rangle$, donc il est dans $k[\theta^p-\theta][\partial^p]$. En effet $P(\theta)P(\theta+1)\dots P(\theta+p-1)$ commute avec ∂, donc est dans le centre. Il suit que $L\in k(\theta^p-\theta)[\partial^p]$. L'inclusion réciproque est évidente.

(iii) Soit $L \in k(\theta)\langle\partial^{\pm 1}\rangle$ un élément du centre. Il existe $n \in \mathbb{N}$ tel que $\partial^{pn} L \in k(\theta)\langle\partial\rangle$ soit un élément du centre, en tant que produits d'éléments centraux. Donc $\partial^{pn} L \in k(\theta^p - \theta)[\partial^p]$ et $L \in k(\theta^p - \theta)[\partial^{\pm p}]$. L'inclusion réciproque est évidente.

□

Lemme 2.2.3.10. — *$\theta^p - \theta$ s'envoie sur $x^p\partial^p$ par l'isomorphisme du Théorème 2.2.3.4.*

Preuve. On va montrer par récurrence un résultat un peu moins puissant :

Lemme. — *Pour tout $n \in \mathbb{N}^*$ il existe $a_{n,1}, \dots, a_{n,n}$ de sorte que*

$$(x\partial)^n = \sum_{i=1}^{n} a_{n,i} x^i \partial^i.$$

Les $a_{n,i}$ vérifient de plus la relation de récurrence $a_{n,1} = a_{n,n} = 1$ et $a_{n,i} = a_{n-1,i-1} + i a_{n-1,i}$ pour tout $n \in \mathbb{N}^*$ et $2 \leqslant i \leqslant n-1$.

Cela est évident au rang $n = 1$. Supposons que ce soit vrai au rang n. Alors

$$\begin{aligned}(x\partial)^{n+1} &= x\partial \sum_{i=1}^{n} a_{n,i} x^i \partial^i \\ &= \sum_{i=1}^{n} a_{n,i}(x^{i+1}\partial^{i+1} + i x^i \partial^i) \\ &= a_{n,n} x^{i+1}\partial^{i+1} + \left(\sum_{i=2}^{n} (a_{n,i-1} + i a_{n,i}) x^i \partial^i\right) + a_{n,1} x\partial.\end{aligned}$$

La récurrence est établie.

Nous savons par ailleurs que $(x\partial)^p - x\partial$ est un élément du centre de $k[x]\langle\partial^{\pm 1}\rangle$ puisqu'il s'agit de l'image par l'isomorphisme 2.2.3.4 de $\theta^p - \theta$. En particulier $(x\partial)^p - x\partial$ commute avec ∂, ce qui se réécrit encore

$$x^p\partial^{p+1} + \sum_{i=2}^{p-1} x^i \partial^{i+1} = x^p\partial^{p+1} + \sum_{i=2}^{p-1} a_{p,i} x^i \partial^{i+1} + \sum_{i=2}^{p-1} a_{p,i} i x^{i-1}\partial^i.$$

On a donc

$$\sum_{i=2}^{p-1} a_{p,i} i x^{i-1}\partial^i = 0$$

et encore $a_{p,i} = 0$ pour $2 \leqslant i \leqslant p-1$, ce qui achève la démonstration. □

Remarque 2.2.3.11. — *On a au passage démontré le résultat combinatoire suivant : si $(a_{n,i})_{\substack{n\in\mathbb{N}^* \\ 1\leqslant i\leqslant n}}$ est la suite d'entiers bi-indexée vérifiant pour tout $n \in \mathbb{N}^*$ $a_{n,1} = a_{n,n} = 1$ et pour tout $i \in [\![2, n-1]\!]$, $a_{n+1,i} = a_{n,i-1} + i a_{n,i}$, alors pour tout p premier, $p | a_{p,i}$ pour $2 \leqslant i \leqslant p-1$. Il s'agit d'un résultat classique sur les nombres de Stirling de seconde espèce.*

Corollaire 2.2.3.12. — *(i) $k[x]\langle\partial^{\pm 1}\rangle$ a pour centre $k[x^p][\partial^{\pm p}]$.*

(ii) $k[x]\langle\partial\rangle$ a pour centre $k[x^p][\partial^p]$.

(iii) $k(x)\langle\partial^{\pm 1}\rangle$ a pour centre $k(x^p)[\partial^{\pm p}]$.

(iv) $k(x)\langle\partial\rangle$ a pour centre $k(x^p)[\partial^p]$.

Preuve. (i) Il vient directement du Théorème 2.2.3.4 et du corollaire précédent que $k[x]\langle\partial^{\pm 1}\rangle$ a pour centre $k[x^p\partial^p][\partial^{\pm p}]$ ce qui peut encore se réécrire $k[x^p][\partial^{\pm p}]$.

(ii) Supposons $L \in k[x]\langle\partial\rangle$ un élément du centre, et $L_1 \in k[x]\langle\partial^{\pm 1}\rangle$. Il existe $n \in \mathbb{N}$ tel que $\partial^{pn} L_1 \in k[x]\langle\partial\rangle$. Alors

$$L.L_1 = L\partial^{-pn}(\partial^{pn} L_1) = \partial^{-pn}(\partial^{pn} L_1)L = L_1.L$$

et L est dans le centre de $k[x]\langle\partial^{\pm 1}\rangle$ et donc $L \in k[x^p][\partial^p]$.

(iii) Soit $L \in k(x)\langle\partial^{\pm 1}\rangle$ un élément du centre. Il existe $P(x) \in k[x]$ tel que $P(x)L \in k[x]\langle\partial^{\pm 1}\rangle$. Alors $P(x)^p L$ est un élément du centre de $k[x]\langle\partial^{\pm 1}\rangle$ et donc $P(x)^p L \in k[x^p][\partial^{\pm p}]$ et encore $L \in k(x^p)[\partial^{\pm p}]$.

(iv) Soit $L \in k(x)\langle\partial\rangle$ un élément du centre. Soit $L_1 \in k(x)\langle\partial^{\pm 1}\rangle$. Il existe $n \in \mathbb{N}$ tel que $\partial^{np} L_1 \in k(x)\partial\rangle$. Alors

$$L.L_1 = L\partial^{-pn}(\partial^{pn} L_1) = \partial^{-pn}(\partial^{pn} L_1)L = L_1.L$$

et L est un élément du centre de $k(x)\langle\partial^{\pm 1}\rangle$ et donc $L \in k(x^p)[\partial^p]$.

□

De la Proposition 2.2.2.8, nous savons que pour tout $L \in k(x)\langle\partial\rangle$, $\chi(A_p(L))$ a pour coefficients des éléments du sous-corps des constantes de $k(x)$ c'est-à-dire des éléments de $k(x^p)$. Il suit immédiatement que $\Xi_{x,\partial}$ est à valeur dans $k(x^p)[\partial^p]$. Un résultat analogue est vrai pour $\Xi_{\theta,\partial}$, il est d'ailleurs plus facile à démontrer. Dorénavant, nous considèrerons par abus de notations que $\Xi_{x,\partial}$ (resp. $\Xi_{\theta,\partial}$) est une application de $k(x)\langle\partial\rangle \to k(x^p)[\partial^p]$ (resp. $k(\theta)\langle\partial\rangle \to k(\theta^p - \theta)[\partial^p]$).

LEMME 2.2.3.13. — *$\Xi_{\theta,\partial}$ est à valeur dans $k(\theta^p - \theta)[\partial^p]$*

Preuve. Un calcul direct montre que pour tout $i \in \mathbb{N}^*$, $\Xi_{\theta,\partial}(\partial^i) = \partial^{pi}$.
Soit $G \in k(\theta)\langle\partial\rangle$. Grâce à la multiplicativité de $\Xi_{\theta,\partial}$, on peut supposer que G possède un terme de degré 0 non nul. Il est immédiat que pour tout $g_r \in k(\theta)$, $P(\theta) = g_r(\theta)\dots g_r(\theta + p - 1)$ vérifie $P(\theta) = P(\theta + 1)$. Ainsi P est un élément du centre de $k(\theta)\langle\partial\rangle$.
Il suffit donc de montrer que les coefficients de $\chi(B_p(G))$ sont dans $k(\theta^p - \theta)$. On note $B_p(G)(\theta) = B(\theta)\dots B(\theta + p - 1)$ où B est la matrice compagnon de G. Comme G est de terme de degré 0 non nul, il vient que $B(\theta)$ est inversible. On a alors :

$$B_p(G)(\theta + 1) = B(\theta)^{-1} B_p(G)(\theta) B(\theta).$$

Il suit que les coefficients de $\chi(B_p(G))$ sont invariants par translation $\theta \mapsto \theta + 1$. Donc ils sont éléments de $k(\theta^p - \theta)$. □

PROPOSITION 2.2.3.14. — *Soit $L \in k(x)\langle\partial\rangle$ (resp. $G \in k(\theta)\langle\partial\rangle$).*

1. *Le degré de $\Xi_{x,\partial}(L)$ (resp. $\Xi_{\theta,\partial}(G)$) en la variable ∂^p est égal au degré de L (resp. de G).*
2. *L (resp. G) divise $\Xi_{x,\partial}(L)$ (resp. $\Xi_{\theta,\partial}(G)$) à droite et à gauche.*
3. *Si L (resp. G) est irréductible alors $\Xi_{x,\partial}(L)$ (resp. $\Xi_{\theta,\partial}(G)$) est une puissance d'un élément irréductible de $k(x^p)[\partial^p]$ (resp. de $k(\theta^p - \theta)[\partial^p]$), le centre de $k(x)\langle\partial\rangle$ (resp. $k(\theta)\langle\partial\rangle$), à multiplication par un élément inversible près.*

Preuve. Les preuves pour $L \in k(x)\langle\partial\rangle$ et $G \in k(\theta)\langle\partial\rangle$ sont identiques. On la réalise pour $L \in k(x)\langle\partial\rangle$.
Le premier point est évident, cela vient du fait que le $k(x)$-espace vectoriel ${}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle L}$ considéré soit de dimension le degré de L.
La divisibilité de $\Xi_{x,\partial}(L)$ par L à droite est une conséquence du théorème de CAYLEY-HAMILTON. De plus comme on sait que $\Xi_{x,\partial}(L)$ est un élément central de $k(x)\langle\partial\rangle$ (puisque le polynôme caractéristique de la p-courbure est à coefficient dans $k(x^p)$), et par intégrité de $k(x)\langle\partial\rangle$, L en est également un diviseur à gauche.
En effet $\Xi_{x,\partial}(L) = QL$ et

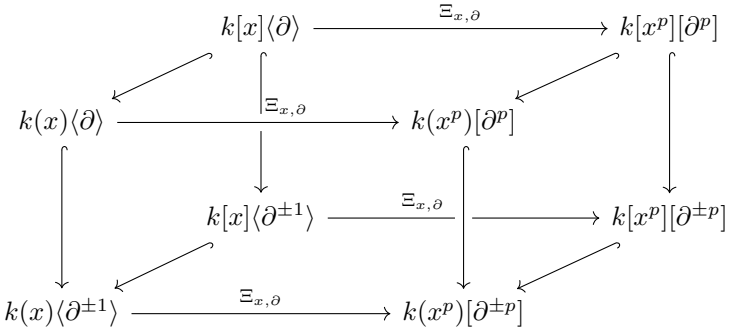
$$\Xi_{x,\partial}(L)L = QL^2 = L\Xi_{x,\partial}(L) = LQL \Rightarrow QL = LQ.$$

Supposons maintenant L irréductible. On commence par remarquer que l'on a un isomorphisme d'anneau $k(x^p)[X] \simeq k(x^p)[\partial^p]$. Il s'agit de prouver que $\Xi_{x,\partial}(L)$ n'a qu'un seul diviseur irréductible dans $k(x^p)[\partial^p]$.

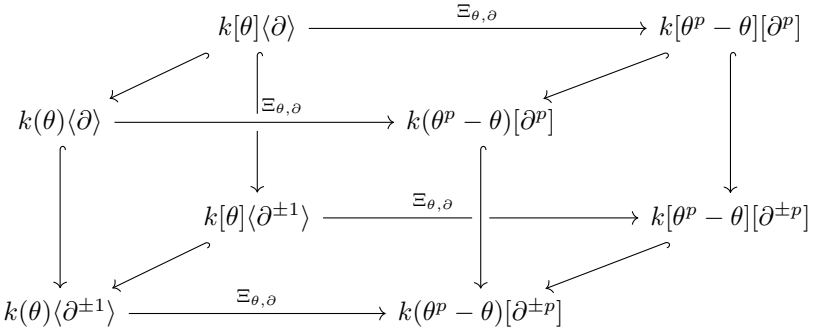
Remarque 2.2.3.15. — *On parle bien ici d'un élément irréductible de l'anneau $k(x^p)[\partial^p]$ est non d'un élément irréductible de $k(x)\langle\partial\rangle$ appartenant au sous-anneau $k(x^p)[\partial^p]$.*

Par l'isomorphisme qui précède, cela revient à voir que $\chi(A_p(L))$ n'a qu'un seul diviseur irréductible dans $k(x^p)[X]$. On va procéder par l'absurde. Supposons que $\chi(A_p(L))$ ait deux diviseurs irréductibles distincts dans $k(x^p)[X]$. Alors il existe $U, V \in k(x^p)[X]$ tels que $UN_1 + VN_2 = 1$ et encore $U(\partial^p)N_1(\partial^p) + V(\partial^p)N_2(\partial^p) = 1$. Alors $\mathrm{rgcd}(L, N_1(\partial^p)) = 1$ ou $\mathrm{rgcd}(L, N_2(\partial^p)) = 1$. En effet si tel n'était pas le cas alors L diviserait $N_1(\partial^p)$ et $N_2(\partial^p)$ à droite puisque L est irréductible et L diviserait 1 à droite ce qui est absurde.
Supposons donc $\mathrm{rgcd}(L, N_1(\partial^p)) = 1$. Alors L est inversible dans ${}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle N_1(\partial^p)}$ (qui possède bien une structure d'anneau car $N_1(\partial^p)$ est un élément du centre, il engendre donc un idéal bilatère). Mais L est un diviseur de $\Xi_{x,\partial}(L)$ égal à 0 dans ${}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle N_1(\partial^p)}$, donc L est un diviseur de zéro (à gauche et à droite). C'est une contradiction. □

Du Lemme 2.2.2.6 et de la définition de B_p il vient que si $L \in k[x]\langle\partial\rangle$ et $G \in k[\theta]\langle\partial\rangle$, alors $\Xi_{x,\partial}(L) \in k[x^p][\partial^p]$ et $\Xi_{\theta,\partial}(G) \in k[\theta^p - \theta][\partial^p]$. Comme ces deux opérateurs sont multiplicatifs, on peut les étendre à $k(x)\langle\partial^{\pm 1}\rangle$ et $k(\theta)\langle\partial^{\pm 1}\rangle$. On résume la situation dans les diagrammes suivants :



et



Notre but est maintenant de montrer que le diagramme suivant commute :

$$\begin{array}{ccc} k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & k[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow{\scriptstyle \Xi_{x,\partial}} & & \downarrow{\scriptstyle \Xi_{\theta,\partial}} \\ k[x^p][\partial^{\pm p}] & \xrightarrow{\sim} & k[\theta^p - \theta][\partial^{\pm p}] \end{array}$$

Pour ce faire nous allons montrer qu'après extension des scalaires, $k(x)\langle\partial\rangle$ et $k(\theta)\langle\partial\rangle$ se comportent comme des algèbres de matrices.

2.2.4 Isomorphisme avec des algèbres de matrices et application

On note dès à présent

$$\begin{aligned}\mathcal{D}_x &:= k[x]\langle\partial^{\pm 1}\rangle\\ \mathcal{Z}_x &:= k[x^p][\partial^{\pm p}]\\ \mathcal{D}'_x &:= k(x)\langle\partial^{\pm 1}\rangle\\ \mathcal{Z}'_x &:= k(x^p)[\partial^{\pm p}]\end{aligned}$$

$$\begin{aligned}\mathcal{D}_\theta &:= k[\theta]\langle\partial^{\pm 1}\rangle\\ \mathcal{Z}_\theta &:= k[\theta^p-\theta][\partial^{\pm p}]\\ \mathcal{D}'_\theta &:= k(\theta)\langle\partial^{\pm 1}\rangle\\ \mathcal{Z}'_\theta &:= k(\theta^p-\theta)[\partial^{\pm p}]\end{aligned}$$

dans le but d'alléger les notations. Nous allons réaliser deux constructions en parallèle, l'une pour la variable x et l'autre pour la variable θ en nous assurant que ces constructions se comportent bien pour nos isomorphismes.
On considère l'extension d'anneaux $\mathcal{Z}_\theta[T] \simeq {}^{\mathcal{Z}_\theta[X]}/_{(X^p-X-\theta^p+\theta)}$ où T est l'image de X par la projection canonique. On remarque dès à présent que $\mathcal{Z}_\theta[T]$ est une $\mathcal{Z}_\theta$-algèbre libre, dont une base est donnée par $(1, T, \dots, T^{p-1})$.
De même, il convient de voir que $\mathcal{D}_\theta$ est une $\mathcal{Z}_\theta$-algèbre libre. Cela revient par le Théorème 2.2.3.4 à prouver le résultat suivant :

PROPOSITION 2.2.4.1. — *$\mathcal{D}_x$ est une algèbre libre sur son centre $\mathcal{Z}_x$. Une base en est $(x^i\partial^j)_{\substack{0\leqslant i<p\\ 0\leqslant j<p}}$.*

Preuve. On commence par voir que la famille précédente est bien génératrice. Tout élément z de $k[x]\langle\partial^{\pm 1}\rangle$ peut s'écrire

$$z = \sum_{i,j} a_{i,j}x^i\partial^j$$

pour i, j variant dans $\mathbb{Z}$ de sorte que les $a_{i,j} \in k$ soient tous nuls sauf un nombre fini.
Il vient alors en notant pour tout élément i de $\mathbb{Z}$ $i = q_ip + r_i$ avec $0 \leqslant r_i < p$,

$$z = \sum_{i,j} a_{i,j}x^{q_ip}x^{r_i}\partial^{q_jp}\partial^{r_j}$$

et encore

$$z = \sum_{i,j} a_{i,j}x^{q_ip}\partial^{q_jp}x^{r_i}\partial^{r_j}$$

Ainsi la famille donnée est bien génératrice.
Il reste à voir qu'elle est libre. Supposons donc que

$$\sum_{i,j} p_{i,j}(x^p, \partial^{\pm p})x^i\partial^j = 0$$

Comme on sait que les $(\partial^j)_{j\in\mathbb{Z}}$ constituent une base de $\mathcal{D}'_x$ en tant que $k(x)$ espace vectoriel, on peut regrouper ces sommes pour classes de congruences de j modulo p :

$$\sum_{j=0}^{p-1}\left(\sum_{i=0}^{p-1} p_{i,j}(x^p, \partial^{\pm p}x_i)\right)\partial j$$

et on en déduit que pour tout j :

$$\sum_{i=0}^{p-1} p_{i,j}(x^p, \partial^{\pm p})x^i = 0$$

Mais on peut encore regrouper par classes de congruence modulo p de i ce qui donne $p_{i,j} = 0$ pour tout i et j. □

$\mathcal{D}_\theta$ est donc libre sur son centre. De plus, une base est donnée par $(\theta^i\partial^{j-i})_{\substack{0\leqslant i<p\\0\leqslant j<p}}$ soit encore, en multipliant par ∂^p certains termes (inversible dans $\mathcal{Z}_\theta$), par $(x_i\partial^j)_{\substack{0\leqslant i<p\\0\leqslant j<p}}$.

L'isomorphisme $\mathcal{Z}_x \simeq \mathcal{Z}_\theta$ induit un isomorphisme $\mathcal{Z}_x[X] \simeq \mathcal{Z}_\theta[X]$, et l'image réciproque de $X^p - X - \theta^p - \theta$ par cet isomorphisme est $X^p - X - x^p\partial^p$ ce qui induit encore un isomorphisme

$$\mathcal{Z}_x[T] = {}^{\mathcal{Z}_x[X]}\!/_{(X^p - X - x^p\partial^p)} \simeq \mathcal{Z}_\theta[T].$$

Par abus de notation on note $\mathcal{D}_\theta[T] = \mathcal{D}_\theta \otimes_{\mathcal{Z}_\theta} \mathcal{Z}_\theta[T]$ et $\mathcal{D}_x[T] = \mathcal{D}_x \otimes_{\mathcal{Z}_x} \mathcal{Z}_x[T]$. Il vient immédiatement des isomorphismes précédents que $\mathcal{D}_x[T] \simeq \mathcal{D}_\theta[T]$.

De ce qui précède on en déduit des bases de $\mathcal{D}_x[T]$ et $\mathcal{D}_\theta[T]$ en tant que $\mathcal{Z}_x$ et $\mathcal{Z}_x[T]$-module et $\mathcal{Z}_\theta$ et $\mathcal{Z}_\theta[T]$-module, respectivement.

On munit $\mathcal{Z}_x[T]$ et $\mathcal{Z}_\theta[T]$ d'une action de $\mathbb{F}_p$ définie par $a.P(T) = P(T+a)$. Ces actions sont bien définies car

$$(X+a)^p - (X+a) - \theta^p - \theta = X^p + a^p - X - a - \theta^p - \theta = X^p - X - \theta^p - \theta$$

d'une part, et

$$(X+a)^p - (X+a) - x^p\partial^p = X^p + a^p - X - a - x^p\partial^p = X^p - X - x^p\partial^p$$

d'autre part. De plus le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathcal{Z}_x[T] & \xrightarrow{T\mapsto T+a} & \mathcal{Z}_x[T] \\ \downarrow\wr & & \downarrow\wr \\ \mathcal{Z}_\theta[T] & \xrightarrow{T\mapsto T+a} & \mathcal{Z}_\theta[T] \end{array}$$

Ces actions permettent en outre permet de munir $\mathcal{D}_x[T]$ et $\mathcal{D}_\theta[T]$ d'actions de $\mathbb{F}_p$ similaires par les applications suivantes :

$$\begin{array}{rccc} \varphi_{*,a} & : \mathcal{Z}_*[T] & \to & \mathcal{D}_*[T] \\ & P(T) & \mapsto & P(T+a)\otimes 1 \end{array}$$

et $\iota_* : \mathcal{D} \hookrightarrow \mathcal{D}_*[T]$ l'injection canonique (où $* = x$ ou θ). Ces deux applications induisent bien une action de $\mathbb{F}_p$ sur $\mathcal{D}_*[T]$ (voir D.3). Le diagramme précédent induit le suivant :

$$\begin{array}{ccc} \mathcal{D}_x[T] & \xrightarrow{T\mapsto T+a} & \mathcal{D}_x[T] \\ \downarrow\wr & & \downarrow\wr \\ \mathcal{D}_\theta[T] & \xrightarrow{T\mapsto T+a} & \mathcal{D}_\theta[T] \end{array}$$

On veut à présent connaître les points fixes de cette action. La commutativité des deux diagrammes précédents permet de n'effectuer cette étude que sur l'une des deux variables x ou θ.

LEMME 2.2.4.2. — *L'ensemble des points fixes de l'action de $\mathbb{F}_p$ sur $\mathcal{Z}_\theta[T]$ est $\mathcal{Z}_\theta$*

Preuve. Tout élément $\overline{P}$ de $\mathcal{Z}_\theta[T]$ peut être vu comme l'image d'un unique $P \in \mathcal{Z}_\theta[X]$ avec P de degré au plus $p-1$. De plus pour tout $a \in \mathbb{F}_p$, ce polynôme est $P(X+a)$. Supposons que $\overline{P}$ soit un point fixe pour l'action de $\mathbb{F}_p$ sur $\mathcal{Z}_\theta[T]$. Alors pour tout $a \in \mathcal{Z}_\theta$, $P(X+a) = P(X)$, en particulier $P(0) = P(1) = \ldots = P(p-1)$. Ainsi $P - P(0)$ a au moins p racines. Comme $\mathcal{Z}_\theta$ est intègre, on en déduit que P est constant donc dans $\mathcal{Z}_\theta$, ainsi que $\overline{P}$. □

On en déduit que les points fixes de l'action de $\mathbb{F}_p$ sur $\mathcal{D}_\theta[T]$ sont les éléments de $\mathcal{D}_\theta$. En effet on a la suite exacte de $\mathcal{Z}_\theta$-modules :

$$0 \to \mathcal{Z}_\theta \to \mathcal{Z}_\theta[T] \xrightarrow{f_1} M \to 0$$

où $f_1 : P(T) \mapsto P(T+1) - P(T)$ et $M = \mathrm{Im}\,(f_1) \subset \mathcal{Z}_\theta[T]$.
Cette suite exacte passe alors au produit tensoriel par $\mathcal{D}_\theta$ qui est plat sur $\mathcal{Z}_\theta$, car libre, ce qui donne le résultat.

On en déduit que les ensembles des points fixes de l'action de $\mathbb{F}_p$ sur $\mathcal{Z}_x[T]$ et $\mathcal{D}_x[T]$ sont respectivement $\mathcal{Z}_x$ et $\mathcal{D}_x$.

On introduit les deux matrices suivantes, vues comme éléments de $M_P(\mathcal{Z}_\theta[T])$:

$$\mathcal{M}_\theta(\theta) = \begin{pmatrix} T & & & \\ & T+1 & & \\ & & \ddots & \\ & & & T+p-1 \end{pmatrix} \text{ et } \mathcal{M}_\theta(\partial) = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \partial^p & & & \end{pmatrix}$$

On vérifie facilement que $\mathcal{M}(\partial)\mathcal{M}(\theta) = (\mathcal{M}(\theta)+1)\mathcal{M}(\partial)$ et que de plus $\mathcal{M}(\partial)$ est inversible dans $M_p(\mathcal{Z}[T])$ car son déterminant est ∂^p, inversible dans $\mathcal{Z}_\theta[T]$. Par 2.2.3.3, on en déduit l'existence d'un unique morphisme $\mathcal{M} : \mathcal{D}_\theta \to M_p(\mathcal{Z}_\theta[T])$ envoyant θ et ∂ sur $\mathcal{M}_\theta(\theta)$ et $\mathcal{M}_\theta(\partial)$ respectivement. Combiné à $\mathcal{Z}_\theta[T] \to M_p(\mathcal{Z}_\theta[T])$, $P(T) \mapsto P(T).I_p$ cela donne encore un morphisme d'anneaux : $\mathcal{M}_\theta : \mathcal{D}_\theta[T] \to M_p(\mathcal{Z}_\theta[T])$.

PROPOSITION 2.2.4.3. — *Soit $L = \sum_{0 \leqslant i,j<p} a_{i,j}\theta^i\partial^j \in \mathcal{D}[T]$ avec $a_{i,j} \in \mathcal{Z}[T]$ pour tout i, j. Alors*

$$\mathcal{M}(L)_{i',j'} = \partial^{i'-j'+r} \sum_{i=0} a_{i,r}.(T+j')^i \tag{2.2.4.1}$$

où r est le reste de la division euclidienne de $j'-i'$ par p.

Preuve. On a

$$\mathcal{M}_\theta(\theta^i\partial^j) = \begin{pmatrix} & & & & T^i & & \\ & & & & & \ddots & \\ & & & & & & (T+p-j-1)^i \\ \partial^p(T+p-j)^i & & & & & & \\ & & \ddots & & & & \\ & & & \partial^p(T+p-1)^i & & & \end{pmatrix}$$

On vérifie alors que l'on a :

$$\mathcal{M}_\theta(\theta^i\partial^j)_{i',j'} = \partial^{i'-j'+r}\delta_{j,r}(T+j')^i$$

où δ est le symbole de Kronecker. On en déduit donc

$$\mathcal{M}_\theta(L)_{i',j'} = \sum_{i,j} \partial^{i'-j'+r} a_{i,j}\delta_{j,r}(T+j')^i$$

et encore

$$\mathcal{M}_\theta(L)_{i',j'} = \partial^{i'-j'+r} \sum_{i=0}^{p-1} a_{i,r}(T+j')^i$$

□

THÉORÈME 2.2.4.4. — *$\mathcal{M}_\theta$ réalise un isomorphisme de $\mathcal{Z}_\theta[T]$-algèbres $\mathcal{D}_\theta[T] \simeq M_p(\mathcal{Z}_\theta[T])$.*

Preuve. Cela revient à voir que connaissant tout les $M_{i',j'}$, on peut retrouver $L = \sum_{i,j} a_{i,j}\theta^i\partial^j$ tel que $\mathcal{M}_\theta(L) = M$.
Or à r fixé (avec les notations de la proposition précédente) cela revient à résoudre le système :

$$\begin{pmatrix} 1 & T & \cdots & T^{p-1} \\ 1 & T+1 & \cdots & (T+1)^{p-1} \\ \vdots & \vdots & & \vdots \\ 1 & T+p-1 & \cdots & (T+p-1)^{p-1} \end{pmatrix} \begin{pmatrix} a_{0,r} \\ a_{1,r} \\ \vdots \\ a_{p-1,r} \end{pmatrix} = \begin{pmatrix} \partial^{-p}M_{p-r,0} \\ \partial^{-p}M_{p-r+1,1} \\ \vdots \\ \partial^{-p}M_{p-1,r-1} \\ M_{0,r} \\ M_{1,r+1} \\ \vdots \\ M_{p-1-r,p-1} \end{pmatrix}$$

Or ce système est de VANDERMONDE et son déterminant vaut :

$$\prod_{0\leqslant i<j<p}(T+j)-(T+i)=\prod_{0\leqslant i<j<p}(j-i)\in\mathbb{F}_p^\times.$$

Il admet donc une unique solution pour tout r. Chaque choix de r faisant intervenir des $M_{i',j'}$ différents (puisque le reste de la division euclidienne de $j'-i'$ par p est différent), ceci achève la preuve de ce théorème. □

COROLLAIRE 2.2.4.5. — *$\mathcal{M}$ induit les isomorphismes suivants :*

$$k[\theta^p-\theta][\partial^{\pm p}][T]\otimes_{k[\theta^p-\theta][\partial^{\pm p}]}k[\theta]\langle\partial^{\pm 1}\rangle\simeq M_p(k[\theta^p-\theta][\partial^{\pm p}][T]) \tag{2.2.4.2}$$

$$k(\theta^p-\theta)[\partial^{\pm p}][T]\otimes_{k(\theta^p-\theta)[\partial^{\pm p}]}k(\theta)\langle\partial^{\pm 1}\rangle\simeq M_p(k(\theta^p-\theta)[\partial^{\pm p}][T]) \tag{2.2.4.3}$$

$$k[x^p][\partial^{\pm p}][T]\otimes_{k[x^p][\partial^{\pm p}]}k[x]\langle\partial^{\pm 1}\rangle\simeq M_p(k[x^p][\partial^{\pm p}][T]) \tag{2.2.4.4}$$

$$k(x^p)[\partial^{\pm p}][T]\otimes_{k(x^p)[\partial^{\pm p}]}k[x]\langle\partial^{\pm 1}\rangle\simeq M_p(k[x^p][\partial^{\pm p}][T]) \tag{2.2.4.5}$$

Preuve. (2.2.4.2) n'est rien d'autre que le théorème précédent. (2.2.4.3) vient en procédant à l'extension des scalaires de $k[\theta^p-\theta]$ à $k(\theta^p-\theta)$ et en appliquant D.5.
(2.2.4.4) se déduit de (2.2.4.2) par le diagramme suivant :

$$\begin{array}{ccc}\mathcal{D}_\theta[T] & \xrightarrow{\mathcal{M}_\theta}_{\sim} & M_p(\mathcal{Z}_\theta[T])\\ \downarrow\wr & & \downarrow\wr\\ \mathcal{D}_x[T] & \overset{\exists!\mathcal{M}_x}{\dashrightarrow}_{\sim} & M_p(\mathcal{Z}_x[T])\end{array}.$$

(2.2.4.5) se déduit de (2.2.4.4) en procédant à l'extension des scalaires de $k[x^p]$ et $k(x^p)$ et en appliquant D.5. □

On voit par ailleurs que $\mathcal{M}_x(x)$ est l'image par l'isomorphisme $\mathcal{Z}_\theta[T]\simeq\mathcal{Z}_x[T]$ de $\mathcal{M}_\theta(\theta)\mathcal{M}_\theta(\partial)^{-1}$. L'isomorphisme $\mathcal{M}_x$ est donc déterminé par

$$\mathcal{M}_x(x)=\begin{pmatrix}T+1 & & & \partial^{-p}T\\ & \ddots & & \\ & & T+p-1 & \end{pmatrix}\text{ et }\mathcal{M}_x(\partial)=\begin{pmatrix}1 & & \\ & \ddots & \\ & & 1\\ \partial^p & & \end{pmatrix}.$$

Munis de ces identifications, nous allons maintenant montrer que l'on peut voir les applications $\Xi_{\theta,\partial}$ et $\Xi_{x,\partial}$ comme des déterminants.
On peut définir les applications

$$\mathcal{N}_\theta:\mathcal{D}'_\theta[T]\overset{\mathcal{M}_\theta}{\simeq}M_p(\mathcal{Z}'_\theta[T])\xrightarrow{\det}\mathcal{Z}'_\theta[T]$$

et

$$\mathcal{N}_x:\mathcal{D}'_x[T]\overset{\mathcal{M}_x}{\simeq}M_p(\mathcal{Z}'_x[T])\xrightarrow{\det}\mathcal{Z}'_x[T].$$

Par ailleurs on a un isomorphisme $\mathcal{Z}_x\simeq\mathcal{Z}_\theta$ qui induit un isomorphisme $M_p(\mathcal{Z}_x[T])\simeq M_p(\mathcal{Z}_\theta[T])$. Ainsi le diagramme suivant commute :

$$\begin{array}{ccccc}\mathcal{D}_x[T] & \xrightarrow{\mathcal{M}_x} & M_p(\mathcal{Z}_x[T]) & \xrightarrow{\det} & \mathcal{Z}_x[T]\\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr\\ \mathcal{D}_\theta[T] & \xrightarrow{\mathcal{M}_\theta} & M_p(\mathcal{Z}_\theta[T]) & \xrightarrow{\det} & \mathcal{Z}_\theta[T]\end{array}$$

(avec $\mathcal{N}_x$ au-dessus et $\mathcal{N}_\theta$ en dessous)

Proposition 2.2.4.6. — *$\mathcal{N}_\theta$ commute à l'action de $\mathbb{F}_p$, cette action étant définie par l'extension des scalaires de $k[\theta^p-\theta]$ à $k(\theta^p-\theta)$, et par l'action de $\mathbb{F}_p$ sur $\mathcal{D}[T]$.*

En particulier cela assurera que $\mathcal{N}(\mathcal{D}'_\theta)$ est fixé par l'action de $\mathbb{F}_p$ et donc que c'est un élément de $\mathcal{Z}'_\theta$.

Preuve. On note $\sigma_\theta : \mathcal{D}_\theta[T] \to \mathcal{D}_\theta[T]$ l'application induite par $T \mapsto T+1$ sur $\mathcal{Z}_\theta[T]$ et par $\mathrm{Id}_{\mathcal{D}_\theta}$. Par abus de notation, on notera aussi σ_θ l'application sur $M_p(\mathcal{Z}[T])$ qui se déduit composante par composante de $T \mapsto T+1$.
Supposons qu'on ait $\mathcal{N}_{\theta|\mathcal{D}_\theta[T]} \circ \sigma_\theta = \sigma_\theta \circ \mathcal{N}_{\theta|\mathcal{D}_\theta[T]}$. Alors $\mathcal{N}_{\theta|\mathcal{D}_\theta[T]}$ commute évidemment à l'action de $\mathbb{F}_p$ sur $\mathcal{D}_\theta[T]$. Par ailleurs pour tout $L = \sum_{i\in I} f_i \otimes D_i$ où $D_i \in \mathcal{D}_\theta[T]$ et $f_i \in k(\theta^p-\theta)$, il existe $f \in k(\theta^p-\theta)$ de sorte que $L = f\left(\sum_{i\in I} p_i \otimes D_i\right)$ avec $p_i \in k[\theta^p-\theta]$ ce qui donne encore

$$L = f \otimes \left(\sum_{i\in I} p_i D_i\right)$$

ce qui permet d'écrire l'image de L par $\mathcal{M}_\theta$ (étendu à $\mathcal{D}'_\theta[T]$ à valeur dans $M_p(\mathcal{Z}'_\theta[T])$) comme étant

$$\mathcal{M}(L) = f\mathcal{M}(\sum_{i\in I} p_i D_i)$$

et encore pour tout $a \in \mathbb{F}_p$:

$$\begin{aligned}
\mathcal{N}_\theta(a.L) &= \det(\mathcal{M}_\theta(a.L)) \\
&= \det\left(\mathcal{M}_\theta\left(f \otimes a.\sum_{i\in I} p_i D_i\right)\right) \\
&= \det\left(f\mathcal{M}_\theta\left(a.\sum_{i\in I} p_i D_i\right)\right) \\
&= f^p \mathcal{N}_{\theta|\mathcal{D}[T]}\left(a.\sum_{i\in I} p_i D_i\right) \\
&= f^p a.\mathcal{N}_{\theta|\mathcal{D}[T]}\left(\sum_{i\in I} p_i D_i\right) \\
&= a.\mathcal{N}_\theta(L)
\end{aligned}$$

Il suffit donc de prouver qu'on a $\mathcal{N}_{\theta|\mathcal{D}[T]} \circ \sigma_\theta = \sigma_\theta \circ \mathcal{N}_{\theta|\mathcal{D}[T]}$.
On va en fait prouver que pour tout $L \in \mathcal{D}[T]$ on a

$$\mathcal{M}_\theta(\sigma_\theta(L)) = \mathcal{M}_\theta(\partial)^{-1}\sigma_\theta(\mathcal{M}_\theta(L))\mathcal{M}_\theta(\partial^{-1})$$

ce qui donnera le résultat en passant au déterminant.
Pour ceci, on remarque que $L \mapsto \mathcal{M}_\theta(\sigma_\theta(L))$ et $L \mapsto \mathcal{M}_\theta(\partial)^{-1}\mathcal{M}_\theta(L)\mathcal{M}_\theta(\partial^{-1})$ sont deux morphismes de $\mathcal{Z}_\theta$-algèbres. Par D.3, ils proviennent donc de deux couples (φ_1,ψ_1) et (φ_2,ψ_2) dans $\mathrm{Hom}_{\mathcal{Z}_\theta\text{-}\mathbf{mod}}(\mathcal{D}_\theta, M_p(\mathcal{Z}_\theta[T])) \times \mathrm{Hom}_{\mathcal{Z}_\theta\text{-}\mathbf{mod}}(\mathcal{Z}_\theta[T], M_p(\mathcal{Z}_\theta[T]))$ et il suffit de voir que $\varphi_1 = \varphi_2$ et $\psi_1 = \psi_2$. Mais encore, l'égalité $\varphi_1 = \varphi_2$ peut se tester uniquement sur θ et ∂ par la Proposition 2.2.3.3. L'égalité pour ∂ est triviale :

$$\mathcal{M}(\sigma_\theta(\theta)) = \mathcal{M}(\theta) = \mathcal{M}(\partial)^{-1}(\mathcal{M}(\theta)+\mathrm{Id})\mathcal{M}(\partial) = \mathcal{M}(\partial)^{-1}\sigma_\theta(\mathcal{M}(\theta))\mathcal{M}(\theta).$$

Il reste encore à voir que $\psi_1 = \psi_2$ c'est-à-dire que pour tout $L \in \mathcal{Z}[T]$ on a bien l'égalité recherchée. Mais cela est évident car $\mathcal{Z}[T]$ commute avec $\mathcal{M}(\partial)$. □

Remarque 2.2.4.7. — *L'action de $\mathbb{F}_p$ sur $\mathcal{D}'_\theta[T]$ peut être vue aussi comme l'action engendrée par $T \mapsto T+a$ sur $\mathcal{Z}'_\theta[T]$ et l'action triviale sur $\mathcal{D}'_\theta$.*

Corollaire 2.2.4.8. — *$\mathcal{N}_x$ commute avec l'action de $\mathbb{F}_p$ sur $\mathcal{D}'_x[T]$.*

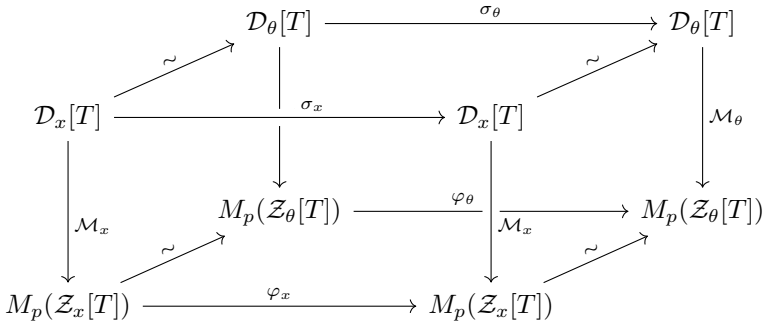
Preuve. Il suffit de voir que c'est le cas sur $\mathcal{D}_x[T]$ (de la même façon qu'on l'a montré pour $\mathcal{D}'_\theta[T]$). Notons $\sigma_x : \mathcal{D}_x[T] \to \mathcal{D}_x[T]$, $T \mapsto T+1$. Il suffit de montrer que $\mathcal{N}_{x|\mathcal{D}_x[T]} \circ \sigma_x = \sigma \circ \mathcal{N}_{x|\mathcal{D}_x[T]}$.
On sait déjà que pour tout $L \in \mathcal{D}_\theta[T]$ on a

$$\mathcal{M}_\theta(\sigma_\theta(L)) = \mathcal{M}_\theta(\partial)^{-1}\sigma_\theta(\mathcal{M}_\theta(L))\mathcal{M}_\theta(\partial)$$

où σ_θ est l'application définie sur $\mathcal{D}_\theta[T]$ similairement à σ_x.
Du diagramme ci-dessous on déduit que

$$\mathcal{M}_x(\sigma_x(L)) = \mathcal{M}_x(\partial)^{-1}\sigma_x(\mathcal{M}_x(L))\mathcal{M}_x(\partial)$$

ce qui donne le résultat.



où φ_x (resp. φ_θ) envoie tout $M \in M_p(\mathcal{Z}_x[T])$ (resp. $M_p(\mathcal{Z}_\theta[T])$) sur $\mathcal{M}_x(\partial)^{-1}\sigma_x(M)\mathcal{M}_x\partial)$ (resp. $\mathcal{M}_\theta(\partial)^{-1}\sigma_\theta(M)\mathcal{M}_\theta\partial)$. La commutativité de la face de devant vient de celle de toutes les autres faces. □

Ainsi $\mathcal{N}_x$ et $\mathcal{N}_\theta$ induisent deux applications de $\mathcal{D}'_\theta \to \mathcal{Z}'_\theta$ et $\mathcal{D}'_\theta \to \mathcal{Z}'_\theta$ respectivement, notées encore $\mathcal{N}_x$ et $\mathcal{N}_\theta$ par abus (minime) de notation. Ces applications sont appelées les normes réduites, respectivement de $\mathcal{D}'_x$ et $\mathcal{D}'_\theta$.

Remarque 2.2.4.9. — *Il suit immédiatement que le diagramme suivant est commutatif :*

$$\begin{array}{ccc} \mathcal{D}_x & \xrightarrow{\mathcal{N}_x} & \mathcal{Z}_x \\ \downarrow\wr & & \downarrow\wr \\ \mathcal{D}_\theta & \xrightarrow{\mathcal{N}_\theta} & \mathcal{Z}_\theta \end{array}$$

Lemme 2.2.4.10. — *$\mathcal{N}_\theta$ est multiplicative. Soit $L \in \mathcal{D}'_\theta$.*

(i) Si $L \in k[\theta]\langle\partial\rangle$ est de degré r en ∂, alors $\mathcal{N}(L)$ est dans $k[\theta^p-\theta][\partial^p]$ de degré exactement r en ∂^p. De plus, si les coefficients de L sont de degré au plus d en θ alors $\mathcal{N}(L)$ a ses coefficients de degré au plus d en $\theta^p-\theta$.

(ii) Si $L \in \mathcal{Z}_\theta$ alors $\mathcal{N}(L) = L^p$.

(iii) Si $L \in k(\theta)\langle\partial\rangle$ alors son coefficient dominant est $l_r(\theta)l_r(\theta+1)\dots l_r(\theta+p-1)$ où l_r est le coefficient dominant de L.

Preuve. La multiplicativité de $\mathcal{N}_\theta$ se déduit immédiatement de celle du déterminant.

(i) Supposons $L \in k[\theta]\langle\partial\rangle$. L'égalité (2.2.4.1) montre que $\mathcal{M}(L)$ ne fait pas intervenir de puissance négative de ∂, donc $\mathcal{N}(L) \in k[\theta^p-\theta][\partial^p]$.
On s'intéresse au degré en ∂. Pour toute matrice A à coefficients dans $k[\theta^p-\theta][\partial^p][T]$ on note $m(A) = \max\left(\sum_{\sigma\in\mathfrak{S}_p} d(A_{i,\sigma(i)})\right)$ où $d(A_{i,j})$ est le degré en ∂ du coefficients $A_{i,j}$. Par définition $\det(A)$ est de degré $m(A)$ en ∂. On voit que $m(\mathcal{M}_\theta(\theta^i\partial^j)) = pj$ pour tous i et j dans $\mathbb{N}$. Ainsi L est de degré r en ∂, d'où il suit immédiatement que $m(\mathcal{M}(L)) = pr$. Ainsi $\mathcal{N}_\theta(L)$ est de degré exactement r en ∂^p.

Supposons maintenant que les coefficients de L soient de degré au plus d en θ. Alors $\mathcal{M}_\theta(L)$ a ses coefficients en T de degré au plus d (ce qui se voit simplement par la formule). Il suit que son déterminant est de degré au plus dp en T. Comme on sait de plus que $\mathcal{N}_\theta(L) \in k[\theta^p - \theta][\partial^p]$ et que $T^p - T = \theta^p - \theta$, on en déduit le résultat.

(ii) Si $L \in \mathcal{Z}_\theta$ alors $\mathcal{M}(L) = L.\mathrm{Id}$ et donc $\mathcal{N}(L) = L^p$.

(iii) En divisant par le coefficient dominant on peut se ramener au cas où L est unitaire, et montrer que $\mathcal{N}_\theta(L)$ l'est aussi. Il est facile de voir que dans la formule du déterminant, la permutation donnant le terme de plus haut degré en ∂ est celle parcourant les termes non nuls de $\mathcal{N}_\theta(\partial^r)$. Le coefficient dominant de ce terme est 1 ce qui donne le résultat.

□

On montre le même résultat sur $\mathcal{D}'_x$. Pour la première fois, le résultat ne se transpose pas directement des isomorphismes entre les algèbres en la variable x et les algèbres en la variable θ.

PROPOSITION 2.2.4.11. — *$\mathcal{N}_x$ est multiplicative. De plus pour tout $L \in k(x^p)[\partial^p]$, $\mathcal{N}_x(L) = L^p$.*

Preuve. La multiplicativité provient directement de celle de déterminant. Le reste de la proposition est évidente. □

PROPOSITION 2.2.4.12. — *Si $L \in k(x)\langle\partial\rangle$ alors $\mathcal{N}(L) \in k(x^p)[\partial^p]$. De plus si L est de degré r en ∂, alors $\mathcal{N}_x(L)$ est de degré r en ∂^p.*

Preuve. La preuve de ce fait n'est pas aussi simple que pour θ, car $\mathcal{M}_x(x)$ fait intervenir une puissance négative de ∂^p. Néanmoins on sait que $\mathcal{N}_x(x) = x^p$, ce qui peut se voir de deux façons : On sait que $x^p \in \mathcal{Z}$ donc $\mathcal{N}(x^p) = \mathcal{N}(x)^p = x^{p^2}$ ce qui donne le résultat, ou alors par calcul direct on voit que

$$\mathcal{N}_x(x) = \left(\prod_{i=0}^{p-1}(T+i)\right)\partial^{-p} = (T^p - T)\partial^{-p} = x^p\partial^p\partial^{-p}.$$

Du calcul direct on voit que les produits de polynômes compensent la puissance négative de ∂^p. On a l'idée de changer de base de sorte que la nouvelle base contienne déjà les informations liées à ce produit.
Supposons donc que $\mathcal{M}_x(x)$ soit la matrice d'une application linéaire φ exprimée dans une base $\mathcal{B} = (e_0, \ldots, e_{p-1})$. On considère la famille $\mathcal{B}' = (e'_0, \ldots, e'_{p-1})$ vérifiant $e'_i = \left(\prod_{j=1}^{i}(T+j)\right)e_i$ pour tout i. Il s'agit bien d'une base, la matrice de changement de base étant inversible puisque tout les $(T+i)$ le sont.
On a alors pour $0 \leqslant i < p-1$

$$\varphi(e'_i) = \left(\prod_{j=1}^{i}(T+j)\right)\varphi(e_i) = \left(\prod_{j=1}^{i+1}(T+j)\right)e_{i+1} = e'_{i+1}$$

et

$$\varphi_{e'_{p-1}} = \left(\prod_{j=1}^{p-1}(T+j)\right)\varphi(e_{p-1}) = \partial^{-p}(T^p - T)e_0 = x^p e'_0.$$

Dans cette nouvelle base on peut donc écrire :

$$\mathcal{M}_x(x) = \begin{pmatrix} & & & x^p \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$$

Similairement on voit que dans cette base :

$$\mathcal{M}_x(\partial) = \begin{pmatrix} & T+1 & & \\ & & \ddots & \\ & & & T+p-1 \\ x^{-p}T & & & \end{pmatrix}$$

Comme le déterminant est invariant par changement de base, on peut le calculer dans cette base. On voit alors qu'aucun $L \in k(x)\langle\partial\rangle$ ne fait intervenir de puissance négative de ∂^p, donc $\mathcal{N}_x(L) \in k(x^p)[\partial^p]$.
On écrit à présent $L = \sum_j P_j(x)\partial^j$. On voit facilement que $\mathcal{M}_x(P_j(x)\partial^j)$ dans cette base n'a que des coefficients nuls ou de degré j en T.
Par ailleurs $\mathcal{N}(P_j(x)\partial^j) = P_j(x)^p\partial^{jp}$ est de degré jp en T. Considérons maintenant $L = \sum_{i=0}^r P_i(x)\partial^i$. On a

$$\det(\mathcal{M}_x(L)) = \sum_{\sigma\in\mathfrak{S}_p} (-1)^{\mathrm{sign}(\sigma)} \prod_{i=1}^p \mathcal{M}_x(L)_{i,\sigma(i)}$$

On peut dans cette somme isoler les termes de degré maximal. Ce sont ceux de degré pr en T. Pour que $\prod_{i=1}^p \mathcal{M}_x(L)_{i,\sigma(i)}$ soit de degré pr, il faut et il suffit que $\mathcal{M}_x(P_r(x)\partial^r)_{i,\sigma(i)}$ soit non nul. On peut alors voir que dans cet isolat, la somme des produits des monômes de degré maximal (r) réalise $\det(\mathcal{M}_x(P_r(x)\partial^p)) = P_r(x)^p\partial^{pr} \neq 0$. Comme toutes les autres combinaisons sont de degré moindre, on en déduit que $\mathcal{N}_x(L)$ est bien de degré r en ∂^p, et que de plus son coefficient dominant et celui de L à la puissance p. □

Nous avons à présent toutes les cartes en main pour identifier $\Xi_{x,\partial}$ avec $\mathcal{N}_x$ et $\Xi_{\theta,\partial}$ avec $\mathcal{N}_\theta$.

Proposition 2.2.4.13. — *Les applications $\Xi_{\theta,\partial}$ et $\mathcal{N}_\theta$ coïncident sur $\mathcal{D}'_\theta$.*

Preuve. Les deux applications sont multiplicatives. De plus, à tout $g(\theta) \in k(\theta)$, elles associent $g(\theta)g(\theta+1)\dots g(\theta+p-1)$.
Il suffit donc de vérifier le résultat pour $L \in k(\theta)\langle\partial\rangle$, irréductible et unitaire. Soit L un tel polynôme de Ore.
On sait que L divise $\Xi_{\theta,\partial}(L)$ à gauche et à droite on peut donc écrire :

$$\Xi_{\theta,\partial}(L) = L.L_1.$$

Il vient alors

$$\mathcal{N}(\Xi_{\theta,\partial}(L)) = \mathcal{N}(N_0^{n_0}) = N_0^{pn_0}$$

avec N_0 irréductible dans $k(\theta^p-\theta)[\partial^p]$ et unitaire, mais aussi

$$\mathcal{N}(\Xi_{\theta,\partial}(L)) = \mathcal{N}(L_0)\mathcal{N}(L_i).$$

Comme N_0 est irréductible, il existe un élément $z \in k(\theta^p-\theta)$ tel que $\mathcal{N}_\theta(L) = zN_0^{n_1}$. Comme $\mathcal{N}_\theta(L)$ et $\Xi_{\theta,\partial}(L)$ ont même degré on en déduit $n_1 = n_0$. De plus ils ont même coefficient dominant (1) donc $z = 1$, ce qui conclut. □

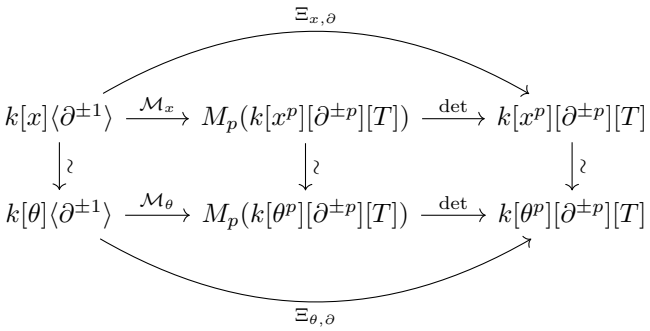
Théorème 2.2.4.14. — *$\Xi_{x,\partial}$ et $\mathcal{N}_x$ coïncident sur $\mathcal{D}'_x$.*

Preuve. De la multiplicativité de ces deux applications et du fait que $\mathcal{N}_x(g(x)) = \Xi_{x,\partial}(g(x))$ pour tout $g(x) \in k(x)$ on voit que l'on peut se contenter de vérifier que $\mathcal{N}_x$ et $\Xi_{x,\partial}$ coïncident sur tout $L \in k(x)\langle\partial\rangle$ irréductible, unitaire.
Soit L un tel polynôme. Comme L divise $\Xi_{x,\partial}(L)$ on peut écrire $L.L_1 = \Xi_{x,\partial}(L)$ avec $L_1 \in k(x)\langle\partial\rangle$. Mais de plus, comme L est irréductible, il existe $N \in k(x^p)[\partial^p]$ irréductible tel que $\Xi_{x,\partial}(L) = N^n$. On en déduit en passant à $\mathcal{N}_x$:

$$\mathcal{N}_x(L)\mathcal{N}_x(L_1) = N^{pn}$$

Comme N est irréductible, on en déduit que il existe $P(x^p) \in k(x^p)$ tel que $\mathcal{N}_x(L)$ soit égal $P(x)N^{n'}$. Comme de plus $\Xi_{x,\partial}(L)$ et $\mathcal{N}_x(L)$ ont même degré on en déduit que $n = n'$ Ils sont par ailleurs tous deux unitaires, donc coïncident. □

Il vient donc que le diagramme suivant commute, ce que l'on voulait démontrer :



3 Algorithmes de calcul du polynôme caractéristique de la p-courbure

Dans cette section nous décrivons plusieurs algorithmes de calcul du polynôme caractéristique de la p-courbure d'un opérateur différentiel, en nous servant des résultats de la section 2. Dans un premier temps nous aborderons la question de son calcul efficace pour un opérateur différentiel en caractéristique p, puis, en nous basant sur la méthode introduite dans la section 1, nous donnerons un algorithme efficace pour le calcul des p-courbures d'un opérateur différentiel en caractéristique 0 en un grand nombre de premiers p. L'intérêt de ce second algorithme vient de la conjecture de Grothendieck-Katz [Kat82] qui suggère qu'un système différentiel $Y' = AY$ en caractéristique 0 admet une base de solutions algébriques si et seulement si sa réduction modulo p admet une base de solutions algébriques (ce qui est équivalent à admettre une base de solutions rationnelles en caractéristique strictement positive) pour presque tout p, c'est-à-dire si sa p-courbure est nulle pour presque tout p premier.

3.1 Calcul efficace de la p-courbure d'un opérateur différentiel

Dans cette sous-section, nous présentons un algorithme de calcul du polynôme caractéristique de la p-courbure d'un opérateur différentiel à coefficients dans $k(x)$ où k est un corps de caractéristique p. Nous tâchons de mettre en lumière les améliorations que nous apporte le travail réalisé dans la section 2, ainsi que de réutiliser des techniques vues dans la section 1.

3.1.1 Calcul naïf

Nous commençons par décrire un algorithme naïf du calcul de la p-courbure.
Nous avions évoqué dans §2.2.2 que lorsque $M = K^n$ avec K un corps différentiel de caractéristique p, et $\partial_M Y = Y' - AY$ pour tout $Y \in M$, la p-courbure de M peut être calculée récursivement par la formule $A_0 = I_n$ et pour tout $k \leqslant p$, $A_k = A'_{k-1} - AA_{k-1}$.
A_p est alors la matrice de la p-courbure.
Dans le cas où $M = {}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$ avec $L \in K\langle\partial\rangle$ la matrice A contient énormément de zéros, on peut simplifier les calculs. Cela revient à trouver pour $p \leqslant k < p+m$, avec m le degré de L, $R_k \in K\langle\partial\rangle$, avec $\deg(R_k) < m$ tel que

$$\exists Q_k \in K\langle\partial\rangle, \partial^k = Q_k L + R_k.$$

On sait qu'un tel R_k existe et qu'il est unique pour tout k.
On note $R_k = \sum_{l=0}^{m-1} R_{k,l}\partial^l$.
Pour $k < m$ il vient immédiatement que $R_k = \partial^k$.
Notons $L = \sum_{k=0}^{m} L_k \partial^k$.

On a maintenant

$$\begin{aligned}
\partial^{k+1} &= \partial\partial^k \\
&= \partial(Q_k L + R_k) \\
&= \partial Q_k L + \partial R_k \\
&= \partial Q_k L + \sum_{l=0}^{m-1} \partial R_{k,l}\partial^l \\
&= \partial Q_k L + \sum_{l=0}^{m-1} R_{k,l}\partial^{l+1} + \sum_{l=0}^{m-1} R'_{k,l}\partial^l \\
&= Q_k L + R'_{k,0} + R_{k,m-1}\partial^m + \sum_{l=1}^{m-1} (R_{k,l-1} + R'_{k,l})\partial^l \\
&= \left(Q_k + \frac{R_{k,m-1}}{L_m}\right) L + R_{k,0} - \frac{R_{k,m-1}}{L_m} l_0 + \sum_{l=1}^{m-1} \left(R_{k,l-1} + R'_{k,l} - \frac{R_{k,m-1}}{L_m} L_l\right) \partial^l
\end{aligned}$$

ce qui donne une formule de récurrence pour les R_k :

$$R_0 = 1$$

puis

$$R_{k+1,0} = R'_{k,0} - \frac{R_{k,m-1}}{L_m} L_0$$

et

$$R_{k+1,l+1} = R_{k,l} + R'_{k,l+1} - \frac{R_{m,m-1}}{L_m} L_{l+1}.$$

On en déduit l'algorithme suivant :

Données : $L \in K\langle\partial\rangle$
Résultat : $A_p(L)$ la matrice de la p-courbure de L dans la base canonique

$R \leftarrow [0, \dots, 0, 1]$ une liste de taille m, indexée de 0 à $m-1$;
$A_p \leftarrow$ la matrice vide ;
pour k *allant de* m *à* $p+m-1$ **faire**
  $R_1 \leftarrow \left[R'_0 - \frac{R_{m-1}}{L_m} L_0, \dots, 0\right]$ une liste de taille m, indexée de 0 à $m-1$;
  pour l *allant de* 1 *à* $m-1$ **faire**
    $R_{1,l} \leftarrow R'_l + R_{l-1} - \frac{R_{m-1}}{L_m} L_l$
  $R \leftarrow R_1$;
  si $k \geqslant p$ **alors**
    Ajouter R à la fin de A_p en tant que vecteur colonne
retourner A_p

Algorithme 12 : Calcul naïf de la p-courbure

On suppose que $K = k(x)$ avec k un corps fini de caractéristique p. Par convention, nous dirons que le degré d'une écriture d'un élément de $k(x)$ est le maximum des degrés de son numérateur et de son dénominateur. Par abus, lorsque l'écriture sera claire dans le contexte, nous parlerons simplement du degré d'une fraction rationnelle.
Pour simplifier, on suppose que L est unitaire et que tous ses coefficients ont même dénominateur P, et on note d le degré maximal de ses coefficients sous cette hypothèse.

Remarque 3.1.1.1. — *Tout élément L de $k(x)\langle\partial\rangle$ peut se ramener à une telle forme. Cependant si les coefficients de L sont de degré maximal d, effectuer une telle transformation donne un opérateur différentiel dont les coefficients sont de degrés pouvant aller jusqu'à dm, où $m = \deg(L)$.*
Nous ne serons pas confrontés à ce problème car nous considèrerons essentiellement des opérateurs initialement à coefficients dans $k[x]$, mais l'utilisateur qui voudrait étendre ces algorithmes à $k(x)$ devra y prendre garde.

Chaque étape de calcul (où l'on calcule un nouveau R) prend $O(m)$ multiplications dans $k(x)$. De plus par hypothèse sur les dénominateurs de L, les coefficients de R ont à chaque étape pour dénominateur une puissance de P, dont on peut montrer par récurrence qu'elle n'excède pas i à la i-ème étape. Il suit que les coefficients de R sont de degrés au plus id à la i-ème étape.
On obtient donc un coût de l'algorithme en $O(mdp^2 \log(dp) \log\log(dp))$ opérations arithmétiques dans k. En particulier lorsque $k = \mathbb{F}_p$ on obtient un coût en

$$O(mdp^2 \log(dp) \log(p) \log\log(dp) \log\log(p) \log\log\log(p)) \text{ opérations binaires.}$$

Remarque 3.1.1.2. — *La complexité qui nous intéresse ici est la complexité en p. Cela n'est pas forcément intuitif dans la mesure où l'on travaille a priori à p fixé, mais notre objectif final est le calcul de la p-courbure d'un opérateur fixé en caractéristique 0 pour un grand nombre de premiers p, ce qui justifie ce choix. A cet égard la complexité de cet algorithme en p est en $O(p^2 \log^2(p) \log\log(p)^2 \log\log\log(p))$.*

Le but de la sous-section suivante est d'arriver à un algorithme de complexité quasi-linéaire pour le calcul du polynôme caractéristique de la p-courbure. Nous améliorerons ensuite encore cette complexité pour arriver à un algorithme effectuant ce calcul en $\tilde{O}(\sqrt{p})$ opérations binaires. Nous n'avons pas encore réalisé le calcul du polynôme caractéristique et nous sommes encore loin du compte. Nous allons, à partir de maintenant, nous servir des résultats de la section 2.

3.1.2 Algorithme quasi-linéaire pour un seul premier p

Soit $L \in k(x)\langle\partial\rangle$. Quitte à multiplier par un multiple commun à tous les dénominateurs des coefficients de L, on peut supposer que L est à coefficients dans $k[x]\langle\partial\rangle$. Pour simplifier les notations on note toujours d le degré maximal des coefficients de L.

Remarque 3.1.2.1. — *Cette notation est un peu abusive, car la multiplication par un multiple commun aux dénominateurs donne des polynômes de degrés jusqu'à éventuellement dm. Par la suite nous ne travaillerons qu'avec des opérateurs différentiels à coefficient dans $k[x]$.*
L'utilisateur qui voudrait appliquer ces algorithmes à des opérateurs à coefficients dans $k(x)$ devra prendre garde à cet abus.

Nous avons prouvé dans la section 2 que l'on a un diagramme commutatif :

$$\begin{array}{ccc} k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & k[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow \Xi_{x,\partial} & & \downarrow \Xi_{\theta,\partial} \\ k[x^p][\partial^{\pm p}] & \xrightarrow{\sim} & k[\theta^p-\theta][\partial^{\pm p}] \end{array}$$

L'algorithme que nous allons en déduire peut donc être résumé ainsi :

Données : $L \in k[x]\langle\partial\rangle$
Résultat : $\chi(A_p(L))(Y) \in k(x)[Y]$

Calculer L' l'image de L par l'isomorphisme ;
Calculer $P := \Xi_{\theta,\partial}(L')$;
Calculer l'image réciproque de P par l'isomorphisme ;
En déduire $\chi(A_p(L))$;
retourner $\chi(A_p(L))$

Nous allons voir comment effectuer chaque étape efficacement.

Théorème 3.1.2.2. — *Soit $L \in k[x]\langle\partial^{\pm 1}\rangle$ de degré m et dont les coefficients sont de degrés au plus $d \in \mathbb{N}$. Le calcul de l'image de L par l'isomorphisme peut s'effectuer en*

$$O(md^2 \log(p) \log\log(p) \log\log\log(p)) \text{ opérations binaires.}$$

Preuve. Le calcul de l'isomorphisme peut se faire naïvement en lisant chaque monôme de L de la forme $ax^k\partial^l$. On sait qu'un tel monôme est envoyé sur $a(\theta\partial^{-1})^k\partial^l$ ce qui peut encore s'écrire : $a\theta(\theta-1)(\theta-2)\dots(\theta-k+1)\partial^{l-k}$. Pour s'épargner de refaire plusieurs fois les mêmes calculs, on peut garder en mémoire les valeurs de $\theta(\theta-1)\dots(\theta-i)$. De plus en notant :

$$\theta(\theta-1)\dots(\theta-i) = \sum_{k=0}^{i+1} u_{i,k}\theta^k$$

on trouve

$$\begin{aligned} u_{i+1,0} &= -(i+1)u_{i,0} \\ u_{i+1,k} &= u_{i,k-1} - (i+1)u_{i,k} \text{ pour } k \leqslant i+1 \\ u_{i+1,i+2} &= 1 \end{aligned}$$

Le calcul des $\theta(\theta-1)\dots(\theta-i)$ peut ainsi n'être effectué qu'une seule fois en $O(d^2)$ opérations arithmétiques dans $\mathbb{Z}/p\mathbb{Z}$.
De plus chaque calcul de l'image des monômes donne un polynôme de degré au plus d. Cela assure

que les coefficients de l'image de L dans $k[\theta]\langle\partial^{\pm 1}\rangle$ sont de degrés au plus d. Chaque calcul de l'image d'un monôme donne lieu à une addition de polynômes de degré au plus d, coûtants au plus d opérations arithmétiques dans $\mathbb{Z}/p\mathbb{Z}$. Le calcul naïf de l'isomorphisme peut donc se faire en $O(md^2\log(p)\log\log(p)\log\log\log(p))$ opérations binaires. □

Remarque 3.1.2.3. — *Ce coût pourrait certainement être amélioré, mais il est négligeable en p par rapport à ce qui suit .*
On voit en revanche qu'en l'état, le simple calcul de l'isomorphisme rend la complexité en d moins bonne que l'algorithme naïf.

On s'intéresse maintenant au calcul de $\chi_{\theta,\partial}(L')$. Pour simplifier les notations nous renotons $L \in k[\theta]\langle\partial^{\pm 1}\rangle$ et tâchons de calculer $\Xi_{\theta,\partial}(L)$.

Remarque 3.1.2.4. — *Pour les besoins de la section 2, nous avions défini $\Xi_{\theta,\partial}(L) := L_m(\theta)\dots L_m(\theta+p-1)\chi(B_p(L))(\partial^p)$, avec L_m le coefficient dominant de L. Si cette écriture est parfaitement adaptée aux besoins de la démonstration mathématique, on préférera dans cette section prendre*

$$\Xi_{\theta,\partial}(L) := L_m(\theta)\dots L_m(\theta+p-1)\chi(B_p(L))(Y) \in k[\theta^p-\theta][Y^{\pm 1}].$$

Similairement on prendra :

$$\Xi_{x,\partial}(L) := L_m^p\chi(A_p(L))(Y) \in k[x^p][Y^{\pm 1}]$$

(pour un autre $L \in k[x]\langle\partial^{\pm 1}\rangle$).

On peut écrire $L = L_1\partial^{-k}$, avec $L_1 \in k[\theta]\langle\partial\rangle$ et $k \in \mathbb{N}$. On sait alors que

$$\Xi_{\theta,\partial}(L) = \Xi_{\theta,\partial}(L_1)\Xi_{\theta,\partial}(\partial^{-k}) = \Xi_{\theta,\partial}(L_1)Y^{-k}.$$

On peut donc supposer que $L \in k[\theta]\langle\partial\rangle$.

Remarque 3.1.2.5. — *Dans les paragraphes qui viennent, nous ne considèrerons que $L \in k[\theta]\langle\partial\rangle$, de degré m et dont les coefficients sont de degrés au plus d. Nous faisons ici un bref récapitulatif, visant à rappeler les valeurs de ces nouveaux L, m et d par rapport à ceux relatifs au $L \in k[x]\langle\partial\rangle$ d'origine.*
Nous avions $L \in k[x]\langle\partial\rangle$ de degré m et dont les coefficients sont de degrés au plus d. Nous calculons son image par l'isomorphisme d'algèbres de polynômes de Ore, $L' \in k[\theta]\langle\partial^{\pm 1}\rangle$. Les coefficients relatifs à ∂^i, pour $i \in \mathbb{Z}$, de L' sont nuls pour i en dehors de $[\![-d, m]\!]$. On en déduit qu'il existe $L_1 \in k[\theta]\langle\partial\rangle$ tel que $L' = L_1\partial^{-d}$.
Les coefficients de L_1 sont alors de degrés au plus d, mais L_1 est de degré au plus $m+d$. Nous effectuons donc maintenant « la réaffectation » :

$$\begin{aligned} L &\leftarrow L_1 \\ d &\leftarrow d \\ m &\leftarrow m+d \end{aligned}$$

Nous devrons nous en souvenir lors du calcul final de la complexité.

On note $B(L)$ la matrice compagnon de L. La première étape consiste à calculer $B(L)(\theta)B(L)(\theta+1)\dots B(L)(\theta+p-1)$. Les seuls coefficients de $B(L)$ non constants étant des fractions rationnelles dont les numérateurs sont, au signe près, les coefficients de L, et les dénominateurs, son coefficient dominant, nous devons d'abord calculer pour tout i et tout $j \in [\![1; p-1]\!]$, $L_i(\theta+j)$ où $L = \sum_i L_i\partial^i$. Dans ce but on remarque que

$$\begin{array}{ccc} k[\theta]_d & \to & k[\theta]_d \\ P & \mapsto & P(\theta+1) \end{array}$$

est une application linéaire dont la matrice dans la base canonique est donnée par :

$$M := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & d \\ 0 & 0 & 1 & \cdots & \binom{d}{2} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

laquelle peut être calculée par récurrence en $O(d^2)$ additions dans $\mathbb{Z}/p\mathbb{Z}$ soit en $O(d^2\log(p))$ opérations binaires.

En écrivant les $L_i = \sum_{j=0}^{d} L_{i,j}x^j$ on obtient, en identifiant tout $P \in k[x]_d$ au vecteur le représentant dans la base canonique,

$$L_i(\theta+1) = M\begin{pmatrix} L_{i,0} \\ L_{i,1} \\ \vdots \\ L_{i,d} \end{pmatrix}$$

Comme on a un certain nombre de vecteurs à translater, on considère la matrice A_0 dont les vecteurs colonnes sont les L_i, complétés par des zéros de sorte que A_0 soit de taille $d \times nd$ pour un certain $n \in \mathbb{N}$. La matrice A_0 est de taille exactement $d \times d\left\lceil \frac{m}{d} \right\rceil$.
La configuration de cette matrice permet d'effectuer le calcul de MA_0 en effectuant exactement $\left\lceil \frac{m}{d} \right\rceil$ multiplication de matrice de tailles $d \times d$ à coefficient dans $\mathbb{Z}/p\mathbb{Z}$.

Remarque 3.1.2.6. — *On introduit la notation $(A_0|A_1|A_2\dots|A_k)$ pour désigner la concaténation des matrices $A_0, A_1, \dots, A_n$, où celles-ci sont des matrices quelconques, dont les colonnes font toutes la même longueur.*

Comme il est évident que $P(\theta+i) = M^iP$ pour tout $i \in [\![0, p-1]\!]$, notre but est de connaitre les M^iA_0 pour $i \in [\![0, p-1]\!]$. Supposons que l'on connaisse les M^iA_0 pour tout $i \leqslant j$. On peut alors connaitre les M^iA_0 pour tout $i \leqslant 2j+1$ en faisant le calcul :

$$M^{j+1}(A_0|MA_0|M^2A_0|\dots|M^jA_0) = (M^{j+1}A_0|M^{j+2}A_0|\dots|M^{2j+1}A_0)$$

On en déduit l'algorithme suivant :

Données : A une matrice de taille $d \times nd$ pour un certain d,$p \in \mathbb{N}$
Résultat : $(A|MA|M^2A|\dots|M^{p-1}A)$

$i \leftarrow 2$;
$M_1 \leftarrow M$;
$A_0 \leftarrow (A|MA)$;
tant que $i < p$ **faire**
  $M_1 \leftarrow M_1^2$;
  $A_0 \leftarrow (A_0|M_1A_0)$;
  $i \leftarrow 2i$
retourner A_0

On applique cet algorithme à A_0 et p. La taille de A_0 double à chaque étape. On peut donc exprimer le coût de cet algorithme $C(m,p)$ en multiplications de matrices de tailles d de la sorte :

$$C(m,p) = \sum_{i=0}^{\lceil \log_2(p) \rceil} 2^i \left\lceil \frac{m}{d} \right\rceil$$

Il en résulte (en notant $\mathrm{MM}(d)$ le coût en opérations arithmétiques dans $\mathbb{A}$, un anneau quelconque, de la multiplication de deux matrices de tailles d à coefficients dans $\mathbb{A}$) le résultat suivant :

Proposition 3.1.2.7. — *Le calcul des $B(L)(\theta), B(L)(\theta+1), \dots, B(L)(\theta+p-1)$ peut s'effectuer en $O\left(p\frac{m}{d}\mathrm{MM}(d)\log(p)\log\log(p)\log\log\log(p)\right)$ opérations binaires.*

Remarque 3.1.2.8. — *Le coût ici est déjà linéaire en p alors que l'on voudrait un algorithme en $p^{1/2+o(1)}$ opérations binaires. Nous devrons être plus astucieux pour le calcul de cette factorielle de matrice pour y parvenir. En attendant nous présentons un algorithme quasi-linéaire en p.*

Par ailleurs le coût de cet algorithme n'est même pas quasi-linéaire en d. Une autre idée aurait été de procéder par évaluation-interpolation : on peut facilement connaitre les valeurs de $P(\theta+1)$ en certains points choisis à partir d'une évaluation multipoints de P. On sait alors réaliser une

interpolation sur d points en temps quasi-linéaire en d (ce que l'on admet). Il suit que l'on aurait pu effectuer ce calcul en $(dpm)^{1+o(1)}$ opérations binaires, ce qui n'est pas le cas ici (à moins de prouver que $\mathrm{MM}(d) = O(d^2)$ bien sûr). Cette méthode oblige cependant à disposer d'au moins d points dans $\mathbb{Z}/p\mathbb{Z}$ et donc à supposer $d \leqslant p$.
Nous ferons cette hypothèse plus tard dans ce mémoire, mais elle rend peu pertinente l'étude de la complexité en d (sauf dans les cas limites $d \sim p$), dont nous avions convenu de toute façon, qu'elle ne nous intéressait qu'assez peu.

En résumé, cette méthode n'est donc pas optimale, mais cela a peu d'importance pour la discussion qui nous occupe.

Calculons maintenant le produit $B(L)B(L)(\theta+1)\dots B(L)(\theta+p-1)$. Nous pourrions faire ce produit naïvement, c'est-à-dire en calculant successivement les

$$B_j(L) = \prod_{i=0}^{j-1} B(L)(\theta+i)$$

par la formule

$$B_{j+1}(L) = B_j(L)B(L)(\theta+j).$$

Cependant comme les $B(L)(\theta+i)$ ont tous des coefficients de degrés au plus d on en déduit que $B_j(L)$ a des coefficients de degrés au plus jd. Le calcul de $B_{j+1}(L)$ à partir de $B_j(L)$ coûte donc

$$O(\mathrm{MM}(m)jd\log(jd)\log(p)\log\log(jd)\log\log(p)\log\log\log(p)) \text{ opérations binaires.}$$

Le coût du calcul de $B_p(L)$ coûte donc $p^{2+o(1)}$ opérations binaires. On pourrait procéder par scindage binaire pour diminuer ce coût, mais on va être plus intelligent.

On sait par 2.2.4.10 que $\Xi_{\theta,\partial}$ a ses coefficients de degrés au plus d en $\theta^p - \theta$.
Supposons que l'on ait $P \in k[\theta^p - \theta]$. On peut écrire P de deux façons différentes :

$$P = \sum_{i=0}^{d} p_i(\theta^p-\theta)^i$$

et

$$P = \sum_{i=0}^{dp} p'_i\theta^i.$$

Le calcul de $\Xi_{\theta,\partial}(L)$ par celui du polynôme caractéristique de $B_p(L)$ nous donnera un polynôme de $k[\theta^p-\theta][Y]$ dont les coefficients seront données sous la deuxième forme.
Comme notre but ultime est de trouver l'image de $\Xi_{\theta,\partial}(L)$ par l'isomorphisme

$$\begin{array}{ccc} k[\theta^p-\theta][\partial^{\pm p}] & \to & k[x^p][\partial^{\pm p}] \\ \theta^p-\theta & \mapsto & x^p\partial^p \end{array}$$

on préfèrerait connaître ses coefficients sous la première forme.

Proposition 3.1.2.9. — *Soit $P \in k[\theta^p-\theta]$. Avec les notations précédentes, on a, pour $0 \leqslant i < p$, $p_i = (-1)^i p'_i$*

Preuve. Cela vient du fait que $(\theta^p-\theta)^d \equiv (-1)^d\theta^d \mod \theta^p$. □

Pour les coefficients p_i avec $i \geqslant p$, on peut effectuer la division euclidienne de P par $(\theta^p-\theta)^p$. En écrivant

$$P = P_1.(\theta^{p^2} - \theta^p) + R.$$

On trouve le reste des coefficients en appliquant le résultat récursivement à P_1.

On fait à présent l'hypothèse que $d < p$. Ce qui précède montre que l'on peut retrouver $\Xi_{x,\partial}$ à partir de $\Xi_{\theta,\partial}$ mod θ^{d+1}. Nous allons donc calculer modulo θ^{d+1}.

Cependant $B(L)$ est à coefficients dans $k(\theta)$, on ne peut donc pas quotienter par l'idéal engendré par θ^{d+1} (puisque celui-ci est inversible dans $k(\theta)$).
On note f le coefficient dominant de L et $P = \prod_{i=0}^{p-1} f(\theta + i)$. On sait que $fB(L)$ est à coefficients dans $k[\theta]$, et donc que $PB_p(L)$ aussi.
Nous voulons calculer $P\chi(B_p(L)) = P\det(Y\mathrm{Id} - B_p(L)) \bmod \theta^{d+1}$. Nous pouvons calculer

$$F(\theta, Y) = \chi(PB_p(L)) = \det(Y\mathrm{Id} - PB_p(L)) \bmod \theta^{d+1}.$$

Nous aurons alors

$$F(\theta, P.Y) = P^{m-1}\Xi_{\theta,\partial}(L) \bmod \theta^{d+1}.$$

Il suffit alors de savoir récupérer $\Xi_{\theta,\partial} \bmod \theta^{d+1}$ à partir de $F(\theta, PY) \bmod \theta^{d+1}$ et $P^{m-1} \bmod \theta^{d+1}$.

Cela peut-être fait en $O(d\log(d)\log\log(d))$ opérations binaires.

THÉORÈME 3.1.2.10. — *Soient $P, Q \in k[X]$ où k est un corps quelconque, $i \in \mathbb{N}^*$. Soient $P_1, A \in k[x]$ tels que $\deg(P_1) < i$ et $\deg(A) < i$ et*

$$P \equiv P_1 \bmod X^i$$

$$PQ \equiv A \bmod X^i$$

On suppose que $P(0) \neq 0$. On peut alors retrouver $Q \bmod X^i$ en une division euclidienne à partir de A et P_1.

Preuve. Supposons $Q \equiv Q_1 \bmod X^i$ avec $\deg(Q_1) < i$. On a alors $PQ \equiv P_1Q_1 \bmod X^i$. Malheureusement P_1Q_1 n'est pas le reste de la division euclidienne de PQ par X^i puisque P_1Q_1 peut être de degré $2(i-1)$.
On sait en revanche que $A \equiv P_1Q_1 \bmod X^i$. Ainsi les derniers termes de A et de P_1Q_1 coïncident. Pour pouvoir effectuer la division euclidienne on a donc l'idée de « retourner » les polynômes.
On commence par écrire $A = P_1Q_1 + X^iR$ pour un certain $R \in k[X]$ avec. On note également $d = \deg(P_1) < i$. Comme P_1Q_1 et de degré au plus $d + i - 1$ on en déduit que R est de degré au plus $d - 1$. On peut alors écrire :

$$X^{i+d-1}A\left(\frac{1}{X}\right) = X^dP_1\left(\frac{1}{X}\right)X^{i-1}Q_1\left(\frac{1}{X}\right) + X^{d-1}R\left(\frac{1}{X}\right)$$

On a écrit la division euclidienne de $X^{i+d-1}A\left(\frac{1}{X}\right)$ par $X^dP_1\left(\frac{1}{X}\right)$ qui est bien de degré d car X ne divise pas P_1. On peut facilement en déduire Q_1. □

Ce théorème et sa preuve nous donne un moyen de retrouver facilement $\Xi_{\theta,\partial}$ lorsque θ ne divise pas P. Nous faisons pour l'heure cette hypothèse.

REMARQUE 3.1.2.11. — *Cette hypothèse revient à demander que f, le coefficient dominant de L n'ait pas de racines dans $\mathbb{F}_p$. Bien que cette hypothèse paraisse forte, elle ne l'est pas tant que ça dans les cas qui nous intéresse.*
En effet les polynômes de ORE qui nous intéresse sont les L_1 provenant d'un $L \in k[x]\langle\partial\rangle$. On se convainc alors facilement que le coefficient dominant de L_1 ne peut être de degré n avec $n \leqslant d$ que si x^n divise le coefficient dominant de L, x^{n-1} divise le coefficient suivant, x^{n-2} le suivant, etc.
Les cas les plus fréquents sont ceux où f est une constante, et la méthode que nous venons de décrire est alors un luxe de complexité superflu car $B(L)$ est en fait à coefficients dans $k[\theta]$, et ceux où f est de degré 1 et nous sommes…coincés pour l'instant. En fait dans ce cas on sait que P^{m-1} a $m-1$ pour valuation θ-adique. On peut alors calculer $F(\theta, PY) \bmod \theta^{d+m}$, diviser par θ^{m-1} puis par la méthode précédente, par $\frac{P^{m-1}}{\theta^{m-1}}$.

Ainsi on peut effectuer le calcul des coefficients de $PB_p(L) \bmod \theta^{d+1}$ de manière naïve en $p-1$ multiplications de matrices carrées de taille m dont les coefficients sont des éléments de $\mathbb{F}_p[\theta]$ de degrés au plus d. On en déduit un coût final en

$$O(p\mathrm{MM}(m)d\log(d)\log(p)\log\log(d)\log\log(p)\log\log\log(p)) \text{ opérations binaires.}$$

Remarque 3.1.2.12. — *En fait à cause du phénomène décrit à la remarque précédente, ce coût augmente avec le nombre de racines de f dans $\mathbb{F}_p$. Ce coût reste quasi-linéaire en p, mais peut aller jusqu'à*

$$O(p\mathrm{MM}(m)dm\log(dm)\log(p)\log\log(dm)\log\log(p)\log\log\log(p))\ \textit{opérations binaires.}$$

En effet si le coefficient dominant est de degré d et a toutes ses racines dans $\mathbb{F}_p$ alors $X^{d(m-1)}|P^{m-1}$. On doit alors effectuer les calculs modulo θ^{dm+1}.
Si cela ne change pas le fait que l'algorithme présenté soit de coût quasi-linéaire en p mais peut avoir une influence significative sur la constante multiplicative de l'algorithme final, notamment lors du calcul du polynôme caractéristique.
Nous aurons besoin de résoudre ce problème avant de nous atteler au calcul du polynôme caractéristique de la p-courbure d'un opérateur différentiel en caractéristique 0 pour un grand nombre de p premiers.

On ne s'intéresse pas à l'algorithme de calcul du polynôme caractéristique. Comme on calcule le polynôme caractéristique d'un élément de $M_m\left({}^{\mathbb{F}_p[\theta]}/_{(\theta^{d+1})}\right)$ on en déduit que le coût de ce calcul peut être effectuer en $O(\log(p)\log\log(p)\log\log\log(p))$ opérations binaires.

Remarque 3.1.2.13. — *Comme nous ne voulons pas détailler l'algorithme de calcul du polynôme caractéristique dans cette partie, la partie du coût dépendant de d et m apparait ici dans la constante du O.*

On en déduit finalement un algorithme de calcul du polynôme caractéristique de la p-courbure en temps quasi-linéaire, sous l'hypothèse que $d < p$:

Données : $L \in \mathbb{F}_p[x]\langle\partial\rangle$
Résultat : $\chi(A_p(L))$

$d \leftarrow$ le maximum des degrés des coefficients de L ;
Calculer $L_1\partial^{-k}$ avec $L_1 \in k[\theta]\langle\partial\rangle$ et k minimal, l'image de L par l'isomorphisme d'algèbres de polynômes de Ore ;
$f \leftarrow$ le coefficient dominant de L_1 ;
$n \leftarrow$ le nombre de racines de f dans $\mathbb{F}_p$, calculé par évaluation multipoints ;
$m_1 \leftarrow \deg(L_1)$;
Calculer les translatés des coefficients de L_1 et construire les $f(\theta+j)B(L_1)(\theta+j)$ pour $0 \leqslant j < p$;
$P \leftarrow \prod_{i=0}^{p-1} f(\theta+i) \bmod \theta^{n(m_1-1)+d+1}$;
$M \leftarrow \prod_{i=0}^{p-1} f(\theta+i)B(L_1)(\theta+i) \in M_{m_1}\left({}^{\mathbb{F}_p[\theta]}/_{(\theta^{n(m_1-1)+d+1})}\right)$;
$F(\theta,Y) \leftarrow \chi(M) \in {}^{\mathbb{F}_p[\theta]}/_{(\theta^{n(m_1-1)+d+1})}$;
Calculer les puissances de P jusqu'à m_1 dans ${}^{\mathbb{F}_p[\theta]}/_{(\theta^{n(m_1-1)+d+1})}$;
En déduire $F(\theta,PY) \bmod \theta^{n(m_1-1)+d+1}$;
$G \leftarrow \frac{F(\theta,PY)}{\theta^{n(m_1-1)}} \bmod \theta^{d+1}$;
$P_1 \leftarrow \frac{P^{m-1}}{\theta^{n(m-1)}} \bmod \theta^{d+1}$;
En déduire $\Xi_{\theta,\partial}(L_1) \bmod \theta^{d+1}$ à partir de $G = P_1\Xi_{\theta,\partial}(L_1) \bmod \theta^{d+1}$ en utilisant 3.1.2.10 ;
En déduire $\Xi_{x,\partial}(L)$ en utilisant 3.1.2.9 ;
retourner $(\chi(A_p(L))$

Algorithme 13 : Calcul de $\chi(A_p(L))$ en $p^{1+o(1)}$ opérations binaires

3.1.3 Résultats « expérimentaux »

Ci-dessous nous présentons une comparaison des temps de calcul des deux algorithmes présentés jusqu'ici. Les deux algorithmes ont été implémentés dans le logiciel de calcul formel **sage**. Les algorithmes tournent ici tout le temps sous l'hypothèse que P n'a pas de racines dans $\mathbb{F}_p$, pour des $L \in \mathbb{F}_p[x]\langle\partial\rangle$ identiques pour les deux algorithmes, tirés au hasard pour chaque p, vérifiant $d \leqslant 5$ et $m \leqslant 7$. Sur les figures 3 (échelle linéaire) et 4 (échelle logarithmique) sont indiqués en bleu les temps de l'algorithme naïf et en rouge ceux de l'algorithme quasi-linéaire.

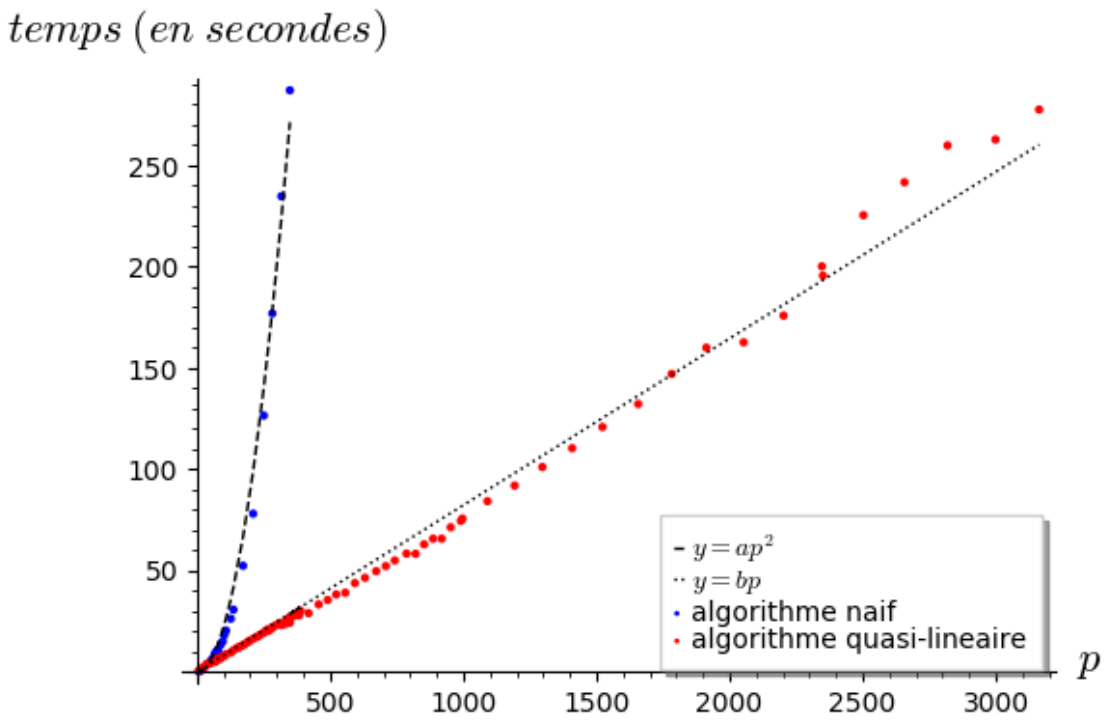


FIG. 3 : Comparaison des temps de calcul des deux algorithmes

La constante a (resp. b) est calculée de manière empirique en prenant la moyenne des rapports entre les temps d'exécution de l'algorithme naïf (resp. quasi-linéaire) pour p premier, et p^2 (resp. p).

On est heureux de se rendre compte que les complexités apparentes de ces algorithmes sont conformes à nos attentes. L'algorithme naïf semble terminer en temps quadratique en p et l'algorithme que nous avons travaillé à mettre en place semble terminer en temps linéaire (ou quasi-linéaire) en p. Les écarts des dernières valeurs (pour l'algorithme quasi-linéaire) avec la droite d'équation $y = bp$ dans la figure 3 pourraient être dus au rôle des facteurs logarithmiques qui commence à se faire ressentir.

Dans la sous-section suivante nous nous attelons à passer d'une complexité quasi-linéaire en p, à une complexité en $p^{1/2+o(1)}$ opérations binaires, pour le calcul de la p-courbure pour un seul p. On déduit d'un tel algorithme une complexité en $N^{3/2+o(1)}$ opérations binaires pour le calcul des p-courbures d'un opérateur $L \in k[x]\langle\partial\rangle$ pour $p \leqslant N$ premier.
La suite de cette sous-section sera consacrée à l'adaptation de l'algorithme de calcul des factorielles vu à la section 1 pour obtenir un algorithme effectuant cette tâche en $p^{1+o(1)}$ opérations binaires. Dans cette optique nous chercherons également à améliorer la constante dans le O de tous les algorithmes vus jusque là, en donnant une manière plus astucieuse de résoudre les problèmes posés par les éventuelles racines du coefficient dominant d'un opérateur $L_1 \in k[\theta]\langle\partial\rangle$.

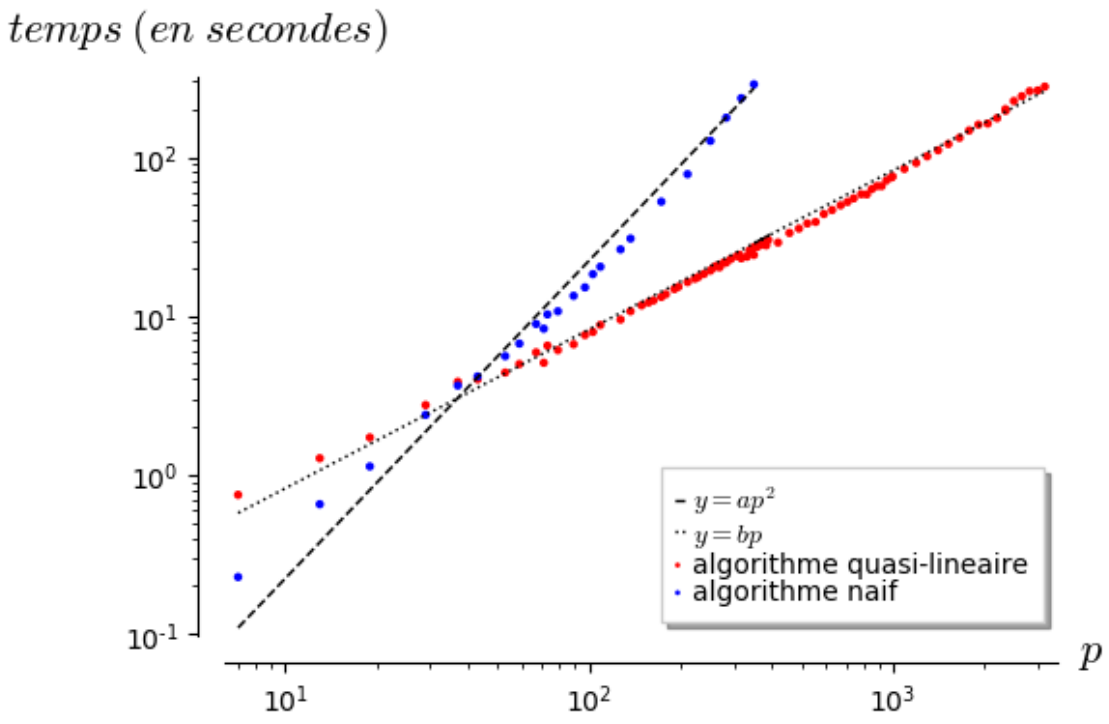


FIG. 4 : Comparaison des temps de calcul des deux algorithmes, échelle logarithmique

3.2 Améliorations des algorithmes

3.2.1 Algorithme en $p^{1/2+o(1)}$

De ce qui précède, nous avons vu que le gros de la complexité de notre algorithme en p vient du calcul de $B_p(L_1)$, où $\Phi(L) = L^1\partial^{-k}$ pour un certain k, avec $\Phi : k[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} k[\theta]\langle\partial^{\pm 1}\rangle$ l'isomorphisme d'algèbres de polynômes de ORE, qui donne son coût quasi-linéaire à l'algorithme précédent. Toutes les autres étapes peuvent être vues comme de coût polynomial en $\log(p)$. C'est donc sur ce calcul que va se porter l'amélioration de la complexité du calcul du polynôme caractéristique de la p-courbure.

Nous allons réutiliser la technique « pas de bébés, pas de géants », vue en §1.2.1. Soit $L \in k[\theta]\langle\partial\rangle$ de degré m et de coefficient dominant f. On suppose que tous les coefficients de L sont de degrés au plus d. On note $P = \prod_{i=0}^{p-1} f(\theta+i)$. Nous voulons calculer P et $PB_p(L) \bmod \theta^\eta$ pour un certain η, en $p^{1/2+o(1)}$ opérations binaires.

REMARQUE 3.2.1.1. — *Dans la sous section précédente nous avons vu que nous pouvions majorer η par $(m-1)\delta + d + 1$ où δ est le nombre de racines de f dans $k = \mathbb{F}_p$.*
Nous verrons plus tard une amélioration de cette borne.

Nous généralisons au problème suivant : soit $M \in M_r(k[\theta])$ pour un certain r. Soit $n \in \mathbb{N}^*$. Nous voulons calculer

$$\prod_{i=0}^{n-1} M(\theta+i) \bmod \theta^\eta.$$

On suppose pour l'instant, pour faciliter le raisonnement, que $n = s^2$ pour un certain s.
On peut alors écrire :

$$\prod_{i=0}^{s^2-1} M(\theta+i) = \prod_{i=0}^{s-1}\prod_{j=0}^{s-1} M(\theta+si+j)$$

Or $P \mapsto P(\theta+\alpha)$ est un automorphisme d'anneaux de $k[\theta]$ pour tout α, et induit donc un

automorphisme d'anneaux :

$$\begin{array}{rcl} M_r(k[\theta]) & \to & M_r(k[\theta]) \\ M & \mapsto & M(\theta+\alpha) \end{array}.$$

Ainsi en écrivant $C = \prod_{j=0}^{s-1} M(\theta+j)$ on a :

$$\prod_{i=0}^{s^2-1} M(\theta+i) = \prod_{i=0}^{s-1} C(\theta+si).$$

En revanche on ne peut pas effectuer tous les calculs modulo θ^η dès le départ puisque ces morphismes ne passent pas au quotient par θ^η.
Nous devons donc calculer C en entier. Nous voulons ensuite connaitre $C(\theta+si) \bmod \theta^\eta$ pour $i \in [\![0, s-1]\!]$. Supposons qu'il existe $P_i \in M_r(k[\theta])$ tel que $C(\theta+si) = C_i(\theta+si) + P_i \cdot \theta^\eta$ pour un certain C_i. Alors

$$C = C_i + P_i(\theta - si)(\theta - si)^\eta.$$

Nous pouvons donc connaître $C \bmod (\theta-si)^\eta$ pour tout $i \in [\![0, s-1]\!]$.
La proposition suivante en découle :

Proposition 3.2.1.2. — *Soient $M \in M_r(k[\theta])$, $\eta \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$. On pose $C := \prod_{i=0}^{s-1} M(\theta+i)$. On suppose qu'il existe $C_i \in M_r(k[\theta])$ pour tout $i \in [\![0; s-1]\!]$ tels que $C_i \equiv C \bmod (\theta-si)^\eta$. Alors*

$$\prod_{i=0}^{s^2-1} M(\theta+i) \equiv \prod_{j=0}^{s-1} C_j(\theta+sj) \bmod \theta^\eta.$$

On en déduit l'algorithme suivant :

Données : $M \in M_r(k[\theta])$, $(s,\eta) \in (\mathbb{N}^*)^2$
Résultat : $\prod_{i=0}^{s^2-1} M(\theta+i) \bmod \theta^\eta$

pour *i allant de* 0 *à* $s-1$ **faire**
  Calculer $M(\theta+i)$
Calculer $C := \prod_{i=0}^{s-1} M(\theta+i)$ par scindage binaire ;
Calculer $C_i := C \bmod (\theta-si)^\eta$ pour $i \in [\![0, s-1]\!]$;
pour *i allant de* 0 *à* $s-1$ **faire**
  $D_i \leftarrow C_i(\theta+si)$
retourner $\prod_{i=0}^{s-1} D_i \bmod \theta^\eta$

Algorithme 14 : Pas de bébé, pas de géant pour le calcul des factorielles de matrices

Avant de résoudre la question de la complexité de cet algorithme, nous donnons un autre algorithme de calcul des translations, plus efficace que celui utilisé dans la sous-section précédente :

Données : $P \in k[\theta]$, $\alpha \in k$
Résultat : $P(\theta+\alpha)$

$d \leftarrow \deg(P)$;
Écrire $P = P_1\theta^{\lceil d/2 \rceil} + P_2$ avec $\deg(P_i) \leqslant d/2$ pour $i \in \{1,2\}$;
Calculer $(\theta+\alpha)^{\lceil d/2 \rceil}$ par exponentiation rapide ;
Calculer récursivement $P_1(\theta+\alpha)$ et $P_2(\theta+\alpha)$;
retourner $P_1(\theta+\alpha)(\theta+\alpha)^{\lceil d/2 \rceil} + P_2(\theta+\alpha)$

On note $C(d)$ le coût de cet algorithme en opérations dans k sur un polynôme de degré d. L'exponentiation rapide coûte $O(d\log(d)\log\log(d))$ opérations dans k. A ceci s'ajoute une multiplication de polynôme de degrés $\lceil d/2 \rceil$ et deux appels récursifs, ce qui donne :

$$C(d) = O(d\log(d)\log\log(d)) + 2C(\lfloor d/2 \rfloor)$$

et encore

$$C(d) = O(d\log^2(d)\log\log(d)).$$

On résout maintenant la question du coût de l'algorithme de calcul de la factorielle de matrices.

Proposition 3.2.1.3. — *On suppose que les coefficients de M sont tous de degrés au plus $\eta - 1$. S'ils ne le sont pas on calcule $M \bmod \theta^\eta$.*
L'algorithme de calcul de $\prod_{i=0}^{s^2-1} M(\theta + i) \bmod \theta^\eta$ présenté ci-dessus termine en

$$O(\mathrm{MM}(r)s\eta \log(s\eta) \log(s) \log\log(s\eta)) \text{ opérations arithmétiques dans } k.$$

Preuve. Par ce qui précède, le calcul des $M(\theta + i)$ pour $i \in [\![0; s-1]\!]$ peut être effectué en $O(r^2 s\eta \log^2(\eta) \log\log(\eta))$ opérations arithmétiques dans k.
Le calcul de C par scindage binaire s'effectue en $O(\mathrm{MM}(r)s\eta \log(s\eta) \max(\log(s), \log(\eta)) \log\log(s\eta))$ opérations arithmétiques dans k.
On doit maintenant calculer les C_i. Cela peut se faire en calculant d'abord l'arbre binaire des diviseurs successifs représenté sur la figure 5. Cela peut être fait récursivement comme dans A.2.

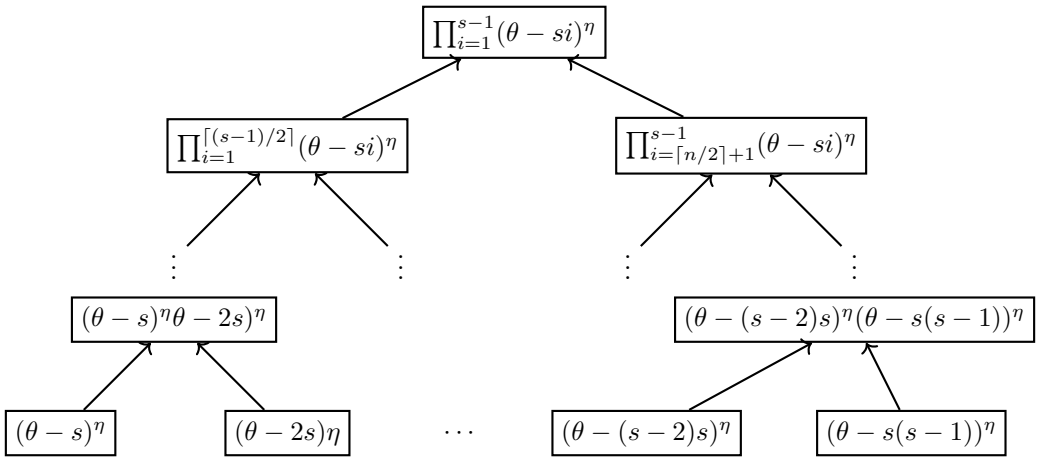


Fig. 5 : Arbre binaire des diviseurs successifs

Le coût du calcul de cet arbre est donc

$$O(s\eta \log(s\eta) \log(s) \log\log(s\eta)) \text{ opérations dans } k.$$

On effectue maintenant les divisions euclidiennes successives en descendant dans l'arbre des restes successifs représenté ci-dessous. Ceci peut être fait en

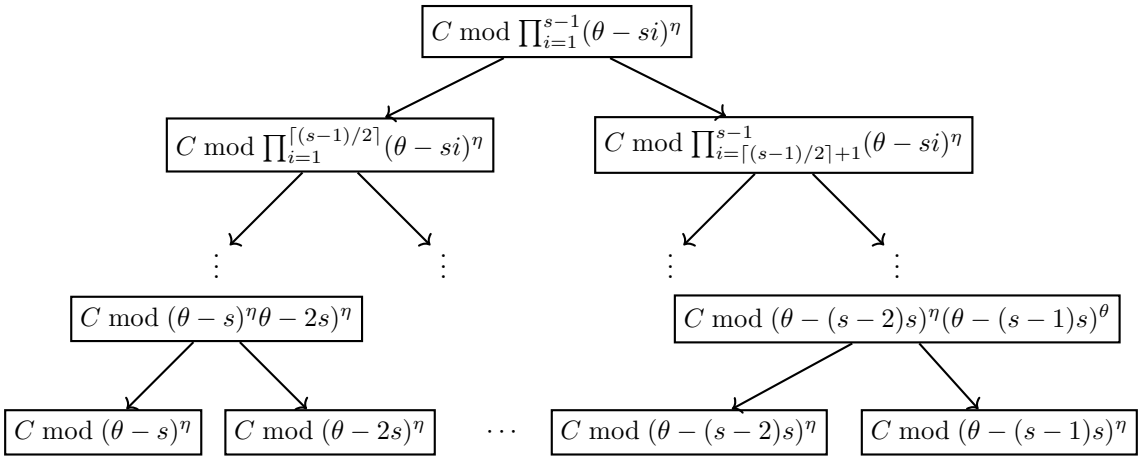


Fig. 6 : Arbre binaire des restes successifs

$$O(r^2 s\eta \log(s\eta) \log(s) \log\log(s\eta)) \text{ opérations arithmétiques dans } k.$$

Il reste encore à calculer les D_i ce qui peut être fait en

$$O(r^2 s\eta \log(\eta)^2 \log\log(\eta)) \text{ opérations arithmétiques dans } k.$$

et à calculer $\prod_{i=0}^{s-1} D_i$ ce qui peut être fait en

$$O(\mathrm{MM}(r) s\eta \log(\eta) \log\log(\eta)) \text{ opérations arithmétiques dans } k.$$

Le résultat suit directement. □

On ne suppose désormais plus que n est un carré parfait. On peut calculer $\prod_{i=0}^{n-1} M(\theta+i)$ par l'algorithme suivant :

Données : $M \in M_r(k[\theta])$, $n, \eta \in \mathbb{N}^*$
Résultat : $\prod_{i=0}^{n-1} M(\theta+i) \bmod \theta^\eta$
$s \leftarrow \lfloor \sqrt{n} \rfloor$;
pour i *allant de* 1 *à* $p - s^2$ **faire**
  Calculer $M(\theta+i)$
Calculer $A := \prod_{i=0}^{p-s^2-1} M(\theta+i) \bmod \theta^\eta$ par scindage binaire ;
$M_1 \leftarrow M(\theta + p - s^2)$;
Calculer $B := \prod_{i=0}^{s^2-1} M_1(\theta+i) \bmod \theta^\eta$ par la technique « pas de bébé, pas de géant » ;
retourner $AB \bmod \theta^\eta$

Cet algorithme termine en

$$O(\mathrm{MM}(r)\sqrt{n}\eta \log(n\eta) \log(\max(\sqrt{n}, \eta)) \log\log(\sqrt{n}\eta)) \text{ opérations arithmétiques dans } k.$$

Remarque 3.2.1.4. — *Cet algorithme peut être utilisé pour le calcul de factorielles de polynômes, en prenant simplement $r = 1$.*

Nous pouvons maintenant nous servir de cet algorithme pour calculer $PB_p(L)$ et P modulo θ^η, où η est majoré par une constante ne dépendant pas de p, en $p^{1/2+o(1)}$ opérations binaires, ce qui donne un algorithme du calcul du polynôme caractéristique de la p-courbure en $p^{1/2+o(1)}$ opérations binaires, ce que nous voulions démontrer.

3.2.2 Gains sur la dépendance aux facteurs secondaires

Nous travaillons maintenant à donner une meilleure borne sur η. On rappelle que dans la sous-section précédente, nous avions déterminé que $\eta \leqslant d(m+d)+1$, lorsque l'on exécute l'algorithme pour $L \in k[x]\langle\partial\rangle$ de degré m dont les coefficients sont de degrés au plus d.
Nous travaillons maintenant à démontrer la proposition suivante :

Proposition 3.2.2.1. — *Soit $L \in k[x]\langle\partial\rangle$ de degré m et dont les coefficients sont de degrés au plus d, et $L_1 \in k[\theta]\langle\partial\rangle$ tel que l'image de L par l'isomorphisme soit $L_1\partial^{-d}$.*
On note f le coefficient dominant de L_1 et $P = \prod_{i=0}^{p-1} f(\theta+i)$. Lors du calcul du polynôme caractéristique de la p-courbure de L, on peut calculer $PB_p(L_1) \bmod \theta^{\eta_1}$ et $P \bmod \theta^{\eta_2}$ avec

$$\eta_1 \leqslant 2d+1$$
$$\eta_2 \leqslant 3d+1$$

L'idée principale est de calculer directement le polynôme caractéristique de $B_p(L_1)$ et non de $PB_p(L_1)$.
Notre principal problème vient de ce que $B_p(L_1)$ est à coefficient dans $k(\theta)$, où la notion de modulo θ^η n'a pas de sens.
Pour résoudre ce problème nous travaillons dans $k((\theta))$, le corps des séries de Laurent formelles à coefficients dans k. On rappelle que ce corps est le corps des fractions de $k[[\theta]]$ (voir A.2 pour une condition nécessaire et suffisante d'inversibilité des séries formelles). À ce titre, on dispose d'un morphisme injectif

$$k(\theta) \hookrightarrow k((\theta))$$

induit par l'injection de l'anneau des polynômes dans l'anneau des séries formelles.
Comme $k((\theta))$ est un corps, on ne peut pas considérer ces éléments « modulo θ^η » comme on pourrait le faire dans $k[[\theta]]$ en regardant leur image dans ${}^{k((\theta))}/_{(\theta^\eta)}$. On considère une notion légèrement plus faible, mais plus utile :

Définition 3.2.2.2. — *Soient $f, g \in k((\theta))$. On dira que $f \equiv g \bmod \theta^\eta$ si et seulement si il existe $h \in k[[\theta]]$ tel que*

$$f - g = h \cdot \theta^\eta.$$

Remarque 3.2.2.3. — *Ainsi connaitre $f \in k((\theta))$ modulo θ^η revient à connaitre son image dans le $k[[\theta]]$-module ${}^{k((\theta))}/_{\theta^\eta k[[\theta]]}$. C'est en ce sens que cette notion est « plus faible » puisque l'on passe d'une structure d'anneau à une structure de module. Elle a en revanche l'avantage de servir à quelque chose dans le cas qui nous intéresse.*
Nous dirons qu'un élément $f \in k((\theta))$ est connu à précision absolue η si on connait $f_1 \in k((\theta))$ tel que $f \equiv f_1 \bmod \theta^\eta$.

La notion de précision absolue est importante, et c'est celle qui nous intéressera ultimement. Malheureusement, du fait du sacrifice de la structure d'anneau, cette notion n'est pas stable par multiplication. Pour remédier à ce problème on introduit la notion de précision relative.

Proposition 3.2.2.4. — *θ est un (le seul) élément irréductible de $k[[\theta]]$.*

Preuve. ${}^{k[[\theta]]}/_{(\theta)} \simeq k$. D'autre part pour tout $f \in k[[\theta]]$ soit $\theta | f$ soit f est inversible. □

La proposition qui suit est évidente :

Proposition 3.2.2.5. — *$k[[\theta]]$ est un anneau factoriel.*

Ceci nous permet de munir $k[[\theta]]$, et donc $k((\theta))$ d'une θ-valuation. On la note $\nu_\theta : k((\theta)) \to \mathbb{Z}$. La proposition suivante suit immédiatement :

Proposition 3.2.2.6. — *Pour tout $f \in k((\theta))$ il existe un unique $f_1 \in k[[\theta]]$ tel que $f = \theta^{\nu_\theta(f)} f_1$.*

Définition 3.2.2.7. — *On dit que $f \in k((\theta))$ est connue à précision relative η si et seulement f est connue à précision absolue $\eta + \nu_\theta(f)$.*

L'intérêt de cette définition vient de sa stabilité par multiplication.

Lemme 3.2.2.8. — *Soient $f, g \in k((\theta))$. Si f et g sont connues à précisions relatives respectives η_1 et η_2 alors fg est connue à précision relative* $\min(\eta_1, \eta_2)$.

Preuve. Soient $f_1, f_2 \in k[[\theta]]$ tels que $f = \theta^{\nu_\theta(f)} f_1 + \theta^{\eta_1 + \nu_\theta(f)} f_2$ et $g_1, g_2 \in k[[\theta]]$ tels que $g = \theta^{\nu_\theta(g)} g_1 + \theta^{\eta_2 + \nu_\theta(f)} g_2$.

$$fg = f_1 g_1 \theta^{\nu_\theta(f)+\nu_\theta(g)} + f_1 g_2 \theta^{\eta_2+\nu_\theta(f)+\nu_\theta(g)} + f_2 g_1 \theta^{\eta_1+\nu_\theta(f)+\nu_\theta(g)} + f_2 g_2 \theta^{\eta_2+\eta_1+\nu_\theta(f)+\nu_\theta(g)}$$

fg est donc connue en précision absolue $\min(\eta_2, \eta_1) + \nu_\theta(f) + \nu_\theta(g)$. Comme fg a pour θ-valuation $\nu_\theta(f) + \nu_\theta(g)$, on en déduit le résultat. □

Remarque 3.2.2.9. — *En revanche la notion de précision relative, à la différence de la précision absolue n'est pas stable par addition.*

Nous pouvons maintenant passer au calcul du polynôme caractéristique.
Soit $M \in M_r(k((\theta)))$ connue à précision absolue η dont les mineurs ont tous une θ-valuation supérieure ou égale à $-\nu$, avec $0 \leqslant \nu < \eta$.

Proposition 3.2.2.10. — *On peut connaitre $\chi(M)$ à précision absolue $\eta - \nu$.*

Remarque 3.2.2.11. — *La nécessité de l'hypothèse sur les mineurs de M vient justement de la non stabilité, au choix de la précision absolue par multiplication, ou de la précision relative par addition.*

Preuve. On cherche à calculer $\det(X\cdot \mathrm{Id} - M) \in k((\theta))[X]$. Comme on sait que $\chi(M)$ est de degré r en X, nous pouvons effectuer les calculs dans ${}^{k((\theta))[X]}/_{(P)}$, où P est un polynôme de degré $r+1$. Or on a un isomorphisme ${}^{k((\theta))[X]}/_{(X^{r+1}-\theta)} \simeq k((X))$.
En effet on a un morphisme

$$\begin{array}{ccc} k((\theta)) & \to & k((X)) \\ f & \mapsto & f(X^{r+1}) \end{array}.$$

Ce morphisme induit par évaluation un morphisme de $\varphi : k((\theta))[X] \to k((X))$ envoyant X sur X. Ce morphisme est surjectif et de plus $X^{r+1}-\theta$ est dans son noyau. Soit $P \in \ker(\varphi)$ tel que $\deg(P) \leqslant r$. On peut écrire $P = \sum_{i=0}^{r} p_i(\theta)X^i$. Mais alors

$$\nu_X(\varphi(p_i(\theta)X^i)) \equiv i \bmod r+1$$

Ainsi les termes ne peuvent s'annuler entre eux, on en déduit qu'ils sont tous nuls, et donc $P=0$. On en déduit que φ a pour noyau $X^{r+1}-\theta$ ce qui donne l'isomorphisme. On peut donc considérer $X\cdot\mathrm{Id} - M$ comme une matrice à coefficients dans $k((X))$ ou dans $k((\theta))[X]$ selon le cas qui nous arrange.

Lemme 3.2.2.12. — *Soit $M \in M_r(k((\theta))[X])$ tels que les mineurs de M aient tous une θ-valuation supérieure ou égale à $-\nu$ avec $\nu \in \mathbb{N}$, et soit $N \in M_r(k((\theta))[X])$ dont les coefficients ont tous une θ-valuation positive.*
Alors les mineurs de $M+N$ ont tous θ-valuation supérieure ou égale à $-\nu$.

Preuve. Soit $I, J \subset [\![1,r]\!]$ de même cardinal k. On écrit $I = \{i_1 < \ldots < i_k\}$ et $J = \{j_1 < j_2 \ldots < j_k\}$. On note $|A_{[I,J]}|$ le mineur d'une matrice A sur les lignes I et les colonnes J.

$$\begin{aligned} |(M+N)_{[I,J]}| &= \sum_{\sigma\in\mathfrak{S}_k} \mathrm{sgn}(\sigma) \prod_{l=1}^{k} (M_{i_l,j_{\sigma(l)}} + N_{i_l,j_{\sigma(l)}}) \\ &= \sum_{\sigma\in\mathfrak{S}_k} \mathrm{sgn}(\sigma) \sum_{f\in\mathcal{F}([\![1,k]\!],\{M,N\})} \prod_{l=1}^{k} f(l)_{i_l,j_{\sigma(l)}} \\ &= \sum_{f\in\mathcal{F}([\![1,k]\!],\{M,N\})} \sum_{\sigma\in\mathfrak{S}_k} \mathrm{sgn}(\sigma) \prod_{l=1}^{k} f(l)_{i_l,j_{\sigma(l)}} \end{aligned}$$

On voit maintenant que

$$\mathcal{F}([\![1,k]\!],\{M,N\}) \simeq \bigcup_{i=0}^{k} \{F \subset [\![1,k]\!] | \,\mathrm{card}(F) = i\}$$

Donnons nous donc $0 \leqslant i \leqslant k$ et $F \subset [\![1,k]\!]$.
Choisir une permutation σ de $\mathfrak{S}_k$ revient à choisir $\sigma(F)$, une permutation τ_1 de $\sigma(F)$ et une permutation τ_2 de ${}^c\sigma(F)$. De plus si on se donne une fois pour toute une permutation $\sigma_{F,\sigma(F)}$ tel que $\sigma_{F,\sigma(F)}(F) = \sigma(F)$ alors on peut s'arranger pour que $\sigma = \tau_2 \circ \tau_1 \circ \sigma_{F,\sigma(F)}$.
On peut donc écrire :

$$|(M+N)_{[I,J]}| = \sum_{\substack{0\leqslant i\leqslant k \\ F,G\subset[\![1,k]\!] \\ \mathrm{card}(F)=i \\ \mathrm{card}(G)=i}} \mathrm{sgn}(\sigma_{F,G}) \sum_{\tau_2\in\mathfrak{S}({}^cG)} \left(\mathrm{sgn}(\tau_2) \prod_{l\in{}^cF} N_{i_l,j_{\tau_2(\sigma_{F,G}(l))}}\right) \sum_{\tau_1\in\mathfrak{S}(G)} \mathrm{sgn}(\tau_1) \prod_{l\in F} M_{i_l,j_{\tau_1(\sigma_{F,G}(l))}}$$

et enfin :

$$|(M+N)_{[I,J]}| = \sum_{\substack{0\leqslant i\leqslant k \\ F,G\subset[\![1,k]\!] \\ \mathrm{card}(F)=i \\ \mathrm{card}(G)=i}} \mathrm{sgn}(\sigma_{F,G}) |N_{[i_{{}^cF},j_{{}^cG}]}||M_{[i_F,j_G]}|.$$

Le résultat en découle immédiatement. □

Il découle immédiatement du lemme que $X\mathrm{Id} - M$ a tous ses mineurs de valuation supérieure ou égale à $-\nu$.

PROPOSITION 3.2.2.13. — *Pour tout $M \in M_r(k((X)))$, il existe $P \in M_r(k[[X]])$ de déterminant ± 1 et $H \in M_r(k((X))$ triangulaire inférieure tel que*

$$M = P \cdot H$$

Preuve. Il s'agit d'un simple pivot de GAUSS en prenant à chaque étape l'élément de la ligne possédant la plus petite X-valuation pour pivot. □

Comme nous connaissons M à précision absolue η, nous connaissons $M_X \in M_r\left(k((\theta))[X]/(X^{r+1-\theta})\right)$ tel que $M_X = X\mathrm{Id} - M + O(\theta^\eta)$.
Nous pouvons calculer une telle décomposition P, H de M_X (vu cette fois comme un élément de $M_r(k((X))))$ module θ^η. On a alors

$$P.(H + O(\theta^n)) = M + O(\theta^n)$$

et donc

$$P.H + O(\theta^n) = M.$$

D'autre part, on déduit de la formule de CAUCHY-BINET (voir 3.2.2.16), que nous démontrerons par la suite, que H a tous ses mineurs de valuation supérieure ou égale à $-\nu$.

REMARQUE 3.2.2.14. — *Nous n'avons pas besoin en pratique de calculer P. Son existence nous suffit. Nous pourrons inférer la valeur de son déterminant et nous souvenant que le coefficient dominant de $\chi(M)$ vaut 1.*

Écrivons

$$H = \begin{pmatrix} \lambda_1 & & & \star \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_r \end{pmatrix}$$

Posons $\delta = \nu_\theta(\det(H))$. Pour tout i on a $\nu_\theta(\lambda_1 \dots \lambda_{i-1}\lambda_{i+1} \dots \lambda_r) \geqslant -\nu$, d'où il vient $\nu_\theta(\lambda_i) \leqslant \delta + \nu$. λ_i est donc connu à précision relative au moins $\eta - \delta - \nu$. La stabilité de la précision relative par multiplication nous indique donc que l'on connait $\det(H)$ à précision relative au moins $\eta - \delta - \nu$. Il suit que l'on connait $\det(H)$ en précision absolue $\eta - \nu$, et donc $\chi(M)$ modulo $\theta^{\eta-\nu}$. □

Appliquons ce théorème au problème qui nous intéresse. Soit $L \in k[\theta]\langle\partial\rangle$ de degré m, de coefficients de degré au plus d et de coefficient dominant f. Notons ν le nombre de racines de f dans $\mathbb{F}_p$, comptées avec multiplicités.

PROPOSITION 3.2.2.15. — *$B_p(L)$ a tous ses mineurs de θ-valuation supérieure ou égale à $-\nu$.*

Preuve. Avant de prouver cette proposition, nous énonçons et démontrons la formule de CAUCHY-BINET

LEMME 3.2.2.16. — *Soit $M \in M_{m\times n}(\mathbb{A})$ où $\mathbb{A}$ est un anneau commutatif quelconque, et soient $(A, B) \in M_{m\times p}(\mathbb{A}) \times M_{p\times n}(\mathbb{A})$ tels que $AB = M$. Soient $I \subset [\![1; m]\!]$ et $J \subset [\![1; n]\!]$ de cardinal $k \leqslant \min(m, n, p)$.*

$$|M_{[I,J]}| = \sum_{\substack{K\subset[\![1;p]\!] \\ \mathrm{card}(K)=k}} |A_{[I,K]}||B_{[K,J]}|$$

Preuve. On commence par montrer le résultat dans le cas $n = m = k \leqslant p$. Pour faciliter l'écriture des calculs, nous notons pour tout $l \in \mathbb{N}^*$, $[l] = [\![1, l]\!]$. Nous pouvons écrire :

$$\begin{aligned}\det(M) &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \left(\sum_{j=1}^{p} A_{i,j} B_{j,\sigma(i)} \right) \\ &= \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \sum_{f\in\mathcal{F}([n],[p])} \prod_{i=1}^{n} A_{i,f(i)} B_{f(i),\sigma(i)} \\ &= \sum_{f\in\mathcal{F}([n],[p])} \prod_{i=1}^{n} A_{i,f(i)} \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} B_{f(i),\sigma(i)}\end{aligned}$$

En notant pour tout $f \in \mathcal{F}([n], [p])$

$$B_f := (B_{f(i),j}) \in M_n(\mathbb{A})$$

on peut encore écrire :

$$\det(M) = \sum_{f\in\mathcal{F}([n],[p])} \det(B_f) \prod_{i=1}^{n} A_{i,f(i)}.$$

Il suit que l'on peut restreindre la somme aux f injectives. Comme deux applications injectives de mêmes images diffèrent d'une permutation de leur image, il suit :

$$\begin{aligned}\det(M) &= \sum_{\substack{K\subset[p]\\ \operatorname{card}(K)=n}} \sum_{\sigma\in\mathfrak{S}(K)} |B_{K,[n]}| \operatorname{sgn}(\sigma) \prod_{i=1}^{n} A_{i,\sigma(K_i)} \\ &= \sum_{\substack{K\subset[p]\\ \operatorname{card}(K)=n}} |A_{[n],K}||B_{K,[n]}|.\end{aligned}$$

Le cas général s'en déduit en voyant que $M_{I,J} = A_{I,[p]} B_{[p],J}$. □

Pour tout anneau $\mathbb{A}$, $i \in [\![1; m]\!]$ et toute $M \in M_m(\mathbb{A})$ on note $\Lambda^i M$ la matrice de ses mineurs de taille i (définie en fixant une fois pour toutes une énumération des parties à i éléments de $[\![1, m]\!]$). De la formule de Cauchy-Binet on déduit que

$$\Lambda^i B_p(L) = \prod_{j=0}^{p-1} \Lambda^i B(L)(\theta + j).$$

D'autre part les coefficients de $B(L)(\theta + j)$ sont tous dans $k[\theta]$ sauf ceux de sa dernière colonne qui ont tous pour dénominateur $f(\theta + j)$. Tous les mineurs de $B(L)(\theta + j)$ ont donc θ-valuation supérieure à $-\nu_j$ où ν_j est la multiplicité de j en tant que racine de f.

Il suit que $\Lambda^i B_p(L)$ à ses coefficients de θ-valuation supérieurs à $-\sum_{j\in\mathbb{F}_p} \nu_j = -\nu$. □

Nous voulons connaître $P\chi(B_p(L))$ à précision absolue $d+1$ (avec $P = \prod_{i=0}^{p-1} f(\theta+i)$). Comme P a pour θ-valuation ν, il suffit de connaitre $\chi(B_p(L))$ à précision absolue $d + 1 - \nu$. Il suffit donc de connaitre $B_p(L)$ à précision absolue $d + 1$.
Le calcul de la factorielle nous donne $PB_p(L) \bmod \theta^\eta$. Comme P à θ-valuation ν il suffit de connaitre $PB_p(L)$ et $\frac{P}{\theta^\nu}$ à précision absolue $d + 1 + \nu$.
Ainsi il nous suffit de connaitre $PB_p(L) \bmod \theta^{d+1+\nu}$ et $P \bmod \theta^{d+1+2\nu}$.
Comme $\nu \leqslant \deg(f) \leqslant d$, nous avons démontré la Proposition 3.2.2.1.

On en déduit l'algorithme final :

Données : $L \in k[x]\langle\partial\rangle$
Résultat : $\chi(A_p(L))$

$m \leftarrow \deg(L)$;
$d \leftarrow \max(\{$ coefficients de $L\})$;
Calculer $L_1 \in k[\theta]\langle\partial\rangle$ tel que L s'envoie sur $L_1\partial^{-d}$ par l'isomorphisme ;
$m_1 \leftarrow \deg(L_1)$;
$f \leftarrow$ le coefficient dominant de L_1 ;
$\nu \leftarrow$ le nombre de racines de f dans $\mathbb{F}_p$, comptées avec multiplicités ;
Écrire $fB(L_1) \bmod \theta^{d+1+\nu}$;
Calculer $P := \prod_{i=0}^{p-1} f(\theta+i) \bmod \theta^{d+1+2\nu}$;
Calculer $PB_p(L) \bmod \theta^{d+1+\nu}$ par la méthode « pas de bébé, pas de géant » ;
En déduire $B_p(L) \bmod \theta^{d+1}$;
Calculer $\chi(B_p(L)) \bmod \theta^{d+1-\nu}$;
En déduire $P\chi(B_p(L)) \bmod \theta^{d+1}$;
$F(x,Y) \leftarrow$ L'image réciproque de $P\chi(B_p(L))$ par l'isomorphisme ;
retourner $F(x,Y)Y^{-d}$

Algorithme 15 : Algorithme en $p^{1/2+o(1)}$

Nous admettons que le calcul du polynôme caractéristique par la méthode étudiée peut se faire en $O(\mathrm{MM}(m_1)dm_1\log(dm_1)\log\log(dm_1))$. L'algorithme présenté termine alors en

$$\begin{aligned}&O(\mathrm{MM}(d+m)p^{1/2}d\log(dp)\log(p)\log\log(dp)\\ &+\mathrm{MM}(d+m)d(m+d)\log(d(m+d))\log\log(d(m+d)))\text{ opérations binaires.}\end{aligned}$$

3.2.3 Calcul des polynômes caractéristiques des p-courbures d'un opérateur en caractéristique nulle

Nous nous intéressons maintenant au problème suivant. Soit $L \in \mathbb{Q}[x]\langle\partial\rangle$. Quitte à multiplier par les dénominateurs des coefficients de L, on peut supposer que $L \in \mathbb{Z}[x]\langle\partial\rangle$.
Pour tout p premier le morphisme $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induit

$$\begin{array}{rccc}\pi_{x,p}: & \mathbb{Z}[x]\langle\partial\rangle & \to & \mathbb{Z}/p\mathbb{Z}[x]\langle\partial\rangle\\ & L & \mapsto & \pi_{x,p}(L)\end{array}$$

et

$$\begin{array}{rccc}\pi_{\theta,p}: & \mathbb{Z}[\theta]\langle\partial\rangle & \to & \mathbb{Z}/p\mathbb{Z}[\theta]\langle\partial\rangle\\ & L & \mapsto & \pi_{\theta,p}(L)\end{array}$$

Nous voulons calculer pour tout $p \leqslant N \in \mathbb{N}$ premier, calculer $\chi(A_p(\pi_{x,p}(L)))$.

Remarque 3.2.3.1. — *Bien que nous restreignons ici notre étude aux seuls opérateurs à coefficients rationnels (dans $\mathbb{Q}$), nous aurions pu la prolonger au cas où L est à coefficients dans une extension algébrique de $\mathbb{Q}$ (en choisissant des extensions algébriques de $\mathbb{Z}/p\mathbb{Z}$).*

Notons $\Phi_p : \mathbb{Z}/p\mathbb{Z}[x]\langle\partial^{\pm1}\rangle \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}[\theta]\langle\partial^{\pm1}\rangle$.
Introduisons également $\Phi : \mathbb{Q}[x]\langle\partial^{\pm1}\rangle \to \mathbb{Q}[\theta]\langle\partial^{\pm1}\rangle$. Notre but est de démontrer le résultat suivant :

Lemme 3.2.3.2. — *Le diagramme suivant est commutatif :*

$$\begin{array}{ccc}\mathbb{Z}[x]\langle\partial^{\pm1}\rangle & \xrightarrow{\Phi} & \mathbb{Z}[\theta]\langle\partial^{\pm1}\rangle\\ \downarrow{\scriptstyle \pi_{x,p}} & & \downarrow{\scriptstyle \pi_{\theta,p}}\\ \mathbb{F}_p[x]\langle\partial^{\pm1}\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm1}\rangle\end{array}$$

Malheureusement, pour l'heure, il n'est même pas dit que Φ soit bien défini. Commençons par démontrer l'existence de $\mathbb{Q}[x]\langle\partial^{\pm 1}\rangle$ et de $\mathbb{Q}[\theta]\langle\partial^{\pm 1}\rangle$. Cela revient à montrer que les anneaux $\mathbb{Q}[x]\langle\partial\rangle$ et $\mathbb{Q}[\theta]\langle\partial\rangle$, munis de la partie multiplicative $S = \{\partial^n | n \in \mathbb{N}\}$ vérifie la condition de Ore à droite, d'après B.10. Nous commençons par le deuxième cas, plus facile. En effet, pour tout $i \in \mathbb{N}$ et tout $L \in \mathbb{Q}[\theta]\langle\partial\rangle$,

$$\partial^i L = L(\theta + i)\partial^i$$

ce qui donne immédiatement le résultat.
On s'attaque maintenant au cas plus complexe de $\mathbb{Q}[x]\langle\partial\rangle$.

Lemme 3.2.3.3. — *Soient $P \in \mathbb{Q}[x]$ de degré d et $i \in \mathbb{N}$. Il existe $L \in \mathbb{Q}[x]\langle\partial\rangle$ tel que*

$$P\partial^{d+i} = \partial^i L$$

Preuve. On procède par récurrence sur d. Si $d = 0$ alors $\partial^i P = P\partial^i$. Supposons désormais le résultat vérifié pour tout $P \in \mathbb{Q}[x]$ de degré $d < n$. Soit $P \in \mathbb{Q}[x]$ de degré n.

$$\begin{aligned} P\partial^{d+i} &= \partial^{d+i}P - \sum_{j=1}^{d+i} \binom{d+i}{j} P^{(j)}\partial^{d+i-j} \\ &= \partial^{d+i}P - \sum_{j=1}^{d} \binom{d+i}{j} P^{(j)}\partial^{d+i-j} \end{aligned}$$

Or $P^{(j)}$ est de degré $d-j$. On peut donc appliquer l'hypothèse de récurrence. Il existe des L_j tels que $P^{(j)}\partial^{d-j+i} = \partial^i L_j$. On a donc

$$P\partial^{d+i} = \partial^{d+i}P - \sum_{j=1}^{d} \partial^i L_j$$

ce qui permet de conclure. La récurrence est établie. □

On en déduit par additivité que la condition de Ore à droite est respectée et que donc, les anneaux considérés sont bien définis.
Le morphisme Φ est alors défini de la même manière que dans le cas de la caractéristique p :

$$\begin{array}{rccc} \Phi : & \mathbb{Q}[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & \mathbb{Q}[\theta]\langle\partial^{\pm 1}\rangle \\ & x & \mapsto & \theta\partial^{-1} \\ & x\partial & \leftarrow\!\shortmid & \theta \\ & \partial & \leftrightarrow & \partial \end{array} .$$

Remarque 3.2.3.4. — *Le travail qui vient d'être effectué sur $\mathbb{Q}$ peut être effectué à l'identique en se restreignant à n'importe quel sous-anneau A de $\mathbb{Q}$ (et en fait sur n'importe quel anneau). On peut alors déduire un morphisme $A[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} A[\theta]\langle\partial^{\pm 1}\rangle$. La propriété universelle de ces anneaux nous indique que ce morphisme coïncident avec celui qui se déduit de Φ en restreignant et corestreignant des coefficients dans A.*

Nous pouvons maintenant prouver 3.2.3.2.

Preuve. Cela n'est rien d'autre que la propriété universelle de $\mathbb{Z}[x]\langle\partial^{\pm 1}\rangle$. □

Soient $L \in \mathbb{Z}[x]\langle\partial\rangle$ de degré m dont les coefficients sont de degré au plus d et $L_1 \in \mathbb{Z}[\theta]\langle\partial\rangle$ tel que $\Phi(L) = L_1\partial^{-d}$. Par abus de notation, nous continuons de noter $B(L')$ la matrice compagnon d'un polynôme de Ore (quelque soit le corps de base). Si $\pi_{\theta,p}(L_1)$ est de même degré que L_1, alors $B(\pi_{\theta,p}(L_1)) = B(L_1) \bmod p$. Comme de plus $\Phi_p(\pi_{x,p}(L)) = \pi_{\theta,p}(\Phi(L)) = \pi_{\theta,p}(L_1)\partial^{-d}$ par ce qui précède, il suit que l'on va chercher à calculer

$$B_p(L_1) := \prod_{i=0}^{p-1} B(L_1)(\theta + i) \bmod p$$

pour tout les $p \leqslant N$ premiers ne divisant pas le coefficient dominant de L_1.

Ce problème est extrêmement proche de celui résolu dans la section 1 et, par un heureux hasard, peut se résoudre de la même façon.
Avant d'écrire le détail de ce calcul, on rappelle que nous n'avons besoin de connaitre $\chi(B_p(L_1))$ que modulo θ^{d+1}.
Notons f le coefficient dominant de L_1, et ν_p le nombre de ses racines dans $\mathbb{F}_p$. On se souvient que nous avions déterminé dans la partie précédente que, pour ce faire, nous pouvions nous contenter de connaitre $P_p := \prod_{i=0}^{p-1} f(\theta+i) \bmod p$ modulo $\theta^{d+1+2\nu_p}$ et $P_p B_p(L_1)$ modulo $\theta^{d+1+\nu_p}$.
Comme nous ne connaitrons pas ici ν_p pour tout p nous effectuerons le calcul de P_p modulo $\theta^{d+1+2\eta}$ et $P_p B_p(L_1)$ modulo $\theta^{d+1+\eta}$ où η est la meilleure majoration de ν_p trouvable sans calcul : le degré de f.

On passe maintenant au calcul à proprement parler. Pour faciliter les choses on peut supposer que N est premier. Posons $\delta := \lceil \log_2(N) \rceil$. Nous réutilisons les notations de la section 1. On pose pour tout $0 \leqslant i \leqslant \delta$ et $0 \leqslant j < 2^i$:

$$U_{i,j} := \left\{ k \in \mathbb{N} \;\middle|\; j\frac{N}{2^i} < k \leqslant (j+1)\frac{N}{2^i} \right\}.$$

On rappelle la relation suivante :

$$U_{i,j} = U_{i+1,2j} \sqcup U_{i+1,2j+1}.$$

Nous écrivons maintenant l'arbre binaire des sous-produits du calcul de $\prod_{i=0}^{N-1} B(L_1)(\theta+i)$. Posons

$$A_{i,j} := \prod_{k \in U_{i,j}} B(L_1)(\theta + k - 1)$$

et

$$S_{i,j} := \prod_{\substack{p \in U_{i,j} \\ p \text{ premier} \\ p \nmid f}} p.$$

On a évidemment les relations

$$A_{i,j} = A_{i+1,2j} A_{i+1,2j+1}$$
$$S_{i,j} = S_{i+1,2j} S_{i+1,2j+1}.$$

et de plus $\prod_{i=0}^{N-1} B(L_1)(\theta+i) = A_{0,0}$.
On peut donc calculer de manière ascendante les arbres binaires des sous-produits et des diviseurs.

Remarque 3.2.3.5. — *On définit un arbre des sous-produits similaire pour le calcul de* $\prod_{i=0}^{N-1} f(\theta+i)$.

Le calcul de l'arbre des diviseurs peut être effectué en $O(N \log^2(N) \log\log(N))$ opérations binaires.
Le coût du calcul de l'arbre des sous-produits du calcul de $A_{0,0}$ peut être vu comme le calcul de l'arbre des sous-produits d'un produit de N matrices de taille $m_1 := \deg(L_1)$ à coefficients dans $\mathbb{Z}[\theta]/(\theta^{d+1+\eta})$ avec $\eta \leqslant d$. Cependant, une fois n'est pas coutume, les calculs ayant lieu dans $\mathbb{Z}$, il nous faut connaitre la taille des entiers manipulés. On suppose que les entiers apparaissant dans l'écriture de L_1 sont de taille au plus n.

Lemme 3.2.3.6. — *Pour tout* $i \in [\![0, N]\!]$, *les coefficients de* $B(L_1)(\theta+i)$ *sont de taille au plus* $n + d + 1 + d\lceil \log_2(N) \rceil$.

Preuve. Soit P apparaissant dans $B(L)$. P est de degré au plus d. On peut donc écrire $P = \sum_{i=0}^{d} p_i \theta^i$ avec $p_i \leqslant 2^n$. On a alors :

$$P(\theta+a) = \sum_{j=0}^{d} \left(\sum_{i=j}^{d} \binom{i}{j} p_i a^{i-j} \right) \theta^j.$$

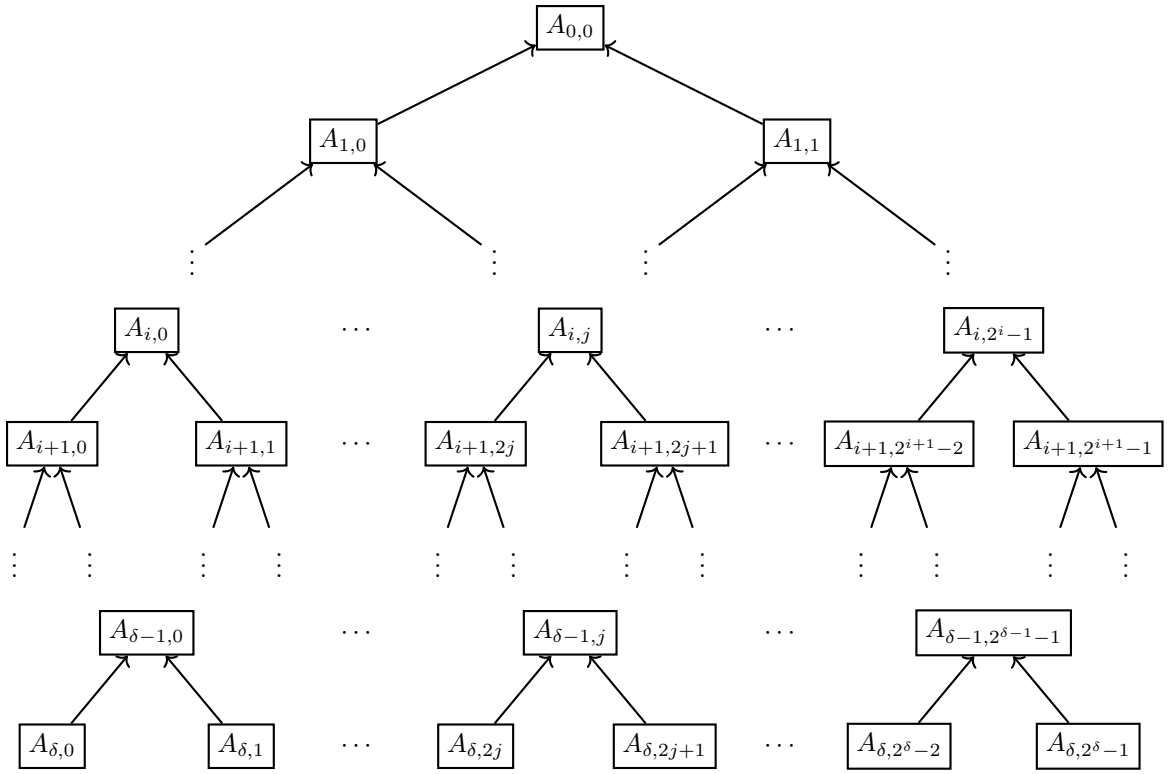


FIG. 7 : Arbre des sous-produits

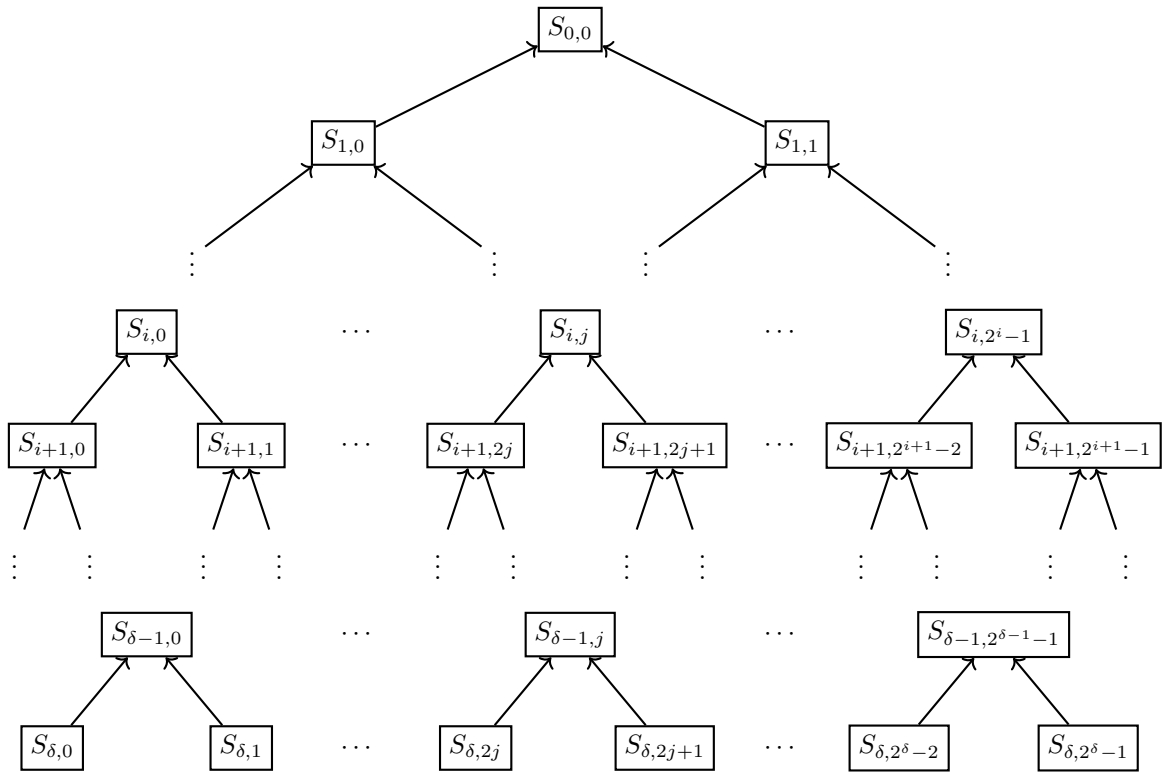


FIG. 8 : Arbre des diviseurs

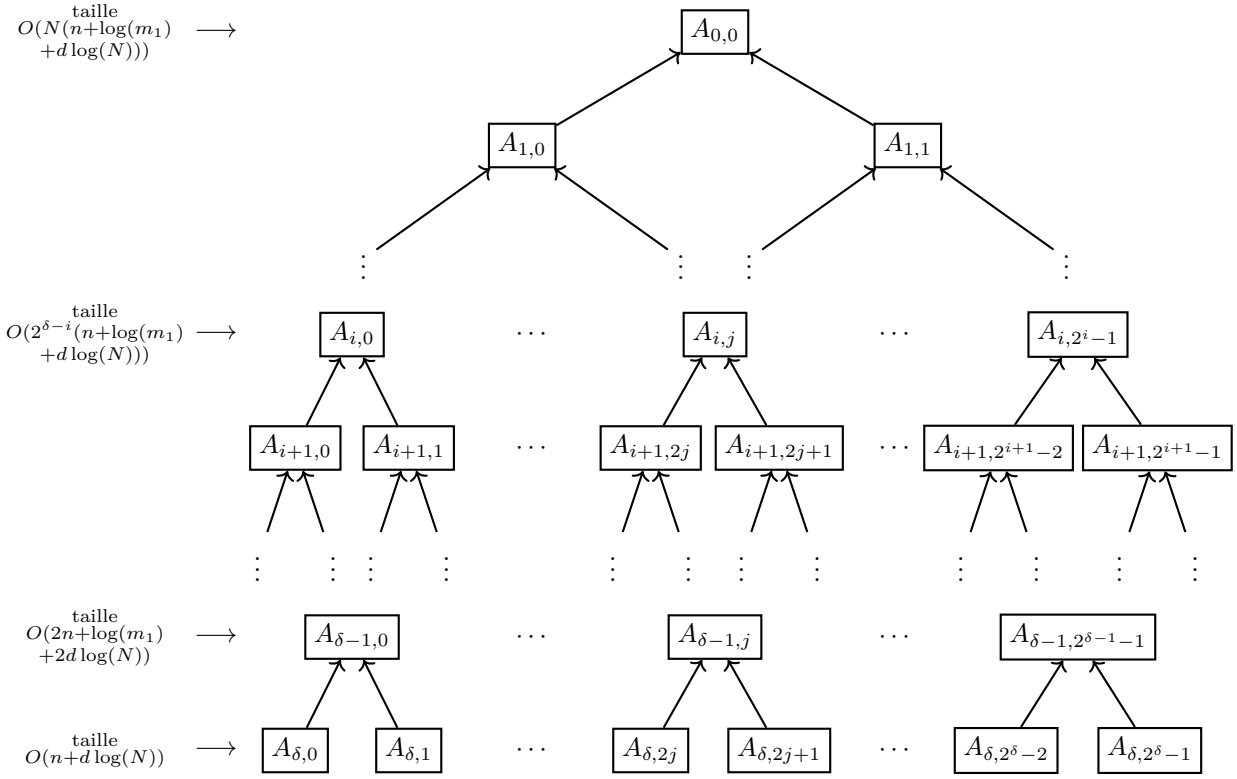


FIG. 9 : Taille des entiers par étage de l'arbre

Il suit que les coefficients de $P(\theta+i)$ sont majorés par

$$2^n N^d \max_j \left(\sum_{i=j}^{d} \binom{i}{j} \right)$$

Or en posant $Q_d = \sum_{i=0}^{d} \theta^d$ il vient que $Q_d(\theta+1) = \sum_{j=0}^{d} \theta^j \sum_{i=j}^{d} \binom{i}{j}$. Mais alors $Q_d(2) = 2^{d+1} - 1 = \sum_{j=0}^{d} \sum_{i=j}^{d} \binom{i}{j}$. On obtient ainsi $\sum_{i=j}^{d} \binom{i}{j} \leqslant 2^{d+1}$.
Les coefficients de $P(X+a)$ sont donc majorés par

$$2^{n+d+1} N^d.$$

Le résultat en découle. □

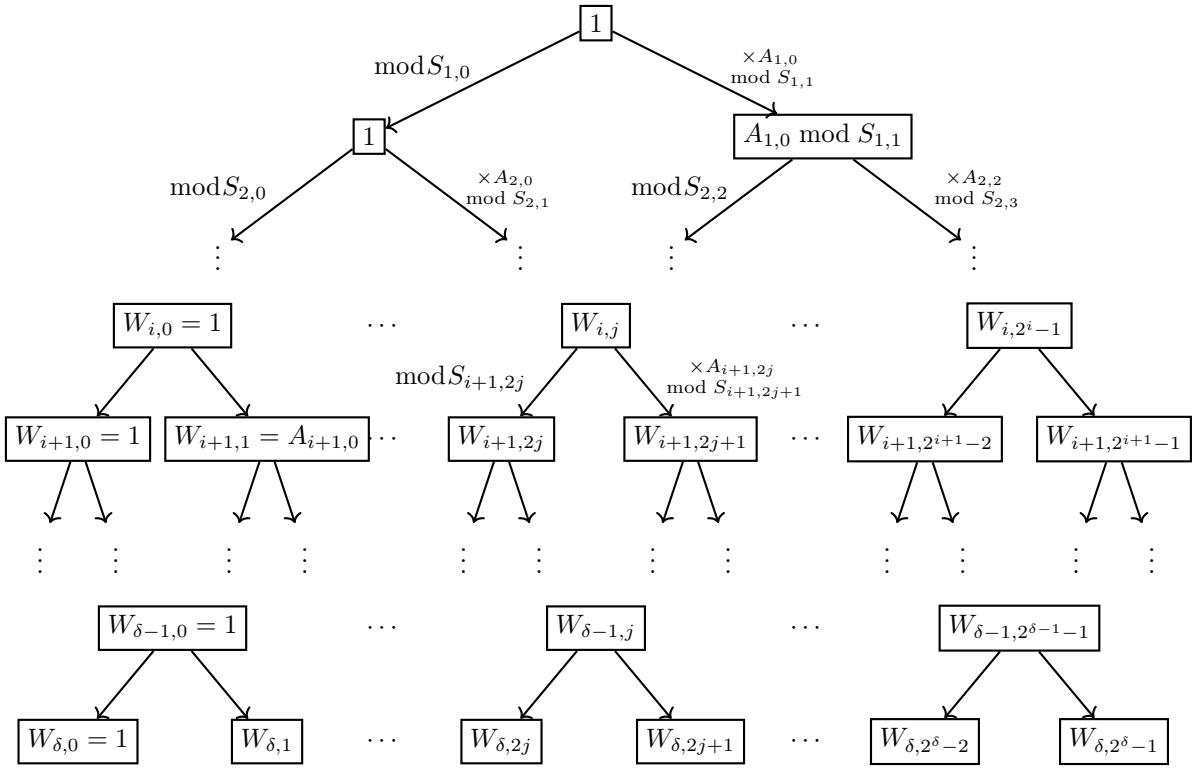
Si A et $B \in M_{m_1}(\mathbb{Z}[\theta])$ ont des coefficients de degré au plus d et ne font intervenir que des entiers de taille au plus n_1, alors le produit AB ne fait intervenir que des entiers de taille au plus $2n_1 + \log_2(d) + \log_2(m_1)$. Il suit que les $A_{i,j}$ font intervenir des entiers de taille au plus $2^{\delta-i}(n+d+1+d\log_2(N)) + (2^{\delta-i}-1)(\log_2(dm))$.

Notons $C(N)$ le coût du calcul d'un tel arbre pour un produit de N matrices en opérations binaires. On obtient

$$\begin{aligned} C(N) = {} & O(\mathrm{MM}(m_1) d\log(d)\log\log(d) N(n+\log(m_1)+d\log(N)) \\ & \log(N(n+\log(m_1)+d\log(N)))\log\log(N(n+\log(m_1)+d\log(N)))) + 2C(N/2) \end{aligned}$$

ce qui donne, en faisant l'hypothèse raisonnable que $N \geqslant n+\log(m_1)+d\log(N)$,

$$C(N) = O(\mathrm{MM}(m_1) d\log(d)\log\log(d) N(n+\log(m_1)+d\log(N))\log^2(N)\log\log(N)\log\log\log(N)).$$



REMARQUE 3.2.3.7. — *En pratique, on peut se contenter de calculer* $\mathrm{mod} S_{0,0}$ *qui est de taille* $O(N)$.

Comme dans la section 1, on introduit pour tout i et j ayant du sens

$$W_{i,j} = \prod_{l=0}^{j-1} A_{i,l} \bmod S_{i,j}$$

On a alors :

$$\begin{aligned} W_{0,0} &= 1 \\ W_{i+1,2j} &= W_{i,j} \bmod S_{i+1,2j} \\ W_{i+1,2j+1} &= A_{i+1,2j} W_{i,j} \bmod S_{i+1,2j+1} \end{aligned}$$

On peut donc calculer l'arbre des $W_{i,j}$

Le calcul de cet arbre depuis la racine prend une multiplication de matrices de $M_{m_1}(\mathbb{Z}[\theta]/(S_{0,0}, \theta^{d+1+\eta}))$ et $O(m_1^2 d)$ division euclidiennes d'entiers.

LEMME 3.2.3.8. — *$S_{i,j}$ est de taille $O(N/2^i)$ pour tout i et j ayant du sens.*

Preuve.

$$\begin{aligned}
\log(S_{i,j}) &= \log\left(\prod_{\substack{p\in U_{i,j}\\ p \text{ premier}}} p\right)\\
&= \sum_{\substack{p\in U_{i,j}\\ p \text{ premier}}} \log(p)\\
&\sim \sum_{k=\alpha/\log(\alpha)}^{\beta/\log(\beta)} \log(k\log(k))\\
&= \sum_{k=\alpha/\log(\alpha)}^{\beta/\log(\beta)} \log(k) + \log\log(k)\\
&= O(\beta-\alpha)
\end{aligned}$$

avec $\alpha = jN2^{-i}+1$ et $\beta = (j+1)N2^{-i}$. La dernière égalité se déduit du lien série-intégrale. □

On en déduit que le calcul de l'arbre des $W_{i,j}$ peut s'effectuer en

$$O(\mathrm{MM}(m_1)d\log(d)\log\log(d)N\log^2(N)\log\log(N) \text{ opérations binaires.}$$

Remarque 3.2.3.9. — *On calcule de manière similaire les* $\prod_{i=0}^{p-1} f(\theta+i) \bmod (p,\theta^{d+1+2\eta})$ *en*

$O(d\log(d)\log\log(d)N(n+d\log(N))\log^2(N)\log\log(N)\log\log\log(N))$ *opérations binaires.*

On peut écrire l'algorithme final :

Données : $L \in \mathbb{Z}[x]\langle\partial\rangle, N \in \mathbb{N}\rangle$
Résultat : $\chi(A_p(\pi_{x,p}(L)))$ pour presque tout $p \leqslant N$ premier
$d \leftarrow$ le degré maximal des coefficients de L ;
$m \leftarrow \deg(L)$;
Calculer $L_1 \in \mathbb{Z}[\theta]\langle\partial\rangle$ tel que $\Phi(L) = L_1\partial^{-d}$;
$m_1 \leftarrow \deg(L_1)$;
$f \leftarrow$ le coefficient dominant de L_1 ;
$\eta \leftarrow \deg(f)$;
$\delta \leftarrow \lceil \log_2(N) \rceil$;
pour $i \in [\![0; N-1]\!]$ **faire**
  Calculer $f(\theta+i) \bmod \theta^{d+1+2\eta}$ et $f(\theta+i)B(L_1)(\theta+i)$
Établir la liste $\mathcal{P}$ des $d < p \leqslant N$ premiers ne divisant pas f et calculer tous les $S_{\delta,j}$;
Calculer l'arbre des sous-produits pour $\prod_{i=0}^{N-1} f(\theta+i)B(L_1)(\theta+i) \bmod \theta^{d+1+\eta}$;
Calculer l'arbre des $W_{i,j}$ associé et en déduire pour tout $p \in \mathcal{P}$,
$\prod_{i=0}^{p-1} f(\theta+i)B(L_1)(\theta+i) \bmod p, \theta^{d+1+\eta}$;
Calculer de même pour tout $p \in \mathcal{P}$, $\prod_{i=0}^{p-1} f(\theta+i) \bmod p, \theta^{d+1+2\eta}$;
pour $p \in \mathcal{P}$ **faire**
  En déduire $B_p(\pi_{\theta,p}(L_1)) \bmod \theta^{d+1}$;
  Calculer $\left(\prod_{i=0}^{p-1} f(\theta+i)\right)\chi(B_p(\pi_{\theta,p}(L_1))) \bmod \theta^{d+1}$;
  En déduire $\chi(A_p(\pi_{x,p}(L)))$
retourner *la liste des* $\chi(A_p(\pi_{x,p}(L)))$

Algorithme 16 : Calcul efficace d'un grand nombre de p-courbures

Du travail qui précède on en déduit enfin le résultat final, et *original*, de ce mémoire :

THÉORÈME 3.2.3.10. — *Étant donné $L \in \mathbb{Z}[x]\langle\partial\rangle$, d'ordre m, dont les coefficients sont de degrés au plus d et faisant intervenir des entiers de taille au plus n, il est possible de calculer tous les polynômes caractéristiques des p-courbures de L pour tous les premiers $p \leqslant N$ en*

$$\tilde{O}(\mathrm{MM}(m+d)dN(n+d+\log(m+d))) \text{ opérations binaires}$$

sous l'hypothèse que $d \ll N$.

A Division euclidienne rapide et évaluation multipoints

Soit A un anneau commutatif. Le but de cette annexe est de donner un algorithme efficace d'évaluation d'un polynôme $P \in A[X]$ avec A un anneau, en $a_1, \ldots, a_n \in A$. Pour ce faire, nous commençons par donner un algorithme rapide de division euclidienne de polynômes. L'idée de s'intéresser d'abord à ce problème vient de ce que l'évaluation de P en $a \in A$ revient à trouver le reste de la division euclidienne de P par $(X - a)$.

Soient P_1 et $P_2 \in A[X]$ de degré respectivement d_1 et d_2 avec $d_1 < d_2$ tel que le coefficient dominant de P_2 soit inversible dans A. Le premier algorithme de division euclidienne consiste à poser la division :

Données : $P_1, P_2 \in A[X]$
Résultat : $Q, R \in A[X]$ tels que $P_1 = QP_2 + R$ avec $\deg(R) < \deg(P_2)$

$Q \leftarrow 0$;
$R \leftarrow P_1$;
tant que $\deg R \geqslant \deg P_2$ **faire**
  $a, b \leftarrow$ les coefficients dominants respectifs de R et P_2 ;
  $Q \leftarrow Q + \frac{a}{b} X^{\deg(R)-\deg(P_2)}$;
  $R \leftarrow R - \frac{a}{b} P_2 X^{\deg(R)-\deg(P_2)}$
retourner Q, R

Chaque étape de l'algorithme coûte au plus $O(\deg(P_2))$ opérations arithmétiques dans A (en effectuant intelligemment les soustractions ; en effet on peut à chaque fois ne s'intéresser qu'au $\deg(P_2)$ premiers coefficients, sans cela le coût est en $O(\deg(P_1))$ opérations) et l'algorithme effectue au plus $\deg(P_1) - \deg(P_2)$ étapes. Cet algorithme a donc un coût en $O(\deg(P_2)(\deg(P_1) - \deg(P_2))$ opérations arithmétiques dans A.
Cet algorithme a donc un coût quadratique en les degrés des polynômes. La sortie étant linéaire en $\deg(P_1)$, on en déduit que cet algorithme n'est pas optimal.
Une amélioration de cette complexité vient de l'inversion des séries formelles.

A.1 Inversion des séries formelles et division euclidienne

On rappelle que l'anneau des séries formelles à coefficients dans A, noté $A[[X]]$, est l'anneau dont l'ensemble sous-jacent et $A^{\mathbb{N}}$ dont les éléments sont représentés sous la forme $(f_i)_{i\in\mathbb{N}} = \sum_{i\in\mathbb{N}} f_i X^i$. Cet anneau est muni de l'addition terme à terme et de la multiplication suivante

$$\left(\sum_{i\in\mathbb{N}} f_i X^i\right)\left(\sum_{j\in\mathbb{N}} g_j X^j\right) = \sum_{i\in\mathbb{N}}\left(\sum_{j=0}^{i} f_j g_{i-j}\right) X^i$$

dont le neutre est 1.

REMARQUE A.1. — *Cet anneau peut être vu comme une extension de $A[X]$.*

PROPOSITION A.2. — *Soit $f = \sum_{i\in\mathbb{N}} f_i X^i$. f est inversible dans $A[[X]]$ si et seulement si $f_0 \in A^\times$.*

Preuve. Supposons f inversible et notons g son inverse. Alors $(fg)_0 = f_0 g_0 = 1$ donc f_0 est inversible. Réciproquement supposons que $f_0 \in A^\times$. On va construire un inverse g par récurrence. Supposons l'existence d'un tel g.

On a alors $g_0 = f_0^{-1}$. Supposons maintenant construits les $n+1$ premiers coefficients $g_0, \dots, g_n$ de g, pour $n \geqslant 0$. On a alors :

$$(fg)_{n+1} = 0 = \sum_{j=0}^{n+1} f_j g_{n+1-j}.$$

On en déduit

$$g_{n+1} = -\frac{1}{f_0} \sum_{j=1}^{n+1} f_j g_{n+1-j}.$$

Réciproquement, on vérifie que la suite g définie par une telle formule de récurrence donne bien l'inverse de f. □

La question se pose à présent du calcul effectif de l'inverse d'une série formelle. Comme on ne peut évidemment pas calculer tous les coefficients de l'inverse d'une série formelle, la question est de savoir en combien de temps, ou opérations dans A, on peut calculer les n premiers coefficients. Un premier algorithme est évidemment donné par la formule de récurrence :

Données : $f_0, f_1, \dots, f_n$ où $f = \sum_{i \in \mathbb{N}} f_i X^i \in A[[X]]$ avec $f_0 \in A^\times$, $n \in \mathbb{N}$
Résultat : $g_0, \dots, g_n$ où $f^{-1} = \sum_{i \in \mathbb{N}} g_i X^i$

si $n = 0$ **alors**
  retourner f_0^{-1}
sinon
  Calculer récursivement $g_0, \dots, g_{n-1}$;
  $g_n \leftarrow -f_0^{-1} \sum_{k=0}^{n-1} g_k f_{n-k}$;
  retourner $g_0, g_1, \dots, g_n$

Comme le calcul de g_n à partir de $g_0, f_0, g_1, f_1, \dots, g_{n-1}, f_{n-1}, f_n$ à un coût en $O(n)$ opérations arithmétiques $(+, -, \times)$ dans A, cet algorithme à un coût total en $O(n^2)$ opérations arithmétiques dans A. Comme la taille de la sortie est linéaire en n, cet algorithme n'est pas optimal.

L'idée qui donne un algorithme en temps quasi-linéaire nous vient de l'analyse, il s'agit de la méthode de Newton.

Proposition A.3. — *Soit $f : I \to \mathbb{R}$ une application $\mathcal{C}^2$, où $I \subset \mathbb{R}$ est un intervalle. On suppose que f admet un zéro x isolé dans I. On suppose également que si $f'(x) = 0$ alors x est un zéro isolé de f'. Sans perte de généralité, on peut supposer, pour faciliter les choses, que $0 \in I$ et $f(0) = 0$ est ce zéro isolé. Soit $a \in I$, et considèrons la suite à valeurs dans $\mathbb{R}$ suivante : $x_0 = a$, $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ si $x_n \neq 0$, et $x_{n+1} = x_n$ sinon.*
Alors il existe $\eta > 0$ tel que si $a < \eta$ alors la suite $(x_n)_{n \geqslant 0}$ est bien définie, et de plus $x_n \xrightarrow[n\infty]{} 0$. De plus, si $x_n \leqslant \varepsilon$ alors $x_{n+1} \leqslant \kappa \varepsilon^2$ avec κ une constante.

Preuve. Quitte à prendre η suffisamment petit, on peut supposer que f et f' n'ont pas d'autres zéros que 0 sur $]-\eta, \eta[$. On commence par faire le constat suivant : comme f est $\mathcal{C}^2$ on peut écrire

$$\frac{1}{f'(x_n)} = \frac{1}{f'(0)} \frac{1}{1 + O(x_n)} = \frac{1}{f'(0)}(1 + O(x_n))$$

Ici le O est une majoration au voisinage de 0. Ainsi quitte à prendre η encore plus petit, on peut supposer qu'il existe $\kappa_1 > 0$ tel que $\left| \frac{1}{f'(0)} - \frac{1}{f'(x)} \right| \leqslant \kappa_1 x$ pour tout $|x| \leqslant \eta$.

Supposons $|x_n| < \eta$. On a alors

$$\begin{aligned}
|x_{n+1}| &= \left| x_n - \frac{f(x_n)}{f'(x_n)} \right| \\
&= \left| x_n - \frac{f'(0)x_n + 2f''(0)x_n^2 + O(x_n^3)}{f'(x_n)} \right| \\
&= \left| x_n - \frac{f'(0)}{f'(0)} x_n(1 + O(x_n)) + 2\frac{f''(0)}{f'(0)} x_n^2 + O(x_n^3) \right| \\
&\leqslant \left(\kappa + 2 \left| \frac{f''(0)}{f'(0)} \right| \right) |x_n|^2 + O(x_n^3).
\end{aligned}$$

Quitte à supposer x_n suffisamment petit (donc η suffisamment petit) de sorte que

$$x_n \left(\kappa + 2 \left| \frac{f''(0)}{f'(0)} \right| \right) < 1$$

et $O(x_n^3)$ suffisamment petit également, on obtient que la suite (x_n) reste à valeurs dans $]-\eta;\eta[$, et que de plus elle vérifie bien les conditions demandées. □

On a donc l'idée d'utiliser une adaptation de itération de Newton pour trouver l'inverse d'une série formelle. L'application dont on cherche un zéro est

$$\begin{array}{rccc}
\Phi_f : & A[[X]] & \to & A[[X]] \\
& g & \mapsto & \frac{1}{g} - f.
\end{array}$$

On a « $\Phi_f' = f$ » et l'itération de Newton s'écrit alors

$$g_{n+1} = g_n + g_n^2 \left(\frac{1}{g_n} - f \right),$$

ou encore

$$g_{n+1} = g_n - (fg_n - 1)g_n.$$

La proposition suivante confirme l'intuition analytique de cette ébauche d'algorithme. On introduit avant cela les notations suivantes :

Définition A.4. — *Soient $f, g \in A[[X]]$. On dit que $f = g + O(X^n)$ avec $n \in \mathbb{N}$ si et seulement si X^n divise $f - g$. Cela revient à dire que les n premiers coefficients de f et g coïncident.*

Proposition A.5. — *Soit $f \in A[[X]]$ inversible, et $f_1 = f + O(X^{2n})$. On suppose que $g = f^{-1} + O(X^n)$. Alors $g - (f_1 g - 1)g = f^{-1} + O(X^{2n})$.*

Preuve. On commence par remarquer qu'il revient au même de dire que $g = f^{-1} + O(X^n)$ et $fg = 1 + O(X^n)$, pour tout f, g et n ayant du sens.

On reprend les notations de la proposition. On note $g_1 = g - (fg - 1)g$. On sait qu'il existe $h_1, h_2 \in A[[X]]$ tels que $fg = 1 + h_1 X^n$ et $f_1 = f + h_2 X^{2n}$.
Alors

$$\begin{aligned}
fg_1 &= fg - fg(f_1 g - 1) \\
&= 1 + h_1 X^n - (1 + h_1 X^n)(fg + gh_2 X^{2n} - 1) \\
&= 1 + h_1 X^n - (1 + h_1 X^n)(h_1 X^n + gh_2 X^{2n}) \\
&= 1 + X^{2n}(h_1^2 + gh_2 + h_1 X^n g h_2),
\end{aligned}$$

ce qui achève la démonstration. □

On en déduit l'algorithme suivant :

Données : $f \bmod X^n \in A[[X]]$ inversible, $n = 2^k$
Résultat : $f^{-1} \bmod X^n$

si $n = 1$ **alors**
  retourner f_0^{-1}
sinon
  Calculer récursivement $g = f^{-1} \bmod X^{n/2}$;
  retourner $g - (fg - 1)g$

Algorithme 17 : Inversion de Newton

Chaque étape du calcul coûte $O(1)$ multiplications de polynômes de degré n, lesquelles peuvent être effectuées en $O(n \log(n) \log\log(n))$ opérations arithmétiques dans A. On notant $C(n)$ le coût de cet algorithme pour $n = 2^k$ en opérations arithmétiques dans A, on trouve :

$$C(n) = \sum_{i=1}^{k} O(2^i i \log(i)) = O(2^k k \log(k))$$

Le coût d'une inversion modulo X^n d'une série formelle est donc $O(n \log(n) \log\log(n))$.

Mais pourquoi s'embêter à inverser des séries formelles alors que nous voulons effectuer des divisions euclidiennes de polynômes ? L'intérêt apparaît en réécrivant

$$P_1 = QP_2 + R$$

avec $\deg(R) < \deg(P_2)$ sous la forme

$$\frac{P_1}{P_2} = Q + \frac{R}{P_2}.$$

Là encore, ferions nous de l'analyse, nous dirions que le comportement de $Q + \frac{R}{P_2}$ est le même en l'infini que celui de Q. Comme nous ne pouvons que très modérément explorer l'infini, nous nous ramènerions au comportement de $Q(1/X) + \frac{R}{P_2}(1/X)$ en 0... Nous ne sommes certes pas analystes, mais c'est exactement ce que nous allons faire.

On a :

$$X^{\deg(P_1)} P_1\left(\frac{1}{X}\right) = X^{\deg(P_1)-\deg(P_2)} Q\left(\frac{1}{X}\right) X^{\deg(P_2)} P_2\left(\frac{1}{X}\right) + X^{\deg(P_1)} R\left(\frac{1}{X}\right)$$

et encore

$$\frac{X^{\deg(P_1)} P_1\left(\frac{1}{X}\right)}{X^{\deg(P_2)} P_2\left(\frac{1}{X}\right)} = X^{\deg(P_1)-\deg(P_2)} Q\left(\frac{1}{X}\right) + X^{\deg(P_1)} R\left(\frac{1}{X}\right) \frac{1}{X^{\deg(P_2)} P_2\left(\frac{1}{X}\right)}$$

Comme $\deg(R) \leqslant \deg(P_2) - 1$, on en déduit que

$$X^{\deg(P_1)} R\left(\frac{1}{X}\right) = O(X^{\deg(P_1)-\deg(P_2)+1})$$

et encore

$$X^{\deg(P_1)} R\left(\frac{1}{X}\right) \frac{1}{X^{\deg(P_2)} P_2\left(\frac{1}{X}\right)} = O(X^{\deg(P_1)-\deg(P_2)+1}).$$

On en déduit que

$$X^{\deg(Q)} Q\left(\frac{1}{X}\right) = \frac{X^{\deg(P_1)} P_1\left(\frac{1}{X}\right)}{X^{\deg(P_2)} P_2\left(\frac{1}{X}\right)} + O(X^{\deg(Q)+1}).$$

On rappelle que pour tout polynôme, l'opération $X^{\deg(P)} P(1/X)$ consiste simplement à inverser l'ordre des coefficients et peut être fait en temps linéaire en le degré de P. Le polynôme ainsi obtenu est alors inversible lorsqu'il est vu comme une série formelle à coefficients dans un corps. D'une

manière plus générale, pouvoir inverser $X^{\deg(P_2)}P_2(1/X)$ dans l'anneau des séries formelles $A[[X]]$ revient à demander que le coefficient dominant de P_2 soit inversible.

On obtient l'algorithme suivant :

Données : $P_1, P_2 \in A[X]$ avec le coefficient dominant de P_2 inversible dans A
Résultat : $Q, R \in A[X]$ tels que $P_1 = QP_2 + R$ avec $\deg(R) < \deg(P_2)$

$d \leftarrow \deg(P_1) - \deg(P_2)$;
$A_1 \leftarrow X^{\deg(P_1)}P_1(1/X)$;
$B_1 \leftarrow X^{\deg(P_2)}P_2(1/X)$;
Calculer $G = B_1^{-1} \bmod X^{d+1}$;
$Q_1 \leftarrow A_1 G \bmod X^{d+1}$;
$Q \leftarrow X^d Q_1(1/X)$;
retourner $Q, P_1 - P_2Q$

Algorithme 18 : Division euclidienne efficace de polynômes

On en déduit que la division euclidienne de deux polynômes P_1 et P_2 peut être effectuée en $O(m\log(m)\log\log(m))$ opérations arithmétiques dans A, avec $m = \max(\deg(P_1) - \deg(P_2), \deg(P_2))$.

Division euclidienne des entiers Avant de passer à la suite et de voir les applications de ce calcul à l'évaluation multipoints d'un polynôme, nous faisons un détour par la division euclidienne des entiers qui repose sur des idées similaires. Soient $b < a \in \mathbb{N}$. On cherche à effectuer la division euclidienne de a par b. Comme pour les polynômes, on va en fait chercher à inverser b avec suffisamment de précision pour connaitre $\frac{a}{b}$ avec une précision à l'unité.
Là encore nous allons calculer $1/b$ par une itération de Newton. On pourrait essayer de refaire cette itération avec $f_b(x) = bx - 1$ mais nous n'aurions rien gagné puisque $f_b'(x) = b$ et que nous devrions alors inverser b. On lui préfèrera $f_b(x) = \frac{1}{x} - b$. La formule de récurrence s'écrit alors :

$$u_{n+1} = x_n + \frac{1/u_n - b}{1/u_n^2} = u_n + u_n - bu_n^2 = u_n(2 - bu_n).$$

Écrivons $u_n = \frac{1}{b} + \varepsilon$. On alors :

$$bu_{n+1} = bu_n(2 - bu_n) = (1 + b\varepsilon)(1 - b\varepsilon) = 1 - b^2\varepsilon^2$$

et encore

$$u_{n+1} = \frac{1}{b} - b\varepsilon^2.$$

On en conclut qu'en prenant $|u_0 - \frac{1}{b}| < \frac{1}{b}$, ie $0 \leqslant u_0 < \frac{2}{b}$, la suite (u_n) converge vers $\frac{1}{b}$. En regardant le nombre de chiffres binaires de b, on peut facilement en déduire un encadrement

$$2^i \leqslant b < 2^{i+1} \Leftrightarrow 2^{-i} < \frac{2}{b} \leqslant 2^{i-1}.$$

Le choix de u_0 est donc facile. On pourrait même vouloir que la précision double à chaque étape ce qui revient à demander $|u_0 - 1/b| \leqslant \frac{1}{2b}$, donc

$$\frac{1}{2b} \leqslant u_0 \leqslant \frac{3}{2b}.$$

On peut alors prendre

$$\frac{1}{2b} \leqslant 2^{-(i+1)} \leqslant u_0 \leqslant \frac{3}{2^{i+2}} \leqslant \frac{3}{2b}$$

et finalement $u_0 = 2^{-(i+1)}$.

Comme on veut s'épargner des calculs sur les flottants, on va maintenant se ramener à un calcul sur des entiers. Supposons que l'on veuille connaître les n premiers chiffres après la virgule de $1/b$

(en base binaire). Cela signifie que l'on veut $|1/b - x| < 2^{-n}$. Cela revient à connaitre $\frac{2^n}{b}$ à l'unité près. On pose donc $v_i = 2^n u_i$. On a la formule de récurrence :

$$v_{i+1} = 2v_i - v_i^2 \frac{b}{2^n}.$$

Cela fait encore apparaître des flottants, c'est pourquoi on prend

$$v_{i+1} = 2v_i - \left\lfloor v_i^2 \frac{b}{2^n} \right\rfloor.$$

On fait la supposition que $\left|\frac{2^n}{b} - v_0\right| \leqslant \frac{2^{n-1}}{b}$.

Proposition A.6. — *La suite ainsi définie vérifie à partir d'un certain rang* $\left|\frac{2^n}{b} - u_n\right| < 1$.

Preuve. Supposons $v_i = \frac{2^n}{b} + \varepsilon$. On a alors

$$bv_{i+1} = 2^{n+1} + 2b\varepsilon - b \left\lfloor \frac{1}{b} \frac{(2^n + b\varepsilon)^2}{2^n} \right\rfloor.$$

On a l'encadrement suivant pour tout $x, y \in \mathbb{N}$ avec $x \neq 0$:

$$y - x < x \left\lfloor \frac{y}{x} \right\rfloor \leqslant y,$$

ce qui donne :

$$2^n - \frac{b^2\varepsilon^2}{2^n} \leqslant bv_{i+1} < 2^n - \frac{b^2\varepsilon^2}{2^n}$$

ou encore

$$v_{i+1} = \left\lceil \frac{2^n}{b} - \frac{b\varepsilon^2}{2^n} \right\rceil.$$

Le résultat en découle puisque l'on a choisi $\left|\frac{2^n}{b} - v_0\right| < \frac{2^{n-1}}{b}$. □

On voit de plus que lorsque $\left|\frac{2^n}{b} - v_i\right| = \varepsilon \geqslant 1$ alors $\left|\frac{2^n}{b} - v_{i+1}\right| \leqslant \frac{b}{2^n}\varepsilon^2$.

Ainsi en supposant $\left|\frac{2^n}{b} - v_0\right| \leqslant \frac{2^{n-1}}{b}$ on déduit par récurrence immédiate que tant que $\frac{2^n}{2^{2^i} b} \geqslant 1$ on a :

$$\left|\frac{2^n}{b} - v_i\right| \leqslant \frac{2^n}{2^{2^i} b}.$$

Il suffit alors de savoir pour quelle valeur de i on a $\frac{2^n}{2^{2^i} b} < 1$. On peut connaitre un encadrement $2^k \leqslant b < 2^{k+1}$ ce qui ramène l'inégalité précédente à :

$$2^{2^i} > 2^{n-k}.$$

On en déduit enfin le théorème suivant :

Théorème A.7. — *Soient $b < a \in \mathbb{N}$. On peut effectuer la division euclidienne de a par b en $O(\log(a) \log\log(a)^2 \log\log\log(a))$ opérations binaires.*

Preuve. On cherche à connaitre une approximation x de $\frac{1}{b}$ de sorte que

$$\left|ax - a\frac{1}{b}\right| < 1.$$

On peut trouver un encadrement $2^{k_a - 1} < a \leqslant 2^{k_a}$. Il suffit de trouver x vérifiant :

$$\left|2^{k_a} x - \frac{2^{k_a}}{b}\right| < 1.$$

On en déduit l'algorithme suivant :

Données : $a, b \in \mathbb{N}$ avec $a > b$
Résultat : $q, r \in \mathbb{N}$ avec $r < b$ tels que $a = qb + r$

Calculer k_a tel que $2^{k_a - 1} < a \leqslant 2^{k_a}$;
Calculer k_b tel que $2^{k_b} \leqslant b < 2^{k_b+1}$;
$u_0 \leftarrow 2^{k_a - k_b - 1}$;
compteur $\leftarrow 1$;
tant que *compteur* $\leqslant k_a - k_b$ **faire**
  $u_0 \leftarrow 2u_0 - \left\lfloor u_0^2 \frac{b}{2^n} \right\rfloor$
$q \leftarrow \left\lceil \frac{au_0}{2^{k_a}} \right\rceil$;
$r \leftarrow a - qb$;
si $r < 0$ **alors**
  retourner $q - 1, r + b$
sinon
  retourner q, r

Algorithme 19 : Division euclidienne efficace

Comme la taille de u_0 double à chaque étape du calcul et que l'algorithme effectue $O(\log(k_a - k_b))$ étapes, soit encore $O(\log(\log(a)))$ étapes, on en déduit que la complexité de cet algorithme est bien en $O(\log(a) \log\log(a) \log\log\log(a))$. □

A.2 Application à l'évaluation multipoints

Soit $P \in A[X]$, où A est un anneau commutatif intègre, et $a_1, a_2, \ldots, a_n \in A$. On cherche à calculer $P(a_1), \ldots, P(a_n)$. L'évaluation naïve en un point peut s'effectuer en $O(d)$ opérations arithmétiques dans A, où d est le degré de P : on calcule d'abord la liste des puissances de ce point jusqu'à d, puis on calcule la combinaison linéaire donnée par P. On en conclut que cette méthode naïve calcule $P(a_1), \ldots, P(a_n)$ en $O(dn)$ opérations arithmétiques dans A.

Cela n'est pas si mal lorsque $\deg(P)$ est petit, puisqu'on peut alors considérer que cet algorithme est linéaire en la taille de la sortie. On va montrer que l'on peut en fait effectuer ce calcul en temps quasi-linéaire en $\max(d - n, n)$. L'idée principale consiste à calculer $P \bmod (X - a_i)$ pour tout i. Bien sûr si l'on effectue simplement le calcul de la division euclidienne de P par $(X - a_i)$ pour tout i, on ne gagne rien. Le raffinement suivant de cette idée permet de gagner : évaluer P en $a_{i_1}, \ldots, a_{i_k}$ revient à évaluer R en $a_{i_1}, \ldots, a_{i_k}$, où $P = Q \prod_{j=1}^{k} (X - a_{i_j}) + R$.

On peut donc effectuer récursivement les calculs de sorte à n'avoir à faire les divisions euclidiennes par $(X - a_i)$ que sur des polynômes de petit degré. L'idée est donc de remplir récursivement, en partant du haut l'arbre binaire des restes successifs, représenté en Figure 10.

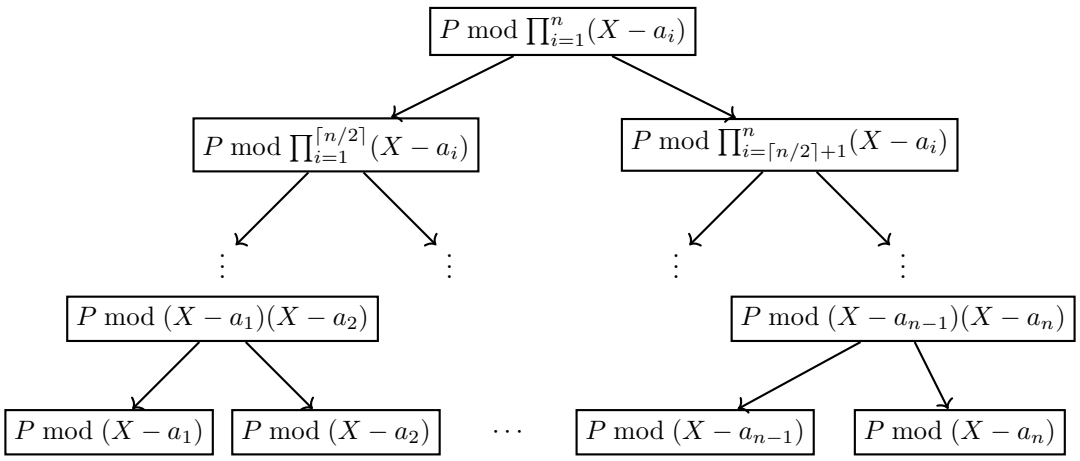


FIG. 10 : Arbre binaire des restes successifs

Pour cela, on doit avant calculer tous les $\prod_{i\in I}(X-a_i)$ par lesquels on va effectuer des divisions euclidiennes. Cela revient à remplir, en partant du bas cette fois, l'arbre binaire des diviseurs successifs représenté en Figure 10.

On suppose que n est divisible par 2. En notant $C(n)$ le coût du calcul de l'arbre binaire des diviseurs successifs pour n points, on voit que le calcul de l'arbre est celui d'une multiplication de deux polynômes de degré $n/2$, ce qui peut être effectué en $O(n\log(n)\log\log(n))$ opérations arithmétiques dans A, et du calcul de deux arbres binaires de diviseurs successifs pour $n/2$ points. On en déduit :

$$C(n) = O(n\log(n)\log\log(n)) + 2C(n/2)$$

et donc

$$C(n) = O(n\log^2(n)\log\log(n)).$$

Connaissant cet arbre, le calcul de l'arbre binaire des restes successifs coûte la division euclidienne de P par $\prod_{i=1}^{n}(X-a_i)$, puis le calcul récursif de deux arbres binaires de restes successifs. Comme passée la première étape on appelle toujours cet algorithme récursivement pour un certain nombre d de points et P vérifiant toujours $\deg(P) \leqslant 2d-1$ on note $C'(n)$ le coût du calcul de l'arbre binaire des restes successifs sous l'hypothèse $\deg(P) \leqslant 2n-1$. On a alors :

$$C'(n) = O(n\log(n)\log\log(n)) + 2C'(n/2)$$

et donc $C'(n) = O(n\log^2(n)\log\log(n))$.

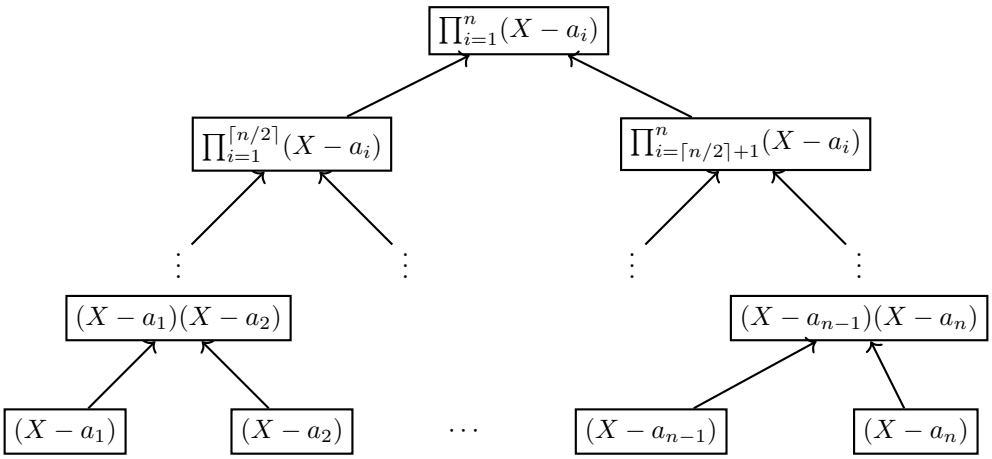


FIG. 11 : Arbre binaire des diviseurs successifs

On en déduit l'algorithme d'évaluation multipoints suivant :

Données : $P \in A[X]$, $a_1, \ldots, a_n \in A$
Résultat : $P(a_1), P(a_2), \ldots, P(a_n)$

Calculer récursivement l'arbre binaire des dividendes successifs ;
$R \leftarrow P \bmod \prod_{i=1}^{n}(X-a_i)$;
Calculer récursivement l'arbre binaire des restes successifs ;
retourner *Les feuilles de l'arbre binaire des restes successifs*

Algorithme 20 : Evaluation multipoints efficace

En utilisant l'algorithme en page 78 pour la division de R par P, l'algorithme ci-dessus termine en $O(m\log(m)\log\log(m)) + O(n\log^2(n)\log\log(n))$ opérations arithmétiques dans A, avec $m = \max(d-n, n)$, ce que l'on avait prédit.

B Localisation dans des anneaux non-commutatifs

Dans cette annexe nous présentons des résultats généraux sur la localisation dans des anneaux non commutatifs, en s'inspirant de [Bre14]. Pour plus de détails sur le sujet, on renvoie le lecteur à [Lam01].

Définition B.1. — *Soit R un anneau (associatif et unitaire) et $S \subset R$. On dit qu'un morphisme $f : R \to R'$ est S-inversible si et seulement si $f(S) \subset R'^{\times}$.*

f est dit universellement S-inversible si tout morphisme S-inversible se factorise par f.

Proposition B.2. — *Pour toute partie $S \subset R$ il existe un morphisme universellement S-inversible.*

Preuve. On pose $R_S = {}^{R_{\mathbb{Z}}\langle (X_s)_{s\in S}\rangle}/_I$ où I est l'idéal bilatère engendré par $\bigcup_{s\in S}\{sX_s - 1, X_s s - 1\}$. On vérifie alors immédiatement que $f : R \to R_S$ est universellement S-inversible. □

Remarque B.3. — *Le problème de cette construction est qu'elle ne donne, hors de la propriété universelle de R_S, aucune information sur sa structure. En particulier R_S peut-être nul, ou plus généralement, f non injective.*

Afin de remédier à ce problème, on cherche à exprimer les éléments de R_S sous la forme de fraction rs^{-1} où $r \in R$ et $s \in S$. Malheureusement une telle construction n'est pas toujours possible, et même lorsqu'elle l'est, ne possède pas toujours la propriété universelle du localisé. Cependant, dans les problèmes que nous aurons à étudier, ce sera le cas.

Définition B.4. — *Soit R un anneau. Un élément $a \in R$ est dit régulier s'il n'est pas un diviseur de zéro à droite ou à gauche.*

Proposition B.5. — *Soit R un anneau, $S \subset R$ contenant un élément non régulier. Alors tout $f : R \to R'$ vérifiant $f(S) \in R'^{\times}$ n'est pas injectif.*

Preuve. Considérons un tel f. Notons $s \in S$ un élément non régulier. Il existe $a \in R - \{0\}$ tel que $sa = 0$ (resp. $as = 0$). Alors $f(sa) = 0 = f(s)f(a)$ (resp. $f(as) = 0 = f(a)f(s)$) et en multipliant à gauche (resp. à droite) par $f(s)^{-1}$ on a $f(a) = 0$. □

La proposition qui précède justifie le parti pris du reste de cette annexe, à savoir de considérer que S ne contiendra que des éléments réguliers. Dans ce cadre on va chercher à donner une condition sur S pour obtenir un morphisme universellement S-inversible se comportant bien, à savoir :

Définition B.6. — *Soit R un anneau et $S \subset R$ multiplicative ne contenant que des éléments réguliers. R_S est appelé un anneau de quotient à droite par S s'il vérifie les conditions suivantes :*

1. *R s'injecte dans R_S ($f : R \hookrightarrow R_S$).*
2. *$S \subset R_S^{\times}$.*
3. *Tout élément de R_S s'écrit sous la forme rs^{-1} avec $r \in R$ et $s \in S$.*

Remarque B.7. — *Lorsque S est l'ensemble des éléments réguliers de R on dira d'un anneau de quotient à droite par S qu'il s'agit de* l'anneau classique *de quotient à droite de R.*

Remarque B.8. — *Il n'est pas évident* a priori *que ces seules conditions définissent un unique anneau à isomorphisme près. En effet comme les éléments de S ne commutent pas entre eux, il n'est pas possible de ramener le test d'égalité $rs^{-1} = r_1 s_1^{-1}$ à un test d'égalité dans R. Pour ces mêmes raisons, il n'est pas évident qu'un tel anneau induise un morphisme universellement S-inversible. Si en revanche les éléments de S commutent entre eux alors ces obstacles disparaissent.*
Nous verrons par la suite que même lorsque ce n'est pas le cas, un anneau de quotient à droite par S défini un morphisme universellement S-inversible.

Remarque B.9. — *Si un tel anneau existe, alors les éléments de R peuvent être multipliés à gauche par les inverses des éléments de S et donc :*

$$\forall r \in R, \forall s \in S, \exists r_1 \in R, \exists s_1 \in S, s^{-1}r = r_1 s_1^{-1},$$

ce que l'on peut réécrire

$$\forall r \in R, \forall s \in S, \exists r_1 \in R, \exists s_1 \in S, rs_1 = sr,$$

ou encore

$$\forall r \in R, \forall s \in S, rS \cap sR \neq \varnothing.$$

On appelle cette condition la ***condition de Ore à droite****.*

Théorème B.10. — *Soit R un anneau et S une partie multiplicative ne contenant que des éléments réguliers. On suppose que le couple (R, S) vérifie la condition de Ore à droite.*
Alors il existe un anneau de quotient à droite par S.
Cet anneau vérifie de plus que, pour tout $(r_1, r_2, s_1, s_2) \in R^2 \times S^2$

$$r_1 s_1^{-1} = r_2 s_2^{-1} \iff \exists u, v \in R, s_1 u = s_2 v \in S \text{ et } r_1 u = r_2 v.$$

On décrit de plus le comportement des opérations sur cet anneau : soient $(r_1, r_2, s_1, s_2) \in R^2 \times S^2$. Il existe $u, v \in R, s_1 u = s_2 v =: s \in S$. Alors :

$$r_1 s_1^{-1} r_2 s_2^{-1} = (r_1 u + r_2 v) s^{-1}$$

Il existe $u', v' \in S$ tels que $s_1 u' = r_2 v'$.

$$(r_1 s_1^{-1})(r_2 s_2^{-1}) = (r_1 u', s_2 v')$$

Preuve. On considère $\mathcal{I} = \{I \subset R \text{ idéal à droite contenant un élément de } S\}$ et $F = \{(f, I) | f : I \to R \text{ morphisme de } R\text{-modules à droite} | I \in \mathcal{I}\}$.

On munit F de la relation d'équivalence suivante :

$$(f, I) \sim (g, J) \iff \exists K \in \mathcal{I}, K \subset I \cap J, f_{|K} = g_{|K}.$$

Il s'agit bien d'une relation d'équivalence : seule la transitivité n'est pas complètement évidente. Supposons $(f, I_1) \sim (g, I_2)$ et $(g, I_2) \sim (h, I_3)$.
Il existe $J_1 \subset I_1 \cap I_2 \in \mathcal{I}$ et $J_2 \subset I_2 \cap I_3 \in \mathcal{I}$ tel que $f_{|J_1} = g_{|J_1}$ et $g_{|J_2} = h_{|J_2}$. Il existe $s_1 \in S \cap J_1$ et $s_2 \in S \cap J_2$.
Mais alors $s_1 S \cap s_2 R \neq \varnothing$ et donc $K := J_1 \cap J_2$ contient un élément de S par multiplicativité.

$$f_{|K} = g_{|K} = h_{|K}$$

ce qui permet de conclure sur la transitivité.
Posons enfin $R_S = {}^F/_{\sim}$. On le munit des lois de composition suivantes :

$$(f_1, I_1) + (f_2, I_2) = (f_1 + f_2, I_1 \cap I_2)$$
$$(f_1, I_1)(f_2, I_2) = (f_1 \circ f_2, f_2^{-1}(I_1))$$

Vérifions pour commencer que ces opérations sont bien définies, à commencer par $f_2^{-1}(I_1) \in \mathcal{I}$.
Soit $s_i \in I_i \cap S$. On sait que $f_2(s_2)S \cap s_1 R \neq \varnothing$ donc il existe $s \in S$ et $r \in R$ tels que $f_2(s_2)s = s_1 r$, ce qui entraine $s_2 s \in f_2^{-1}(I_1)$. L'addition est évidemment bien définie. Montrons que c'est aussi le cas de la multiplication. Il suffit en fait de le voir pour des idéaux emboités ($I \subset J$), et c'est alors évident (en traitant séparément l'équivalence sur le terme de gauche et sur le terme de droite).

L'addition est évidemment associative, commutative et distributive sur la multiplication. Elle est munie d'un neutre $(0, R)$ et tout élément (f, I) a pour opposé $(-f, I)$. La multiplication est également associative et munie d'un neutre, (Id_R, R).

En outre, R s'injecte dans R_S par l'application

$$\begin{array}{rccc} f : & R & \to & R_S \\ & r & \mapsto & (a \mapsto ra, R) \end{array}$$

Celle-ci est bien injective. En effet, un élément $(\varphi, I) \in R_S$ est nul si et seulement si φ s'annule sur un $s \in S \cap I$. Or S est composé d'éléments réguliers donc f est injective.

On a $S \subset R_S^\times$. En effet (s, R) a pour inverse $(sr \mapsto r, sR)$.

Tout élément de R_S est de la forme rs^{-1} pour $r \in R$ et $s \in S$. Soit $(f, I) \in R_S$. On peut supposer que I est de la forme sR pour $s \in R$.
Alors $(f, I) = (f(s), R)(s^{-1}, sR)$.
R_S est donc bien un anneau de quotient à droite par S.
Soit maintenant $(r_1, r_2, s_1, s_2) \in R^2 \times S^2$ de sorte que $r_1 s_1 = r_2 s_2 \in R_S$.
Cela peut encore se réécrire

$$(f_1, s_1 R) = (f_2, s_2 R) \in R_S$$

où $f_i : s_i r \mapsto r_i r$ avec $i \in \{1, 2\}$.
Par définition, il existe $K \subset s_1 R \cap s_2 R$ tel que $f_{1|K} = f_{2|K}$ et $S \cap K \neq \varnothing$. Soit $s \in K$. Alors $f_{1|sR} = f_{2|sR}$ et $sR \subset s_1 R \cap s_2 R$.
Ainsi il existe $u, v \in R$ tel que $s = s_1 u = s_2 v$. De plus $f_1(s) = r_1 u = f_2(s) = r_2 v$.
Réciproquement on voit que si il existe $u, v \in R$ tel que $s_1 u = s_2 v \in S$ et $r_1 u = r_2 v$ alors les applications f_1 et f_2 coïncident sur sR qui est un élément de $\mathcal{I}$ inclut dans $s_1 R \cap s_2 R$, donc $(f_1, s_1 R) = (f_2, s_2 R) \in R_S$.

Vérifions maintenant le comportement des opérations pour l'addition. Soit $(r_1, r_2, s_1, s_2) \in R^2 \times S^2$. On a déjà montrer qu'il existe $s \in s_1 R \cap s_2 R$ que l'on peut donc écrire $s = s_1 u = s_2 v$ pour $u, v \in R$.
On a alors $(r_1, s_1 R) = (r_1 u, sR)$ et $(r_2, s_2 R) = (r_2 v, sR)$. On en déduit immédiatement que $(r_1, s_1) + (r_2, s_2) = (r_1 u + r_2 v, sR)$.
On a également montré que $s_1 R \cap r_2 S \neq \varnothing$ donc il existe $(u', v') \in R \times S$ tel que $s_1 u' = r_2 v'$.
On a alors $s_2 v' \subset r_2^{-1}(s_1 R \cap r_2 R)$. Par ailleurs $r_1 \circ r_2(s_2 v') = r_1(s_1 u') = r_1 u'$.
Ainsi $(r_1, s_1)(r_2, s_2) = (r_1 u', s_2 v')$. □

Corollaire B.11. — *Soit R un anneau et S une partie multiplicative de R tels que (R, S) vérifie la condition de Ore à droite. $R \hookrightarrow R_S$ est un morphisme universellement S-inversible.*

Preuve. Soit $\varphi : R \to A$ un morphisme S-inversible. Montrons qu'il existe un unique morphisme $\overline{\varphi} : R_S \to A$ prolongeant φ.
L'unicité est évidente : si un tel $\overline{\varphi}$ existe alors pour tout $r, s \in R \times S$, $\overline{\varphi}(rs^{-1}) = \overline{\varphi}(r)\overline{\varphi}(s)^{-1} = \varphi(r)\varphi(s)^{-1}$. Il faut voir qu'un morphisme donné par cette formule est bien défini et définit bien un morphisme.
Supposons donc $r_1 s_1^{-1} = r_2 s_2^{-1}$. Alors il existe $s := s_1 u = s_2 v \in S$ tels que $r_1 u = r_2 v$. On remarque $\varphi(u)$ et $\varphi(v)$ sont inversibles dans A.

On a

$$\begin{aligned}
&\varphi(r_1)\varphi(s_1)^{-1} = \varphi(r_2)\varphi(s_2)^{-1} \\
\iff &\varphi(r_1) = \varphi(r_2)\varphi(s_2)^{-1}\varphi(s_1) \\
\iff &\varphi(r_1)\varphi(u) = \varphi(r_2)\varphi(s_2)^{-1}\varphi(s_1)\varphi(u) \\
\iff &\varphi(r_1 u) = \varphi(r_2)\varphi(s_2)^{-1}\varphi(s_2)\varphi(v),
\end{aligned}$$

et cette dernière égalité est une conséquence de $r_1 u = r_2 v$.

Une telle application est donc bien définie. On ne suppose désormais plus que $r_1 s_1 = r_2 s_2$. Il existe $s = s_1 u = s_2 v$. On peut alors écrire $r_1 s_1^{-1} = r_1 u (s_1 u)^{-1}$ et $r_2 s_2^{-1} = r_2 v (s_2 v)^{-1}$. Alors

$$\begin{aligned}
\overline{\varphi}(r_1 s_1^{-1} + r_2 s_2^{-1}) &= \overline{\varphi}((r_1 u + r_2 v) s^{-1}) \\
&= (\varphi(r_1 u) + \varphi(r_2 v))\varphi(s)^{-1}
\end{aligned}$$

D'autre part,

$$\begin{aligned}
\overline{\varphi}(r_1 s_1^{-1}) + \overline{\varphi}(r_2 s_2^{-1}) &= \varphi(r_1)\varphi(s_1)^{-1} + \varphi(r_2)\varphi(s_2)^{-1} \\
&= \varphi(r_1 u)\varphi(s)^{-1} + \varphi(r_2 v)\varphi(s)^{-1} \\
&= (\varphi(r_1 u) + \varphi(r_2 v))\varphi(s).
\end{aligned}$$

Montrons enfin que $\overline{\varphi}$ est multiplicative. Soit $r_1, r_2, s_1, s_2 \in R^2 \times S^2$. Il existe $(u', v') \in R \times S$ tel que $s_1 u' = r_2 v'$. On a alors

$$\begin{aligned}
\overline{\varphi}(r_1 s_1^{-1})\overline{\varphi}(r_2 s_2^{-1}) &= \varphi(r_1)\varphi(s_1)^{-1}\varphi(r_2)\varphi(s_2)^{-1} \\
&= \varphi(r_1)\varphi(s_1)^{-1}\varphi(r_2)\varphi(v)\varphi(v)^{-1}\varphi(s_2)^{-1} \\
&= \varphi(r_1)\varphi(s_1)^{-1}\varphi(s_1)\varphi(u)\varphi(s_2 v)^{-1} \\
&= \varphi(r_1 u)\varphi(s_2 v)^{-1} \\
&= \overline{\varphi}(r_1 s_1^{-1} r_2 s_2^{-1}).
\end{aligned}$$

□

Corollaire B.12. — *Un anneau de quotient à droite par S est uniquement défini à unique R-isomorphisme près (i.e., un isomorphisme préservant R).*

Preuve. Soit R un anneau et S une partie multiplicative de R de sorte que (R, S) vérifie la condition de Ore à droite. Soit A_S un anneau de quotient à droite par S.
On a un morphisme injectif $\varphi : R \to A_S$ rendant tous les éléments de S inversibles. Par le corollaire précédent on sait qu'il existe un unique morphisme $\overline{\varphi} : R_S \to A_S$ prolongeant φ. De plus comme tous les éléments de A_S peuvent s'écrire sous la forme rs^{-1}, $\overline{\varphi}$ est surjectif.
Il est de plus injectif car $\overline{\varphi}(rs^{-1}) = 0 \iff rs^{-1} = 0 \in A_S \iff r = 0 \in A_S \iff r = 0 \in R \iff rs^{-1} = 0 \in R_S$.
Ainsi $R_S \simeq A_S$.

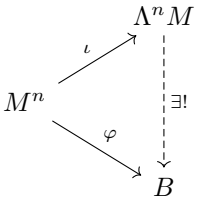
□

Remarque B.13. — *S'il existe des anneaux de quotients à droite et une condition de Ore à droite, on se doute qu'il en existe des analogues à gauche. Plutôt que de refaire ses constructions nous nous contentons de dire qu'elles se ramènent à celles-ci par le foncteur $A \mapsto A^{op}$.*
Par ailleurs on voit que si un couple (R, S) vérifie les conditions de Ore à gauche et à droite, alors ses anneaux de quotients par S à gauche et à droite sont isomorphes, et que cet isomorphisme est de plus unique si on suppose qu'il conserve R.

C Produit extérieur et connexion

Dans cette annexe nous présentons les propriétés de base du produit extérieur et son lien avec les connexions sur un module différentiel.

Définition C.1. — *Soit R un anneau commutatif et M un R-module. La n-ième puissance extérieure de M est un couple $(\Lambda^n M, \iota)$ où $\Lambda^n M$ est un R-module et $\iota : M^n \to \Lambda^n M$ est une application R-multilinéaire alternée vérifiant la propriété universelle suivante : pour toute application R-multilinéaire alternée $\varphi : M^n \to B$, où B est un R-module, il existe une unique application R-linéaire faisant commuter le diagramme suivant :*



Proposition C.2. — *Pour tout R-module M, $\Lambda^n M$ existe.*

Preuve. On considère $\Lambda^n M = {}^{M^{\otimes n}}/_F$ où F est le sous-espace vectoriel engendré par $\{x_1 \otimes ... \otimes x_n | \exists i \in [\![1; n-1]\!], x_i = x_{i+1}\}$. □

Proposition C.3. — *Soit R un anneau commutatif, R_1 une R algèbre commutative et M un R_1-module. $\Lambda^n_{R_1} M \simeq {}^{\Lambda^n_R M}/_{F'}$ où F' est le sous-espace vectoriel engendré par $\{\lambda x_1 \wedge ... \wedge x_n - x_1 \wedge ...x_{i-1} \wedge \lambda x_i \wedge x_{i+1} \wedge ...x_n | \lambda \in R_1\}$.*

Preuve. On vérifie que le R-module défini ci-dessus est en fait muni d'une structure de R_1-module bien définie, et qu'il vérifie de plus la même propriété universelle que $\Lambda^n_{R_1} M$. □

Proposition C.4. — *Soient R un anneau différentiel, et (M, ∂_M) un R-module différentiel. ∂_M induit une connexion $\partial_{\Lambda^n M}$ sur $\Lambda^n M$.*

Preuve. On note R_c le sous-anneau des constantes de R. On a une application R_c-multilinéaire alternée

$$\begin{array}{rccc} \partial_{\Lambda^n M} : & M^n & \to & \Lambda^n_R M \\ & (x_1, ..., x_n) & \mapsto & \sum_{i=1}^n x_1 \wedge ...x_{i-1} \wedge \partial_M(x_i) \wedge x_{i+1} \wedge ...x_n \end{array} .$$

Cette application induit donc une application $\partial_{\Lambda^n M} : \Lambda^n_{R_c} M \to \Lambda^n_R M$.
Il suffit de voir que cette application est nulle sur F' (avec les notations de la proposition précédente). On constate que c'est le cas, ce qui achève la démonstration. □

D Produit tensoriel d'algèbres et isomorphisme utile

LEMME D.1. — *Soit R un anneau commutatif, $n \in \mathbb{N}$ et $A_1, \dots, A_n, B_1, \dots, B_n$ des R-modules. Toute égalité entre des applications R-multilinéaires de source $\prod_{i=1}^n A_i \otimes_R B_i$ peut se tester sur les tenseurs purs.*

Preuve. On va procéder par récurrence sur n. On sait que c'est vrai au rang 1. Supposons $\varphi, \psi : \prod_{i=1}^n A_i \otimes_R B_i \to X$ R-multilinéaires et coïncidant sur les tenseurs purs.
On peut alors définir des applications R-$(n-1)$linéaires pour tout $x \in A_1 \otimes B_1$:

$$\begin{array}{rccc} \varphi_x : & \prod_{i=2}^n A_i \otimes_R B_i & \to & X \\ & (x_2, ..., x_n) & \mapsto & \varphi(x, x_2, ..., x_n) \end{array}$$

et

$$\begin{array}{rccc} \psi_x : & \prod_{i=2}^n A_i \otimes_R B_i & \to & X \\ & (x_2, ..., x_n) & \mapsto & \psi(x, x_2, ..., x_n) \end{array} .$$

Lorsque x est un tenseur pur, φ_x et ψ_x coïncident sur les tenseurs purs par hypothèse, donc elles sont égales par hypothèse de récurrence. Mais alors les applications R-linéaires :

$$\begin{array}{rccc} \Phi : & A_1 \otimes B_1 & \to & \mathrm{Bil}(\prod_{i=2}^n A_i \otimes_R B_i, X) \\ & x & \mapsto & \varphi_x \end{array}$$

et

$$\begin{array}{rccc} \Psi : & A \otimes B & \to & \mathrm{Bil}(\prod_{i=2}^n A_i \otimes_R B_i, X) \\ & x & \mapsto & \psi_x \end{array}$$

coïncident sur les tenseurs purs et donc sont égales. Ainsi $\varphi = \psi$. □

PROPOSITION D.2. — *Soit R un anneau commutatif, A et B deux R-algèbres. Le produit tensoriel $A \otimes_R B$ est munie d'une structure de R-algèbre vérifiant sur les tenseurs purs :*

$$a_1 \otimes b_1 \cdot a_2 \otimes b_2 = a_1 a_2 \otimes b_1 b_2$$

Preuve. Soit $(a, b) \in A \times B$. On note $i : A \times B \to A \otimes B$ l'application R-bilinéaire canonique. On a une application R-bilinéaire

$$\begin{array}{rccc} \varphi_{a,b} : & A \times B & \to & A \otimes B \\ & (x, y) & \mapsto & i(xa, yb) \end{array}$$

et par la propriété universelle du produit tensorielle on en déduit $\varphi_{a,b} : A \otimes B \to A \otimes B$. Alors l'application :

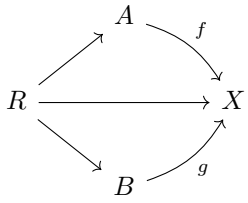
$$\begin{array}{rccc} \Phi : & A \times B & \to & \mathrm{End}_{R\text{-}\mathbf{mod}}(A \otimes B) \\ & (a, b) & \mapsto & \varphi_{a,b} \end{array}$$

est R-bilinéaire. En effet pour tout $(x, y) \in A \times B$ on a $\varphi_{ra+a',b}(x, y) = ri(xa, yb) + i(xa', yb) = (r\varphi_{a,b} + \varphi_{a',b})(x, y)$ car R est dans le centre de A, et cette égalité passe donc sur les applications induites sur $A \otimes B$. De la même façon, Φ est R-linéaire en la seconde variable. On en déduit donc $\Phi : A \otimes B \to \mathrm{End}_{R\text{-}\mathbf{mod}}(A \otimes B)$.

On peut donc définir la loi de composition suivante sur $A \otimes B$: pour tout $(x, y) \in (A \otimes B)^2$, $x \cdot y = \Phi(y)(x)$. On constate sans problème que cette loi est distributive sur l'addition, par construction.
Montrons que cette loi est associative. Les applications $(x, y, z) \in (A \otimes_R B)^3 \mapsto x.(y.z) \in A \otimes_R B$ et $(x, y, z) \in (A \otimes_R B)^3 \mapsto (x.y).z \in A \otimes_R B$ sont R-multilinéaires. Leur égalité se teste donc sur les tenseurs purs, où le résultat est évident. De plus $1_A \otimes 1_B$ est évidemment un neutre à droite, et on vérifie facilement que c'est un neutre à gauche. En effet cela revient à dire que l'application R-linéaire $y \mapsto 1_A \otimes 1_B \cdot y$ est l'identité, ce qui se vérifie sur les tenseurs purs. □

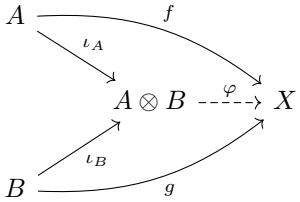
On donne à présent la propriété universelle du produit tensoriel de R-algèbre dans la catégorie des anneaux. Pour démontrer le résultat final, et principal de cette annexe, nous ne pouvons pas nous contenter de sa propriété universelle dans la catégorie des R-algèbres.

Proposition D.3. — *Soit X un anneau muni d'un morphisme $R \to X$ (lui donnant une structure de R-module) et $f : A \to X$ et $g : B \to X$ tels que pour tout $(a, b) \in A \times B$, $f(a)g(b) - g(b)f(a) = 0$ et de sorte que le diagramme suivant commute :*



Remarque D.4. — *Dit autrement, f et g induisent des applications R-linéaires.*

Il existe un unique morphisme $\varphi : A \otimes_R B \to X$ faisant commuter le diagramme suivant :



De plus toute application $A \otimes_R B \to X$ provient d'un tel diagramme.

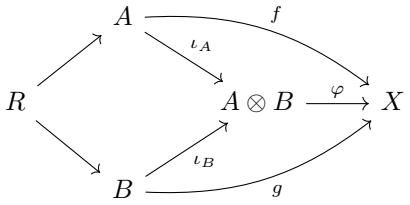
Preuve. L'application $\varphi : A \otimes_R B \to X$ est engendré par l'application R-bilinéaire de $A \times B \to X$ qui envoie tout (a, b) sur $f(a)g(b)$. Il s'agit bien d'une application R-bilinéaire par l'hypothèse de commutation de f et g. Il reste à voir qu'il s'agit bien d'un morphisme d'anneaux. Cela revient à voir que les applications R-bilinéaires $(x, y) \mapsto \varphi(xy)$ et $(x, y) \mapsto \varphi(x)\varphi(y)$ coïncident ce qui se vérifie sur les tenseurs purs. Voyons tout de même avant cela que ces applications sont bien R-bilinéaires. Cela est évident pour la première. Pour la seconde on veut voir que pour tout r $\varphi(x)\varphi(ry) = r\varphi(x)\varphi(y)$.
Cela revient à montrer que $\varphi(x)r.\varphi(y) = r\varphi(x)\varphi(y)$. Mais comme f et g induisent des morphismes de R-modules, cela peut se réécrire $\varphi(x)\varphi(r) = \varphi(r)\varphi(x)$. Cette égalité se teste sur les tenseurs purs :

$$\varphi(a \otimes b)\varphi(r) = f(a)g(b)f(r) = f(a)g(r)g(b) = \varphi(r)\varphi(a \otimes b).$$

La bilinéarité étant établie, montrons l'égalité des deux applications.

$$\begin{aligned}
\varphi((a_1 \otimes b_1)(a_2 \otimes b_2)) &= \varphi(a_1a_2 \otimes b_1b_2) \\
&= f(a_1a_2)g(b_1b_2) \\
&= f(a_1)f(a_2)g(b_1)g(b_2) \\
&= f(a_1)g(b_1)f(a_2)g(b_2) \text{ par hypothèse} \\
&= \varphi(a_1 \otimes b_1)\varphi(a_2 \otimes b_2).
\end{aligned}$$

Pour finir on voit que si un morphisme d'anneaux $\varphi : A \otimes_R B \to X$ existe alors il induit un diagramme commutatif :



et alors pour tout $(a, b) \in A \times B$ on a

$$\begin{aligned}
\varphi(a \otimes b) &= \varphi(a \otimes 1_B)\varphi(1_A \otimes b) \\
&= f(a)g(b) \\
&= \varphi(1_A \otimes b)\varphi(a \otimes 1_B) \\
&= g(b)f(a)
\end{aligned}$$

□

THÉORÈME D.5. — *Soit R un anneau commutatif, A et R_1 deux R-algèbres commutatives, B et C deux R_1-algèbres, non nécessairement commutative. Alors*

$$A \otimes_R (B \otimes_{R_1} C) \simeq (A \otimes_R B) \otimes_{A \otimes_R R_1} (A \otimes_R C)$$

Preuve. On commence par voir que $(A \otimes_R B) \otimes_{A \otimes_R R_1} (A \otimes_R C)$ possède bien une structure de $A \otimes_R R_1$-algèbres, ie que $A \otimes_R B$ et $A \otimes_R C$ en possède une. Soit $a, r_1 \in A \times R_1$. On peut définir une application R-bilinéaire :

$$\begin{array}{rccc} f_{a,r_1} : & A \times B & \to & A \otimes_R B \\ & (a', b) & \mapsto & (aa' \otimes r_1 b) \end{array}$$

On en déduit $f_{a,r_1} : A \otimes_R B \to A \otimes_R B$. De plus $(a, r_1) \mapsto f_{a,r_1}$ est également R-bilinéaire. On en déduit la structure de $A \otimes_R R_1$-module sur $A \otimes_R B$ et donc $f : A \otimes_R R_1 \to A \otimes_R B$ un morphisme d'anneaux.
Il suffit alors de montrer que les deux applications

$$\begin{array}{rcl} (A \otimes_R R_1) \times (A \otimes_R B) & \to & A \otimes_R B \\ (x, y) & \mapsto & f(x).y \end{array}$$

et

$$\begin{array}{rcl} (A \otimes_R R_1) \times (A \otimes_R B) & \to & A \otimes_R B \\ (x, y) & \mapsto & y.f(x) \end{array}$$

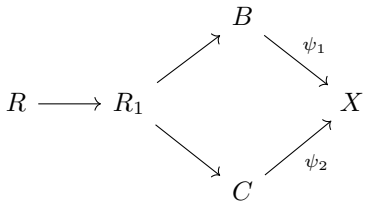
sont égales. Cela peut se vérifier directement sur les tenseurs purs.
On démontre de la même façon que $A \otimes_R C$ possède une structure de $A \otimes_R C$-algèbre.

On va montrer que le membre de gauche vérifie la même propriété universelle que le membre de droite.
On commence par donner $\iota_1 : A \to (A \otimes_R B) \otimes_{A \otimes_R R_1} (A \otimes_R C)$ induit par le morphisme $A \to A \otimes_R B$, $a \mapsto a \otimes 1_B$.
On a par ailleurs

$$\begin{array}{rccccc} \iota_2 & : B \times C & \to & (A \otimes_R B) \times (A \otimes_R C) & \to & (A \otimes_R B) \otimes_{A \otimes_R R_1} (A \otimes_R C) \\ & (b, c) & \mapsto & (1_A \otimes b), (1_A \otimes c)) & & \end{array}$$

dont on vérifie qu'il est R_1 linéaire et induit $\iota_2 : B \otimes_{R_1} C \to (A \otimes_R B) \otimes_{A \otimes_R R_1} (A \otimes_R C)$.

Soit maintenant X un anneau muni d'un morphisme $R \to X$ et $\varphi : A \to X$, ainsi que $\psi : B \otimes_{R_1} C \to X$ deux morphismes d'anneaux induisant autant de morphismes de R-modules, tels que $\varphi(a)\psi(x) = \psi(x)\varphi(a)$ pour tout a et x ayant du sens.
La structure de R_1 algèbre sur $B \otimes_{R_1} C$ induit $R_1 \to B \otimes_{R_1} C \xrightarrow{\psi} X$ et muni X d'une structure de R_1-module pour laquelle ψ est par construction un morphisme de R_1-modules.
Ils proviennent donc par ce qui précède de $\psi_1 : B \to X$ et $\psi_2 : C \to X$ morphismes d'anneaux R_1-linéaires vérifiant $\psi_1(b)\psi_2(c) = \psi_2(c)\psi_1(b)$ pour tout b et c ayant du sens. La structure de R_1-module ayant été fabriquée pour, on voit que la condition induire un morphisme de R_1-modules n'est autre qu'induire un morphisme de R-modules et coïncider sur R_1. Autrement dit, le diagramme suivant est commutatif dans la catégorie des anneaux.



Il vient alors naturellement que $\varphi(a)\psi_1(b) = \psi_1(b)\varphi(a)$ et $\varphi(a)\psi_2(c) = \psi_2(c)\varphi(a)$ pour tout a, b, c.
On en déduit $\Phi_1 : A \otimes_R B \to X$ et $\Phi_2 : A \otimes_R C \to X$ dont on vérifie que $\Phi_1(x)\Phi_2(y) = \Phi_2(y)\Phi_1(x)$

pour tout x et y ayant du sens.
Il reste à voir que ces morphismes d'anneaux sont $A \otimes_R R_1$ linéaires. X est muni d'une structure de A-module via φ. La structure de $A \otimes_R R_1$-module sur X est donc donnée par :

$$R_1 \to B \Rightarrow A \otimes_R R_1 \to A \otimes_R B \xrightarrow{\Phi_1} X.$$

La $A \otimes_R R_1$ linéarité devient alors évidente par la commutativité du diagramme précédent. On en déduit donc l'existence d'une bonne application. L'unicité se vérifie sur les tenseurs purs. □

Références

[BCG+17] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy et Éric Schost : *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (auto-édit.), Palaiseau, septembre 2017. URL https://hal.archives-ouvertes.fr/AECF/. 686 pages. Imprimé par CreateSpace. Aussi disponible en version électronique.

[BCS14] Alin Bostan, Xavier Caruso et Éric Schost : A fast algorithm for computing the characteristic polynomial of the p-curvature. *In ISSAC 2014—Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, pages 59–66. ACM, New York, 2014. doi :10.1145/2608628.2608650.

[BCWDV16] Moulay Barkatou, Thomas Cluzeau, Jacques-Arthur Weil et Lucia Di Vizio : Computing the Lie algebra of the differential Galois group of a linear differential system. *In Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 63–70. ACM, New York, 2016. doi :10.1145/2930889.2930932.

[Bre14] Matej Brešar : *Introduction to noncommutative algebra*. Universitext. Springer, Cham, 2014. doi :10.1007/978-3-319-08693-4.

[CGH14] Edgar Costa, Robert Gerbicz et David Harvey : A search for Wilson primes. *Math. Comp.*, 83(290) :3071–3091, 2014. doi :10.1090/S0025-5718-2014-02800-7.

[Clu03] Thomas Cluzeau : Factorization of differential systems in characteristic p. *In Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 58–65. ACM, New York, 2003. doi :10.1145/860854.860875.

[Har14] David Harvey : Counting points on hyperelliptic curves in average polynomial time. *Ann. of Math. (2)*, 179(2) :783–803, 2014. doi :10.4007/annals.2014.179.2.7.

[Kat82] Nicholas M. Katz : A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2) :203–239, 1982. URL http://www.numdam.org/item?id=BSMF_1982__110__203_0.

[Lam01] Tist-Yuen Lam : *A First Course in Noncommutative Rings*, volume 131 de *Graduate Texts in Mathematics*. Springer-Verlag New York, 2001. doi :10.1007/978-1-4419-8616-0.

[vdPS03] Marius van der Put et Michael F. Singer : *Galois theory of linear differential equations*, volume 328 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003. doi :10.1007/978-3-642-55750-7.