Factoring differential operators in positive characteristic.

Raphaël Pagès

université de BORDEAUX

THÈSE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR DE

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE MATHÉMATIQUES ET INFORMATIQUE

SPÉCIALITÉ MATHÉMATIQUES PURES

Par Raphaël Pagès

Factorisation des opérateurs différentiels en caractéristique positive

Sous la direction de : Alin BOSTAN et Xavier CARUSO

Soutenue le 21/02/2024

Membres du jury :

Mme Elena BERARDINI, Chaire de professeure junior, CNRS et Université de Bordeaux (Talence), Examinatrice
M. Alin BOSTAN, Directeur de Recherche, INRIA Saclay Île-de-France (Palaiseau), ***Directeur de thèse***
Mme Irene BOUW, Professeure des universités, Ulm Universität (Ulm), Examinatrice
M. Xavier CARUSO, Directeur de Recherche, CNRS et Université de Bordeaux (Talence), ***Directeur de thèse***
Mme Charlotte HARDOUIN, Maîtresse de conférences, Université Paul Sabatier (Toulouse), Examinatrice
M. Mark VAN HOEIJ, Professeur des universités, Florida State University (Tallahassee, États-Unis), Rapporteur
M. Julien ROQUES, Professeur des universités, Université Claude Bernard (Lyon 1) (Villeurbanne), Examinateur
M. Bernard LE STUM, Maître de conférences, Université de Rennes 1 (Rennes), Rapporteur

Titre : Factorisation des opérateurs différentiels linéaires en caractéristique positive

Résumé : L'étude des opérateurs différentiels linéaires est une partie importante de l'étude algébrique des équations différentielles. Les anneaux d'opérateurs différentiels linéaires partagent de nombreuses propriétés avec les anneaux de polynômes, mais le caractère non commutatif de la multiplication rend la conception d'algorithmes de factorisation plus compliquée. L'objet de cette thèse est le développement d'un algorithme calculant un facteur droit irréductible d'un opérateur différentiel linéaire donné dont les coefficients sont des éléments d'un corps de fonctions algébriques de caractéristique p. La situation diffère grandement du problème analogue en caractéristique 0 car les corps de fonctions algébriques de caractéristique positive sont de dimension finie sur leur corps des constantes. De ceci découle une structure additionnelle d'algèbre d'Azumaya qui fournit des outils supplémentaires pour attaquer le problème de la factorisation.

Une première étape est le calcul de la p-courbure, un invariant classique de première importance des opérateurs différentiels en caractéristique p. Le premier résultat significatif de cette thèse est un algorithme calculant, pour un opérateur différentiel L en caractéristique 0 et un entier $N \in \mathbb{N}$ donnés, tous les polynômes caractéristiques des p-courbures des réductions de L modulo p, pour tous les nombres premiers $p \leqslant N$.

La deuxième partie de la thèse est consacrée à la factorisation en elle-même. Nous utilisons la structure d'algèbre d'Azumaya pour montrer que la recherche de facteurs irréductibles à droite revient à la résolution de l'équation de p-Riccati

$$f^{(p-1)} + f^p = a^p$$

dans K[a], où a est une certaine fonction algébrique sur K. Cette observation nous permet de développer deux algorithmes importants. Le premier est une application du principe global-local conduisant à un test d'irréductibilité de complexité polynomiale pour les opérateurs différentiels. Le second est un algorithme de résolution de l'équation de p-Riccati utilisant plusieurs outils de la géométrie algébriques pour les courbes, dont les espaces de Riemann-Roch et les groupes de Picard. Nous effectuons une analyse de complexité approfondie de cet algorithme et montrons que l'équation de p-Riccati admet toujours une solution dont la taille est comparable à celle du paramètre a. Cet algorithme rend en particulier possible la factorisation des opérateurs centraux (un cas qui a souvent été laissée de côté par le passé) et diminue la taille des facteurs droits irréductibles d'opérateurs différentiels linéaires d'un facteur p en comparaison des travaux précédents. On en déduit finalement un algorithme de factorisation complet pour les opérateurs différentiels linéaires de caractéristique positive.

Mots clés : Opérateurs différentiels, Algèbre d'Azymaya, Courbes algébriques,

Calcul formel, Caractéristique p

Title :Factorisation of linear differential operators in positive characteristic

Abstract : The study of linear differential operators is an important part of the algebraic study of differential equations. Rings of linear differential operators share many properties with rings of polynomials, but the noncommutative aspect of the multiplication makes the design of factorisation algorithms harder. This thesis focuses mainly on developing an algorithm computing an irreducible right factor of a given linear differential operator with coefficients in an algebraic function field of positive characteristic p. The situation differs greatly from the same problem in characteristic 0 because algebraic function fields of characteristic p are finite dimensional over their field of constants. This simple fact provides the ring of differential operators in characteristic p with an additional structure of Azumaya algebra, which gives additional tools to attack our problem. A first step in this direction is the computation of the p-curvature, a classical invariant of primary importance attached to differential operations in characteristic p. The first important result of this thesis is an algorithm computing, for a given operator L in characteristic 0 and an integer N , all the characteristic polynomials of the p-curvatures of its reduction modulo p, for all primes $p \leqslant N$. The second part of the thesis is dedicated to the factorisation itself. We use the Azumaya algebra structure to show that finding irreducible right irreducible factors reduces to solving the p-Riccati equationc
$f^{ (p-1) }+ f^p = a^p$
in K[a], where a is a suitable algebraic function over K. This observation leads to two important algorithms. The first one is an application of the global-local principle which eventually provides a polynomial time irreducibility test for differential operators. The second one is an actual resolution algorithm for the p-Riccati equation that uses tools of algebraic geometry for curves such as Riemann-Roch spaces and Picard group. We perform a complexity analysis of this algorithm, and show that the p-Riccati equation always admits a solution whose size is comparable to that of the parameter a. As a byproduct, this algorithm makes the factorisation of central operators possible (a situation which was often left aside) and lower the size of right factors of general operators by a factor p compared to previous works. We finally deduce a full factorisation algorithm for differential operators of positive characteristic.

Keywords : Differential operators, Azumaya algebras, Symbolic computation, Algebraic curves, Positive characteristic

Institut de Mathématiques de Bordeaux

351 cours de la Libération, 33405 Talence CEDEX

Remerciements

Un grand nombre de personnes ont joué un rôle important pendant ces années de doctorat dont ce manuscrit est l'aboutissement. Je les ici remercie de leur soutien et de leurs apports sans lesquels ce travail n'aurait pas vu le jour. Je veux tout d'abord remercier mes directeurs de thèse, Alin Bostan et Xavier Caruso. J'ai rencontré Alin en 2019 alors que je suivais encore son cours de calcul formel à Paris. C'est grâce à ses conseils que je contactai à l'époque Xavier dans le but d'effectuer mon mémoire, puis ma thèse sous leur direction conjointe. Xavier et Alin me fournirent un sujet particulièrement intéressant et leur aide fut précieuse durant les quatre années où j'ai travaillé sous leur direction.

Je remercie également messieurs Bernard Le Stum et Mark van Hoeij, mes rapporteurs, pour avoir accepté de relire mon travail et l'avoir apprécié. Leur aide et leur travail minutieux m'ont permis d'améliorer ce manuscrit, je l'espère, à la hauteur de leur attentes.

Il me faut bien sûr également remercier Elena Berardini, Irene Bouw, Charlotte Hardouin et Julien Roques pour avoir accepté de faire partie de mon jury. Je dois en outre remercier Elena pour son aide concernant la théorie des espaces de Riemann-Roch.

J'ai été accueilli au sein de l'université de Bordeaux dans l'équipe CANARI dont je remercie tous les membres pour leur aide. Je tiens également à remercier chaleureusement tous les membres de l'équipe MATHEXP au centre INRIA de Saclay dont j'ai été membre toutes ces années, quoique à distance. Je remercie particulièrement Frédéric Chyzak ainsi que Marc Mezzarobba pour les discussions enrichissantes que nous avons eues, ainsi que Alexandre Goyer qui a effectué sa thèse sur un sujet analogue au mien en caractéristique nulle au sein de cette équipe et avec lequel j'ai pu à plusieurs reprises discuter de nos avancées respectives dans nos recherches.

Je remercie Martin Weimann de m'avoir accueilli pour le séminaire de théorie des nombres au LMNO ainsi que tous les membres de l'équipe de théorie des nombres. Les conversations que j'ai pu y avoir ont été particulièrement enrichissantes. Les indications de Martin sur les factorisations-OM ont été d'une aide précieuse pour évaluer la complexité du test d'irréductibilité présenté dans ce manuscrit. Par ailleurs, mon entretien avec Martin et Denis Simon ont révélé des pistes de preuves très intéressantes pour l'Heuristique 3.4.31.

Mes années de doctorat ont également été pour moi des années d'enseignement, au sens littéral puisque j'ai par quatre fois dispensé des cours et TD de mathématiques à de jeunes étudiants. À ce titre je remercie les équipes pédagogiques avec lesquelles j'ai travaillé, en particulier Éric Balandraud qui fut toujours de très bonne conversation. Je remercie également tous mes étudiants et étudiantes et leur souhaite une très bonne continuation, quoiqu'ils et elles décident de faire par la suite.

Il me faut également citer mes camarades doctorant, ceux dont je partageais le couloir, voire le bureau, au sein de l'IMB et qui ont été de très bonne compagnie au cours de ces années. Je remercie tout particulièrement mes compagnons de manifestation, Gabrielle et Martin.

Je remercie mes professeurs et professeures, de mathématiques comme d'autres choses. Je remercie particulièrement M. Trotabas, dont les conseils et le soutien furent très importants pour moi.

Si les années de doctorat furent des années enrichissantes à n'en point douter, des années de découvertes assurément, elles ne furent en revanche pas des années reposantes. C'est pourquoi il me faut remercier mes proches pour leur soutien indéfectible. Mes parents, en premier lieu, qui ont toujours été là pour moi et sur lesquels j'ai toujours pu compter. Mes adelphes ensuite, Antonin, Clément et Sarah. Je vous aime très fort et vous souhaite le meilleur. Mes ami·e·s enfin. Merci à Laura et Steven, merci à Loën et merci à Aloÿs, Simon et Hélène, d'avoir été à mes côtés quand j'en avais besoin. Vous comptez beaucoup pour moi.

Contents

Résumé étendu de la thèse

Les équations différentielles sont depuis longtemps un objet d'étude privilégié des mathématiciens puisqu'elles apparaissent dans de nombreux domaines des sciences physiques, en particulier dans le cas où la variable est réelle ou complexe. L'étude de ces équations peut prendre différentes formes et mobilise une grande variété d'outils différents. Il existe également un pendant plus algébrique de l'étude des équations différentielles, qui peut inclure une plus grande variété d'objets, dont des anneaux p-adiques ou de caractéristique positive. Dans cette autre configuration, une dérivation $u \mapsto u'$ sur un anneau $\mathcal{A}$ est définie comme un morphisme additif vérifiant la règle de Leibniz : pour tout $u, v \in \mathcal{A}$,

$$(uv)' = u'v + uv'.$$

Un anneau commutatif muni d'une dérivation est appelé un anneau différentiel.

Dans ce cadre, il est possible de considérer des équations différentielles p-adiques ou en caractéristique positive, lesquelles ont trouvé de nombreuses applications, par exemple au comptage des points [Lau04], au calcul d'isogénies [LV16, Eid21] ou, de manière plus générale, à l'étude de la cohomologie des variétés arithmétiques.

Une sous-classe d'équations différentielles intéressantes sont les équations homogènes linéaires, de la forme

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$$

où $n \in \mathbb{N}^*$ et les a_i sont des fonctions de la variable x, tandis que $y^{(i)}$ désigne la i-ème dérivée de la fonction y. Dans le contexte algébrique que nous mentionnions plus tôt, ces équations peuvent elles-mêmes être représentées par les éléments d'un certain anneau, quoique non commutatif, appelé anneau d'opérateurs différentiels. Nous définissons un opérateur différentiel comme étant une combinaison linéaire formelle

$$a_n \partial^n + a_{n-1} \partial^{n-1} + \cdots + a_1 \partial + a_0$$

où les a_i sont des éléments d'un anneau différentiel $\mathcal{A}$. Si $a_n \neq 0$, on dit que cet opérateur est d'ordre n. La multiplication dans ces anneaux vérifie la règle de commutation suivante, déduite de la règle de Leibniz :

$$\partial u = u\partial + u'$$

pour tout $u \in \mathcal{A}$. Par la suite on notera $\mathcal{A}\langle\partial\rangle$ l'anneau des opérateurs différentiels linéaires à coefficients dans $\mathcal{A}$.

Comme les opérateurs différentiels peuvent être multipliés entre eux, une question naturelle est celle de la factorisation : étant donné un opérateur différentiel L, est-on capable de l'écrire comme produit de deux opérateurs plus petits? Cette question n'est pas intéressante simplement

pour notre curiosité, mais également car elle est très liée aux solutions de l'équation $L(y) = 0$. En effet, si R est un facteur à droite de L, alors l'espace des solutions de $R(y) = 0$ est un sous-espace vectoriel de l'espace des solutions de $L(y) = 0$.
Cette question a déjà suscité la curiosité d'un certain nombre de mathématiciens qui se sont plus souvent intéressé au cas des opérateurs à coefficients dans $\mathbb{Q}(x)$ ou $\mathbb{C}(x)$ pour lesquels plusieurs algorithmes ont été proposés [Gri90, Van97, vdH07a, CGM22].

Dans ce manuscrit, nous noterons K un corps de fonctions algébriques de caractéristique positive p, c'est-à-dire une extension séparable du corps des fonctions rationnelles $\mathbb{F}_p(x)$. Nous noterons également ∂ la dérivation $\frac{d}{dx}$ sur K. Le but de cette thèse est d'étudier la factorisation des opérateurs différentiels linéaires dans $K\langle\partial\rangle$ et de présenter un algorithme complet de factorisation. Bien que les deux problèmes soient similaires, les outils utilisés en caractéristique positive et en caractéristique nulle diffèrent grandement. L'origine en est la différence de « taille » du corps des constantes dans les deux situations. En effet, les seules fonctions de dérivée nulle sur $\mathbb{C}(x)$ sont les fonctions constantes, identifiables à $\mathbb{C}$ sur lequel le corps $\mathbb{C}(x)$ est transcendant. En revanche, dans K, toutes les puissances p-ièmes ont une dérivée nulle. Il s'ensuit que K est de dimension finie p sur son corps des constantes, noté ici C.

Cette différence fondamentale a de nombreuses conséquences sur la structure de l'anneau des opérateurs différentiels en caractéristique p ; de manière générale, on démontre que c'est une algèbre libre de dimension finie sur son centre. Ainsi, la résolution rationnelle des équations différentielles se ramène simplement à la résolution d'un système linéaire de taille $p \times p$ et les solutions rationnelles peuvent être de « taille » arbitrairement grande. Ces deux faits ont des conséquences importantes pour la factorisation des opérateurs différentiels linéaires en caractéristique p.

Le premier chapitre de cette thèse est dédié à l'étude d'un invariant classique de première importance des opérateurs différentiels linéaires en caractéristique positive : la p-courbure. Cette application linéaire associée à chaque opérateur différentiel possède de nombreuses propriétés très importantes. Parmi elles, Cartier a démontré que la dimension du noyau de la p-courbure de L était la même que la dimension de l'espace des solutions polynomiales (resp. rationnelles, resp. algébriques) sur le corps des constantes. La p-courbure est par ailleurs intimement liée à la conjecture de Grothendieck-Katz qui stipule qu'un opérateur différentiel en caractéristique nulle possède une base de solutions algébriques si, et seulement si, presque toutes ses réductions modulo p ont une base de solutions rationnelles.

La p-courbure joue également un rôle très important dans la factorisation des opérateurs différentiels en caractéristique p ; en témoignent les travaux de van der Put [vdP95, vdP96, vdP97] et de Cluzeau sur le sujet [Clu03]. Cela est dû au lien entre p-courbure et opérateurs centraux. En effet, on peut démontrer que le centre de $K\langle\partial\rangle$ est $C[\partial^p]$. En outre, tout opérateur $L \in K\langle\partial\rangle$ admet des multiples centraux non triviaux. Puisque le centre de $K\langle\partial\rangle$ n'est rien d'autre qu'un anneaux de polynômes (bivariés), des algorithmes de factorisation performants existent dans ce contexte [BLS+04, Lec06, Lec10, Wei15]. Deux questions se posent alors :

- Comment calculer un multiple central de L ?
- Peut-on utiliser les factorisations polynomiales des multiples centraux de L pour en déduire des informations sur L ?

Dans la suite de ce manuscrit, nous noterons $\mathcal{D}_L$ le $K\langle\partial\rangle$-module à gauche ${}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$. La

p-courbure de L, que nous noterons désormais ψ_p^L, est définie comme l'application K-linéaire

$$\begin{array}{rccc} \psi_p^L : & \mathcal{D}_L & \to & \mathcal{D}_L \\ & M & \mapsto & \partial^p M \end{array}.$$

Il est possible de montrer qu'il existe une certaine K-base de $\mathcal{D}_L$ dans laquelle la matrice de ψ_p^L est à coefficients constants (c'est-à-dire dans C). Il suit que ses invariants de Frobenius, et en particulier son polynôme minimal et son polynôme caractéristique, sont à coefficients constants. Il est alors relativement aisé de démontrer que tout multiple central de L est un multiple du polynôme minimal de ψ_p^L appliqué à ∂^p, ce qui répond à notre première question. En lien avec la seconde question, nous démontrerons dans le chapitre 2 le résultat suivant, qui est un raffinement d'un résultat déjà connu sur les décompositions isotypiques. La notation gcrd désigne le plus grand diviseur commun à droite d'une famille d'opérateurs.

Théorème. — *Soit $L \in \mathcal{A}\langle\partial\rangle$. Supposons que $\chi(\psi_p^L) = N_1 \cdots N_n$, où les N_i sont des polynômes irréductibles sur C, pas nécessairement deux à deux distincts. Alors il existe une factorisation $L = L_1 \cdots L_m$ vérifiant :*

i) Pour tout $i \in [\![1; m]\!]$ il existe $j \in [\![1; n]\!]$ tel que L_i soit un diviseur de $N_j(\partial^p)$.

ii) $L_m = \mathrm{gcrd}(L, N_n(\partial^p))$.

Un théorème similaire dans le cadre des polynômes tordus sur les corps finis a été publié par Caruso et Le Borgne dans [CLB17]. Il est à noter que les facteurs de cette première décomposition ne sont pas irréductibles en général. Ce théorème nous permettra dans le chapitre suivant, consacré pleinement à la factorisation, de nous limiter au cas où L est un diviseur d'un certain $N(\partial^p)$ pour N un polynôme irréductible sur C.

Le chapitre 2 se poursuit avec la description d'un algorithme efficace de calcul de p-courbures. Plus précisément, l'algorithme présenté calcule, pour un opérateur L en caractéristique 0 et un entier N donnés, tous les polynômes caractéristiques des p-courbures des réductions modulo p de L, pour tout nombre premier $p \leqslant N$. Cet algorithme repose sur une combinaison d'idées publiées dans [BCS14] et [Har14] : nous commençons par ramener le calcul du polynôme caractéristique de la p-courbure à celui d'une factorielle de matrices, sur laquelle on peut alors appliquer des méthodes de calcul de type « pas de bébé / pas de géant ». Plus précisément, nous nous servons des propriétés d'algèbre d'Azumaya de l'anneau des opérateurs différentiels et des polynômes tordus. L'idée principale est d'expliciter une correspondance entre les deux anneaux de polynômes de Ore et de montrer la compatibilité de cette correspondance avec le calcul du polynôme caractéristique des p-courbures. C'est au moment de démontrer cette compatibilité que la structure susmentionnée intervient. Grâce à cela, nous ramenons le calcul à celui d'une factorielle d'une matrice de la forme

$$B(\theta)B(\theta+1)\cdots B(\theta+p-1) \mod p, \theta^d$$

pour tout p et un certain d. Nous réutilisons alors les idées de [Har14] qui résout un problème similaire. Nous obtenons ainsi le résultat suivant.

Théorème. — *Soit A un anneau de caractéristique 0, $L \in A[x]\langle\partial\rangle$ et $N \in \mathbb{N}$. Il existe un algorithme calculant les polynômes caractéristiques des p-courbures de L mod p pour tout nombre premier $p \leqslant N$ en un nombre d'opérations arithmétiques dans A linéaire en N et polynomial en l'ordre et le degré des coefficients de L.*

Le chapitre 3 est consacré à la factorisation des opérateurs différentiels en tant que telle. Nous avons montré précédemment que nous pouvions nous restreindre à la factorisation d'un opérateur $L \in K\langle\partial\rangle$ divisant un opérateur de la forme $N(\partial^p)$ où $N \in C[Y]$ est irréductible. Il est important d'observer qu'un tel opérateur n'est pas nécessairement irréductible. Par exemple pour tout nombre premier p, ∂^2 divise ∂^p (c'est-à-dire le cas où $N = Y$) mais n'est jamais irréductible.

Les diviseurs de L sont très étroitement liés à la structure du module quotient $\mathcal{D}_L$. En effet, on peut démontrer qu'il existe une bijection entre les diviseurs à droite de L et les sous-modules de $\mathcal{D}_L$. Or il se trouve maintenant que $N(\partial^p)$ étant central, le quotient $\mathcal{D}_{N(\partial^p)}$ a une structure d'anneau et que $\mathcal{D}_L$ a une structure de $\mathcal{D}_{N(\partial^p)}$-module à gauche. Or puisque N est irréductible et que $K\langle\partial\rangle$ a une structure d'algèbre d'Azumaya, il suit que $\mathcal{D}_{N(\partial^p)}$ est une algèbre simple centrale de dimension p^2 sur son centre ${}^{C[\partial^p]}/_{N(\partial^p)}$. En vertu du théorème d'Artin-Wedderburn ainsi que d'une analyse dimensionnelle, il suit que $\mathcal{D}_{N(\partial^p)}$ est soit une algèbre à division, soit isomorphe à $M_p(C_N)$ avec $C_N = {}^{C[Y]}/_{N(Y)}$. Dans le premier cas, l'on constate que $N(\partial^p)$ est nécessairement irréductible ; ainsi $L = N(\partial^p)$ l'est également.

Intéressons-nous donc au second cas. Notons dès à présent y_N l'image de Y dans C_N et $K_N = K[y_N]$. $\mathcal{D}_L$ peut donc être vu comme un $M_p(C_N)$-module à gauche. Le théorème de Morita ([AF92, Corollary 22.6]) nous permet de ramener notre problème à de l'algèbre linéaire sur C_N, à condition de savoir trouver un facteur irréductible de $N(\partial^p)$. Pour ce faire, nous nous ramenons au cas où N est de degré 1 par l'isomorphisme de C_N-algèbres suivant :

$$\begin{array}{rccl} \varphi_N : & \mathcal{D}_{N(\partial^p)} & \mapsto & {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)} \\ & Q & \mapsto & Q \mod \partial^p - y_N \end{array}$$

Cet isomorphisme nous permet de déduire des facteurs irréductibles de $N(\partial^p)$ de ceux de $\partial^p - y_N$. On démontre que ces derniers sont de la forme $\partial - f$ où $f \in K_N$ vérifie l'équation

$$f^{(p-1)} + f^p = y_N$$

que nous appelons *équation de p-Riccati* relative à N. La résolution de cette équation est fondamentale à l'écriture d'un algorithme complet de factorisation. L'existence ou non de solutions à cette équation est équivalente à l'irréductibilité de $N(\partial^p)$. Soient $L, R \in K\langle\partial\rangle$ tels que $LR = N(\partial^p)$.

DÉFINITION. — Pour tout $g \in K_N$, on pose

$$\mathcal{L}_g := \mathrm{lclm}(\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - g)), R) \cdot R^{-1}$$

où la notation lclm désigne le plus petit multiple commun à gauche d'une famille d'opérateurs.

THÉORÈME. — *Soit $S_N \subset K_N$ l'ensemble des solutions de l'équation de p-Riccati relative à N appartenant à K_N.*

1. *Si $L = N(\partial^p)$ alors $g \mapsto \mathcal{L}_g$ est une bijection de S_N dans l'ensemble des diviseurs irréductibles de $N(\partial^p)$.*
2. *En général, tous les diviseurs à droite irréductibles de L sont de la forme $\mathcal{L}_g$ avec $g \in \mathcal{S}_N$.*
3. *Pour tout $g \in \mathcal{S}_N$, il existe $\{i_1, ..., i_k\} \subset [\![0; p-1]\!]$ avec $k = \frac{\mathrm{ord}(L)}{\deg(N)}$ tels que*

$$L = \mathrm{lclm}\left(\mathcal{L}_{g+\frac{i_1}{x}}, \mathcal{L}_{g+\frac{i_2}{x}}, \ldots, \mathcal{L}_{g+\frac{i_k}{x}}\right).$$

Nous consacrons une grande partie de la suite du chapitre 3 à la résolution de l'équation de p-Riccati. Nous commençons par un bref écart par la résolution d'équations de p-Riccati pour les séries de Laurent. Grâce à un algorithme de type itération de Newton nous démontrons le résultat suivant.

Théorème. — *Il existe $\eta_1, \eta_2 \in \mathbb{Z}$ ne dépendant que de g et $a \in \mathbb{F}_q((t))$ tels que l'équation*

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p$$

admette une solution dans $\mathbb{F}_q((t))$ si et seulement si il existe $(f_{\eta_1}, f_{\eta_1+1}, \ldots, f_{\eta_2}) \in \mathbb{F}_q^{\eta_2-\eta_1+1}$ tel que $f := \sum_{k=\eta_1}^{\eta_2} f_k t^k$ vérifie

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p + O(t^{p(\eta_2+1)}).$$

Nous utilisons ensuite ce résultat pour mettre au point un test d'irréductibilité de $N(\partial^p)$. Cet algorithme utilise le principe local-global qui indique qu'une algèbre simple centrale sur un corps de fonctions ne peut-être déployée qu'à condition que ses complétions en toutes les places du corps de fonctions le soient. Les complétions de K_N étant toutes des corps de séries de Laurent, cela nous amène à vérifier l'existence de solutions à des équations de p-Riccati du type précédent. On montre que l'existence de ces solutions est immédiate pour presque toutes les places de K_N sauf un nombre fini d'entre elles pour lesquelles on peut appliquer le théorème précédent. Ceci nous conduit au résultat suivant.

Théorème. — *Soit $N \in C[Y]$ un polynôme irréductible et $N_* \in K[Y]$ tel que $N_*^p(Y) = N(Y^p)$. Il existe un algorithme terminant en temps polynomial en la taille de N_*, prenant N_* en entrée et testant si $N(\partial^p)$ est irréductible.*

Enfin, à l'aide de ce test d'irréductibilité et d'outils de la géométrie algébrique sur les courbes (espaces de Riemann-Roch et groupe de classe de diviseur), nous pouvons résoudre l'équation de p-Riccati sur K_N. Notre résultat final est le suivant :

Théorème. — *Soit $N \in C[Y]$ un polynôme irréductible et $N_* \in K[Y]$ tel que $N_*^p(Y) = N(Y^p)$.*

- *Il existe une solution à l'équation de p-Riccati relative à N de taille polynomiale en la taille de N_* et un algorithme prenant N_* en entrée et retournant une telle solution en temps linéaire en p et polynomial en la taille de N_*.*
- *$N(\partial^p)$ a des facteurs irréductibles de taille polynomiale en la taille de N_*. Il existe un algorithme prenant N_* en entrée et retournant un tel facteur en temps linéaire en p et polynomial en la taille de N_*.*

Soit $L \in K\langle\partial\rangle$ un opérateur différentiel linéaire d'ordre r.

- *L a des facteurs irréductibles de taille linéaire en p et polynomiale en r et en la taille des coefficients de L. Il existe un algorithme prenant L en entrée et retournant un tel facteur en temps linéaire en p^2 et polynomial en r et en la taille des coefficients de L.*

Chapter 1

Introduction

Differential equations have been an object of study for mathematicians for a long time as they naturally appear in several domains of physical science, especially in the case where x is a real or complex variable. The study of those equations can take many different forms and mobilise a variety of different tools, among which the numerical approximation of solutions or the qualitative analysis of the (solutions of) autonomous equations.
However, there also exists a more algebraic side to the study of differential equations which encompasses more general functions, among which we find functions of a p-adic variable or functions defined in positive characteristic. In this new setting a derivation $u \mapsto u'$ over a ring $\mathcal{A}$ is defined as an additive map verifying the Leibniz rule: for any $u, v \in \mathcal{A}$,

$$(uv)' = u'v + uv'.$$

Any commutative ring $\mathcal{A}$ provided with a derivation is called a differential ring.

This setting allows for considering differential equations on a wider variety of objects, including p-adic differential equations as already mentioned. The latter find numerous applications, *e.g.* to count points on elliptic curves [Lau04], to compute isogenies [LV16, Eid21] and, more generally, to study (the cohomology of) many algebraic varieties.

An interesting subclass of differential equations are homogeneous linear differential equations of the form

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$$

where $n \in \mathbb{N}^*$ and the a_i are (known) functions of a variable x while $y^{(i)}$ denotes the i-th derivative of the function y of x. In the aforementioned algebraic setting, those equations can themselves be represented as elements of a ring, albeit a noncommutative one, of differential operators. We define a linear differential operator as a formal linear combination

$$a_n \partial^n + a_{n-1} \partial^{n-1} + \cdots + a_1 \partial + a_0$$

where the a_i are elements of a differential field $\mathcal{A}$. If $a_n \neq 0$, we will say that this operator has order n. The multiplication of these operators is governed by the following commutation rule, stemming from the Leibniz rule:

$$\partial u = u\partial + u'$$

for $u \in \mathcal{A}$. We denote by $\mathcal{A}\langle\partial\rangle$ the ring of linear differential operators with coefficients in $\mathcal{A}$.
If linear differential operators can be multiplied, a natural question that arises is that of factorisation: given a linear differential operator L, can one find operators whose product is L? This

question is also quite closely related to that of solving differential equations: given a differential equation $L(y) = 0$ where L is a linear differential operator, then if R is a right factor of L, the vector space of solutions of $R(y) = 0$ is a subspace of the space of solutions of $L(y) = 0$.

The question of the factorisation of differential operators has already been studied in the past by several mathematicians. For the specific case of operators with coefficients in $\overline{\mathbb{Q}}(x)$ or $\mathbb{C}(x)$, several algorithms have been proposed, among which one can cite the work of D. Yu Grigoriev [Gri90], or that of Mark van Hoeij [Van97]. More recently, Frédéric Chyzak, Alexandre Goyer and Marc Mezzarobba have published an improved factorisation algorithm in the case of Fuchsian operators (operators whose solutions only have regular singularities) with a finite number of factorisations [CGM22]; this approach combines van Hoeij's local-to-global method with symbolic-numeric techniques suggested by Joris van der Hoeven [vdH07a, vdH07b]. Those algorithms usually rely on tools such as the monodromy group which do not have an obvious analogue in positive characteristic.
Interestingly, operators with a finite number of factorisations are also a case where factorisation is significantly easier in positive characteristic, although the tools used in both cases are radically different.

Throughout this manuscript, we denote by K an algebraic function field of characteristic p, that is to say, a separable field extension of the rational function field $\mathbb{F}_p(x)$. The goal of this thesis is to study the factorisation for differential operators in $K\langle\partial\rangle$, with coefficients in algebraic functions fields of positive characteristic, and to present a full factorisation algorithm. While the two problems are similar, the tools used in positive characteristic and characteristic 0 greatly differ. The main difference between differential algebra in characteristic 0 and characteristic p is the "size" of the ring of constants. Indeed, in the differential ring $\mathbb{C}(x)$ equipped with its usual derivation $\frac{\mathrm{d}}{\mathrm{d}x}$, the only elements with zero derivative are elements of $\mathbb{C}$, over which $\mathbb{C}(x)$ is transcendental. However over K, every p-th power has a zero derivative, given that

$$(f^p)' = pf'f^{p-1} = 0.$$

It follows that the field of constants is large; for example, if $K = \mathbb{F}_p(x)$, it is $\mathbb{F}_p(x^p)$, over which K has finite dimension p. In full generality, we denote by C the field of constants of K; its elements are the p-th powers of elements of K and, once again, $[K : C] = p$.
This difference has major implications. One of them is that any linear differential operator with coefficients in $\mathbb{F}_p(x)$ has central multiples which is never the case in characteristic zero. Another one is that, while the rational solutions of a linear differential equation in characteristic zero have always bounded degree, differential operators over $\mathbb{F}_p(x)$ have rational solutions of arbitrarily high degree as soon as they have rational solutions. Both of those facts have implications on the factorisation of linear differential operators.

An important part of this thesis will focus not only on the way to factor differential operators, but also on the cost of doing it. We of course want to be able to do it in the most efficient way possible, but we will take special interest in trying to estimate the size of the coefficients of the factors found.
Indeed, although it is not a focus of our work, a natural question about factorisation in positive characteristic is whether or not it can be applied to factorisation in characteristic zero. In the differential case, there are two main obstacles to a positive answer to this question. The first is the non-uniqueness of factorisations, even up to permutations. The second issue concerns the

size of the factors. It is actually directly related to the previous one because an infinite number of factorisations readily implies that we can find factors whose coefficients are arbitrarily big. In the perspective of finding modular algorithms to factor differential operators in characteristic zero, whether it is possible or not to find factors whose coefficients have degrees independent on the characteristic remains an open question. That is why we will pay special attention to point out where this dependence on p arises.

It should be mentioned finally that by "full factorisation algorithm", we do not mean an algorithm which will completely factorise a linear differential operator (although such an algorithm can easily be deduced from our work), but an algorithm which will return a right irreducible factor of any input linear differential operator, no matter its form.

Complexity basics We use the soft-O notation $\tilde{O}$ which indicates that polylogarithmic factors are not displayed. More precisely, if $\lambda, \mu : \mathbb{N} \to \mathbb{R}_+$ are increasing functions, saying that $\lambda(n) = \tilde{O}(\mu(n))$ means that there exists an integer $k \in \mathbb{N}$ such that $\lambda(n) = O(\mu(n)\log^k(\mu(n)))$. We will also locally use the notation O_ε. With the same notations, saying that $\lambda(n) = O_\varepsilon(\mu(n))$ means that for any $\varepsilon > 0$, $\lambda_n = O(\mu(n)^{1+\varepsilon})$.

We denote by $2 \leqslant \omega \leqslant 3$ a feasible exponent for matrix multiplication, that is, by definition, a real number for which we are given an algorithm that computes the product of two m-by-m matrices over a ring R for a cost of $O(m^\omega)$ operations in R. From [AVW21], we know that we can take $\omega < 2.3728596$. We shall also need estimates on the cost of computing characteristic polynomials. Let denote $\Omega \in \mathbb{R}_+^*$ such that the computation of the characteristic polynomial of a square matrix of size m with coefficients in a ring R can be done in $\tilde{O}(m^\Omega)$ arithmetic operations in R. From [KV05, Section 6], we know that it is theoretically possible to take $\Omega \simeq 2.697263$. Finally, we assume that any two polynomials of degree d over a ring R (resp. integers of bit size n) can be multiplied in $\tilde{O}(d)$ operations in R (resp. $\tilde{O}(n)$ bit operations); FFT-like algorithms allow for these complexities [CK91, HvdH21].

1.1 State of the art

Several mathematicians have already studied the problem of factorisation of differential operators. Below, we give an overview of the most significant work that has already been accomplished in that regard, focusing mostly on the case of positive characteristics.

The first significant work in this direction is due to Marius van der Put in an article from 1995 [vdP95] in which he established a classification of differential modules in positive characteristic. This is directly related to the problem of factorisation since the structure of the differential module ${}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$ reflects the factorisation properties of L. In particular, right divisors of L are in one-to-one correspondence with differential submodules of ${}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$. In his article, van der Put makes use of two specific properties of differential operators in characteristic p. The first one is that the ring of differential operators $K\langle\partial\rangle$ is a finite dimensional free algebra over its centre. A consequence of this is that any linear differential operator (resp. finite dimensional differential module) has a non zero central multiple (resp. central element of the annihilator). This first property allows to decompose differential modules as direct sums of submodules according to the factorisation of a central element of their annihilator. The next important tool is the Azumaya structure of the ring $K\langle\partial\rangle$. Indeed, it can be shown, and we will do it later, that for any maximal ideal $\mathfrak{m}$ of the centre $\mathcal{Z}$ of $K\langle\partial\rangle$, the quotient ring $K\langle\partial\rangle \otimes_{\mathcal{Z}} {}^{\mathcal{Z}}/_{\mathfrak{m}}$ is a

central simple algebra, meaning it is isomorphic to a matrix algebra over a division algebra (Artin-Wedderburn theorem [GS06, Thm. 2.1.3]). Combining this result with Morita's theorem (which establishes a categorical equivalence between vector spaces and modules over matrix rings [AF92, Corollary 22.6]), van der Put deduces an equivalence of categories between isotypical differential modules (that are, finite dimensional differential modules whose annihilator contains a central element with only one irreducible component) and vector spaces provided with a nilpotent endomorphism.

After these results, van der Put further investigated the question of factorisation and published in 1996 [vdP96] in which he explored the possibility of using his classification and Grothendieck-Katz conjecture [Kat82] in the perspective of factoring differential operators with coefficients in $\mathbb{Q}(x)$ using modular methods. Using factorisations in positive characteristic to recover factorisations of operators in characteristic zero is a natural idea as the same principle is used in many factorisation algorithms for polynomials (see for example [van02]). Unfortunately, in the case of differential operators the non-commutativity of the multiplication is the origin of a number of issues, the first one being that factorisations of a differential operator are generally not unique (even up to permutation) and actually not even finite in many cases; this makes recombination algorithms much harder to handle. In addition, lifting algorithms from factorisations modulo p to factorisations modulo p^2 (and higher powers of p) do not yet exist up to our knowledge.The final straw making general modular factorisations methods harder to design at the moment concerns the size of the factors. Indeed, if an operator $L \in \mathbb{Q}(x)\langle\partial\rangle$ had a nontrivial factorisation, it would generate nontrivial factorisations of $L \mod p$ for all but a finite number of p. In particular, one would expect the size of the factors to be independent of p. Unfortunately there are at the moment no known bounds on the size of the factors of an operator in $\mathbb{F}_p(x)\langle\partial\rangle$ which do not depend at least linearly on p. Nonetheless, van der Put presents in [vdP96] his ideas to recover factors of order 1 of an operator in $\mathbb{Q}(x)\langle\partial\rangle$ using modular methods.

Van der Put continued to work on that subject, as he wrote in 1997 a manuscript pursuing the goal of developing modular methods to factor differential operators with coefficients in $\mathbb{Q}(x)\langle\partial\rangle$ [vdP97]. In this article, van der Put describes a nearly complete algorithm to factor differential operators in positive characteristic, reusing the ideas he introduced two years before. The p-curvature, which was anecdotally referenced beforehand is now an explicit component of the algorithm and is used to efficiently compute a nice central multiple of the operator he wishes to factor and then compute an isotypical decomposition of it. To further continue the factorisation of the isotypical components, a dichotomy is made according to the form of the minimal polynomial of their p-curvature. The case where this minimal polynomial is an irreducible polynomial reduces to the case where it is simply $T - a^p$ after a suitable scalar extension. It then further reduces to the case $a = 0$, provided that one is able to solve the following equation, which we shall call the p-Riccati equation in this thesis:

$$f^{(p-1)} + f^p = a^p. \tag{1.1}$$

Here, the unknown is f and being able to solve this equation in finite separable extensions of $\mathbb{F}_p(x)$ (of which a is a primitive element) is vital for factorisation. This is actually not the first time this equation appeared in van der Put's work as it was already an important part of a discussion on the existence of skew field extension of dimension p^2 in [vdP95, section 1.5] and also showed up in [vdP96].

Before moving to the resolution of the p-Riccati equation, we mention that in his manuscript, van der Put also tackles the case where the minimal polynomial of the p-curvature has multiple roots, but while this case is important for lclm (least common left multiple) decompositions of operators, it can easily be avoided in the case of classical factorisation.
In his manuscript, van der Put presents an algorithmic way to solve the p-Riccati equation over $\overline{\mathbb{F}_p}(x)$. In general, he also shows that solutions can be found directly after a gcrd (greatest common right divisor) computation, with one notable exception: the case of central operators. However, in van der Put's perspective of designing modular algorithms for factorisation, the latter case is of little interest; indeed when considering an operator $L \in \mathbb{Q}(x)\langle\partial\rangle$ there are only a finite number of primes p (if any) such that $L \mod p$ is central and those can be ignored. Another issue, however, was that the size of the solution to the p-Riccati equation obtained by this method grows linearly with respect to p. Despite including methods to reduce the size of the factors obtained, van der Put stated in his manuscript that a precise complexity analysis and precise size bounds were seemingly impossible to obtain. The manuscript ultimately remained unpublished, though I was lucky enough to obtain a copy of it.

Since then, other mathematicians have been interested in the problem of factorisation of differential operators in positive characteristic, among which is Thomas Cluzeau. In a paper from 2003 [Clu03], he presented an algorithm inspired from van der Put's work, intended to factor differential systems. Factorisation in the context of differential systems can mean one of two things. Consider a system of the form $Y' = AY$ with $A \in M_n(\mathbb{F}_q(x))$. The basis change formula is given by $A \mapsto G^{-1}AG + G^{-1}G'$ where $G \in \mathrm{GL}_n(\mathbb{F}_q(x))$ is the matrix of the new basis and G' is the matrix obtained from G by differentiating each entry.
Factoring a differential system can mean finding a basis of $\mathbb{F}_q(x)^n$ such that the resulting system would be a diagonal block matrix. Such a decomposition is the analogue of lclm decompositions for differential operators. A second option, which corresponds to the classical factorisation of differential operators, is to find a basis where the system would be written as a triangular block matrix. The approach followed by Cluzeau is to diagonally reduce the system as much as possible (until each block is indecomposable), and then to triangularly reduce as much as possible the resulting blocks. The analogue decomposition for differential operators would be to write an operator as an lclm of indecomposable right factors and, in a second time, to write those factors as classical product of irreducible operators.
In order to achieve this goal, Cluzeau begins, as van der Put did, by computing an isotypical decomposition of his system by using the p-curvature. This step done, he attempts, if necessary, to complete the diagonalisation by repeating the same process (the one used with the p-curvature to compute the isotypical decomposition) with a random element of the eigenring of the system. The eigenring of the system can be seen as the ring of endomorphism of the system and exists for all differential systems, not just those of characteristic p. A most remarkable element however of the eigenring in positive characteristic is precisely the p-curvature. Cluzeau's idea is thus to apply to other randomly chosen elements of the eigenring the same algorithm as for the p-curvature and hopes that it yields a better decomposition. While this idea works well to compute lclm decompositions of operators with coefficients in $\mathbb{C}(x)$, later experiences have shown that it may not be as efficient in positive characteristic. This is probably due to the difference in nature of the constant fields in both cases. Indeed it can be shown that elements of the eigenring have a characteristic polynomial with constant coefficients. In characteristic zero, this means coefficients in $\mathbb{C}$ over which any polynomial is split, whereas in characteristic

p, the constant field of $\mathbb{F}_p(x)$ is $\mathbb{F}_p(x^p)$ which does not share this property (in fact a random polynomial over $\mathbb{F}_p(x^p)$ is most usually irreducible). Thus the probability that Cluzeau's idea works in practice is unfortunately too low for a realistic use.
However, it appears that Cluzeau was aware of this issue as in the same paper he proposed two ways of finishing the diagonalisation, should his method come to fail. The first one consists in falling back to van der Put's approach and solve the p-Riccati equation which, while more computationally expensive, will return the desired result provided that the system is of the right size (which corresponds to differential operators with no central divisor). His second proposal is similar to another work on factorisation published the same year by Mark Giesbrecht and Yang Zhang [GZ03] on the factorisation of Ore polynomials (of which differential operators are a specific case) over $\mathbb{F}_q(t)$, which we are going to discuss briefly now.
In [GZ03], the authors establish a direct connection between nontrivial factors of an Ore polynomial and nontrivial zero divisors in its eigenring. Giesbrecht and Zhang then use an algorithm to find nontrivial zero divisors in an algebra. It was shown later by José Gómez-Torrecillas, Francisco Javier Lobillo and Gabriel Navarro in an article from 2015 [GTLN15, GTLN19] that this algorithm could not be used in full generality. For example it does not work if the eigenring is a simple Artinian algebra which is the case when factoring central operators. The issue appears more generally when looking at the lclm of similar Ore polynomials (meaning that their quotient modules are isomorphic). In the specific case of differential operators, van der Put's way of solving the p-Riccati equation solves most of those cases, except the case of central operators which stayed unsolved to this day.

As a conclusion, we have partial significant results towards the factorisation of differential operators in positive characteristic but, in all cases, it appears that the case of central operators in not fully covered. One important goal of the present thesis is to fill this gap and provide a close study of factorisation of central operators, together with efficient algorithms and tight bounds on the size of the factors.

1.2 Chapter 2: Around the p-curvature and its computation

As we have seen previously, the p-curvature of a linear differential operator (or more generally of a differential module) is a vital tool in the algebraic study of linear differential equations in positive characteristic. Among the various properties of this linear map, Cartier proved that if L is a linear differential operator over $\mathbb{F}_p(x)$, the dimension of the kernel of the p-curvature of L agrees with the dimension of the space of rational (resp. algebraic) solutions of L over the field of constants.

REMARK. — It should be noted that unlike in characteristic 0, the field of constants of $\mathbb{F}_p(x)$ is strictly smaller than the field of constant of its separable closure. This is why the dimension over $\mathbb{F}_p(x^p)$ of the space of rational solutions of an operator $L \in \mathbb{F}_p(x)\langle\partial\rangle$ can be the same as the dimension of the space of its algebraic solutions, even though not all algebraic solutions are rational.

The p-curvature is also tightly linked to the Grothendieck-Katz conjecture which states that a differential operator L with coefficients in $\mathbb{Q}(x)$ has a basis of algebraic solutions if and only if its reductions modulo p have a basis rational solutions for all primes p, except a finite number of them. From what precedes, it follows that checking whether the reduction modulo p of L has a

basis of rational solutions is equivalent to checking whether the p-curvature of L vanishes or not. The p-curvature is also related to the arithmetic properties of D-finite functions in characteristic 0, as it was shown ([CC85], [And89, Chap.VI]) that the minimal-order vanishing operators of G-functions are globally nilpotent (meaning that the p-curvatures of their reduction modulo p are all nilpotent).

As already underlined earlier, the p-curvature also plays a very important role in the question of factorisation. Being a little more precise, we first notice that the centre of $K\langle\partial\rangle$ is exactly $C[\partial^p]$, which is an ordinary polynomial ring over an algebraic function field. An important ingredient in all aforementioned algorithms is to reduce the factorisation in $K\langle\partial\rangle$ to the factorisation in $C[\partial^p]$, which has been intensively studied for a long time. For making this strategy work, one needs to address the following two questions:

- How does one compute a central multiple of L?
- How does one use this central multiple to factor L?

Throughout this manuscript, if L is a linear differential operator in $\mathcal{A}\langle\partial\rangle$, where $\mathcal{A}$ is a differential field of positive characteristic, we will denote by $\mathcal{D}_L$ the left quotient module ${}^{\mathcal{A}\langle\partial\rangle}/_{\mathcal{A}\langle\partial\rangle L}$. For $L \in K\langle\partial\rangle$, the p-curvature of L, denoted in what follows by ψ_p^L, is defined as the K-linear map:

$$\begin{array}{rccc} \psi_p^L : & \mathcal{D}_L & \to & \mathcal{D}_L \\ & M & \mapsto & \partial^p M \end{array}.$$

We denote by $\chi(\psi_p^L)$ (resp. by $\chi_{min}(L)$) the characteristic polynomial (resp. the minimal polynomial) of the p-curvature of L. It can be shown that there exists a K-basis of $\mathcal{D}_L$ in which the matrix of ψ_p^L has constant coefficients. In particular, its minimal and characteristic polynomial have coefficients in C, as well as all its Frobenius invariants. Then, central multiple of L are all multiples of $\chi_{min}(L)(\partial^p)$. In particular, the latter is the central multiple of L of minimal order. This answers the first question.

Regarding the second question, we get the following theorem which extends van der Put and Cluzeau's approaches discussed earlier [vdP95, vdP97, Clu03].

Theorem 1.2.1 (see Theorem 2.2.11). — *Let $L \in \mathcal{A}\langle\partial\rangle$ and suppose that $\chi(\psi_p^L) = N_1 \cdots N_n$ with the N_i being irreducible polynomials in $\mathcal{C}[Y]$, not necessarily pairwise distinct. Then there exists a factorisation $L = L_1 \cdots L_m$ with:*

i) for any $i \in [\![1; m]\!]$ there exists $j \in [\![1; n]\!]$ such that L_i is a divisor of $N_j(\partial^p)$.

ii) $L_m = \mathrm{gcrd}(L, N_n(\partial^p))$.

A similar result in the context of Ore polynomials over finite fields was published by Caruso and Le Borgne in [CLB17]. The factors of the decomposition are still not irreducible in general; however, it is the best factorisation one can deduce from the factorisation of $\chi(\psi_p^L)$ or $\chi_{min}(L)$, or more generally of a central multiple of L.

We begin Chapter 2 by establishing some basic properties of linear differential operators. For a general commutative ring $\mathfrak{A}$ provided with a endomorphism $\theta : \mathfrak{A} \to \mathfrak{A}$ and a θ-derivation $\partial : \mathfrak{A} \to \mathfrak{A}$, we spend some time to give a complete proof of the existence and uniqueness of

the Ore polynomial ring $\mathfrak{A}[X, \theta, \partial]$, defined as the ring of polynomials in the variable X with coefficients in $\mathfrak{A}$ with multiplication given by the rule

$$X \cdot a = \theta(a)X + \partial(a)$$

for any $a \in \mathfrak{A}$. Rings of linear differential operators can be seen as a special case of Ore polynomial rings when $\theta = \mathrm{Id}_{\mathfrak{A}}$. Although a complete and rigorous construction of the ring $\mathfrak{A}[X, \theta, \partial]$ can be found in [BE23, §1.4, Proposition 7], we take the time to reestablish it. We then recall the basic properties of linear differential operators, among which the existence of an Euclidean division, of greatest common right divisor (which we will denote by gcrd) or of least common left multiple (which we will denote by lclm). We then move to the core of Chapter 2 which consists of two parts. Firstly, we relate the p-curvature to factorisation, by proving Theorem 1.2.1 already mentioned above. Secondly, we present an algorithm computing, for a given linear differential operator L with coefficients in a polynomial ring of characteristic zero $A[x]$ and an integer N, all the characteristic polynomials of the p-curvatures of the reductions modulo p of L, for all primes p smaller than N, in a number of operations in A quasilinear in N.

THEOREM 1.2.2. — *Let A be a ring of characteristic 0, $L \in A[x]\langle\partial\rangle$ and $N \in \mathbb{N}$. There exists an algorithm computing the characteristic polynomials of the p-curvatures of $L \bmod p$ for all primes $p \leqslant N$ in a number of operations in A polynomial in the order of L and the degrees of its coefficients, and quasilinear in N.*

This theorem is a generalisation of [Pag21, Theorem 3.13] which was set in the case where $A = \mathbb{Z}$. Since A is a ring of characteristic 0, operations in A can be of an arbitrarily high cost in bit operations, since the bit size of the objects cannot be bounded. When $A = \mathbb{Z}$, we have the following more precise statement.

THEOREM 1.2.3. — *Let $L \in \mathbb{Z}[x]\langle\partial\rangle$ and $N \in \mathbb{N}$. There exists an algorithm computing the characteristic polynomials of the p-curvatures of $L \bmod p$ for all primes $p \leqslant N$ in a number of bit operations polynomial in the order of L and the degrees of its coefficients, and quasilinear in N.*

We now briefly sketch the main ideas behind the previous result. Suppose that L is a monic operator with coefficients in $A_p(x)$ where A_p is an integral domain of characteristic p. One of the first algorithms to compute the p-curvature is due to Katz (and is sometimes referred to as Katz's algorithm [vdPS03, p. 324]). Let M be the companion matrix of L and r be the order of L. We define the recursive sequence of matrices $(M_i)_{i\in\mathbb{N}}$ by

$$M_1 = M \text{ and } M_{i+1} = M_i' + M \cdot M_i.$$

One shows that the matrix of ψ_p^L in the basis $(1, \partial, \ldots, \partial^{r-1})$ is given by M_p. This result is a consequence of the Leibniz rule. An easy complexity analysis shows that M_i has coefficients of degree $O(i)$. Using this recursive sequence to compute the p-curvature of L thus has a cost of $O(p^2)$ operations in A_p. However, since the characteristic polynomial of the p-curvature of L has coefficients in $A_p(x^p)$, it can be represented by $O(1)$ elements in A_p. While quasi-optimal (with respect to p) algorithms to compute the p-curvature exists [BCS15], the best known algorithm to compute its characteristic polynomial finishes in $\tilde{O}(\sqrt{p})$ operations in A_p [BCS14]. Whether or not the exponent $1/2$ is optimal is still an open question.

The algorithm we design is a combination of the ideas from [BCS14] and those from [Har14] for factorial computations. The fundamental theoretical input relies on an isomorphism between two rings of Ore polynomials: the rings of linear differential operators $A_p[x]\langle\partial\rangle$, on the one hand, and the ring $A_p[\theta][\Phi, \theta \mapsto \theta + 1, 0]$ of skew polynomials in Φ, on the other hand. This isomorphism is obtained by associating the variable θ to the Euler operator $x\partial$ and ∂ to Φ. Both Ore polynomial rings share similar properties: they are free algebras of dimension p^2 over their respective centres and, after localising with respect to ∂ and Φ respectively, both have a structure of Azumaya algebra.

Azumaya algebras are a generalisation of finite dimensional central simple algebras to the case where the centre is not a field. One way to think about them is to say that Azumaya algebras are locally isomorphic to central simple algebras for the Zariski topology. One important fact here is that Azumaya algebras are equipped with a reduced norm map, with is multiplicative and takes values in the centre. Following [BCS14], but giving alternative proofs, we relate it to the characteristic polynomials of the p-curvatures. This allows us to bring back the computation of the characteristic polynomial of the p-curvatures to that of a matrix factorial

$$B(\theta)B(\theta+1)\cdots B(\theta+p-1)$$

where B is a square matrix with coefficients in $A[\theta]$, easily deduced from L. After establishing the compatibility of this transformation with reductions modulo p, it only remains to efficiently compute

$$B(\theta)B(\theta+1)\cdots B(\theta+p-1) \mod p$$

for all primes $p \leqslant N$. Here we reuse the ideas of [Har14] in which the author presents an algorithm to compute similar matrix factorials.

1.3 Chapter 3: Factorisation and p-Riccati equation

Let $L \in K\langle\partial\rangle$. Thanks to Theorem 1.2.1, the problem of factoring L reduces to the case where L is a divisor of some $N(\partial^p)$ where $N \in C[Y]$ is an irreducible polynomial. Such operators are not necessarily irreducible. For example, $L = \partial^2$ is a divisor of ∂^p ($N = Y$) for all prime p and yet is never irreducible.

As mentioned before, right factors of L are closely related to the structure of the quotient $\mathcal{D}_L$, as there is a bijection between the monic right factors of L and submodules of $\mathcal{D}_L$. Besides, since L is supposed to be a divisor of $N(\partial^p)$, the space $\mathcal{D}_L$ has a structure of $\mathcal{D}_{N(\partial^p)}$-module ($\mathcal{D}_{N(\partial^p)}$ is indeed a ring since $N(\partial^p)$ is a central element). Since N is an irreducible polynomial over C, it follows from the Azumaya algebra structure of $K\langle\partial\rangle$ that $\mathcal{D}_{N(\partial^p)}$ is a central simple algebra of dimension p^2 over its centre. The Artin-Wedderburn theorem, along with some elementary dimension analysis, then implies that $\mathcal{D}_{N(\partial^p)}$ must either be isomorphic to a matrix algebra over its centre, which is $C[\partial^p]/N(\partial^p)$, or be a division algebra itself. In the latter case, $\mathcal{D}_{N(\partial^p)}$ has no nontrivial zero divisor, meaning that $N(\partial^p)$ has no nontrivial divisor in $K\langle\partial\rangle$. In such a situation, L is irreducible.

We now discuss the first case where $\mathcal{D}_{N(\partial^p)}$ is isomorphic to a matrix algebra. Let C_N denote the field extension $C[Y]/N(Y)$ and and y_N be the image of Y in C_N. We also write $K_N = K[y_N]$. Morita's theorem ([AF92, Corollary 22.6]) is an equivalence of categories which relates modules over matrix algebras (over a field) to vector spaces over the underlying field. We deduce from

this that the only irreducible factors of $N(\partial^p)$ are those whose order is exactly the degree of N. Even better, this frame of mind allows us to think of irreducible divisors of L as hyperplanes of some vector space and finding them reduces to an exercise of affine geometry. As $\mathcal{D}_L$ can also be seen as a submodule of $\mathcal{D}_{N(\partial^p)}$ we deduce moreover that irreducible factors of L can be recovered from irreducible factors of $N(\partial^p)$ by means of lclm computations which are the translation in terms of operators of computing intersections with hyperplanes of $\mathcal{D}_{N(\partial^p)}$.

Unfortunately, Morita's theorem does not provide an efficiently computable equivalence. It should also be noted that it is not even easy to determine whether or not $\mathcal{D}_{N(\partial^p)}$ is a division algebra. To tackle these issues, we first reduce the problem to the case where N is of degree 1. For this, we shall show that the map

$$\begin{array}{rccc} \varphi_N : & \mathcal{D}_{N(\partial^p)} & \mapsto & K_N\langle\partial\rangle/(\partial^p - y_N) \\ & Q & \mapsto & Q \mod \partial^p - y_N \end{array}$$

is an isomorphism of C_N-algebras. This isomorphism allows us to deduce irreducible factors of $N(\partial^p)$ from irreducible factors of $\partial^p - y_N$. The latter are operators of the form $\partial - f$ with $f \in K_N$ verifying

$$f^{(p-1)} + f^p = y_N.$$

We call this equation the *p-Riccati equation* relative to N and denote by S_N the set of solutions of this equation in K_N. From what precedes we can see that $\mathcal{D}_{N(\partial^p)}$ is a division algebra, *i.e.* that $N(\partial^p)$ is irreducible, if and only if $S_N = \varnothing$. The first important result of Chapter 3 allows to deduce an irreducible divisor of L from any element of S_N. Let L and R in $K\langle\partial\rangle$ be two operators such that $LR = N(\partial^p)$.

DEFINITION 1.3.1. — For any $g \in K_N$ we set

$$\mathcal{L}_g := \operatorname{lclm}(\operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - g)), R) \cdot R^{-1}.$$

THEOREM 1.3.2. — *1. If $L = N(\partial^p)$ then $g \mapsto \mathcal{L}_g$ is a bijection between $\mathcal{S}_N$ and the set of monic irreducible right divisors of $N(\partial^p)$.*

2. In general, all monic irreducible right divisors of L are of the form $\mathcal{L}_g$ with $g \in \mathcal{S}_N$.

3. For all $g \in \mathcal{S}_N$, there exists $\{i_1, ..., i_k\} \subset [\![0; p-1]\!]$ with $k = \frac{\operatorname{ord}(L)}{\deg(N)}$ such that

$$L = \operatorname{lclm}\left(\mathcal{L}_{g+\frac{i_1}{x}}, \mathcal{L}_{g+\frac{i_2}{x}}, \ldots, \mathcal{L}_{g+\frac{i_k}{x}}\right).$$

Before this thesis, the only available algorithm to solve the p-Riccati equation was given in [vdPS03, §13.2.1]; it is due to van der Put and Singer and works when K_N is a rational function field $\mathbb{F}_q(x)$. In the general case, van der Put used a method that allowed him to recover a solution to the p-Riccati equation from the gcrd of a non trivial factor and $\partial^p - y_N$. However, as already mentioned earlier, this method cannot be used to factorise central operators of which no nontrivial divisor is already known. Furthermore using this method generally yields a solution whose size is linear in p, which we would like to avoid.

A consequent part of Chapter 3 is dedicated to the resolution of the p-Riccati equation over algebraic function fields. We begin this study by a detour in the world of Laurent series where we consider more generally equations of the type

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p$$

which appears as a slight generalisation of p-Riccati equations. Here g and a are known functions in $\mathbb{F}_q((t))$, with g verifying some additional conditions. Using a Newton-type algorithm, we are able to show the following result.

Theorem 1.3.3. — *There exist $\eta_1, \eta_2 \in \mathbb{Z}$ depending uniquely on g and a such that the equation*

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p$$

has a solution in $\mathbb{F}_q((t))$ if and only if there exists $(f_{\eta_1}, f_{\eta_1+1}, \ldots, f_{\eta_2}) \in \mathbb{F}_q^{\eta_2-\eta_1+1}$ such that $f := \sum_{k=\eta_1}^{\eta_2} f_k t^k$ verifies

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p + O(t^{p(\eta_2+1)}).$$

After evaluating carefully the complexity of our Newton iteration algorithm, we use the previous theorem to design a polynomial time irreducibility test for $N(\partial^p)$. In order to explain this, we first need to introduce some notation. If K (resp. K_N) is an algebraic function field, we will denote by $\mathbb{P}_K$ (resp. $\mathbb{P}_{K_N}$) the set of places of K. We will often denote places of K by $\mathfrak{P}$, while $\nu_{\mathfrak{P}}$ will denote the associated valuation and $t_{\mathfrak{P}}$ a prime element of $\mathfrak{P}$. Over an algebraic function field, there is a local-global principle which states that a central simple algebra over K_N splits if and only if its completion in $\mathfrak{P}$ splits for every $\mathfrak{P} \in \mathbb{P}_{K_N}$. Since completions of algebraic function fields in their places are all Laurent series rings, this implies that $N(\partial^p)$ is reducible if and only if all of the p-Riccati equations

$$\left(t'_{\mathfrak{P}}\frac{\mathrm{d}}{\mathrm{d}t_{\mathfrak{P}}}\right)^{p-1}(f) + f^p = y_N$$

have a solution, where $t'_{\mathfrak{P}}$ is the derivative of $t_{\mathfrak{P}}$ as an element of K_N. Whether or not this equation has a solution can be checked by Theorem 1.3.3. Furthermore, we show that outside the poles of y_N and x, we always have $\eta_1 > \eta_2$ so that the condition of Theorem 1.3.3 is empty. Hence, only a finite number of places have to be checked, which can be easily achieved. This eventually leads to the following result.

Theorem 1.3.4. — *Let $N \in C[Y]$ be an irreducible polynomial and $N_* \in K[Y]$ such that $N_*^p(Y) = N(Y^p)$. There exists a polynomial time algorithm taking N_* as its input and determining whether or not $N(\partial^p)$ is irreducible.*

We then tackle the question of solving the p-Riccati equation over algebraic function fields. The main idea is basically the same as the rational resolution of Singer and van der Put in [vdPS03, §13.2.1]; it consists in finding *a priori* bounds on the denominator of one particular solution. They allow them to then deduce a bound on the degree of the numerator and to conclude using linear algebra, the p-Riccati equation being linear of $\mathbb{F}_p$.

Nevertheless, in the general case, new difficulties occur. The first one is that, contrarily to the case of $\mathbb{F}_q(x)$, it is not true in general that the p-Riccati equation admits a solution whose poles are contained within the poles of y_N. In order to get around this issue, we use tools from algebraic geometry on curves: Riemann-Roch spaces and divisor class group (or Picard group) of a curve and Jacobians. We begin our work by showing that although a random solution of the p-Riccati equation may have more poles than y_N, these "additional poles" can have large order.

We then show that it is possible to remove poles one by one by replacing a solution $f \in S_N$ with $f - \frac{g'}{g}$ for a suitable function g. However, this process has some limitation because the substitution $f \to f - \frac{g'}{g}$ may introduce new poles. Indeed, over a general function field, it is not possible to have a sharp control on all the zeroes and poles of a function. The object that measures this failure is called the divisor class group of K_N; it will be denoted by $\mathrm{Cl}(K_N)$ in what follows. Studying this object, we are able to construct a divisor A such that S_N is either empty or contains an element of the Riemann-Roch space associated to A. More precisely, if

- (g) denotes the principal divisor associated to a function g,
- D_- denotes the negative part of a divisor D,
- $\mathcal{L}(D)$ denotes the Riemann-Roch space associated to a divisor D, and
- $\mathrm{Diff}(K_N)$ denotes the different of K_N over K (viewed as a divisor on K_N),

we shall prove the following theorem.

THEOREM 1.3.5. — *We consider the finite commutative group $\mathfrak{G}_N^p = {}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$. Let $(D_1, \dots, D_n) \in \mathrm{Div}(K_N)^n$ be a lifting of a generating family of $\mathfrak{G}_N^p$ viewed as a $\mathbb{F}_p$-vector space. Let $S = \bigcup_{i=1}^n \mathrm{Supp}\, D_N$ and set*

$$A := \max\left(\sum_{\mathfrak{P}\in S} \mathfrak{P} + \mathrm{Diff}(K_N) - 2(x)_-, \frac{(y_N)_-}{p}\right).$$

If S_N is not empty then it contains an element of $\mathcal{L}(A)$.

We then use this theorem and the irreducibility test designed earlier (see Theorem 1.3.4) to compute a solution to the p-Riccati equation. Unfolding all the theoretical constructions, we finally end up with a complete factorisation algorithm, whose complexity is summarised in the following theorem.

THEOREM 1.3.6. — *Let $N \in C[Y]$ be an irreducible polynomial and $N_* \in K[Y]$ such that $N_*^p(Y) = N(Y^p)$.*

- *There exists a solution to the p-Riccati equation relative to N of size polynomial in the size of N_* and an algorithm taking N_* in input and outputting this solution in time linear in p and polynomial in the size of N_*.*
- *$N(\partial^p)$ has irreducible factors of size polynomial in the size of N_*. There exists an algorithm taking N_* in input and outputting such a factor in time linear in p and polynomial in the size of N_*.*

Let $L \in K\langle\partial\rangle$ be a differential operator of order r.

- *L has irreducible factors of size linear in p and polynomial in r and the size of the coefficients of L. There exists an algorithm taking L in input and outputting such a factor in time linear in p^2 and polynomial in r and the size of the coefficients of L.*

Chapter 2

Around the p-curvature and its computation

The goal of this chapter is to establish the importance of the p-curvature for differential operators of characteristic p. The applications we will mention concern the factorisation as a main part, but also the conjecture of Grothendieck-Katz. This conjecture motivates the ability to compute for a given operator in characteristic 0 the p-curvatures, or information on it, of its reductions modulo p.
In the first sections of this chapter we establish the basic properties of differential operators and of the p-curvature in positive characteristic. In particular we will show how the ring of differential operators in positive characteristic is an Azumaya algebra, which is a generalisation of central simple algebras to rings whose central elements do not constitute a field, and that the p-curvature is closely related to this structure. We also take time to establish the properties of the p-curvature which make it such a powerful tool in the setting of this thesis on the factorisation of differential operators. Finally, in the latter sections of this chapter we present an algorithm to compute, given a linear differential operator L in characteristic 0 and an integer N, all of the characteristic polynomials of its p-curvatures for all (save for a finite number depending solely on L and not on N) primes $p \leqslant N$. We discuss its complexity, implementations and timings.

2.1 Preliminaries

In this section we will lay down the basic properties of differential operators, of characteristic p and otherwise, from their very definition to the more specific aspects of central operators which will prompt the existence of the p-curvature.

2.1.1 Ore polynomial rings

To begin this document we first need to introduce the object of our study: the ring of differential operators. Differential operators are actually part of a larger class of noncommutative polynomials called Ore polynomials. Since it will be useful to us later, in particular in section 2.3, we take some time to introduce these "polynomials" and their basic properties in all of their generality. The first object we need to introduce are θ-derivations.

DEFINITION 2.1.1. — Let $\mathfrak{A}$ be a commutative ring and $\theta : \mathfrak{A} \to \mathfrak{A}$ be an endomorphism of $\mathfrak{A}$. A map $\partial : \mathfrak{A} \to \mathfrak{A}$ is called a θ- derivation of $\mathfrak{A}$ if and only if it is additive and for any a and $b \in \mathfrak{A}$,

$$\partial(ab) = \theta(a)\partial(b) + \partial(a)b.$$

REMARK 2.1.2. — Note that in the case where $\theta = \mathrm{Id}_{\mathfrak{A}}$, this rule is the usual Leibniz rule. This specific case is the setting when studying differential operators. In this case we will speak simply of derivation.

EXAMPLE 2.1.3. — i) The usual derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ defines a derivation on $A(x)$, where A is a field.

ii) If $\theta \neq \mathrm{Id}_{\mathfrak{A}}$, let $a \in \mathfrak{A}$ be such that $\theta(a) \neq a$. For any $f \in \mathfrak{A}$ there exists a unique θ-derivation such that $\partial_f(a) = f$. Furthermore, for any $g \in \mathfrak{A}$,

$$\partial_f(g) = f\frac{\theta(g) - g}{\theta(a) - a}.$$

In particular, the $\mathfrak{A}$-module of θ-derivations of $\mathfrak{A}$ is equal to $\mathfrak{A}(\theta - \mathrm{Id}_{\mathfrak{A}})$

Proof. i) This is a well known fact.

ii) We suppose that a derivation ∂_f exists. Then for any $g \in \mathfrak{A}$ we have

$$\begin{aligned}\partial_f(ag) &= \theta(a)\partial_f(g) + g\partial_f(a)\\ &= \theta(a)\partial_f(g) + gf.\end{aligned}$$

But also

$$\begin{aligned}\partial_f(ag) &= \theta(g)\partial_f(a) + a\partial_f(g)\\ &= \theta(g)f + a\partial_f(g).\end{aligned}$$

It follows that

$$\partial_f(g)(\theta(a) - a) = f(\theta(g) - g)$$

and finally

$$\partial_f(g) = f\frac{\theta(g) - g}{\theta(a) - a}.$$

It now suffices to show that ∂_f thus defined is indeed a θ-derivation. Let $g_1, g_2 \in \mathfrak{A}$.

$$\begin{aligned}\partial_f(g_1g_2) &= \frac{f}{\theta(a) - a}(\theta(g_1g_2) - g_1g_2)\\ &= \frac{f}{\theta(a) - a}(\theta(g_1)\theta(g_2) - \theta(g_1)g_2 + \theta(g_1)g_2 - g_1g_2)\\ &= \frac{f}{\theta(a) - a}(\theta(g_1)(\theta(g_2) - g_2) + (\theta(g_1) - g_1)g_2)\\ &= \theta(g_1)f\frac{\theta(g_2) - g_2}{\theta(a) - a} + g_2f\frac{\theta(g_1) - g_1}{\theta(a) - a}\\ &= \theta(g_1)\partial_f(g_2) + g_2\partial_f(g_1).\end{aligned}$$

□

Let now $\mathfrak{A}$ be fixed, as well as an endomorphism θ of $\mathfrak{A}$ and a θ-derivation ∂. We want to provide $\mathfrak{A}[X]$ with a ring structure compatible with its left-$\mathfrak{A}$-module structure verifying for any $a \in \mathfrak{A}$,

$$X \cdot a = \theta(a)X + \partial(a).$$

This peculiar commutation rule is motivated by the wish to make this ring structure act upon $\mathfrak{A}$ with the left multiplication by X being the θ-derivation ∂. For all $a \in \mathfrak{A}$ and all $b \in \mathfrak{A}$ we must then have

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

from which the commutation rule is deduced.

REMARK 2.1.4. — If $\partial = 0$ then instead of the multiplication by X being the map ∂, we want it to be the morphism θ. One can check that the commutation rule deduced then is the same.

We now show that this commutation rules uniquely defines a ring structure on $\mathfrak{A}[X]$, although a proof can be found in [BE23, §1.4 Proposition 7]. While it could be argued that the uniqueness of such a structure is obvious, part of its existence are highly nontrivial, such as the associativity of the multiplication law. One may be tempted to pass this ring structure as a representation of the subalgebra generated by ∂ of the ring of additive endomorphism of $\mathfrak{A}$, but this representation does not take into account the possible polynomials relations verified by ∂.

For example, over $\mathbb{F}_p[x]$, the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ verifies $\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^p = 0$ and yet we do not want X^p to be equal to 0.

Most of the time, texts about Ore polynomials are satisfied with just showing that for any a and $b \in \mathfrak{A}$,

$$(X \cdot a) \cdot b = X \cdot (ab)$$

and

$$X \cdot (a + b) = X \cdot a + X \cdot b.$$

As a matter of fact, it can be shown that given such a commutation rule on X and elements of $\mathfrak{A}$, the above verifications are all that is needed to define a unique ring structure on $\mathfrak{A}[X]$ verifying this commutation rule but it requires a bit of work.

DEFINITION 2.1.5. — Let $f : \mathfrak{A}[X] \to \mathfrak{A}[X]$ be a map. We say that f is a commutation rule on $\mathfrak{A}[X]$ if and only if:

i) f is additive.

ii) $f(1) = X$.

iii) For all $P \in \mathfrak{A}[X]$ and all $i \in \mathbb{N}$

$$f(PX^i) = f(P)X^i.$$

REMARK 2.1.6. — The commutation rule f represents the left multiplication of elements of $\mathfrak{A}[X]$ by X. Its structure is made so that if $f : \mathfrak{A} \to \mathfrak{A}[X]$ is an additive map mapping 1 to X, then there exists a unique commutation rule $\tilde{f}$ on $\mathfrak{A}[X]$ extending f. Indeed if such a commutation rule existed then for all $P = \sum_{k=0}^{n} a_k X^k$ we would have

$$\begin{aligned}\tilde{f}(P) &= \tilde{f}\left(\sum_{k=0}^{n} a_k X^k\right) \\ &= \sum_{k=0}^{n} \tilde{f}(a_k X^k) \\ &= \sum_{k=0}^{n} \tilde{f}(a_k) X^k \\ &= \sum_{k=0}^{n} f(a_k) X^k\end{aligned}$$

It is easy to check that $\tilde{f}$ thus defined is a commutation rule.

DEFINITION 2.1.7. — Let f be a commutation rule on $\mathfrak{A}[X]$. If for all $a, b \in \mathfrak{A}$,

$$f(a)(f)(b) = f(ab) \tag{2.1}$$

then we say that f is an associative commutation rule on $\mathfrak{A}[X]$.

REMARK 2.1.8. — We recall that for all $a \in \mathfrak{A}$, $f(a)$ is a polynomial with coefficient in $\mathfrak{A}$. It can thus be applied to f and yields $f(a)(f)$ an additive endomorphism of $\mathfrak{A}[X]$. Finally this endomorphism can be applied to any element $b \in \mathfrak{A}$ which is the meaning of $f(a)(f)(b)$. Since f is supposed to represent the left multiplication by X, the condition $f(a)(f)(b) = f(ab)$ corresponds to verifying that

$$(X \cdot a) \cdot b = X \cdot (ab).$$

THEOREM 2.1.9. — *Let f be an associative commutation rule on $\mathfrak{A}[X]$. There exists a unique composition law $\cdot$ on $\mathfrak{A}[X]$ verifying:*

$$\begin{gathered}\forall a \in \mathfrak{A},\ X \cdot a = f(a) \\ \forall (i,j) \in \mathbb{N}^2,\ X^i \cdot X^j = X^{i+j}\end{gathered}$$

and providing $\mathfrak{A}[X]$ with a ring structure compatible with its structure of $\mathfrak{A}$-module. We will denote this ring structure by $\mathfrak{A}[X; f]$.

Proof. Let $\cdot$ be such a composition law. Let $P = \sum_{k=0}^{n} a_k X^k$. By induction on n we show that for any P and $Q \in \mathfrak{A}[X]$ we must have

$$P \cdot Q = P(f)(Q).$$

This is obviously true for $n = 0$. Then suppose this property shown for some $n \in \mathbb{N}$ and let $P \in \mathfrak{A}$ of degree $n+1$. Then we can write $P = P_1 \cdot X + a$ for some $P_1 \in \mathfrak{A}[X]$ of degree at most

n and some $a \in \mathfrak{A}$. Then for any $Q = \sum_{i=0}^{m} b_i X^i$ we must have

$$\begin{aligned}
P \cdot Q &= (P_1 \cdot X + a) \cdot Q \\
&= (P_1 \cdot X) \cdot Q + a \cdot Q \\
&= P_1 \cdot (X \cdot Q) + a \cdot Q \\
&= P_1 \cdot f(Q) + aQ && \text{by additivity of } \cdot \\
&= P_1(f) \circ f(Q) + aQ && \text{by recurrence hypothesis} \\
&= (P_1 \cdot X)(f)(Q) + aQ && \text{since for all } i \in \mathbb{N}, X^i \cdot X = X^{i+1} \\
&= P(f)(Q) && \text{since } \cdot \text{ must be compatible with} \\
& && \text{the } \mathfrak{A}\text{-module structure of } \mathfrak{A}[X]
\end{aligned}$$

It remains to be seen that the composition defined by $P \cdot Q = P(f)(Q)$ provides $\mathfrak{A}[X]$ with a ring structure, that is to say that it is distributive on the addition and associative.

The fact that this composition law is distributive is easy to see. By definition, f is additive. Thus for all $P \in \mathfrak{A}$, $P(f)$ is also additive. It follows that $\cdot$ is distributive on the right. Since for all $P_1, P_2 \in \mathfrak{A}[X]$ we have $P_1(f) + P_2(f) = (P_1 + P_2)(f)$ it follows that $\cdot$ is also distributive on the left.

Let us now show that $\cdot$ is associative. We begin by showing by induction on i that for any $i \in \mathbb{N}$, any $a \in \mathfrak{A}$ and any $R \in \mathfrak{A}[X]$,

$$(X \cdot aX^i) \cdot R = X \cdot (aX^i \cdot R).$$

If $i = 0$ then for $R = bX^j$ with $b \in \mathfrak{A}$ and $j \in \mathbb{N}$ we have

$$\begin{aligned}
(X \cdot a) \cdot bX^j &= f(a) \cdot bX^j \\
&= f(a)(f)(b)X^j \\
&= f(ab)X^j \\
&= X \cdot (abX^j) \\
&= X \cdot (a \cdot bX^j)
\end{aligned}$$

Since $\cdot$ is distributive on the right, it follows that for any $R \in \mathfrak{A}[X]$ and any $a \in \mathfrak{A}$

$$(X \cdot a) \cdot R = X \cdot (aR).$$

Suppose that we have shown for some $i \geqslant 0$ that $(X \cdot aX^i) \cdot R = X \cdot (aX^i \cdot R)$ for any $a \in \mathfrak{A}$ and any $R \in \mathfrak{A}[X]$. Let $j \in \mathbb{N}$ and $b \in \mathfrak{A}$. Then

$$\begin{aligned}
X \cdot (aX^{i+1} \cdot bX^j) &= X \cdot (af^{i+1}(bX^j)) \text{ by definition of } \cdot \\
&= X \cdot (af^i(f(bX^j)) \\
&= X \cdot (aX^i \cdot (f(bX^j)) \\
&= (X \cdot aX^i) \cdot f(bX^j) \text{ by induction hypothesis} \\
&= (f(a) \circ f^i)(f(bX^j))) \text{ by definition of } \cdot \\
&= (f(a) \circ f^{i+1})(bX^j) \\
&= (X \cdot aX^{i+1}) \cdot bX^j
\end{aligned}$$

Now using the distributivity of $\cdot$ we show that for any $R \in \mathfrak{A}[X]$, $(X \cdot aX^{i+1}) \cdot R = X \cdot (aX^{i+1} \cdot R)$ and the recurrence is established.

Again by using the distributivity of $\cdot$ we show that for any Q and $R \in \mathfrak{A}[X]$, $(X \cdot Q) \cdot R = X \cdot (Q \cdot R)$. By recurrence on the degree of Q we also show that for any $R \in \mathfrak{A}[X]$ and any $a \in \mathfrak{A}$,

$$a(Q \cdot R) = (aQ) \cdot R.$$

We write $Q = Q_1 \cdot X + b$ and get

$$\begin{aligned}(aQ) \cdot R &= (aQ_1 \cdot X + ab) \cdot R \\ &= (aQ_1) \cdot (X \cdot R) + abR \\ &= a(Q_1 \cdot (X \cdot R)) + a(bR) \text{ by recurrence} \\ &= a(Q_1 \cdot (X \cdot R) + bR) \\ &= a(Q \cdot R) \text{ by definition.}\end{aligned}$$

Let now $P = P_1 \cdot X + a \in \mathfrak{A}$. Then

$$\begin{aligned}(P \cdot Q) \cdot R &= (P_1 \cdot (X \cdot Q) + aQ) \cdot R \\ &= (P_1 \cdot (X \cdot Q)) \cdot R + (aQ) \cdot R \\ &= P_1 \cdot ((X \cdot Q) \cdot R) + a(Q \cdot R) \text{ by recurrence on the degree of } P \\ &= P_1 \cdot (X \cdot (Q \cdot R)) + a(Q \cdot R) \\ &= P \cdot (Q \cdot R) \text{ by definition.}\end{aligned}$$

Thus we have proven that $\cdot$ does indeed define a ring structure $\mathfrak{A}[X; f]$. □

With this proven, the usual proof of the good definition of Ore polynomials can be written.

COROLLARY 2.1.10. — *Let $\mathfrak{A}$ be a ring, θ be an endomorphism of $\mathfrak{A}$ and ∂ be a θ-derivation on $\mathfrak{A}$. Then there is a unique ring structure on $\mathfrak{A}[X]$, denoted by $\mathfrak{A}[X; \theta; \partial]$, compatible with its $\mathfrak{A}$-module structure and such that*

$$\begin{aligned}\forall a \in \mathfrak{A},\ X \cdot a &= \theta(a)X + \partial(a) \\ \forall (i,j) \in \mathbb{N}^2,\ X^i \cdot X^j &= X^{i+j}.\end{aligned}$$

REMARK 2.1.11. — Since $\mathfrak{A}[X; \theta; \partial]$ acts upon $\mathfrak{A}$, with $X \cdot a = \partial(a)$ for all $a \in \mathfrak{A}$, we will often refer to elements of $\mathfrak{A}[X; \theta; \partial]$ as operators.

Proof of Corollary 2.1.10. This is just Theorem 2.1.9 applied with $f : a \mapsto \theta(a)X + \partial(a)$. Since θ and ∂ are both additive, so is f. Furthermore, $f(1) = \theta(1)X + \partial(1) = X + \partial(1)$. But $\partial(1)$ is necessarily equal to 0. Indeed

$$\begin{aligned}\partial(1) &= \partial(1 \cdot 1) \\ &= \theta(1)\partial(1) + \partial(1) \\ &= 2\partial(1)\end{aligned}$$

thus $\partial(1) = 0$ and $f(1) = X$. Following remark 2.1.6 we see that f defines a unique commutation rule and we only have to check that for any $a, b \in \mathfrak{A}$ $f(a)(f)(b) = f(ab)$ which follows from the following computation:

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

□

Though Theorem 2.1.9 is more general that just the framework of Ore polynomials, it is actually unclear whether or not other associative commutation rules exist or are interesting.

The ring $\mathfrak{A}[X;\theta;\partial]$ is equipped with a notion of degree similar to that of polynomials. To avoid confusion, since $\mathfrak{A}$ will often be a ring of polynomials or rational functions later on, we call it the order of an operator.

DEFINITION 2.1.12. — Let $P = \sum_{k=0}^{n} a_k X^K \in \mathfrak{A}[X;\theta;\partial]$. We call the order of P, which we denote by $\mathrm{ord}(P)$, the highest integer k for which $a_k \neq 0$. If $P = 0$ then by convention we say that $\mathrm{ord}(P) = -\infty$.

We will see that the order of operators provides $\mathfrak{A}[X;\theta;\partial]$ with similar properties to the degree for polynomial rings. For now we tackle an important aspect of Ore polynomials concerning their morphism:

THEOREM 2.1.13. — *We suppose given an associative commutation rule f on $\mathfrak{A}[X]$.*

Let B be a ring and $\varphi : \mathfrak{A} \to B$ a ring homomorphism. We still denote by φ the unique ring homomorphism from $\mathfrak{A}[X]$ to $B[X]$ extending φ and mapping X to X.

Let $\xi \in B$ be such that for all $a \in \mathfrak{A}$

$$\xi\varphi(a) = \varphi(f(a))(\xi)$$

Then there exists a unique ring homomorphism $\tilde{\varphi} : \mathfrak{A}[X, f] \to B$ extending $\varphi : \mathfrak{A} \to B$ and mapping X to ξ.

Furthermore, for any ring homomorphism $\tilde{\varphi} : \mathfrak{A}[X, f] \to B$ extending φ, $\tilde{\varphi}(X)$ is of this form.

Proof. We begin by the second statement. Let $\tilde{\varphi} : \mathfrak{A}[X, f] \to B$ be a ring homomorphism extending φ. Then for any $a \in \mathfrak{A}$,

$$\tilde{\varphi}(X)\varphi(a) = \tilde{\varphi}(Xa) = \tilde{\varphi}(f(a)).$$

Let $f(a) = \sum_{k=0}^{n} a_k X^k$. Then

$$\tilde{\varphi}(f(a)) = \sum_{k=0}^{n} \tilde{\varphi}(a_k X^k) = \sum_{k=0}^{n} \varphi(a_k)\tilde{\varphi}(X)^k = \varphi(f(a))(\tilde{\varphi}(X))$$

which is precisely the desired property.

Now suppose ξ fixed. Let $P = P_1X + a \in \mathfrak{A}[X, f]$. If such a $\tilde{\varphi}$ exists then it must verify

$$\begin{aligned}\tilde{\varphi}(P) &= \tilde{\varphi}(P_1)\tilde{\varphi}(X) + \tilde{\varphi}(a)\\ &= \tilde{\varphi}(P_1)\xi + \varphi(a)\end{aligned}$$

By induction on the order of P we see that this uniquely defines $\tilde{\varphi}$. Furthermore we see that we have $\tilde{\varphi}(P) = \varphi(P)(\xi)$. This yields for any $a \in \mathfrak{A}$:

$$\tilde{\varphi}(Xa) = \tilde{\varphi}(f(a)) = \varphi(f(a))(\xi).$$

But also

$$\tilde{\varphi}(X)\tilde{\varphi}(a) = \xi\varphi(a) = \varphi(f(a))(\xi).$$

Thus

$$\tilde{\varphi}(Xa) = \tilde{\varphi}(X)\tilde{\varphi}(a).$$

Let us show that $\tilde{\varphi}$ defined this way is indeed a ring homomorphism. Let $P = P_1X + a$ and $Q = Q_1X + b$. Then

$$\begin{aligned}\tilde{\varphi}(P+Q) &= \tilde{\varphi}((P_1+Q_1)X + (a+b))\\ &= \tilde{\varphi}(P_1+Q_1)\xi + \varphi(a) + \varphi(b)\\ &= \tilde{\varphi}(P_1)\xi + \tilde{\varphi}(Q_1)\xi + \varphi(a) + \varphi(b) \text{ by induction on the order of } P+Q\\ &= \tilde{\varphi}(P) + \tilde{\varphi}(Q)\end{aligned}$$

For any $a \in \mathfrak{A}$ and any $Q \in \mathfrak{A}[X, f]$ we have

$$\begin{aligned}\tilde{\varphi}(aQ) &= \varphi(aQ)(\xi)\\ &= \varphi(a)\varphi(Q)(\xi)\\ &= \tilde{\varphi}(a)\tilde{\varphi}(Q)\end{aligned}$$

Suppose that we have shown that for any $P \in \mathfrak{A}[X, f]$ of degree less than some $k \geqslant 0$ and any $Q \in \mathfrak{A}[X, f]$, $\tilde{\varphi}(PQ) = \tilde{\varphi}(P)\tilde{\varphi}(Q)$. Let $P = P_1X + a$ of degree $k+1$, $b \in \mathfrak{A}$ and $j \in \mathbb{N}$.

$$\begin{aligned}\tilde{\varphi}(PbX^j) &= \tilde{\varphi}(P_1XbX^j + abX^j)\\ &= \tilde{\varphi}(P_1f(b)X^j) + \tilde{\varphi}(abX^j)\\ &= \tilde{\varphi}(P_1)\tilde{\varphi}(f(b)X^j) + \tilde{\varphi}(a)\tilde{\varphi}(bX^j) \text{ by induction hypothesis}\\ &= \tilde{\varphi}(P_1)\tilde{\varphi}(f(b))\xi^j + \tilde{\varphi}(a)\tilde{\varphi}(bX^j)\\ &= \tilde{\varphi}(P_1)\tilde{\varphi}(Xb)\xi^j + \tilde{\varphi}(a)\tilde{\varphi}(bX^j)\\ &= \tilde{\varphi}(P_1)\tilde{\varphi}(X)\tilde{\varphi}(b)\xi^j + \tilde{\varphi}(a)\tilde{\varphi}(bX^j)\\ &= \tilde{\varphi}(P_1X)\tilde{\varphi}(bX^j) + \tilde{\varphi}(a)\tilde{\varphi}(bX^j) \text{ by induction hypothesis}\\ &= \tilde{\varphi}(P)\tilde{\varphi}(bX^j)\end{aligned}$$

By additivity of $\tilde{\varphi}$, we show that for any $Q \in \mathfrak{A}[X, f]$

$$\tilde{\varphi}(PQ) = \tilde{\varphi}(P)\tilde{\varphi}(Q)$$

and the induction is established.

Thus $\tilde{\varphi}$ is indeed a ring homomorphism □

COROLLARY 2.1.14. — *Let θ be an endomorphism of $\mathfrak{A}$ and ∂ be a θ-derivation of $\mathfrak{A}$. Let $\varphi : \mathfrak{A} \to B$ be a ring homomorphism. For any $\xi \in B$ verifying for all $a \in \mathfrak{A}$*

$$\xi\varphi(a) = \varphi(\theta(a))\xi + \varphi(\partial(a))$$

there exists a unique ring homomorphism $\tilde{\varphi} : \mathfrak{A}[X;\theta;\partial] \to B$ extending φ and sending X to ξ.

Furthermore, for any ring homomorphism $\tilde{\varphi} : \mathfrak{A}[X;\theta;\partial] \to B$ extending φ, $\tilde{\varphi}(X)$ is such an element ξ.

Proof. This is just the previous theorem applied with $c : a \mapsto \theta(a)X + \partial(a)$. □

An important corollary of this theorem concerns the $\mathfrak{A}[X;\theta;\partial]$-modules. We consider θ and ∂ fixed.

DEFINITION 2.1.15. — Let M be an $\mathfrak{A}$-module. An additive map $c : M \to M$ is called a (θ,∂)-connexion if and only if for all $a \in \mathfrak{A}$ and all $m \in M$,

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

EXAMPLE 2.1.16. — Let $n \in \mathbb{N}^*$. For any $M \in M_n(\mathfrak{A})$,

$$\begin{array}{rccc} \partial_M : & \mathfrak{A}^n & \to & \mathfrak{A}^n \\ & m & \mapsto & \partial(m) - M\theta(m) \end{array}$$

defines a (θ,∂)-connexion on $\mathfrak{A}$ ($\partial(m)$ and $\theta(m)$ denotes the application of those maps to m coordinates-wise).

When $\theta = \mathrm{Id}_{\mathfrak{A}}$, the connexion ∂_M corresponds to the linear differential system

$$Y' = MY.$$

Solving this linear differential system is the same as finding a basis of $\mathfrak{A}^n$ of horizontal vectors for ∂_M, that is to say a basis $(e_1, \cdots, e_n)$ such that

$$\partial_M(e_i) = 0$$

for all $i \in [\![1;n]\!]$. It must be noted that such a basis does not always exist in $\mathfrak{A}^n$.

COROLLARY 2.1.17. — *Let M be an $\mathfrak{A}$-module. For every (θ,∂)-connexion c on M, there is a unique structure of left $\mathfrak{A}[X;\theta;\partial]$-module such that for every $m \in M$,*

$$X \cdot m = c(m).$$

Furthermore, if M is a left $\mathfrak{A}[X;\theta;\partial]$-module then $m \mapsto X \cdot m$ is a connexion on M.

Proof. Let M be a left $\mathfrak{A}[X;\theta;\partial]$-module. Then for any $a \in \mathfrak{A}$ and any $m \in M$

$$X \cdot (am) = (Xa) \cdot m = (\theta(a)X) \cdot m + \partial(a) \cdot m = \theta(a)(X \cdot m) + \partial(a)m.$$

Conversely let M be a $\mathfrak{A}$-module and $c : M \to M$ a (θ,∂)-connexion.
A structure of $\mathfrak{A}[X;\theta;\partial]$-module is the same as a $\mathfrak{A}$-algebra homomorphism $\varphi : \mathfrak{A}[X;\theta;\partial] \to \mathrm{End}_{\mathfrak{A}}(M)$. From corollary 2.1.14 we know that there is a unique such morphism φ such that $\varphi(X) = c$. □

As previously mentioned, the ring of Ore polynomials over $\mathfrak{A}$ shares many properties with the ring of polynomials over $\mathfrak{A}$ despite being noncommutative. The first is the notion of order of an element which we already introduced. It is analogous to the notion of degree for polynomials and has similar properties as illustrated by the following proposition.

PROPOSITION 2.1.18. — *For all $P, Q \in \mathfrak{A}[X;\theta;\partial]$:*

i) $\operatorname{ord}(PQ) \leqslant \operatorname{ord}(P) + \operatorname{ord}(Q)$. *This is an equality when $\mathfrak{A}$ is an integral domain and θ is injective.*

ii) $\operatorname{ord}(P+Q) \leqslant \max(\operatorname{ord}(P), \operatorname{ord}(Q))$ *with it being an equality if* $\operatorname{ord}(P) \neq \operatorname{ord}(Q)$.

Proof. The proof of the second point is exactly the same as in the polynomial case since it is only a statement about the $\mathfrak{A}$-module structure of $\mathfrak{A}[X;\theta;\partial]$ which is the same as that of $\mathfrak{A}[X]$.

To prove the first point we can proceed by recurrence on $\operatorname{ord}(P)$. Suppose that $\operatorname{ord}(P) = n$. Then we can write $P = f_n X^n + P'$ with $\operatorname{ord}(P') \leqslant n-1$. We find

$$PQ = f_n X^n Q + P'Q.$$

By recurrence, $\operatorname{ord}(P'Q) \leqslant \operatorname{ord}(Q) + n - 1$.
Furthermore

$$f_n X^n Q = f_n X^{n-1}(XQ).$$

It is easy to see that if $Q = \sum_{i=0}^{m} q_i X^i$ then

$$XQ = \sum_{i=0}^{m} \theta(q_i) X^{i+1} + \sum_{i=0}^{m} \partial(q_i) X^i$$

is of order smaller than $\operatorname{ord}(Q)+1$, with it being an equality if θ is injective. Thus, applying our recurrence hypothesis, we find that $\operatorname{ord}(f_n X^n Q) \leqslant n - 1 + 1 + \operatorname{ord}(Q) = \operatorname{ord}(Q) + n$ with it being an equality if $\mathcal{A}$ is an integral domain and θ is injective.
Applying (ii) yields the result. □

COROLLARY 2.1.19. — *If $\mathfrak{A}$ is an integral domain and θ is injective then $\mathfrak{A}[X;\theta;\partial]$ has no nontrivial zero divisors.*

Proof. Suppose that $\mathfrak{A}$ is an integral domain and θ is injective. If $P, Q \neq 0$ then $\operatorname{ord}(P), \operatorname{ord}(Q) \geqslant 0$. Thus $\operatorname{ord}(P,Q) = \operatorname{ord}(P) + \operatorname{ord}(Q) \geqslant 0$ and $PQ \neq 0$. □

Just as the degree for the polynomials, the order provides the ring of differential operators with an Euclidean division and grants it similar properties.

PROPOSITION 2.1.20. — *Let L_1 and L_2 be two operators $\in \mathfrak{A}[X;\theta;\partial]$. We suppose that L_2 has an invertible leading coefficient. Then there exists a unique pair $Q_r, R_r \in \mathfrak{A}[X;\theta;\partial]$ such that* $\operatorname{ord}(R_r) < \operatorname{ord}(L_2)$ *and*

$$L_1 = Q_r L_2 + R_r.$$

Furthermore, if θ is an automorphism then there exists a unique pair $Q_l, R_l \in \mathfrak{A}[X;\theta;\partial]$ such that $\operatorname{ord}(R_l) < \operatorname{ord}(L_2)$ *and*

$$L_1 = L_2 Q_l + R_l.$$

Proof. We proceed by recurrence on $\mathrm{ord}(L_1)$. If $\mathrm{ord}(L_1) < \mathrm{ord}(L_2)$ then $(Q_r, R_r) = (Q_l, R_l) = (0, L_1)$ fits.

Now suppose that $L_1 = f_n X^n + L_1'$ with $f_n \neq 0$ and $\mathrm{ord}(L_1') < \mathrm{ord}(L_1)$ and set $m := \mathrm{ord}(L_2)$ and u the leading coefficient of L_2. If u is invertible then so is $\theta^{n-m}(u)$. Then $\frac{f_n}{\theta^{n-m}(u)} X^{n-m} L_2$ is of order n and has leading coefficient f_n. It follows that

$$L_1 - \frac{f_n}{\theta^{n-m}(u)} X^{n-m} L_2$$

is of order strictly smaller than n. We conclude by induction.

Now if θ is an automorphism then $L_2 \cdot \theta^{-m}\left(\frac{f_n}{u}\right) X^{n-m}$ is of order n and has leading coefficients f_n. Thus

$$L_1 - L_2 \cdot \theta^{-m}\left(\frac{f_n}{u}\right) X^{n-m}$$

is of order strictly smaller than n and we can again conclude by recurrence.

For uniqueness, suppose that we have $L_1 = Q_{r,1} L_2 + R_{r,1} = Q_{r,2} L_2 + R_{r,2}$. Then $(Q_{r,1} - Q_{r,2}) L_2 = R_{r,2} - R_{r,1}$. Since L_2 has an invertible leading coefficient, if $Q_{r,1} - Q_{r,2} \neq 0$ then $\mathrm{ord}(Q_{r,1} - Q_{r,2}) L_2) \geqslant \mathrm{ord}(L_2)$. Since $\mathrm{ord}(R_{r,2} - R_{r,1}) < \mathrm{ord}(L_2)$ we must have $Q_{r,1} - Q_{r,2} = 0$ and $R_{r,2} - R_{r,1} = 0$.

The proof is the same *mutatis mutandis* for Q_l and R_l. □

COROLLARY 2.1.21. — *If $\mathfrak{A}$ is a field then all left ideals of $\mathfrak{A}[X;\theta;\partial]$ are generated by a unique element. If θ is an automorphism then so are its right ideals.*

Proof. Since $\mathfrak{A}$ is a field, every non zero element is invertible hence, according to proposition 2.1.20, we have a right Euclidean division. The proof is then perfectly analogous to the case of Euclidean rings. In the case where θ is an automorphism then according to proposition 2.1.20 we have a left Euclidean division and the proof is again analogous to the case of Euclidean rings. □

Thus, under the hypothesis that $\mathfrak{A}$ is a field, we see that apart from not being commutative, the ring of differential operators has all the characteristic of a principal ideal domain (and even of an Euclidean domain). Follows from this a notion of greatest common right/left divisor and of least common left/right multiple, defined, as in the commutative case, as a generator of the sum and intersection of the ideals respectively. Moreover, those two operations can be computed with a noncommutative variant of Euclidean algorithm. This way of computing gcd and lcm is actually not the most efficient for differential operators, however it is enough for now to know that these two (in fact four) operations are computable. One may check [Gri90] and [BCSL12] for more advanced algorithms for gcrd and lclm respectively.

DEFINITION 2.1.22. — We assume that $\mathfrak{A}$ is a field. Let $P, Q \in \mathfrak{A}[X;\theta;\partial]$. There exists $D \in \mathfrak{A}[X;\theta;\partial]$ such that $\mathfrak{A}[X;\theta;\partial]P + \mathfrak{A}[X;\theta;\partial]Q = \mathfrak{A}[X;\theta;\partial]D$. We call D the greatest right commom divisor of P and Q, which we denote $\mathrm{gcrd}(P, Q)$.

Similarly we define the least common left multiple of P and Q, which we denote by $\mathrm{lclm}(P,Q)$ as an element $M \in \mathfrak{A}[X;\theta;\partial]$ such that $\mathfrak{A}[X;\theta;\partial]P \cap \mathfrak{A}[X;\theta;\partial]Q = \mathfrak{A}[X;\theta;\partial]M$.

REMARK 2.1.23. — From those definitions we can see that the gcrd and lclm of two operators are only defined up to a multiplicative element of $\mathfrak{A}^\times$. In practice we will consider that gcrd and lclm are always monic.

REMARK 2.1.24. — When θ is an automorphism, gcld and lcrm are similarly defined by considering instead right ideals.

Finally, we can talk about irreducible operators. An operator is said irreducible if it is not invertible and cannot be written as a product of two non invertible operators. When $\mathfrak{A}$ is a field, an operator is irreducible if and only if it cannot be written as a product of two operators of strictly smaller order and an immediate induction yields the following result:

PROPOSITION 2.1.25. — *If $\mathfrak{A}$ is a field, any $L \in \mathfrak{A}[X;\theta;\partial]$ can be written as a product $L := \prod_{i=1}^{n} P_i$ where each P_i is irreducible and $n \in \mathbb{N}$.*

As previously mentioned, unlike the polynomial case, factorisations of Ore polynomials are usually not unique, even up to permutations. For example, in $\mathbb{F}_2(x)[X, \mathrm{Id}_{\mathbb{F}_2(x)}, \frac{\mathrm{d}}{\mathrm{d}x}]$,

$$X^2 = \left(X + \frac{f'}{f}\right)^2$$

for all $f \in \mathbb{F}_2(x)$. The goal of this thesis is to present an algorithm able to find one of such factorisations, or at the very least a nontrivial right divisor when it exists, for a given linear differential operator. Linear differential operators are a specific subclass of Ore polynomials which we will introduce in a moment, and consist of the case where θ is the identity morphism. This will be developed in the following chapters of this thesis.

Although the following considerations are not necessary to the computation of the p-curvature developed in this chapter, they are the main guideline of our later work on factorisation. Furthermore, they are important for some applications of the p-curvature that we will expose in the next section.

From now on, until otherwise specified, we suppose that $\mathfrak{A}$ is a field.

Notation 2.1.26. For the rest of this document we denote by $\mathcal{D}_L$ the left $\mathfrak{A}[X;\theta;\partial]$-module ${}^{\mathfrak{A}[X;\theta;\partial]}/_{\mathfrak{A}[X;\theta;\partial]L}$ and for any $L' \in \mathfrak{A}[X;\theta;\partial]$, we denote by $\mathcal{D}_L L'$ the left submodule of $\mathcal{D}_L$ generated by the image of L'.

PROPOSITION 2.1.27. — *Let $L \in \mathfrak{A}[X;\theta;\partial]$. The application which maps a right divisor L_1 of L to $\mathcal{D}_L L_1 = {}^{\mathfrak{A}[X;\theta;\partial]L_1}/_{\mathfrak{A}[X;\theta;\partial]L}$ is a bijection between the set of right divisor of L (up to a multiplicative element in $\mathfrak{A}^\times$) and the set of sub-$\mathfrak{A}[X;\theta;\partial]$-modules of $\mathcal{D}_L$.*
Furthermore, this bijection is decreasing for the orders given by inclusion and right divisibility.

Proof. To show that it is indeed a bijection we define the reciprocal application. Let M be a sub-$\mathfrak{A}[X;\theta;\partial]$-module of $\mathcal{D}_L$. Then we can consider the canonical projection $\pi_M : \mathfrak{A}[X;\theta;\partial] \twoheadrightarrow {}^{\mathcal{D}_L}/_M$, which is a morphism of left-$\mathfrak{A}[X;\theta;\partial]$-modules. It follows that $I = \ker(\pi_M)$ is a left ideal of $\mathfrak{A}[X;\theta;\partial]$ containing L. Thus there exists $L_M \in \mathfrak{A}[X;\theta;\partial]$ such that $I = \mathfrak{A}[X;\theta;\partial]L_M$ and since $L \in I$, L_M is a right divisor of L. Since M is the image of $\ker(\pi_M)$ by the canonical projection of $\mathfrak{A}[X;\theta;\partial]$ onto $\mathcal{D}_L$, it follows that $M = \mathcal{D}_L L_M$. □

In our later work on factorisation, we will try to exhibit nontrivial submodules of $\mathcal{D}_L$ to use this proposition and find a factorisation of a given operator L.

This bijection also has consequences on the form of the quotient modules of $\mathcal{D}_L$ which will be of use later on.

COROLLARY 2.1.28. — *Let $L \in \mathfrak{A}[X;\theta;\partial]$. All quotient $\mathfrak{A}[X;\theta;\partial]$-modules of $\mathcal{D}_L$ are isomorphic to a $\mathcal{D}_{L'}$ for some right divisor L' of L.*

A consequence is the translation of classical operations on the submodules, such as the sum or the intersection, in terms of their generator.

LEMMA 2.1.29. — *Let $L \in \mathfrak{A}[X;\theta;\partial]$ and L_1, L_2 be right divisors of L.*

i) $\mathcal{D}_L L_1 + \mathcal{D}_L L_2 = \mathcal{D}_L \mathrm{gcrd}(L_1, L_2)$.

ii) $\mathcal{D}_L L_1 \cap \mathcal{D}_L L_2 = \mathcal{D}_L \mathrm{lclm}(L_1, L_2)$.

Proof. From proposition 2.1.27, we know that $L' \mapsto \mathcal{D}_L L'$ is a decreasing bijection between right divisors of L and submodules of $\mathcal{D}_L$. Thus it must map the greatest common right divisor of L_1 and L_2 to the smallest submodule of $\mathcal{D}_L$ containing both $\mathcal{D}_L L_1$ and $\mathcal{D}_L L_2$.
Similarly, it must map the least common left multiple of L_1 and L_2 to the largest submodule included both in $\mathcal{D}_L L_1$ and $\mathcal{D}_L L_2$. □

REMARK 2.1.30. — (i) actually still holds even if L_1 and L_2 are not right divisors of L. This is because

$$\begin{aligned}(\mathfrak{A}[X;\theta;\partial]L_1 + \mathfrak{A}[X;\theta;\partial]L) + (\mathfrak{A}[X;\theta;\partial]L_2 + \mathfrak{A}[X;\theta;\partial]L)\\ = (\mathfrak{A}[X;\theta;\partial]L_1 + \mathfrak{A}[X;\theta;\partial]L_2) + \mathfrak{A}[X;\theta;\partial]L.\end{aligned}$$

The same is not true about (ii) because the intersection is not distributive over the sum.

Those relations will be used mainly in the next chapters to construct new submodules from previously known ones.

The following corollary won't be of much use for the computation of the p-curvature or the factorisation in itself, but is a translation in the language of gcrd and lclm of what it means for a differential module to be a direct sum and is useful for lclm decompositions.

COROLLARY 2.1.31. — *Let $L \in \mathfrak{A}[X;\theta;\partial]$ and L_1 and L_2 be two right divisors of L. The two following propositions are equivalent:*

i) $\mathcal{D}_L = \mathcal{D}_L L_1 \oplus \mathcal{D}_L L_2$.

ii) $\mathrm{lclm}(L_1, L_2) = L$ *and* $\mathrm{gcrd}(L_1, L_2) = 1$.

In this case

$$\begin{array}{rcl}\mathcal{D}_L & \to & \mathcal{D}_{L_1} \oplus \mathcal{D}_{L_2}\\ M & \mapsto & (M \mod L_1) + (M \mod L_2)\end{array}$$

is an isomorphism.

Proof. The equivalence is obvious from Lemma 2.1.29. We suppose that (ii) is true. Then saying that L_1 and L_2 are both right divisors of some M is equivalent to saying that $\mathrm{lclm}(L_1, L_2) = L$ is a right divisor of M. Thus the morphism is injective. Since L_1 and L_2 are (right) coprime, there exists Q_1 and Q_2 such that $Q_1L_1 + Q_2L_2 = 1$. Thus for any $R_1, R_2 \in \mathfrak{A}[X;\theta;\partial]$,

$$\begin{aligned} R_2Q_1L_1 + R_1Q_2L_2 &\equiv R_2 \mod L_2 \\ &\equiv R_1 \mod L_1 \end{aligned}$$

It follows that the morphism is surjective and thus is an isomorphism. □

Finally we end this general discussion on Ore polynomials on an interesting relation between gcrd and lclm, analog to the commutative case.

LEMMA 2.1.32. — *Let $L_1, L_2 \in \mathfrak{A}[X;\theta;\partial]$. There is an exact sequence*

$$0 \to \mathcal{D}_{\mathrm{lclm}(L_1,L_2)} \to \mathcal{D}_{L_1} \oplus \mathcal{D}_{L_2} \to \mathcal{D}_{\mathrm{gcrd}(L_1,L_2)} \to 0.$$

In particular $\mathrm{ord}(\mathrm{lclm}(L_1, L_2)) + \mathrm{ord}(\mathrm{gcrd}(L_1, L_2)) = \mathrm{ord}(L_1) + \mathrm{ord}(L_2)$.

Proof. We define $\varphi : \mathcal{D}_{\mathrm{lclm}(L_1,L_2)} \to \mathcal{D}_{L_1} \oplus \mathcal{D}_{L_2}$ as the sum of the canonical projections and

$$\begin{array}{rccc} \psi : & \mathcal{D}_{L_1} \oplus \mathcal{D}_{L_2} & \to & \mathcal{D}_{\mathrm{gcrd}(L_1,L_2)} \\ & (P_1, P_2) & \mapsto & P_1 - P_2 \end{array}.$$

Let $P \in \ker(\varphi)$. Then P is both a multiple of L_1 and a multiple of L_2 so it is a multiple of $\mathrm{lclm}(L_1, L_2)$ so φ is injective. The restriction of ψ to $\mathcal{D}_{L_1} \oplus \{0\}$ is the canonical projection. In particular, ψ is surjective.
We have $\mathrm{Im}\,(\varphi) \subset \ker(\psi)$. Let $P_1, P_2 \in \ker(\psi)$. Then there exists $Q \in \mathfrak{A}[X;\theta;\partial]$ such that $P_1 = P_2 + Q\mathrm{gcrd}(L_1, L_2)$. By definition, we know that there exists $U, V \in \mathfrak{A}[X;\theta;\partial]$ such that $UL_1 + VL_2 = \mathrm{gcrd}(L_1, L_2)$. We deduce that $P_1 - QUL_1 = P_2 + QVL_2$. Let P be a lift of $P_1 - QUL_1$. Then $(P_1, P_2) = \varphi(P) \in \mathrm{Im}\,(\varphi)$.

Thus we do have an exact sequence. It follows that

$$\begin{aligned} \mathrm{ord}(\mathrm{lclm}(L_1, L_2)) + \mathrm{ord}(\mathrm{gcrd}(L_1, L_2)) &= \dim_{\mathfrak{A}}(\mathcal{D}_{\mathrm{lclm}(L_1,L_2)}) + \dim_{\mathfrak{A}}(\mathcal{D}_{\mathrm{gcrd}(L_1,L_2)}) \\ &= \dim_{\mathfrak{A}}(\mathcal{D}_{L_1} \oplus \mathcal{D}_{L_2}) \\ &= \dim_{\mathfrak{A}}(\mathcal{D}_{L_1}) + \dim_{\mathfrak{A}}(\mathcal{D}_{L_2}) \\ &= \mathrm{ord}(L_1) + \mathrm{ord}(L_2). \end{aligned}$$

□

2.1.2 The differential case

We end there this general overview of the properties of Ore polynomials to focus on the subject of this study which are differential operators which we now define.

DEFINITION 2.1.33. — We say that a couple $(\mathcal{A}, \partial)$ defines a differential ring if and only if $\mathcal{A}$ is a ring and ∂ is a derivation on $\mathcal{A}$. The subring $\mathcal{C} = \{a \in \mathcal{A} | \partial(a) = 0\}$ is called the ring of constant of $(\mathcal{A}, \partial)$ (or $\mathcal{A}$ if the derivation is implied).

Let $(\mathcal{A}, \partial)$ be a commutative differential ring. The relevant case for this chapter is $\mathcal{A}$ of the form $A[x]$ for some commutative ring A, provided with the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$. In the next chapter $\mathcal{A}$ will be the field of rational functions over the finite field of cardinality p, $\mathbb{F}_p(x)$, or K, a separable extension of it.

DEFINITION 2.1.34. — The algebra of linear differential operators over $\mathcal{A}$, $\mathcal{A}\langle\partial\rangle$ is the set of polynomials in the variable ∂, isomorphic to $\mathcal{A}[X, \mathrm{Id}_{\mathcal{A}}, \partial]$ by mapping ∂ to X.

For any $f \in \mathcal{A}$, the multiplication follows the following commutation rule:

$$\partial f = f\partial + \partial(f).$$

REMARK 2.1.35. — Here ∂ designates both a derivation map and a formal operator which is an abuse of notation. In hopes of making it less confusing, from now on we will denote

$$f' = \partial(f)$$

and

$$f^{(k)} = \partial^k(f)$$

for any $f \in \mathcal{A}$ unless otherwise specified.

DEFINITION 2.1.36. — Let M be a $\mathcal{A}$-module. We say that M is a differential module (over $(\mathcal{A}, \partial)$ if it is not implied) if M is equipped with a $(\mathrm{Id}_{\mathcal{A}}, \partial)$-connexion. According to Corollary 2.1.17, this is equivalent to saying that M is a left $\mathcal{A}\langle\partial\rangle$-module.

Differential operators can be considered in a wide variety but in the context of this thesis we will almost always suppose that $\mathcal{A}$ is a ring of prime positive characteristic p. The main difference between the case of characteristic zero and the positive characteristic is the size of the subring of constants of $\mathcal{A}$. Whereas it is generally of infinite codimension in $\mathcal{A}$, in characteristic p this codimension is finite and equal to p in all of our practical cases.

For the rest of this section we make the following assumptions:

HYPOTHESIS 2.1.37. — $\mathcal{A}$ is a differential ring of characteristic p. Let $\mathcal{C}$ be the ring of constant of $\mathcal{A}$. We suppose that:

1. $\mathcal{C}$ is an integral domain.
2. $\mathcal{A}$ is a free algebra of dimension p over $\mathcal{C}$.
3. There exists $x \in \mathcal{A}$ such that $\partial(x) \in \mathcal{C}\backslash\{0\}$.

EXAMPLE 2.1.38. — Let K be a separable extension of $\mathbb{F}_p(x)$ and $C := \{f^p | f \in K\}$ provided with the usual derivation $\frac{\mathrm{d}}{\mathrm{d}x}$.

- $[K : C] = p$.
- C is the constant field of K.
- $K = C[x]$.

Proof. We first suppose that K is a finite separable extension of $\mathbb{F}_p(x)$. Let f be primitive element of K and P_f be its minimal polynomial. Then f^p is a primitive element of C as an extension of $\mathbb{F}_p(x^p)$ (since $K \simeq C$). Thus

$$[K : \mathbb{F}_p(x^p)] = [K : C][C : \mathbb{F}_p(x^p)] = [K : \mathbb{F}_p(x)][\mathbb{F}_p(x) : \mathbb{F}_p(x^p)].$$

Since $K \simeq C$ we have $[C : \mathbb{F}_p(x^p)] = [K : \mathbb{F}_p(x)]$. Thus $[K : C] = [\mathbb{F}_p(x^p) : \mathbb{F}_p(x)] = p$.
Let C' be the constant field of K. We obviously have $C \subset C' \subset K$ and since $\frac{\mathrm{d}}{\mathrm{d}x}$ is not trivial on K, we have $C = C'$. Furthermore since K is separable over $\mathbb{F}_p(x)$, C is separable over $\mathbb{F}_p(x^p)$, thus it does not contain x. Thus we have $C \subsetneq C[x] \subset K$. □

Example 2.1.38 is the canonical setting of the study of differential operators in prime characteristic p and is the natural setting of our work on factorisation. It allows to study differential equations with regular coefficients over algebraic curves over $\mathbb{F}_p$. Algebraic functions fields can be seen as the field of regular functions over some algebraic curve.

The fact that algebraic function fields such as in example 2.1.38 verify Hypothesis 2.1.37 is very useful for finding solutions in K to differential equations with coefficients in K, which reduces to solving a finite dimensional linear system over C. Unfortunately, this method yields solutions of bit size linear in p.
Another useful example is the following:

EXAMPLE 2.1.39. — Let A be an integral domain of characteristic p. $A[x]$ (resp. $A(x)$) provided with the $\frac{\mathrm{d}}{\mathrm{d}x}$ derivation are rings verifying Hypothesis 2.1.37 and its ring of constant is $A[x^p]$ (resp. $A(x^p)$).

When $\mathcal{A}$ verifies Hypothesis 2.1.37 the derivation is p-nilpotent as illustrated here:

PROPOSITION 2.1.40. — *For any $f \in \mathcal{A}$, $f^{(p)} = 0$. It follows that $\partial^p f = f\partial^p$.*

Proof. We consider the algebra $\mathcal{C}^{-1}\mathcal{A} := \mathcal{A} \otimes_{\mathcal{C}} \mathrm{Frac}(\mathcal{C})$. Since $\mathcal{A}$ is a free $\mathcal{C}$-algebra of dimension p, $\mathcal{C}^{-1}\mathcal{A}$ is a free $\mathrm{Frac}(\mathcal{C})$ algebra of dimension p. We have an injection $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathcal{C}}$ and there is a unique derivation on $\mathcal{A}_{\mathcal{C}}$ which coincide with the derivation on $\mathcal{A}$. Thus we can suppose that $\mathcal{C}$ is a field.

Since we can suppose that $\mathcal{C}$ is a field, by replacing x by $\frac{x}{\partial(x)}$ we can also suppose that $\partial(x) = 1$. In particular $x \notin \mathcal{C}$. From Leibniz rule we get

$$\partial(x^i) = ix^{i-1}$$

for $i \in \mathbb{N}$. Thus $\mathcal{C}[x]$ is of dimension p over $\mathcal{C}$ and $\mathcal{A} = \mathcal{C}[x]$. For all $i \in [\![0; p-1]\!]$, $\partial^p(x^i) = 0$ thus for all $f \in \mathcal{A}$, $f^{(p)} = 0$.

For all $f \in \mathcal{A}$,

$$\begin{aligned}\partial^p f &= \sum_{k=0}^{p} \binom{p}{k} f^{(p-k)}\partial^k \\ &= f\partial^p + f^{(p)} \\ &= f\partial^p.\end{aligned}$$

□

REMARK 2.1.41. — The hypothesis that $\partial^p(\mathcal{A}) = 0$ is actually the good setting for our work and is equivalent to (3) in Hypothesis 2.1.37 if the other two conditions are verified.

A direct consequence of this is that $\mathcal{A}\langle\partial\rangle$ is a finite dimensional algebra over its centre. This simple fact is what sets the theory of linear differential equations in characteristic p apart from its analog in characteristic zero.

COROLLARY 2.1.42. — *$\mathcal{C}[\partial^p]$ is the centre of $\mathcal{A}\langle\partial\rangle$.*

To prove this result we need the following lemma:

LEMMA 2.1.43. — *Let $\mathcal{A}$ be a differential ring of characteristic p verifying Hypothesis 2.1.37 and let $\mathcal{C}$ be its ring of constants. Let $x \in \mathcal{A}$ be such that $\partial(x) \in \mathcal{C}\backslash\{0\}$. Then the family $(1, x, \dots, x^{p-1})$ is linearly independent over $\mathcal{C}$.*
In particular if $\mathcal{C}$ is a field, then it is a basis of $\mathcal{A}$.

Proof. Since $\mathcal{A}$ is of dimension p over $\mathcal{C}$, the family $(1, x, \dots, x^p)$ is linearly dependent over $\mathcal{C}$. Thus there exists $P_x = \sum_{i=0}^{k} \lambda_i Y^i \in \mathcal{C}[Y]\backslash\{0\}$ with $k \leqslant p$ such that $P_x(x) = 0$. We can assume that k is taken minimal. Furthermore we have

$$\begin{aligned}\partial(P_x(x)) &= 0\\ &= c\left(\frac{\mathrm{d}}{\mathrm{d}Y}P_x\right)(x).\end{aligned}$$

Since $c \neq 0$, by minimality of k we must have $\frac{\mathrm{d}}{\mathrm{d}Y}P_x = 0$. But since $P_x \neq 0$ this means that $k = p$. This means that the family $(1, x, \dots, x^{p-1})$ is linearly independent over $\mathcal{C}$. □

Proof of Corollary 2.1.42. There is a natural injection $\mathcal{A}\langle\partial\rangle \to \mathcal{C}^{-1}\mathcal{A}\langle\partial\rangle$. Furthermore if $L \in \mathcal{C}^{-1}\mathcal{A}\langle\partial\rangle$ there exists $c \in \mathcal{C}$ such that $cL \in \mathcal{A}\langle\partial\rangle$. It follows that if S is an operator in the centre of $\mathcal{A}\langle\partial\rangle$ then S also commutes with all the operators of $\mathcal{C}^{-1}\mathcal{A}\langle\partial\rangle$. Thus

$$\mathcal{Z}(\mathcal{C}^{-1}\mathcal{A}\langle\partial\rangle) \cap \mathcal{A}\langle\partial\rangle \subset \mathcal{Z}(\mathcal{A}\langle\partial\rangle) \subset \mathcal{Z}(\mathcal{C}^{-1}\mathcal{A}\langle\partial\rangle) \cap \mathcal{A}\langle\partial\rangle$$

and finally

$$\mathcal{Z}(\mathcal{A}\langle\partial\rangle) = \mathcal{Z}(\mathcal{C}^{-1}\mathcal{A}\langle\partial\rangle) \cap \mathcal{A}\langle\partial\rangle.$$

We deduce that we can suppose that $\mathcal{C}$ is a field.

It is obvious that $\mathcal{C}[\partial^p]$ is included in the centre of $\mathcal{A}\langle\partial\rangle$, since all its elements commutes with both elements of $\mathcal{A}$ and ∂. Let L be a central element of $\mathcal{A}\langle\partial\rangle$ and write

$$L = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} l_{i,j}x^i\partial^j$$

with $l_{i,j} \in C[\partial^p]$ (any $L \in \mathcal{A}\langle\partial\rangle$ can be written as such since according to Lemma 2.1.43, $(1, x, \dots, x^{p-1})$ is a $\mathcal{C}$-basis of $\mathcal{A}$).
L commutes with x and ∂. It follows that

$$xL - Lx = \sum_{i=0}^{p-1}\sum_{j=1}^{p-1} jl_{i,j}x^i\partial^{j-1} = 0.$$

It follows that if $j \neq 0$, $l_{i,j} = 0$ and $L \in \mathcal{A}[\partial^p]$.
Furthermore we also have

$$\partial L - L\partial = \sum_{i=1}^{p-1} i l_{i,0} x^{i-1} = 0$$

Thus $l_{i,0} = 0$ for all $i \geqslant 1$. We conclude that $L \in \mathcal{C}[\partial^p]$. □

2.1.3 Azumaya algebra and reduced norm

Corollary 2.1.42 is also the first requirement to show that the rings of differential operators that we will study have an Azumaya algebra structure. This structure, which is a generalisation of central simple algebras will be fundamental for the factorisation, and will also play an important part in the later computation of the p-curvature. Additionally, it was used before by van der Put to classify differential modules in positive characteristic [vdP95]. From now on, we suppose that in addition of verifying Hypothesis 2.1.37, $\mathcal{A}$ contains an element whose derivative is invertible in $\mathcal{C}$.

DEFINITION 2.1.44. — Let $\mathcal{Z}$ be a commutative ring and R be a central $\mathcal{Z}$-algebra. We say that R is an Azumaya algebra if and only if for any prime ideal $\mathfrak{p}$ of $\mathcal{Z}$, $R \otimes_{\mathcal{Z}} \mathrm{Frac}(\mathcal{Z}/\mathfrak{p})$ is a central simple $\mathrm{Frac}(\mathcal{Z}/\mathfrak{p})$-algebra.

THEOREM 2.1.45. — *Let $\mathcal{A}$ be a differential ring of characteristic p verifying Hypothesis 2.1.37. In addition, we suppose that $\mathcal{A}$ contains an element x such that $\partial(x) \in \mathcal{C}^\times$. $\mathcal{A}\langle\partial\rangle$ is an Azumaya $\mathcal{C}[\partial^p]$-algebra in the sense of Definition 2.1.44.*

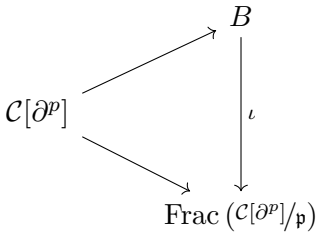
Proof. We have a natural morphism $\mathcal{C} \to \mathrm{Frac}\left(\mathcal{C}[\partial^p]/\mathfrak{p}\right)$. Let $\mathfrak{a}$ be its kernel. Then $\mathfrak{a}$ is a prime ideal of $\mathcal{C}$ and we have a natural morphism

$$\mathrm{Frac}(\mathcal{C}/\mathfrak{a})[\partial^p] \to \mathrm{Frac}\left(\mathcal{C}[\partial^p]/\mathfrak{p}\right).$$

Let $\mathfrak{p}'$ be its kernel. Again, $\mathfrak{p}'$ is a prime ideal, and since $\mathrm{Frac}(\mathcal{C}/\mathfrak{a})[\partial^p]$ is a prime ideal domain, it is either $\{0\}$ or a maximal ideal. In the former case we set $B = \mathcal{C}/\mathfrak{a}(\partial^p)$ and in the latter $B = \mathrm{Frac}(\mathcal{C}/\mathfrak{a})[\partial^p]/\mathfrak{p}'$. We deduce a natural injection

$$\iota : B \to \mathrm{Frac}\left(\mathcal{C}[\partial^p]/\mathfrak{p}\right).$$

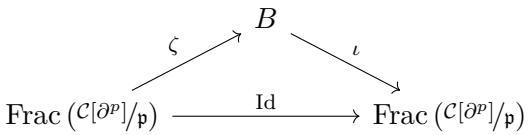
By construction the following diagram commutes:



It follows that we have a morphism

$$\zeta : \mathcal{C}[\partial^p]/\mathfrak{p} \to B$$

and that $\iota \circ \zeta$ is the natural injection of ${}^{\mathcal{C}[\partial^p]}/_{\mathfrak{p}}$ in its fraction field. Thus we get the following commutative diagram:



It follows that ι is both injective and surjective and is an isomorphism. It follows that

$$\begin{aligned}\mathcal{A}\langle\partial\rangle \otimes_{\mathcal{C}[\partial^p]} \operatorname{Frac}\left({}^{\mathcal{C}[\partial^p]}/_{\mathfrak{p}}\right) &\simeq \mathcal{A}\langle\partial\rangle \otimes_{\mathcal{C}[\partial^p]} B \\ &\simeq \mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})\langle\partial\rangle \otimes_{\operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})[\partial^p]} B\end{aligned}$$

Let's show that $\mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$ is a differential ring verifying Hypothesis 2.1.37. Since we supposed that $\partial(x) \in \mathcal{C}^\times$, in particular $\partial(x) \notin \mathfrak{a}$. It follows that $\mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$ verifies (3) in Hypothesis 2.1.37. In a similar manner to the proof of Lemma 2.1.43, we show that $(1, x, \dots, x^{p-1})$ is a $\operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$-basis of $\mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$. We show that the ring of constants of $\mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$ is reduced to $\operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$. Let $\overline{f} \in \mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$. exists $c \in \mathcal{C} \backslash \mathfrak{a}$ and $P_f \in \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})[Y]$ such that $c\overline{f} = P_f(x)$. Then $\overline{f}$ is a constant if and only if $\partial(P_f(x)) \in \mathfrak{a}$. But $\partial(P_f(x)) = \partial(x)\frac{\mathrm{d}P_f}{\mathrm{d}Y}(x)$ so it belongs in $\mathfrak{a}$ if and only if P_f is of the form $ax + b$ with $a \in \mathfrak{a}$ and $b \in \mathcal{C}$. But in that case we have $\overline{f} = \frac{b}{c}$ so $\overline{f} \in \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$. It follows that $\mathcal{A} \otimes_{\mathcal{C}} \operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$ verifies Hypothesis 2.1.37.

Thus by replacing $\mathcal{C}$ by $\operatorname{Frac}({}^{\mathcal{C}}/_{\mathfrak{a}})$ we can suppose that $\mathcal{C}$ is a field. We still must show that

Then $\mathfrak{p}$ is either equal to zero or of the form $\mathcal{C}[\partial^p]N(\partial^p)$ where N is an irreducible polynomial over $\mathcal{C}$. We denote

$$\mathcal{D}_{\mathfrak{p}} := \mathcal{A}\langle\partial\rangle \otimes_{C[\partial^p]} {}^{\mathcal{C}[\partial^p]}/_{\mathfrak{p}}$$

in the latter case and

$$\mathcal{D}_{\mathfrak{p}} := \mathcal{A}\langle\partial\rangle \otimes_{\mathcal{C}[\partial^p]} \mathcal{C}(\partial^p)$$

in the former. Let $\pi : \mathcal{A}\langle\partial\rangle \to \mathcal{D}_{\mathfrak{p}}$ denote the canonical projection.
Any $L \in \mathcal{A}\langle\partial\rangle$ can be uniquely written

$$L = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} l_{i,j} x^i \partial^j$$

with $l_{i,j} \in \mathcal{C}[\partial^p]$. We denote $\deg(L) = \max\{i \in [\![0; p-1]\!] | \exists j \in [\![0; p-1]\!], l_{i,j} \neq 0\}$.

Let $\mathcal{I}$ be a two-sided ideal of $\mathcal{D}_{\mathfrak{p}}$. Then $\tilde{\mathcal{I}} := \pi^{-1}(\mathcal{I})$ is a two-sided ideal of $\mathcal{A}\langle\partial\rangle$.

Let's assume that $\mathcal{I}$ is not reduced to 0. Thus neither is $\tilde{\mathcal{I}}$. We consider L a nonzero element of $\tilde{\mathcal{I}}$ such that the order of L is minimal. In addition, we suppose that $\deg(L)$ is minimal among the elements of $\tilde{\mathcal{I}}$ of the same order. Then since $\tilde{\mathcal{I}}$ is two-sided, $xL - Lx \in \tilde{\mathcal{I}}$. But $\operatorname{ord}(xL - Lx) < \operatorname{ord}(L)$. Thus $xL - Lx = 0$. In addition $\partial L - L\partial$ has at most the same order as L. Furthermore since $\deg(\partial L - L\partial) < \deg(L)$, $\partial L - L\partial = 0$. Thus L is central and is of the form $P(\partial^p)$ with $P \in C[Y]$. Furthermore, since $\mathcal{C}$ is a field, L has an invertible leading coefficient. By Euclidean division, we deduce that L is a generator of $\tilde{I}$. If $\mathfrak{p} = \mathcal{C}[\partial^p]N(\partial^p)$, since N is irreducible, P is either equal to 0 or invertible modulo N. If $\mathfrak{p} = \{0\}$ then P is also

either equal to 0 or invertible in $C(\partial^p)$. Since we supposed that $\tilde{\mathcal{I}}$ is not reduced to 0, we are in the later case and $\mathcal{I} = \mathcal{D}_{\mathfrak{p}}$.

To show that $\mathcal{D}_{\mathfrak{p}}$ is central, let us suppose that $\overline{L} \in \mathcal{D}_{\mathfrak{p}}$ is central. First we suppose that $\mathfrak{p}$ is of the form $\mathcal{C}[\partial^p]N(\partial^p)$. Then a lift of $\overline{L}$, say L, is of order strictly less than that of $N(\partial^p)$. But then $xL - Lx$ and $\partial L - L\partial$ are multiples of $N(\partial^p)$ of order strictly less than $N(\partial^p)$. Thus $\partial L - L\partial = xL - Lx = 0$ and L is central and $\overline{L} \in {}^{\mathcal{C}[\partial^p]}/_{\mathfrak{p}}$.

If now $\mathfrak{p}$ is reduced to zero then there exists $P(\partial^p) \in \mathcal{C}[\partial^p]$ such that $L := P(\partial^p)\overline{L} \in \mathcal{Z}(\mathcal{A}\langle\partial\rangle) = \mathcal{C}[\partial^p]$. Thus $L \in \mathcal{C}(\partial^p)$.

All that is left is to prove that $\mathcal{D}_{\mathfrak{p}}$ is of dimension p^2 but this is obvious since $\mathcal{A}\langle\partial\rangle$ is a free algebra of dimension p^2 over $\mathcal{C}[\partial^p]$. □

The notion of Azumaya algebra is thus a generalisation of the notion of central simple algebra. Hence, the properties of those central simple algebras are very important to our study. It is a well-known fact that a k-central simple algebra R, where k is a field, is isomorphic to a matrix algebra $M_n(K)$ after a scalar extension K/k. K is what is called a splitting field of R. The determinant map of $M_n(K)$ restricts well on R in the sense that $\det(A) \subset k$ and furthermore the restriction of the determinant map to R does not depend on the choice of the splitting field K. All those properties make this restriction of the determinant map very interesting to study.

DEFINITION 2.1.46. — Let k be a field and R be a central simple k-algebra. The restriction of the determinant map to R is called the reduced norm of R. We denote this map $\mathrm{Nrd}_R : R \to k$.

While this is the canonical definition of the reduced norm, we can define it in another way under some conditions on the central simple algebra R.

DEFINITION 2.1.47. — Let C be a commutative ring and R be a finite dimensional free C-algebra. For any $r \in R$ we denote by $N_{R/C}(r)$ the determinant of the C-linear map

$$\begin{array}{rccc} m_r : & R & \to & R \\ & a & \mapsto & ar \end{array}.$$

THEOREM 2.1.48. — *Let k be a field, R be a central simple k-algebra of dimension n^2 and $C \subset R$ a subalgebra such that R is a free C-module of dimension n. We suppose that for a separable closure $\tilde{k}$ of k, $C \otimes_k \tilde{k}$ is generated by a unique element as a $\tilde{k}$-algebra. Then for any $r \in R$,*

$$\mathrm{Nrd}_R(r) = N_{R/C}(r)$$

Proof. See [Car18, Proposition 3.3.9] □

This allows us to define a reduced norm on Azumaya algebras under some more restrictive hypothesis, which will be verified in our practical cases.

HYPOTHESIS 2.1.49. — Let $\mathcal{Z}$ be a commutative ring and R an Azumaya algebra over $\mathcal{Z}$. We suppose that R contains a free commutative subalgebra C such that the following hypothesis are verified:

i) $\mathcal{Z}$ has no nontrivial nilpotent elements.

ii) There exists $n \in \mathbb{N}$ such that C is a free $\mathcal{Z}$-algebra and admits a basis $(1, c_1, \cdots, c_{n-1})$.

iii) R is a free C-module of dimension n.

iv) For any prime ideal $\mathfrak{p}$ of $\mathcal{Z}$, $C \otimes_{\mathcal{Z}} \mathrm{Frac}(\mathcal{Z}/\mathfrak{p})$ verifies the hypothesis of theorem 2.1.48 with respect to $R \otimes_{\mathcal{Z}} \mathrm{Frac}(\mathcal{Z}/\mathfrak{p})$.

PROPOSITION 2.1.50. — *Let $\mathcal{A}$ be a differential ring of characteristic p verifying the hypothesis of Theorem 2.1.45. $\mathcal{A}\langle\partial\rangle$ verifies the conditions of Hypothesis 2.1.49*

Proof. We already know that the center of $\mathcal{A}\langle\partial\rangle$ is $\mathcal{C}[\partial^p]$. Since $\mathcal{C}$ is an integral domain by hypothesis, so is $\mathcal{C}[\partial^p]$. In particular it has no nontrivial nilpotent elements.

We consider the subalgebra $\mathcal{A}[\partial^p]$. Since we know that $\mathcal{A}$ is a free $\mathcal{C}$-algebra of dimension p, $\mathcal{A}[\partial^p]$ is a free $\mathcal{C}[\partial^p]$-algebra of dimension p. A $\mathcal{A}[\partial^p]$-basis of $\mathcal{A}\langle\partial\rangle$ is given by $(1, \partial, \ldots, \partial^{p-1})$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{C}[\partial^p]$. Like we did in the proof of Theorem 2.1.45, we can assume that $\mathcal{C}$ is a field, in which case $\mathcal{A}$ is generated by x as a $\mathcal{C}$-algebra. Thus $\mathcal{A}[\partial^p]$ is also generated by x as a $\mathcal{C}[\partial^p]$-algebra. □

We now define the reduced norm of Azumaya algebras.

DEFINITION 2.1.51. — Let R be an Azumaya algebra verifying Hypothesis 2.1.49. Then we define the reduced norm over R as

$$\mathrm{Nrd}_R(r) = N_{R/C}(r)$$

for all $r \in R$.

The reduced norm of Azumaya algebras is not a construction limited to rings verifying the restrictive conditions of Hypothesis 2.1.49. One way to define Azumaya algebras is to say that they are algebras locally isomorphic to matrix algebras for the étale topology and the reduced norm is locally defined as the determinant.
For the sake of simplicity, we stick to algebras verifying the conditions of Hypothesis 2.1.49 which will be verified in all our examples.

PROPOSITION 2.1.52. — *Let R be an Azumaya algebra over some commutative ring $\mathcal{Z}$ verifying Hypothesis 2.1.49. Then* Nrd_R *does not depend on the choice of the subalgebra C and* $\mathrm{Nrd}_R(R) \subset \mathcal{Z}$.

Proof. Let $(1, c_1, \ldots, c_{n-1})$ be a $\mathcal{Z}$ basis of C. Then the images of $(1, c_1, \ldots, c_{n-1})$ (let denote them $(1, c_{1,\mathfrak{p}}, \ldots, c_{n-1,\mathfrak{p}})$) also constitute a $\mathrm{Frac}\,(\mathcal{Z}/\mathfrak{p})$-basis of $C \otimes_{\mathcal{Z}} \mathrm{Frac}(\mathcal{Z}/\mathfrak{p})$ for all ideal prime $\mathfrak{p}$ of $\mathcal{Z}$. Let $r \in R$. We know that $N_{R/C}(r) \in C$ so there exists $\lambda_0, \ldots, \lambda_{n-1} \in \mathcal{Z}$ such that $N_{R/C}(r) = \lambda_0 + \lambda_1 c_1 + \cdots + \lambda_{n-1} c_{n-1}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{Z}$ and $\pi_{\mathfrak{p}} : \mathcal{Z} \twoheadrightarrow \mathcal{Z}/\mathfrak{p}$ denote the canonical projection. Then according to Theorem 2.1.48, we have

$$N_{R/C}(r) \mod \mathfrak{p} = \pi_{\mathfrak{p}}(\lambda_0) + \sum_{i=1}^{n-1} \pi_{\mathfrak{p}}(\lambda_i) c_{i,\mathfrak{p}} = \mathrm{Nrd}_{R \otimes_{\mathcal{Z}} \mathrm{Frac}(\mathcal{Z}/\mathfrak{p})}(r \mod \mathfrak{p}) \in \mathrm{Frac}\,(\mathcal{Z}/\mathfrak{p})\,.$$

It follows that for all prime ideal $\mathfrak{p}$ of $\mathcal{Z}$, $\lambda_i \in \mathfrak{p}$ for $i \geqslant 1$. Thus the λ_i are nilpotent and so are equal to 0 for $i \geqslant 1$.
Now if C and C' are two subalgebra of R verifying Hypothesis 2.1.49 then again by using Theorem 2.1.48 we see that for all prime ideal $\mathfrak{p}$ of $\mathcal{Z}$, $N_{R/C} = N_{R/C'} \mod \mathfrak{p}$. Since R has no nontrivial nilpotent element this means that $N_{R/C} = N_{R/C'}$. □

REMARK 2.1.53. — If $\mathcal{Z}$ is an integral domain then (ii) in Hypothesis 2.1.49 not necessary since in this case $N_{A/C} = \mathrm{Nrd}_{R\otimes_{\mathcal{Z}}\mathrm{Frac}(\mathcal{Z})|R}$.

LEMMA 2.1.54. — *Let R be a Azumaya algebra over $\mathcal{Z}$ verifying Hypothesis 2.1.49 of dimension n^2. Then:*

- *For any $a \in \mathcal{Z}$, $\mathrm{Nrd}_R(a) = a^n$.*
- *For all $r, q \in R, \mathrm{Nrd}_R(rq) = \mathrm{Nrd}_R(r)\mathrm{Nrd}_R(q)$.*

Proof.
- For any subalgebra C verifying the conditions of Hypothesis 2.1.49, the matrix of the multiplication by a is the scalar matrix whose diagonal elements are a.
- This is an immediate consequence of the multiplicative properties of the determinant.

□

The reduced norm of an Azumaya algebra verifying Hypothesis 2.1.49 has many more properties which are true in general. For example, it can be shown that for any $r \in R$, $\mathrm{Nrd}_R(r)$ is a multiple of r. One way to show this is to introduce the adjoint of r, which is locally defined as the adjoint matrix of r, which verifies $x \cdot \mathrm{adj}(x) = \mathrm{Nrd}(r)$.
We choose not to take this path in this document and will only show those results for some specific Azumaya algebras ($\mathcal{A}\langle\partial\rangle$ and $A(\theta)\langle\Phi^{\pm 1}\rangle$, see section 2.3).

2.2 Central elements and p-curvature.

Now that all the most essential elements of the theory of differential equations, both in positive characteristic and otherwise, have been set we can talk about the p-curvature and its various applications, in particular to the factorisation of differential operators.

In this section we suppose that $\mathcal{A}$ is a field of characteristic p verifying Hypothesis 2.1.37. As a consequence, $\mathcal{C}$, its ring of constant, is also a field.
As we have seen, the ring of differential operators being a finite dimensional free algebra over its centre in characteristic p is what sets it apart from the case of characteristic 0. One of the consequences of this fact is that any nonzero differential operator is a divisor of some central operator. Since $\mathcal{C}[\partial^p]$ is isomorphic to a ring of classic polynomials, classical factorisation algorithms can be applied to it. One can wonder whether polynomial factorisations of a central element can be used to factor divisors of this central element. In [vdP95], van der Put used this idea to produce a classification of differential modules in positive characteristic and later, in an unpublished manuscript [vdP97], used his previous work to design an (incomplete) algorithm for factorisation. In both his works, an important step is to reduce the problem to the case of "isotypical" operators, that is to say operators which are divisor of a central elements with only one irreducible component (when viewed as a polynomial). We begin by showing how that is

done.

Let $L \in \mathcal{A}\langle\partial\rangle$ be a linear differential operator. Then one can consider $\mathcal{D}_L := {}^{\mathcal{A}\langle\partial\rangle}\big/_{\mathcal{A}\langle\partial\rangle L}$. $\mathcal{D}_L$ is in particular a $\mathcal{A}$-vector space of dimension $\mathrm{ord}(L)$, and a $\mathcal{C}$-vector space of finite dimension $p \cdot \mathrm{ord}(L)$. Thus the morphism of $\mathcal{C}[\partial^p]$-module

$$\begin{array}{ccc} \mathcal{C}[\partial^p] & \to & \mathcal{D}_L \\ N & \mapsto & N \mod L \end{array}$$

has a nontrivial kernel of the form $\chi_{min}(L)(\partial^p)\mathcal{C}[\partial^p]$, with $\chi_{min}(L) \in \mathcal{C}[Y]$. This proves the aforementioned result:

Lemma 2.2.1. — *For any $L \in \mathcal{A}\langle\partial\rangle$, there exists $N \in \mathcal{C}[Y]$ such that L is a divisor of $N(\partial^p)$. We denote by $\chi_{min}(L)$ such a monic N of smallest degree.*

Remark 2.2.2. — L is both a right and left divisor of $N(\partial^p)$. Indeed we have shown that there exists $R \in \mathcal{A}\langle\partial\rangle$ such that

$$RL = N(\partial^p)$$

But then we have

$$\begin{aligned} N(\partial^p)L &= RL^2 \\ &= LN(\partial^p) \text{ since } N(\partial^p) \text{ is central} \\ &= LRL \end{aligned}$$

Thus we find that $(RL - LR)L = 0$ and since $\mathcal{A}\langle\partial\rangle$ has no nontrivial zero divisor, $LR = RL = N(\partial^p)$ so L is also a left divisor.

It is easy to see that $\chi_{min}(L)$ is actually the minimal polynomial of the multiplication by ∂^p on $\mathcal{D}_L$, seen as a $\mathcal{C}$-linear map:

$$\begin{array}{cccc} \psi_p^L : & \mathcal{D}_L & \longrightarrow & \mathcal{D}_L \\ & L' \mod L & \mapsto & \partial^p \cdot L' \mod L \end{array}. \tag{2.2}$$

Indeed if $N(\partial^p)$ is a multiple of L then for any $L' \in \mathcal{D}_L$, $N(\psi_p^L)(L') = L' \cdot N(\partial^p) \equiv 0 \mod L$. Thus $\chi_{min}(L)$ is a multiple of the minimal polynomial of ψ_p^L. Conversely, if P is such that $P(\psi_p^L) = 0$ then $P(\partial^p) \mod L = P(\psi_p^L)(1) \equiv 0 \mod L$. Thus the minimal polynomial of ψ_p^L is a multiple of $\chi_{min}(L)$.

ψ_p^L is actually a $\mathcal{A}\langle\partial\rangle$-endomorphism, in particular it is a $\mathcal{A}$-linear map. One might then be inclined to take a look at its minimal polynomial over $\mathcal{A}$. The following result states that it actually makes no difference.

Lemma 2.2.3. — *Let M be a finite dimensional differential $\mathcal{A}$-module and φ be a differential endomorphism of M. There exists a suitable differential field extension ξ of $\mathcal{A}$ and a ξ-basis $\mathcal{B}$ of $M \otimes_{\mathcal{A}} \xi$ such that $\mathrm{Mat}_{\mathcal{B}}(\varphi \otimes_{\mathcal{A}} \mathrm{Id}_\xi)$ has constant coefficients.*

Proof. Let ξ be a differential extension of $\mathcal{A}$ such that $M \otimes_{\mathcal{A}} \xi$ admits a basis $(e_1, \ldots, e_n)$ of vectors such that $\partial \cdot e_i = 0$ for all i. The existence of such a differential extension is a

consequence of Picard-Vessiot theory in positive characteristic which was developed by Okugawa in 1962 [Oku62, Proposition 5.2]. Write

$$\varphi(e_i) = \sum_{j=1}^{n} \lambda_{i,j} e_j.$$

Then

$$\partial.\varphi(e_i) = \sum_{j=1}^{n} \partial(\lambda_{i,j}) e_j + \lambda_{i,j} \partial \cdot e_j = \sum_{j=1}^{n} \partial(\lambda_{i,j}) e_j.$$

But also

$$\partial \cdot \varphi(e_i) = \varphi(\partial \cdot e_i) = \varphi(0) = 0.$$

Thus $\varphi \otimes_{\mathcal{A}} \mathrm{Id}_\xi$ has constant coefficients in the basis $(e_1, \ldots, e_n)$.

□

It follows that any $\mathcal{A}\langle\partial\rangle$-endomorphism of a finite dimensional differential module has a minimal polynomial, a characteristic polynomial and Frobenius invariants with coefficients in $\mathcal{C}$ which proves the following result:

COROLLARY 2.2.4. — *Let M be a finite dimensional differential $\mathcal{A}$-module and φ be a differential endomorphism of M. Then there exists a basis of M in which the matrix of φ has constant coefficient.*

In particular ψ_p^L, when viewed has a $\mathcal{A}$-endomorphism, is equivalent to a matrix with coefficients in $\mathcal{C}$, and its minimal polynomial over $\mathcal{C}$ is equal to its minimal polynomial over $\mathcal{A}$. In particular

$$\deg(\chi_{min}(L)) \leqslant \mathrm{ord}(L).$$

ψ_p^L thus plays a very important role in our and in van der Put's work (as well as Cluzeau's) and in general in the theory of linear differential equations in characteristic p.

DEFINITION 2.2.5. — Let $L \in \mathcal{A}\langle\partial\rangle$. The endomorphism ψ_p^L defined in (2.2) is called the p-curvature of L.

Amongst its various interesting properties, Cartier showed that L has a basis of solutions in $\mathcal{A}$ if and only if its p-curvature is zero [vdPS03, Lemma 13.2]. Furthermore, if $\mathcal{B}$ is a differential field extension of $\mathcal{A}$ verifying Hypothesis 2.1.37 then the p-curvature of L over $\mathcal{B}$ is just $\psi_p^L \otimes_{\mathcal{A}} \mathrm{Id}_{\mathcal{B}}$. This implies that the following propositions are equivalent:

i) L has a basis of solutions in $\mathcal{A}$.

ii) L has a basis of solutions in a separable closure of $\mathcal{A}$.

iii) L has a basis of solutions in any differential field extension of $\mathcal{A}$ verifying Hypothesis 2.1.37.

iv) $\psi_p^L = 0$.

REMARK 2.2.6. — Note that "a basis of solutions" is always meant as a basis of solutions over the field of constants which varies with the base field.

The p-curvature is thus an important tool to detect the algebraic character of the solutions of a differential operators and enables us to solve this question way easier than in characteristic 0. A most important conjecture in the algebraic theory of differential equations is the Grothendieck-Katz conjecture [Kat82] which states that the solutions of an operator L in $\mathbb{Q}(z)\langle\partial\rangle$ are algebraic if and only if $L \mod p$ has an algebraic basis of solutions for almost all primes p (meaning all but a finite number).
Another example of the interest of the p-curvature, even for operators of characteristic 0 comes from André-Chudnovsky-Katz theorem which states that vanishing operators L of minimal order in $\mathbb{Q}(z)\langle\partial\rangle$ for functions of a certain type ($\mathcal{G}$-functions) are globally nilpotent [And89], which is to say that $\psi_p^L \mod p$ is nilpotent for almost all primes p. Moreover, it is well known that the nilpotent character of an endomorphism can be determined solely from its characteristic polynomial.

In his work on factorisation, van der Put focuses on the minimal polynomial of the p-curvature of L. While the reason for this are understandable, in our work we will be more interested in its characteristic polynomial which, while it doesn't verify the minimality condition, has very interesting properties, among which multiplicativity. It is also tightly connected to the reduced norm of $\mathcal{A}\langle\partial\rangle$ induced by its Azumaya algebra structure (see Theorem 2.3.26), structure used by van der Put for his classification of differential modules [vdP95].

Definition 2.2.7. — Let $L \in \mathcal{A}\langle\partial\rangle$. The characteristic polynomial of its p-curvature, seen as a $\mathcal{A}$-linear map, is denoted by $\chi(\psi_p^L)$

Proposition 2.2.8. — *The following facts are true:*

i) *Let $L \in \mathcal{A}\langle\partial\rangle$. L is a left and right divisor of $\chi(\psi_p^L)(\partial^p)$ and $\deg(\chi(\psi_p^L)) = \operatorname{ord}(L)$.*

ii) *The map $L \mapsto \chi(\psi_p^L)$ is multiplicative.*

iii) *If $L \in \mathcal{A}\langle\partial\rangle$ is irreducible then $\chi(\psi_p^L)$ is a power of an irreducible polynomial.*

iv) *If L is central then $\chi(\psi_p^L)(\partial^p) = L^p$.*

Proof. [BCS14, section 3.1] (i) is a direct consequence of the above discussion. Indeed the minimal polynomial of the p-curvature of L is equal to $\chi_{min}(L)$. Since $\chi(\psi_p^L)(\partial^p)$ is central every right divisor is also a left divisor.
Let $L = L_1 L_2$. Then we have a map

$$\begin{array}{rccc} \varphi : & \mathcal{D}_{L_1} & \to & \mathcal{D}_L \\ & L' \mod L_1 & \mapsto & L'L_2 \mod L \end{array}$$

and

$$0 \to \mathcal{D}_{L_1} \xrightarrow{\varphi} \mathcal{D}_L \xrightarrow{\pi} \mathcal{D}_{L_2} \to 0$$

is an exact sequence. Then the multiplication by ∂^p induces an endomorphism of this exact sequence. This means that in a good $\mathcal{A}$-basis of $\mathcal{D}_L$ the matrix of ψ_p^L is

$$\begin{pmatrix} \psi_p^{L_1} & * \\ 0 & \psi_p^{L_2} \end{pmatrix}$$

and so $\chi(\psi_p^L) = \chi(\psi_p^{L_1})\chi(\psi_p^{L_2})$ which proves (ii). Let now suppose that L is irreducible and assume that $\chi(\psi_p^L)$ has two distinct irreducible divisor N_1 and N_2. Then L is coprime with $N_1(\partial^p)$ or $N_2(\partial^p)$. Assume that L is coprime with $N_1(\partial^p)$. This means that the multiplication by $N_1(\partial^p)$ defines an invertible endomorphism of $\mathcal{D}_L$. But this is in direct contradiction with N_1 being an irreducible factor of the characteristic polynomial of ψ_p^L so (iii) holds.
To prove (iv), suppose that $L = N(\partial^p)$ with $N \in \mathcal{C}[Y]$ then $\chi_{min}(L) = N$. Since the characteristic polynomial of the p-curvature is a multiplicative map, it is enough to prove it when N is irreducible. In this case, it follows that $\chi(\psi_p^L)$ is a power of N with

$$\deg(\chi(\psi_p^L)) = \operatorname{ord}(L) = p\deg(N).$$

We get $\chi(\psi_p^L) = N^p$ and $\chi(\psi_p^L)(\partial^p) = L^p$. □

THEOREM 2.2.9. — *Let $L \in \mathcal{A}\langle\partial\rangle$. Write $\chi(\psi_p^L) = N_1^{\nu_1}\cdots N_n^{\nu_n}$ where the N_i are pairwise distinct irreducible polynomials in $\mathcal{C}[Y]$. Then there exists a factorisation $L = L_1\cdots L_n$ with:*

i) $\chi(\psi_p^{L_i}) = N_i^{\nu_i}$ *for all* $i \in [\![1;n]\!]$.

ii) $L_n = \operatorname{gcrd}(L, N_n^{\nu_n}(\partial^p))$.

Proof. As per the kernel decomposition lemma we find that

$$\mathcal{D}_L = \bigoplus_{i=1}^{n} \ker N_i^{\nu_i}(\psi_p^L).$$

We proceed by induction on n. First notice that $\chi(\psi^L_{p|\ker N_n^{\nu_n}(\psi_p^L)}) = N_n^{\nu_n}$. Furthermore, since $\ker N_n^{\nu_n}(\psi_n^L)$ is isomorphic to a quotient module of $\mathcal{D}_L$, it is of the form $\mathcal{D}_{L_n}$ with L_n being a right divisor of L, and $\chi(\psi_p^{L_n}) = N_n^{\nu_n}$. It follows that L_n is a common right divisor of L and $N_n^{\nu_n}(\partial^p)$, so it divides $\operatorname{gcrd}(L, N_n^{\nu_n}(\partial^p))$. We can write $\operatorname{gcrd}(L, N_n^{\nu_n}(\partial^p)) = L'_nL_n$ and $L = ML'_nL_n$. Then if L'_n was not of order 0 then $N_n^{\nu_n+1}$ would divide $\chi(\psi_p^L)$ which is not true. We can thus suppose $L'_n = 1$ and $L_n = \operatorname{gcrd}(L, N_n^{\nu_n}(\partial^p))$.
Thus we have $L = ML_n$ with $\chi(\psi_p^M) = N_1^{\nu_1}\cdots N_{n-1}^{\nu_{n-1}}$ and we conclude by induction. □

REMARK 2.2.10. — One can see that this first factorisation comes from the decomposition of $\mathcal{D}_L$ as a direct sum of submodules. This induces another type of factorisation as the least common left multiple of fully coprime operators (see Definition 3.5.3) as follow

$$L = \operatorname{lclm}_{i=1}^{n}(\operatorname{gcrd}(L, N_i^{\nu_i}(\partial^p)))$$

This first factorisation comes from a decomposition of $\mathcal{D}_L$ as a direct sum of submodules. Its factors are not irreducible in general, and it is not possible to obtain a more refined decomposition of this sort solely from a factorisation of $\chi(\psi_p^L)$ or $\chi_{min}(L)$. In his works on the classification of differential modules [vdP95] and factorisation [vdP97], van der Put works directly on this reduction, as does Cluzeau in [Clu03] for the analog decomposition on differential systems. Our concern being, for now, to find a simple factorisation of linear differential operators, we allow ourselves a small refinement of this first factorisation which in general does not correspond to a decomposition of $\mathcal{D}_L$ as a direct sum of submodules:

THEOREM 2.2.11. — *Let $L \in \mathcal{A}\langle\partial\rangle$ and suppose that $\chi(\psi_p^L) = N_1\cdots N_n$ with the N_i being irreducible polynomials in $\mathcal{C}[Y]$, not necessarily pairwise distinct. Then there exists a factorisation $L = L_1\cdots L_m$ with:*

i) for any $i \in [\![1; m]\!]$ there exists $j \in [\![1; n]\!]$ such that L_i is a divisor of $N_j(\partial^p)$.

ii) $L_m = \mathrm{gcrd}(L, N_n(\partial^p))$.

Proof. We actually show a more general result, replacing $\chi(\psi_p^L)$ with any vanishing polynomial of ψ_p^L over $\mathcal{C}$. In practice we will only apply it to $\chi(\psi_p^L)$ in our algorithm.
Let $N = N_1 \cdots N_n \in \mathcal{C}[Y]$ be such that $N(\partial^p)$ is a multiple of L. Set $L_m = \mathrm{gcrd}(L, N_n(\partial^p))$ and $L = L'_m L_m$. Let us show that $N' = N_1 \cdots N_{n-1}$ is a vanishing polynomial of $\psi_p^{L'_m}$.
We have the exact sequence

$$0 \to \mathcal{D}_{L'_m} \to \mathcal{D}_L \to \mathcal{D}_{L_m} \to 0.$$

In particular $\mathcal{D}_{L'_m} \simeq \mathcal{D}_L L_m$. Furthermore $\mathcal{D}_L L_m = \mathrm{Im}\,(N_n(\psi_p^L))$ which comes from the Bezout relation. It follows that

$$\begin{aligned} N'(\psi_p^L)(\mathcal{D}_{L'_m}) &= N'(\psi_p^L)(\mathcal{D}_L L_m) \\ &= N'(\psi_p^L)(N_n(\psi_p^L)(\mathcal{D}_L)) \\ &= N(\psi_p^L)(\mathcal{D}_L) \\ &= 0 \end{aligned}$$

We conclude by recurrence on n. □

The factors of this second decomposition are still not irreducible in general but the problem of factorisation is now reduced to the case of a divisor L of some $N(\partial^p)$ with N being an irreducible polynomial over $\mathcal{C}$. In the next chapter 3 we will use the already established structure of Azumaya algebra (theorem 2.1.45) of $\mathcal{A}\langle\partial\rangle$ to study the structure of $\mathcal{D}_L$ (as was done by van der Put in [vdP95]).

We have seen that the p-curvature and in particular its characteristic polynomial are very important tools for the study of differential operators, in characteristic p for example in the perspective of factorisation, but also in characteristic zero as illustrated by the conjecture of Grothendieck-Katz or the theorem of Chudnovsky-Chudnovsky. While fast algorithms to compute the characteristic polynomial of the p-curvature of a given operator of characteristic p exist, among which Bostan, Caruso and Schost's algorithm [BCS14], another interesting algorithmic question is the way of computing the characteristic polynomials of the p-curvatures of a given operator L in characteristic 0 for a large amount of primes p.
In the following sections we present an algorithm tackling this question.

2.3 p-curvatures and reduced norm

In this section we lay down some theory around the characteristic polynomial of the p-curvature which we will use to build an algorithm computing the characteristic polynomials of the p-curvatures of the reductions modulo p of a given differential operator in characteristic 0, for all primes p less than a given integer N, in quasilinear time with regard to N.

The most commonly known algorithm to compute the p-curvature of a differential module is due to Katz (and is often referred to as Katz algorithm [vdPS03, p. 324]) and rely on the following result:

LEMMA 2.3.1. — *Suppose that $\mathcal{A}$ is a differential field of characteristic p verifying Hypothesis 2.1.37. Let $L \in \mathcal{A}\langle\partial\rangle$ of order r and M be the companion matrix of L. We set $M_1 = M$ and*

$$M_{i+1} = M_i' + M \cdot M_i$$

Then the matrix of the p-curvature in the $\mathcal{A}$-basis $\mathcal{B} = (1, \partial, \cdots, \partial^{r-1})$ of $\mathcal{D}_L$ is given by M_p.

Proof. Let $\mathcal{B} = (e_0, \ldots, e_{r-1})$ be the canonical basis of $\mathcal{D}_L$, such that e_i is the image in $\mathcal{D}_L$ of ∂^i. We claim that $M_i \cdot e_j$ is the image of $\partial^{i+j} \mod L$ written in the basis $\mathcal{B}$. This is obvious for $i = 1$. If now Y is an element of $\mathcal{D}_L$ represented by the vector $\tilde{Y}$ in the basis $\mathcal{B}$, then $\partial \cdot Y$ is represented by the vector $\tilde{Y}' + M\tilde{Y}$ as per the Leibniz rule. Note that $\tilde{Y}'$ denote the derivative of $\tilde{Y}$ coefficient-wise. Thus if $M_i \cdot e_j$ is the image of $\partial^{i+j} \mod L$ in the basis $\mathcal{B}$, then the image of $\partial^{(i+1)+j} \mod L$ in the basis $\mathcal{B}$ is given by

$$\begin{aligned}(M_i e_j)' + M \cdot M_i \cdot e_j &= (M_i' e_j + M \cdot M_i) \cdot e_j \\ &= M_{i+1} \cdot e_j\end{aligned}$$

It follows that M_p is the matrix whose columns are precisely the image of $\partial^{p+j} \mod L$ written in $\mathcal{B}$, for $j \in [\![0; r-1]\!]$ which is by definition the matrix of the p-curvature of L in $\mathcal{B}$. □

EXAMPLE 2.3.2. — Let $L = (x+1)^2\partial^3 - x\partial + x^3 \in \mathbb{F}_3(x)\langle\partial\rangle$. Then the matrix of ψ_p^L in the canonical basis of $\mathcal{D}_L$ is given by

$$M_p = \begin{pmatrix} \frac{2x^3}{x^2+2x+1} & \frac{2x^3}{x^3+1} & \frac{2x^4}{x^4+x^3+x+1} \\ \frac{x}{x^2+2x+1} & \frac{2x^4+2x^3+2x+1}{x^3+1} & \frac{x^4+x^3+x^2+2x+2}{x^4+x^3+x+1} \\ 0 & \frac{x}{x^2+2x+1} & \frac{2x^4+2x^3+x+2}{x^3+1} \end{pmatrix}.$$

We find

$$\chi(\psi_p^L) = Y^3 + \frac{2}{x^3+1}Y + \frac{x^6+2x^3}{x^3+1}.$$

From here, one can just compute the characteristic polynomial of M_p if that is what one is interested in. Katz algorithm teaches us some things on the size of the p-curvature of an operator. Indeed if L is a differential operator in $A(x)\langle\partial\rangle$ of size $O(1)$, one can easily check that the entries of M_i are rational functions over A of degree $O(i)$. It follows that the matrix of the p-curvature in the canonical basis of $\mathcal{D}_L$ is of size $O(p)$.

REMARK 2.3.3. — The meaning of "size" can be a bit unclear. Here we mean by it the number of elements of A necessary to represent the object considered. Furthermore here the notations $O(1)$ and $O(p)$ hide the dependence in secondary parameters, such as the order of the operator L or the degree of its coefficients.

As previously said, it follows that Katz algorithm computes the p-curvature, and subsequently its characteristic polynomial, in $O(p^2)$ operations in A. However we know from Corollary 2.2.4 that $\chi(\psi_p^L)$ has coefficients in $A[x^p]$ and so can be represented by $O(1)$ elements in A. The best known algorithm to compute its characteristic polynomial finishes in $\tilde{O}(\sqrt{p})$ operations in A [BCS14]. Whether or not the 1/2-exponent is optimal is still an open question. Regarding the goal of this chapter, one can see that the simple iteration of this last algorithm would yield the desired result in $\tilde{O}(N^{3/2})$ operations in A.

Our algorithm is a combination of the ideas from [BCS14] and those from [Har14] for factorial computations. In order to use this algorithm we need to introduce a new ring of operator. From now on we assume that $\mathcal{A}$ is of the form $A[x]$ or $A(x)$ with A an integral domain as in Example 2.1.39

DEFINITION 2.3.4. — We define the ring of skew polynomials $A(\theta)\langle\Phi\rangle$ (resp. $A[\theta]\langle\Phi\rangle$) as the set of Ore polynomials $A(\theta)[\Phi, \theta \mapsto \theta + 1, 0]$ (resp. $A[\theta][\Phi, \theta \mapsto \theta + 1, 0]$).
The multiplication verifies the following commutation rule:

$$\Phi\theta = (\theta + 1)\Phi.$$

These rings share a number of similar properties with $\mathcal{A}\langle\partial\rangle$. Besides the properties common to all rings of Ore polynomials, the ring of skew polynomials is also a finite dimensional algebra over its centre of dimension p^2 as we now show:

LEMMA 2.3.5. — *The centre of $A(\theta)\langle\Phi\rangle$ (resp. $A[\theta]\langle\Phi\rangle$) is $A(\theta^p - \theta)[\Phi^p]$ (resp. $A[\theta^p - \theta][\Phi^p]$)*

Proof. Let $L = \sum_{k=0}^{n} f_k(\theta)\Phi^K$ be a central element of $A(\theta)\langle\Phi\rangle$. Then $L\theta - \theta L = 0$. But

$$\begin{aligned} L\theta - \theta L &= \sum_{k=0}^{n} f_k(\theta)(\Phi^k\theta - \theta\Phi^k) \\ &= \sum_{k=0}^{n} (\theta + k - \theta) f_k(\theta)\Phi^k \\ &= \sum_{k=0}^{n} k f_k(\theta)\Phi^k \end{aligned}$$

We deduce that $f_k(\theta) \neq 0$ is and only if $p|k$.
Furthermore since L is central we have $L\Phi - \Phi L = 0$. But

$$L\Phi - \Phi L = \sum_{k=0}^{n} (f_k(\theta) - f_k(\theta + 1))\Phi^{k+1}$$

It follows that for all k, $f_k(\theta) = f_k(\theta + 1)$. Let $A(\theta)^\Phi$ be the subfield of $A(\theta)$ invariant under the morphism $\theta \mapsto \theta + 1$. We see that $A(\theta^p - \theta) \subset A(\theta)^\Phi$. But since $[A(\theta) : A(\theta^p - \theta)] = p$ and $A(\theta)^\Phi \neq A(\theta)$ it follows that $A(\theta^p - \theta) = A(\theta)^\Phi$.
Thus $L \in A(\theta^p - \theta)[\Phi^p]$. If furthermore $L \in A[\theta]\langle\Phi\rangle$ then $L \in A(\theta^p - \theta)[\Phi^p] \cap A[\theta]\langle\Phi\rangle = A[\theta^p - \theta][\Phi^p]$.
Furthermore we see that any element of $A(\theta^p - \theta)[\Phi^p]$ is central.
Finally a basis of the ring of skew polynomials over its centre is given by $(\theta^i\Phi^j)_{i,j\in[\![0;p-1]\!]}$. □

While an analog of Theorem 2.1.45 is not true on the ring of skew polynomials as is, we only need to introduce an inverse to Φ for it to work.

EXAMPLE 2.3.6. — $\{\sum_{k=1}^{p-1} f_k\Phi^k | f_k \in A(\theta)\}$ is a nontrivial two-sided ideal of ${}^{A(\theta)\langle\Phi\rangle}/_{\Phi^p}$. This is a counterexample of why $A(\theta)\langle\Phi\rangle$ is not an Azumaya algebra in the sense of Definition 2.1.44.

DEFINITION 2.3.7. — We denote by $A(\theta)\langle\Phi^{\pm 1}\rangle := A(\theta)\langle\Phi\rangle \otimes_{A(\theta^p-\theta)[\Phi^p]} A(\theta^p - \theta)[\Phi^{\pm p}]$
(resp. $A[\theta]\langle\Phi^{\pm 1}\rangle := A[\theta]\langle\Phi\rangle \otimes_{A[\theta^p-\theta][\Phi^p]} A[\theta^p - \theta][\Phi^{\pm p}]$).

REMARK 2.3.8. — We will then use the notation Φ^{-k} for $\Phi^{pk'-k} \cdot \Phi^{-pk'}$ where k' is such that $pk' \geqslant k$. This notation is justified as Φ^{-k} is the inverse of Φ^k.

THEOREM 2.3.9. — *$A(\theta)\langle\Phi^{\pm 1}\rangle$ (resp. $A[\theta]\langle\Phi^{\pm 1}\rangle$) is an Azumaya algebra over $A(\theta^p-\theta)[\Phi^{\pm p}]$ (resp. $A[\theta^p-\theta][\Phi^{\pm p}]$) in the sense of Definition 2.1.44.*

Proof. As in the proof of Theorem 2.1.45 we show that we can suppose that we are working on $A(\theta)\langle\Phi^{\pm 1}\rangle$. We denote

$$\mathcal{D}_{\mathfrak{p}} := A(\theta)\langle\Phi^{\pm 1}\rangle \otimes_{A(\theta^p-\theta)[\Phi^{\pm p}]} \mathrm{Frac}(A(\theta^p-\theta)[\Phi^{\pm p}]/\mathfrak{p}).$$

Let $\pi : A(\theta)\langle\Phi\rangle \to \mathcal{D}_{\mathfrak{p}}$ be the natural morphism.

Let I be a two-sided ideal of $\mathcal{D}_{\mathfrak{p}}$ and $\tilde{I} = \pi^{-1}(I)$. $\tilde{I}$ is a two-sided ideal of $A(\theta)\langle\Phi\rangle$ not containing Φ^p. Let L be a generator of $\tilde{I}$ and set $L = \sum_{k=0}^{n} f_k(\theta)\Phi^k$ with $f_n(\theta) \neq 0$. With no loss of generality, we can suppose that $f_n = 1$.
Since $\tilde{I}$ is two sided ideal of $A(\theta)\langle\Phi\rangle$, $L\theta - \theta L \in \tilde{I}$. In particular L is a right divisor of $L\theta - \theta L$. But

$$L\theta - \theta L = \sum_{k=0}^{n} k f_k(\theta)\Phi^k.$$

Thus $\mathrm{ord}(L\theta - \theta L) \leqslant \mathrm{ord}(L)$. It follows that we have $L\theta - \theta L = nL$. But then we must have $nf_k(\theta) = kf_k(\theta)$ which is to say that $(n-k)f_k(\theta) = 0$ for all k. Thus we either have $f_k(\theta) = 0$ or $p|n-k$. It follows that L is of the form $\sum_{k=0}^{n'} f_{pk+\lambda}(\theta)\Phi^{pk+\lambda}$ for some λ and k'. But then λ must be equal to 0 since Φ is invertible in $\mathcal{D}_{\mathfrak{p}}$, otherwise $L' = \sum_{k=0}^{n'} f_{pk}(\theta)\Phi^{pk}$ would be an element of $\tilde{I}$ of lesser order than L.
But since $\Phi^{pk}\theta = \theta\Phi^{pk}$ for all $k \in \mathbb{Z}$, $L\theta - \theta L = 0$.

Furthermore we have $\Phi L - L\Phi \in \tilde{I}$. But

$$\Phi L - L\Phi = \sum_{k=0}^{n} (f(\theta+1) - f(\theta))\Phi^{k+1}.$$

Again, since Φ is invertible in $\mathcal{D}_{\mathfrak{p}}$, $L' = \sum_{k=0}^{n}(f_k(\theta+1) - f_k(\theta))\Phi^k \in \tilde{I}$. Since we assumed that $f_n(\theta) = 1$, it follows that $\mathrm{ord}(L') \leqslant n-1$. Thus $L' = 0 = \Phi L - L\Phi$.
This means that L is in the centre of $A(\theta)\langle\partial\rangle$. But then, $\mathfrak{p}$ is either equal to zero, in which case L is either equal to zero or is invertible in $A(\theta^p-\theta)(\Phi^p)$, or is of the form $A(\theta^p-\theta)[\Phi^{\pm p}]N(\Phi^p)$ where N is an irreducible polynomial over $A(\theta^p-\theta)$. Then L is again either invertible modulo $N(\Phi^p)$ or is equal to 0 mod $N(\Phi^p)$. Thus I is either equal to 0 or to $\mathcal{D}_{\mathfrak{p}}$.

We now show that $\mathcal{D}_{\mathfrak{p}}$ is central. The case when $\mathfrak{p} = 0$ is the same as the differential case. Suppose that $\mathfrak{p}$ is of the form $N(\Phi^p)$ with N an irreducible polynomial over $A(\theta^p-\theta)$ of degree n and let $\overline{L}$ be an element of its centre. Let $L = \sum_{k=0}^{pn-1} l_k(\theta)\Phi^k$ be a lift of $\overline{L}$ in $A(\theta)\langle\partial\rangle$ of order strictly less than pn. Then $L\theta - \theta L$ is a multiple of $N(\Phi^p)$. But since it is of order strictly less than pn, it must be equal to 0. Thus $L \in A(\theta)[\Phi^p]$.
Furthermore $(\Phi\overline{L} - \overline{L}\Phi)\cdot\Phi^{-1} = 0 \mod N(\Phi^p)$. But a lift of $(\Phi\overline{L} - \overline{L}\Phi)\cdot\Phi^{-1}$ is given by

$$\sum_{k=0}^{pn-1} (l_k(\theta+1) - l_k(\theta))\Phi^k$$

of order strictly less than pn. It follows that

$$\sum_{k=0}^{pn-1}(l_k(\theta+1)-l_k(\theta))\Phi^k = 0$$

and thus $\Phi L - L\Phi = \left(\sum_{k=0}^{pn-1}(l_k(\theta+1)-l_k(\theta))\Phi^k\right)\Phi = 0$.
Thus L is a central element of $A(\theta)\langle\Phi\rangle$ and $\overline{L} \in {}^{A(\theta^p-\theta)[\partial^{\pm p}]}/_{\mathfrak{p}}$. □

Finally we can define the p-curvature of a skew polynomial in $A(\theta)\langle\Phi\rangle$ in a perfectly analogous way to what we did for differential operators:

DEFINITION 2.3.10. — Let $L \in A(\theta)\langle\Phi\rangle$. We define the p-curvature of L as the $A(\theta)$-endomorphism:

$$\begin{array}{rccc} \Lambda_p^L : & {}^{A(\theta)\langle\Phi\rangle}/_{A(\theta)\langle\Phi\rangle L} & \to & {}^{A(\theta)\langle\Phi\rangle}/_{A(\theta)\langle\Phi\rangle L} \\ & Q \mod L & \mapsto & \Phi^p Q \mod L \end{array}.$$

Like for differential operators, we can draw a simple algorithm to compute this p-curvature.

LEMMA 2.3.11. — *Let $L \in A(\theta)\langle\Phi\rangle$ be a skew polynomial and let $B(\theta)$ be its companion matrix. Then the matrix of the p-curvature of L in the canonical basis of ${}^{A(\theta)\langle\Phi\rangle}/_{A(\theta)\langle\Phi\rangle L}$ is given by*

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

Proof. Let $B_i = B(\theta)B(\theta+1)\cdots B(\theta+i-1)$. Let $e_j =^t (0\cdots 0,1,0\cdots 0)$ be the vector representing $\Phi^j \mod L$ (for $j < \mathrm{ord}(L)$) in the canonical basis of ${}^{A(\theta)\langle\Phi\rangle}/_{A(\theta)\langle\Phi\rangle L}$. For the sake of simplicity we identify elements of ${}^{A(\theta)\langle\Phi\rangle}/_{A(\theta)\langle\Phi\rangle L}$ to their representation in the canonical basis. As for differential operators we claim that $\Phi^{j+i} \mod L = B_i e_j$. This is easy to see for $i = 1$. Now for any $f(\theta) \in A(\theta)$,

$$\Phi f(\theta)\Phi^j \mod L = f(\theta+1)\Phi^{i+1} \mod L = f(\theta+1)B(\theta)e_j.$$

It follows that for any $Y(\theta) \in {}^{A(\theta)\langle\Phi\rangle}/_{A(\theta)\langle\Phi\rangle L}$,

$$\Phi Y(\theta) \mod L = B(\theta)Y(\theta+1).$$

Finally we get that

$$\begin{aligned} \Phi^{i+j} &= \Phi\Phi^{i-1+j} \\ &= \Phi\cdot(B(\theta)B(\theta+1)\cdots B(\theta+i-2)e_j) \\ &= B(\theta)\cdot(B(\theta+1)B(\theta+2)\cdots B(\theta+i-1)e_j) \end{aligned}$$

□

Unlike the differential case, this formula directly provides a quasi-optimal (with regard to p) algorithm to compute Λ_p^L. Indeed a simple divide and conquer algorithm allows us to compute products of n matrices in $M_n(A(\theta))$ in $\tilde{O}(n)$ operations in A (considering each matrix to be of size $O(1)$). Furthermore, if one is only interested in computing Λ_p^L modulo some power of θ, baby-steps giant-steps methods can compute matrix factorials of size n (Λ_p^L is a matrix factorial of length p) in $\tilde{O}(\sqrt{n})$ operations in A. This principle is what is used in [BCS14] to compute the characteristic polynomial of the p-curvature of differential operators in $\mathbb{F}_{p^n}(x)\langle\partial\rangle$ in $\tilde{O}(\sqrt{p})$ binary operations.

Notation 2.3.12. Let $L \in A(\theta)\langle\Phi\rangle$ be a skew polynomial. We denote by $\chi(\Lambda_p^L)$ the characteristic polynomial of its p-curvature Λ_p^L.

The characteristic polynomial of Λ_p^L has analogous properties to that of the p-curvature of differential operators:

PROPOSITION 2.3.13. — *The following facts are true:*

i) Let $L \in A(\theta)\langle\Phi\rangle$. L is a left and right divisor of $\chi(\Lambda_p^L)(\Phi^p)$ and $\deg(\chi(\psi_p^L)) = \operatorname{ord}(L)$.

ii) The map $L \mapsto \chi(\Lambda_p^L)$ is multiplicative.

iii) If $L \in A(\theta)\langle\Phi\rangle$ is irreducible then $\chi(\Lambda_p^L)$ is a power of an irreducible polynomial.

iv) If L is central then $\chi(\Lambda_p^L)(\Phi^p) = L^p$.

Proof. The proof is the same as in the differential case (cf Proposition 2.2.8). □

Finally, in an analogous way to the case of differential operators we can show that $\chi(\Lambda_p^L)$ is invariant under the action of Φ.

LEMMA 2.3.14. — *Let $L \in A(\theta)\langle\Phi\rangle$. $\chi(\Lambda_p^L)$ the characteristic polynomial of the p-curvature of L has its coefficients in $A(\theta^p - \theta)$.*

Proof. We begin by showing that $\chi(\Lambda_p^{\Phi^i})(X) = X^i$. Indeed $\Lambda_p^{\Phi} = 0$ so $\chi(\Lambda_p^{\Phi})(X) = X$. Thus by multiplicativity $\chi(\Lambda_p^{\Phi^i})(X) = X^i$.
Since $M \mapsto \chi(\Lambda_p^M)$ is a multiplicative map we can suppose that L is not a multiple of Φ. Thus $B(\theta)$ the companion matrix of L is invertible since its characteristic polynomial has no root in 0, which means that $B(\theta)$ has a nonzero determinant. Let $B_p(\theta) = B(\theta)\dots B(\theta+p-1)$ be the matrix of Λ_p^L. Then

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

Thus $B_p(\theta+1)$ and $B_p(\theta)$ are equivalent matrices. It follows that $\chi(\Lambda_p^L)(\theta+1) = \chi(\Lambda_p^L)(\theta)$. Since the coefficients of $\chi(\Lambda_p^L)$ are invariant under $\theta \mapsto \theta+1$, it follows that those coefficients are in $A(\theta^p - \theta)$. □

REMARK 2.3.15. — We can actually show that Λ_p^L is equivalent to a matrix with coefficients in $A(\theta^p - \theta)$ but we will not need it for this work.

The reason we are so interested in this new ring of operators is the existence of the so-called Euler's operators $\theta = x\partial$. This operator verifies a familiar commutation rules with ∂:

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

The idea of our algorithm is thus the following: by mapping $x\partial$ to θ and ∂ to Φ we create a correspondence between differential operators and skew polynomials. The goal is thus to reduce the computation of the characteristic polynomials of the former to that of the latter. Of course, it is not clear for now that knowing the characteristic polynomial of the p-curvature of a skew polynomial would allow us to compute that of the corresponding differential polynomial.

Furthermore, not all differential operators can be converted into skew polynomials. For example x cannot be mapped to a skew polynomial in $A(\theta)\langle\Phi\rangle$. To solve this issue we need to introduce an inverse to ∂.
We recall that by hypothesis, $\mathcal{A}$ is either equal to $A(x)$ or to $A[x]$ where A is an integral domain.

DEFINITION 2.3.16. — We denote by $\mathcal{A}\langle\partial^{\pm 1}\rangle$ the ring

$$\mathcal{A}\langle\partial\rangle \otimes_{\mathcal{C}[\partial^p]} \mathcal{C}[\partial^{\pm p}]$$

where $\mathcal{C}[\partial^{\pm p}]$ is the localisation of $\mathcal{C}[\partial^p]$ in ∂^p.

All powers of ∂ are invertible in $\mathcal{A}\langle\partial^{\pm 1}\rangle$ since $\partial \cdot \frac{\partial^{p-1}}{\partial^p} = 1$.

Notation 2.3.17. We denote by ∂^{-k} the inverse of ∂^k in $\mathcal{A}\langle\partial^{\pm 1}\rangle$ for all k.

LEMMA 2.3.18. — *Let R be a ring and $\mathcal{Z}$ be its centre. Let $\mathcal{C} \subset \mathcal{Z}$ be a multiplicative subset of $\mathcal{Z}$ and B be another ring. If $\gamma : R \to B$ is a morphism which maps $\mathcal{C}$ to invertible elements of B then there exists a unique morphism $\tilde{\gamma}$ making the following diagram commute:*

$$\begin{array}{ccc} R & \xrightarrow{\gamma} & B \\ \downarrow & \overset{\tilde{\gamma}}{\nearrow} & \\ R \otimes_{\mathcal{Z}} \mathcal{C}^{-1}\mathcal{Z} & & \end{array}$$

Proof. By the universal property of $\mathcal{C}^{-1}\mathcal{Z}$ there exists a unique morphism $\gamma_1 : \mathcal{C}^{-1}\mathcal{Z} \to B$ which extend $\gamma_{|\mathcal{Z}}$. Then there exists a unique morphism $R \otimes_{\mathcal{Z}} \mathcal{C}^{-1}\mathcal{Z} \to B$ which maps pure tensor $b \otimes z$ to $\gamma(b)\gamma_1(z)$. □

REMARK 2.3.19. — The previous statement is a special case of localisation for noncommutative rings, when inverting central elements. If R is a (not necessarily commutative) ring and $S \subset R$ is a multiplicative subset of R, we say that a morphism $\iota : R \to R'$ is a localisation of R over S if and only if $\iota(S) \subset (R')^\times$ and if any morphism $\gamma : R \to B$ which maps S to invertible elements uniquely factorises in the following way:

$$\begin{array}{ccc} R & \xrightarrow{\gamma} & B \\ \downarrow{\scriptstyle \iota} & \overset{\tilde{\gamma}}{\nearrow} & \\ R' & & \end{array} .$$

Localisations of noncommutative rings always exist. They have however, no simple description in general like in the commutative case.

We say that $\iota : R \to R'$ is a right ring of fractions of R over S if

- $\iota(S) \subset R'^{-1}$.
- Every element of R' can be written as $\iota(r)\iota(s)^{-1}$ for some $r \in R$ and some $s \in S$.
- $\ker \iota = \{r \in R | \exists s \in S, rs = 0\}$.

Such a right ring of fractions does not always exists. However if it does then we can see that for any $s \in S$ and any $r \in R$ there must exists $r' \in R$ and $s' \in S$ such that

$$\iota(s)^{-1}\iota(r) = \iota(r')\iota(s')^{-1}$$

which means that

$$\iota(sr' - rs') = 0.$$

In virtue of the third condition we see that this means that there exists $s'' \in S$ such that $rs's'' = sr's''$. This means that

$$rS \cap sR \neq \varnothing.$$

This condition on S is the condition said of *right permutability*. We say also that S is a *right Ore set* of R.

We also see that if a ring of right fractions over S exists then if for $a \in R$ there exists $s' \in S$ such that $s'a = 0$ then $\iota(s')\iota(a) = 0$ so $\iota(a) = 0$ since $\iota(s')$ is invertible. It follows that there exists $s \in S$ such that $as = 0$. This conditions is said of *right reversibility*.

It is shown in [Lam99, Section 10A] that if S is both right permutable and right reversible then a right ring of fractions of R over S exists. It then is a localisation of R over S and S is then called a *right denominator set*.

COROLLARY 2.3.20. — *The following morphism is an isomorphism.*

$$\begin{array}{rccl} \gamma_p : & A[x]\langle\partial^{\pm 1}\rangle & \leftrightarrow & A[\theta]\langle\Phi^{\pm 1}\rangle \quad : \gamma_p^{-1} \\ & x & \mapsto & \theta\Phi^{-1} \\ & x\partial & \leftarrow\!\shortmid & \theta \\ & \partial & \leftrightarrow & \Phi \end{array}$$

Proof. We know from the discussion that precedes that $x \mapsto \theta\Phi^{-1}$ and $\partial \mapsto \Phi$ uniquely define a morphism from $A[x]\langle\partial\rangle$ to $A[\theta]\langle\Phi^{\pm 1}\rangle$ for which the image of ∂^p is invertible. Thus it uniquely defines a morphism $\gamma_p : A[x]\langle\partial^{\pm 1}\rangle \to A[\theta]\langle\Phi^{\pm 1}\rangle$. Similarly γ_p^{-1} is also well defined and we see now that $\gamma_p \circ \gamma_p^{-1}$ is the only endomorphism of $A[\theta]\langle\Phi^{\pm 1}\rangle$ that maps θ and Φ to themselves respectively which is the identity. Conversely, $\gamma_p^{-1} \circ \gamma_p$ is the only morphism mapping x and ∂ to themselves respectively, the identity, so γ_p and γ_p^{-1} are indeed inverse of one another. □

EXAMPLE 2.3.21. —

$$\gamma_3((x+1)^2\partial^3 - x\partial + x^3) = \Phi^3 + 2\theta\Phi^2 + (\theta^2 - \theta)\Phi + \theta + (\theta^3 + 2\theta)\Phi^{-3}.$$

REMARK 2.3.22. — It is important to note that the above isomorphism only works over polynomial ring and cannot be extended to $A(x)\langle\partial^{\pm 1}\rangle$ and $A(\theta)\langle\Phi^{\pm 1}\rangle$. An easy way to see this is that if such an extension existed then $\gamma_p((x+1)\partial)$ would be invertible in $A(\theta)\langle\Phi^{\pm 1}\rangle$. However $\gamma_p((x+1)\partial) = \theta + \Phi$ which is not an invertible element. Indeed if it were there would be $P \in A(\theta)\langle\Phi\rangle$ and $i \in \mathbb{N}$ such that

$$(\theta + \Phi)P = \Phi^i.$$

But then $\chi(\Lambda_p^{\theta+\Phi})(\Phi^p)$ would be invertible too since

$$\chi(\Lambda_p^{\theta+\Phi})(\Phi^p)\chi(\Lambda_p^P)(\Phi^p) = \chi(\Lambda_p^{(\theta+\Phi)P})(\Phi^p) = \chi(\Lambda_p^{\Phi^i})(\Phi^p) = \Phi^{pi}.$$

But $\chi(\Lambda_p^{\theta+\Phi})(\Phi^p) = \Phi^p + \theta^p - \theta$ which is not invertible in $A(\theta^p-\theta)[\partial^{\pm p}]$ (which is commutative) since it is not a multiple of Φ^p.

The goal now is to prove that in a certain sense

$$\gamma_p(\chi(\psi_p^L)) = \chi(\Lambda_p^{\gamma_p(L)}) \tag{2.3}$$

and to use it to compute the characteristic polynomial of the p-curvature of differential operators. Of course this formula does not make sense as $\chi(\psi_p^L)$ is not even an element of $A[x]\langle\partial^{\pm p}\rangle$. Nonetheless this is the general idea of what we are going to do now.

In order to prove the aforementioned result we will make use of our rings of operators' structure of Azumaya algebras and of their reduced norm.

LEMMA 2.3.23. — *$A(\theta)\langle\Phi^{\pm 1}\rangle$ (resp. $A[\theta]\langle\Phi^{\pm 1}\rangle$) is a $A(\theta^p-\theta)[\Phi^{\pm p}]$ (resp. $A[\theta^p-\theta][\Phi^{\pm p}]$) Azumaya algebra verifying Hypothesis 2.1.49.*

Proof. Since $A(\theta)$ is a field we know that $A(\theta)\langle\Phi\rangle$ is a domain so it is also the case of $A(\theta)\langle\Phi^{\pm 1}\rangle$. In particular its centre has no nontrivial nilpotent element.

We can consider the subalgebra $C = A(\theta^p-\theta)\langle\Phi^{\pm 1}\rangle$ (resp. $C = A[\theta^p-\theta]\langle\Phi^{\pm 1}\rangle$) generated by Φ.
Since $A(\theta^p-\theta)\langle\Phi\rangle$ (resp. $A[\theta^p-\theta]\langle\Phi\rangle$) is a free algebra of dimension p over $A(\theta^p-\theta)[\Phi^p]$ (resp. $A[\theta^p-\theta][\Phi^p]$) and $(1,\Phi,\dots,\Phi^{p-1})$ is a basis of it, this is also the case of $A(\theta^p-\theta)\langle\Phi\rangle$ (resp. $A[\theta^p-\theta]\langle\Phi\rangle$).
A C-basis of $A(\theta)\langle\Phi\rangle$ (resp. $A[\theta]\langle\Phi\rangle$) is given by $(1,\theta,\dots,\theta^{p-1})$. Finally, C is generated by the element Φ so it verifies condition (iv) of Hypothesis 2.1.49. □

LEMMA 2.3.24. — *Let $L \in A(x)\langle\partial\rangle$ (resp. $P \in A(\theta)\langle\Phi\rangle$). Then* $\mathrm{ord}(\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L)) = p\cdot\mathrm{ord}(L)$. *(resp.* $\mathrm{ord}(\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(P)) = p\cdot\mathrm{ord}(P)$.*)*

Proof. We only do the proof in the case of differential operators. Mutatis mutandis, the proof is the same in the case of skew polynomials.

It is easy to see that if L is of degree d, then the matrix M_L of the right multiplication by L has coefficients in $A(x^p)\langle\partial\rangle$ of order at most d. Then since M_L is a square matrix of size p, it follows that

$$\mathrm{ord}(\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L)) \leqslant pd.$$

Now we know that L is a divisor of $\chi(\psi_p^L)(\partial^p)$ and that $\chi(\psi_p^L)(\partial^p) \in A(x^p)[\partial^p]$.

Thus there exists $R \in A(x)\langle\partial\rangle$ such that $RL = \chi(\psi_p^L)(\partial^p)$. Since $\mathrm{ord}(\chi(\psi_p^L)(\partial^p)) = p\cdot\mathrm{ord}(L)$ it follows that R is of order $(p-1)\mathrm{ord}(L)$.

Furthermore

$$\begin{aligned}\mathrm{Nrd}_{A(x)\langle\partial\rangle}(\chi(\psi_p^L)(\partial^p)) &= \chi(\psi_p^L)^p(\partial^p)\\ &= \mathrm{Nrd}_{A(x)\langle\partial\rangle}(R)\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L)\end{aligned}$$

and so

$$\begin{aligned}p^2\mathrm{ord}(L) &= \mathrm{ord}(\mathrm{Nrd}_{A(x)\langle\partial\rangle}(R)) + \mathrm{ord}(\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L))\\ &\geqslant p(p-1)\mathrm{ord}(L) + p\cdot\mathrm{ord}(L)\\ &= p^2\mathrm{ord}(L)\end{aligned}$$

We can have an equality only if $\mathrm{ord}(\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L)) = p\cdot\mathrm{ord}(L)$. □

The final property we need is the following:

PROPOSITION 2.3.25. —
- *Let $L \in A(x)\langle\partial\rangle$ (resp. $L \in A(\theta)\langle\Phi\rangle$). If L is monic then so is* $\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L)$ *(resp.* $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(L)$*).*
- *If $l \in A(x)$ (resp. $l \in A(\theta)$) then* $\mathrm{Nrd}_{A(x)\langle\partial\rangle}(l) = l^p$ *(resp.* $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(l) = \prod_{a=0}^{p-1} l(\theta+a)$*).*

Proof.
- If $L \in A(x)\langle\partial\rangle$ is monic of order d then the only coefficients of order d of the matrix M_L of the right multiplication by L in the $A(x^p)\langle\partial\rangle$ basis $(1, x, \cdots, x^{p-1})$ of $A(x)\langle\partial\rangle$ are on the diagonal and are all monic. Thus the leading coefficient of $\mathrm{Nrd}_{A(x)\langle\partial\rangle}$ comes from the product of the diagonal elements which is also monic.

  In $A(\theta)\langle\partial\rangle$ the proof is the same but we take instead the basis $(1, \theta, \theta(\theta+1), \ldots, \prod_{a=0}^{p-2}(\theta+a))$ of $A(\theta)\langle\Phi\rangle$ over $A(\theta^p-\theta)\langle\Phi\rangle$.
- Let $l \in A(x)$. If $l \in A(x^p)$, then the result in already known. If this is not the case, then $(1, l, l^2, \cdots, l^{p-1})$ is a $A(x^p)\langle\partial\rangle$-basis of $A(x)\langle\partial\rangle$. In this basis the matrix of the right multiplication by l is just
$$\begin{pmatrix} & & & l^p\\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$$
  which yields the result.

  For $l \in A(\theta)$, if $l \in A(\theta^p-\theta)$, the result is already know since $l(\theta+a) = l$ for any $a \in \mathbb{Z}$. If this is not the case, then we consider the $A(\theta)\langle\Phi^{\pm p}\rangle$-basis $(1, l(\theta)\Phi, l(\theta)l(\theta+1)\Phi^2, \ldots, \prod_{a=0}^{p-2} l(\theta+a)\Phi^{p-1})$ of $A(\theta)\langle\Phi^{\pm 1}\rangle$. In this basis the matrix of the multiplication by $l\Phi$ is
$$\begin{pmatrix} & & & \prod_{a=0}^{p-1} l(\theta+a)\Phi^p\\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

Thus $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(l\Phi) = \prod_{i=0}^{p-1} l(\theta+a)\Phi^p$. But by considering the subalgebra $A(\theta)[\Phi^{\pm p}]$ and the basis $(1, \Phi, \dots, \Phi^{p-1})$ we see that $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(\Phi) = \Phi^p$ and we deduce the result by multiplicativity.

□

We can now show the most important result of this section:

THEOREM 2.3.26. — • *For any $L \in A(x)\langle\partial\rangle$ of leading coefficient l,*

$$\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L) = l^p \chi(\psi_p^L)(\partial^p).$$

• *For any $L \in A(\theta)\langle\Phi\rangle$ of leading coefficient l,*

$$\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(L) = \prod_{a=0}^{p-1} l(\theta+a)\chi(\Lambda_p^L)(\Phi^p).$$

Proof. Since both the reduced norm and the characteristic polynomial of the p-curvature are multiplicative maps, we can suppose that L is irreducible. Furthermore from proposition 2.3.25 we see that we can assume that L is monic. Then we know (Proposition 2.2.8 (iii) and Proposition 2.3.13 (iii)) that there exists $N \in A(x^p)[Y]$ irreducible and monic, and $n \in \mathbb{N}$ such that $\chi(\psi_p^L)(\partial^p) = N^n(\partial^p)$ (resp. $\chi(\Lambda_p^L)(\Phi^p) = N^n(\Phi^p)$). But then

$$\mathrm{Nrd}_{A(x)\langle\partial\rangle}(\chi(\psi_p^L)(\partial^p)) = N^{pn}(\partial^p)$$

(resp. $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(\chi(\Lambda_p^L)(\Phi^p)) = N^{pn}(\Phi^p)$).

But since L divides the characteristic polynomial of its p-curvature applied to ∂^p (resp. Φ^p) and is monic it follows that $\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L)$ (resp. $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(L)$) is a power of $N(\partial^p)$. By equality of the orders, we conclude that

$$\mathrm{Nrd}_{A(x)\langle\partial\rangle}(L) = \chi(\psi_p^L)(\partial^p)$$

(resp. $\mathrm{Nrd}_{A(\theta)\langle\Phi^{\pm 1}\rangle}(L) = \chi(\Lambda_p^L)(\Phi^p)$). □

COROLLARY 2.3.27. — *For any $L \in A(x)\langle\partial^{\pm 1}\rangle$ (resp. $L \in A(q)\langle\Phi^{\pm 1}\rangle$) of leading coefficient l, we denote $\Xi_{x,\partial} : L \mapsto l^p\chi(\psi_p^L)(\partial^p)$ (resp. $\Xi_{\theta,\Phi}(L) \mapsto \prod_{a=0}^{p-1} l(\theta+a)\chi(\Lambda_p^L)(\Phi^p)$).*

• $\Xi_{x,\partial}(A[x]\langle\partial^{\pm 1}\rangle) \subset A[x^p][\partial^{\pm p}]$.

• $\Xi_{\theta,\Phi}(A[\theta]\langle\Phi^{\pm 1}\rangle) \subset A[\theta^p-\theta][\Phi^{\pm p}]$.

• $\Xi_{\theta,\Phi} \circ \gamma_p = \gamma_p \circ \Xi_{x,\partial}$, *where we recall that $\gamma_p : A[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} A[\theta]\langle\Phi^{\pm 1}\rangle$ is the isomorphism defined in Corollary 2.3.20.*

Proof. • We know $\Xi_{x,\partial}$ agrees with $\mathrm{Nrd}_{A[x]\langle\partial\rangle}$ on $A[x]\langle\partial\rangle$. Furthermore, since both maps are multiplicative and $\Xi_{x,\partial}(\partial) = \mathrm{Nrd}_{A[x]\langle\partial\rangle}(\partial) = \partial^p$, $\Xi_{x,\partial}$ is equal to $\mathrm{Nrd}_{A[x]\langle\partial^{\pm 1}\rangle}$ on $A[x]\langle\partial^{\pm 1}\rangle$ which yields the result.

• We know $\Xi_{\theta,\Phi}$ agrees with $\mathrm{Nrd}_{A[\theta]\langle\Phi\rangle}$ on $A[\theta]\langle\Phi\rangle$. Furthermore, since both maps are multiplicative and $\Xi_{\theta,\Phi}(\Phi) = \mathrm{Nrd}_{A[\theta]\langle\Phi\rangle}(\Phi) = \Phi^p$, $\Xi_{\theta,\Phi}$ is equal to $\mathrm{Nrd}_{A[\theta]\langle\Phi^{\pm 1}\rangle}$ on $A[\theta]\langle\Phi^{\pm 1}\rangle$ which yields the result.

- This is due to $\Xi_{\theta,\Phi}$ being equal to $\mathrm{Nrd}_{A[\theta]\langle\Phi^{\pm 1}\rangle}$.
- We denote $\mathcal{Z}_x := A[x^p][\partial^{\pm p}]$ and $\mathcal{Z}_\theta := A[\theta^p - \theta][\Phi^{\pm p}]$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{Z}_x$. Since γ_p is an isomorphism it maps prime ideals of the centre to prime ideals of the centre. Thus we have an isomorphism

$$\varphi^p : A[x]\langle\partial^{\pm 1}\rangle \otimes_{\mathcal{Z}_x} \mathrm{Frac}(\mathcal{Z}_x/\mathfrak{p}) \to A[\theta]\langle\Phi^{\pm 1}\rangle \otimes_{\mathcal{Z}_\theta} \mathrm{Frac}(\mathcal{Z}_\theta/\gamma_p(\mathfrak{p})).$$

  Since both sides are simple central algebras, up to scalar extensions K and K' of $\mathrm{Frac}(\mathcal{Z}_x/\mathfrak{p})$ and $\mathrm{Frac}(\mathcal{Z}_\theta/\gamma_p(\mathfrak{p}))$ respectively (such that γ_p extends to an automorphism $\gamma_p : K \to K'$), we have an isomorphism $\gamma_p : M_p(K) \xrightarrow{\sim} M_p(K')$. Let $\det_K$ (resp. $\det_{K'}$) denote the determinant map over $M_p(K)$ (resp. $M_p(K')$).
  We want to show that

$$\gamma_p^{-1} \circ \det_{K'} \circ \gamma_p = \det_K.$$

  Since γ_p^{-1} in this equation is only applied to elements in K' we can see it as the extension of the scalar morphism

$$\begin{array}{rccc} \iota : & K' & \to & K \\ & s & \mapsto & \gamma_p^{-1}(s) \end{array}.$$

  As a ring isomorphism from K' to K, ι can be extended into a ring isomorphism $\iota : M_p(K') \to M_p(K)$ which commutes with the determinant maps. Thus we have

$$\gamma_p^{-1} \circ \det_{K'} \circ \gamma_p = \iota \circ \det_{K'} \circ \gamma_p = \det_K \circ \iota \circ \gamma_p.$$

  But then $\iota \circ \gamma_p$ is an automorphism of $M_p(K)$. Since all ring automorphism of matrix rings are interior, we have

$$\det_K \circ (\iota \circ \gamma_p) = \det_K$$

  which is the desired result.

  Then we deduce that for any $L \in A[x]\langle\partial^{\pm 1}\rangle$ and any prime ideal $\mathfrak{p}$ of $\mathcal{Z}_\theta$

$$\Xi_{\theta,\Phi}(\gamma_p(L)) \equiv \gamma_p(\Xi_{x,\partial}(L)) \mod \mathfrak{p}.$$

  Since $\mathcal{Z}_\theta$ has no nontrivial nilpotent element we deduce the result.

□

EXAMPLE 2.3.28. — Let $L = (x+1)^2\partial^3 - x\partial + x^3 \in \mathbb{F}_3(x)\langle\partial\rangle$. Then

$$\Xi_{x,\partial}(L) = (x^3+1)\partial^9 + 2\partial^3 + x^6 + 2x^3$$

and

$$\Xi_{\theta,\Phi}(\gamma_p(L)) = \Phi^9 + (\theta^3-\theta)\Phi^6 + 2\Phi^3 + 2(\theta^3-\theta)\Phi^{-3} + (\theta^3-\theta)^2\Phi^{-6}.$$

Thus we have both rewritten equation 2.3 in a way that make sense and shown that it is correct. In the following section we are going to see how to apply corollary 2.3.27 to the efficient computation of the characteristic polynomials of the p-curvature, by taking inspiration from a factorial computation method published in [Har14]. Before that we state a small result which will be useful later.

Corollary 2.3.29. — *We have*

$$\gamma_p^{-1}(\theta^p - \theta) = x^p \partial^p.$$

Proof. It is easy to see that $x^p\partial^p = \Xi_{x,\partial}(x\partial)$. Thus

$$\begin{aligned}\gamma_p(x^p\partial^p) &= \gamma_p(\Xi_{x,\partial}(x\partial)) \\ &= \Xi_{\theta,\Phi}(\gamma_p(x\partial)) \\ &= \Xi_{\theta,\Phi}(\theta) \\ &= \theta^p - \theta.\end{aligned}$$

□

2.4 Computing characteristic polynomials of p-curvatures

In this section we consider A an integral domain of characteristic 0. We present our algorithm to compute the characteristic polynomials of the p-curvatures of a given differential operators L with coefficient in $A[x]$, for all primes p smaller than a given $N \in \mathbb{N}$. We make the additional assumption that for any prime number $p \in \mathbb{Z}$, $A_p = {}^{A}/_{pA}$ is an integral domain.

Example 2.4.1. — We can take $A = \mathbb{Z}$ or $A = \mathbb{Z}[X_1, \ldots, X_n]$. We can also think of A as the ring of integers of a number field. However in this case we need to exclude the primes p which are not irreducible in A.
It may be possible possible to extend this setting to prime p for which the leading coefficient of L is not a divisor of 0 in A_p.

We will evaluate the complexity of our algorithm in terms of the number of operations in A. For the sake of simplicity, we will count operations in $A \mod n$ as $O(1)$ operations in A (this includes computing the image of an element of A modulo n).

Remark 2.4.2. — Since A is a ring in characteristic 0, measuring the complexity of the algorithm in terms of operations in A does not account well for the actual bit size of objects in A which cannot be bounded by a constant since A is infinite. Thus we will also give more precise statements on the complexity of our algorithm in terms of bit operations when $A = \mathbb{Z}$.

Although the p-curvature is defined for operators of $A(x)\langle\partial\rangle$, we can define the p-curvature of an element of $A[x]\langle\partial\rangle$, since the canonical morphism $A \to A_p$ induces a ring homomorphism

$$A[x]\langle\partial\rangle \to A_p[x]\langle\partial\rangle.$$

Similarly to the case of characteristic p we introduce the ring of skew polynomials $A[\theta]\langle\Phi\rangle$, defined as the Ore polynomials ring $A[\theta][\Phi, \theta \mapsto \theta + 1, 0]$. Our goal is to introduce an isomorphism similar to γ_p between $A[x]\langle\partial^{\pm 1}\rangle$ and $A[\theta]\langle\partial^{\pm 1}\rangle$. Of course, one must first check that those two rings are well defined since we can't just invert ∂^p as we did in characteristic 0.

We define $A[x]\langle\partial^{\pm 1}\rangle$ (resp. $A[\theta]\langle\Phi^{\pm 1}\rangle$) as the right ring of fractions of $A[x]\langle\partial\rangle$ (resp. $A[\theta]\langle\Phi\rangle$) with respect to $\{\partial^n | n \in \mathbb{N}\}$ (resp. $\{\Phi^n | n \in \mathbb{N}\}$) as mentioned in Remark 2.3.19.

PROPOSITION 2.4.3. — *The rings $A[x]\langle\partial^{\pm 1}\rangle$ and $A[\theta]\langle\Phi^{\pm 1}\rangle$ are well defined and we have an isomorphism:*

$$\begin{array}{rccc} \gamma_0 : & A[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & A[\theta]\langle\Phi^{\pm 1}\rangle \\ & x & \mapsto & \theta\Phi^{-1} \\ & \partial & \mapsto & \Phi \end{array} .$$

Proof. We need to check that the multiplicative subset $S = \{\Phi^n | n \in \mathbb{N}\}$ is a right denominator set of the ring $A[\theta]\langle\Phi\rangle$ (see Remark 2.3.19). Since this ring has no nontrivial zero divisor, we only have to check that S is right permutable, that is to say that

$$\forall g \in A[\theta]\langle\Phi\rangle, \forall n \in \mathbb{N}, \exists g_1 \in A[\theta]\langle\Phi\rangle, \exists m \in \mathbb{N}, g\Phi^m = \Phi^n g_1.$$

This is the case since for all $n \in \mathbb{N}$ and all $g \in A[\theta]$, $\Phi^n g(\theta - n) = g\Phi^n$ and the fact that $A[\theta]\langle\Phi^{\pm 1}\rangle$ is well defined follows by additivity.

We now show that $S = \{\partial^n | n \in \mathbb{N}\}$ is a right denominator set of $A[x]\langle\partial\rangle$. Let $f \in A[x]$ and suppose that $f^{(m)} = 0$. Then

$$f\partial^{m+1} = \partial \sum_{k=0}^{m-1} (-1)^k f^{(k)} \partial^{m-k}.$$

Let now $L = \sum_{i=0}^{r} f_i \partial^i$ and let's take $m \in \mathbb{N}$ such that for all i, $f_i^{(m)} = 0$. Then

$$\begin{aligned} L\partial^{m+1} &= \sum_{i=0}^{r} f_i \partial^{i+1+m} \\ &= \sum_{i=0}^{r} f_i \partial^{m+1} \partial^i \\ &= \sum_{i=0}^{r} \partial \left(\sum_{k=0}^{m-1} (-1)^k f_i^{(k)} \partial^{m-k+i} \right) \\ &= \partial \sum_{i=0}^{r} \sum_{k=0}^{m-1} (-1)^k f_i^{(k)} \partial^{m-k+i} \end{aligned}$$

This shows that $LS \cap \partial A[x]\langle\partial\rangle \neq \varnothing$. Let $i \in \mathbb{N}^*$. We now want to show that

$$LS \cap \partial^i A[x]\langle\partial\rangle \neq \varnothing.$$

By induction on i we prove the following result: If $L \in A[x]\langle\partial\rangle$ is such that all its coefficients have m-th derivative equal to 0 then there exists $L_i \in A[x]\langle\partial\rangle$ such that

$$L\partial^{m+i} = \partial^i L_i.$$

We know the result to be true for $i = 1$. Suppose it proven for some $i \in \mathbb{N}^*$. By absurdity, suppose that there existed $L \in A[x]\langle\partial\rangle$ whose coefficients all have zero m-th derivatives but such that for no $L_{i+1} \in A[x]\langle\partial\rangle$ will we have $f\partial^{m+i+1} = \partial^{i+1} f_{i+1}$.

Let us consider the minimal integer m such that such a L exists. $m > 0$ since 0 commutes with ∂. By induction there exists $L_i \in A[x]\langle\partial\rangle$ such that

$$L\partial^{m+i} = \partial^i L_i$$

But then we have

$$\begin{aligned}\partial L\partial^{m+i} &= L\partial^{m+i+1} + L'\partial^{m+i}\\ &= \partial^{i+1}L_i\end{aligned}$$

where L' is the operator whose coefficients are the derivatives of those of L. But then all the coefficients of L' have a zero $m-1$-th derivative. Since m was taken minimal, there exists $G_{i+1} \in A[x]\langle\partial\rangle$ such that $L'\partial^{m+i} = L'\partial^{m-1+i+1} = \partial^{i+1}G_{i+1}$ and so

$$\partial^{m+i+1}f = \partial^{i+1}(L_i - G_{i+1}).$$

This is absurd since we supposed that this could not happen and the induction is established.

Thus for all $i \in \mathbb{N}$, $LS \cap \partial A[x]\langle\partial^i\rangle \neq \varnothing$ and S is a right denominator set which shows that $A[x]\langle\partial^{\pm 1}\rangle$ is well defined.

We show that γ_0 is an isomorphism the same way we did for γ_p (*cf.* Corollary 2.3.20). □

Denoting by $\pi_p : A \to A_p$ the canonical reduction modulo p, we can easily see that $\pi_p \circ \gamma_0 = \gamma_p \circ \pi_p$ (where we extend naturally π_p to suitable rings of operators). This enables us, for a given operator in $A[x]\langle\partial\rangle$, to compute the characteristic polynomials of its p-curvatures, by computing the isomorphism γ_0 before the reduction modulo p. We will now see how to use this fact.

We now give an outline of our algorithm.

Input: $L_x \in A[x]\langle\partial\rangle$, $N \in \mathbb{N}$
Output: A list of the characteristic polynomials of the p-curvatures of L_x, for all primes p with $p < N$ except a finite number not depending on N.

1. Set l_x the leading coefficient of L_x.
2. Compute $L_\theta := \varphi_0(L_x) \in A[\theta]\langle\partial^{\pm 1}\rangle$.
3. Set l_θ the leading coefficient of L_θ.
4. Compute $\mathcal{P}_{l_\theta}$, the list of all primes $p < N$ which do not divide l_θ.
5. Construct $B(\theta)$ the companion matrix of $l_\theta^{-1} \cdot L_\theta$.
6. Compute $\left(\prod_{i=0}^{p-1} l_\theta(\theta+i)\right) \bmod p$ for all $p \in \mathcal{P}_{l_\theta}$.
7. Compute $B(\theta)\cdots B(\theta+p-1) \bmod p$ for all $p \in \mathcal{P}_{l_\theta}$.
8. Deduce all the $\Xi_{\theta,\Phi,p}(L_\theta)$, for $p \in \mathcal{P}_{l_\theta}$.
9. Deduce all $\chi(A_p(L_x)) = l_x^{-p}\varphi_p^{-1}(\Xi_{\theta,\Phi,p}(L_\theta))$, for $p \in \mathcal{P}_{l_\theta}$.

Remark 2.4.4. — We only do the computation for the primes which do not divide the leading coefficient of L_θ because for the other ones, the companion matrix of its reduction modulo p is not the reduction modulo p of its companion matrix.

LEMMA 2.4.5. — *Let $L_\theta \in A_p[\theta]\langle\Phi\rangle$ be a skew polynomial with coefficients of degree at most $d \in \mathbb{N}$. Then $\Xi_{\theta,\partial}(L_\theta)$ has coefficients of degree at most dp.*

Proof. Let $C = A_p[\theta][\Phi^{\pm p}]$. C is a subalgebra of $A_p[\theta]\langle\Phi^{\pm 1}\rangle$ verifying Hypothesis 2.1.49. We consider the C-basis $(1, \Phi, \dots, \Phi^{p-1})$ of $A[\theta]\langle\Phi^{\pm 1}\rangle$. It is easy to see that the matrix of the right multiplication by L has coefficients of degree at most d in θ. Then its determinant has coefficients of degree at most dp in θ. □

From Lemma 2.4.5, we deduce that at the end of step (8) we have a list of (lists of) polynomials of degree linear in p, which means that the bit size of the output of this step is quadratic in N. This seems to remove all hope of ending up with a quasi-linear algorithm. Fortunately those polynomials lie in $A_p[\theta^p - \theta]$ (see corollary 2.3.27). Thus each of them can be represented by $O(d)$ elements of A_p. We explain how in Section 2.4.1.

REMARK 2.4.6. — The same problem is also present at the end of step (9), but is easy to solve as we only need to determine the coefficients of x^i when i is a multiple of p. Thus we in fact compute polynomials $P_p \in A_p[x, Y]$ such that $P_p(x^p, Y) = \chi(A_p(L))$ for all $p < N$.

2.4.1 Reverse isomorphism, computation modulo θ^{d+1}

We know from Corollary 2.3.27 that for $L_\theta \in A_p[\theta]\langle\partial\rangle$, the operator $\Xi_{\theta,\partial}(L_\theta)$ has coefficients in $A_p[\theta^p - \theta]$.

LEMMA 2.4.7. — *Let $Q \in A_p[\theta^p - \theta]$ be a polynomial of degree d in $\theta^p - \theta$ with $d < p$. Write:*

$$Q = \sum_{i=0}^{d} q_i(\theta^p - \theta)^i \quad \text{and} \quad Q = \sum_{i=0}^{dp} q'_i\theta^i.$$

For all $i \leqslant d$, we have $q_i = (-1)^i q'_i$.

Proof. This comes from the fact that $(-1)^i\theta^i$ is the only monomial of degree less than p in $(\theta^p - \theta)^i$. □

When p is strictly greater than d, it follows that we only need to compute the $\Xi_{\theta,\partial,p}$ modulo θ^{d+1} where d is the highest degree of the coefficients of the operator (in both variables x or θ), as one can see in Algorithm 1. We deduce the following lemma:

LEMMA 2.4.8. — *If $Q_\theta \in A_p[\theta^p - \theta][Y]$ is of degree m in Y and dp in θ with $d < p$, then Algorithm 1 computes $Q_x \in A_p[x, Y]$ such that $Q_x(x^p, \partial^p) = \gamma_p^{-1}(Q_\theta(\Phi^p))$ in $O(dm)$ operations in A.*

Input: $Q_\theta \in A_p[\theta^p - \theta][Y]$, of degree m in Y and degree at most dp in θ, known modulo θ^{d+1}.
Output: $Q_x \in A_p[x, Y]$ such that $Q_x(x^p, \partial^p) = \gamma_p^{-1}(Q_\theta(\Phi^p))$.

1. $Q_x \leftarrow 0$.
2. For all $i \leqslant m$:
   (a) Let $Q_{\theta,i}$ be the coefficient of Φ^i of Q_θ and write $Q_{\theta,i} = \sum_{j=0}^{d} q_{i,j}\theta^j + O(\theta^{d+1})$.
   (b) $Q_x \leftarrow Q_x + \sum_{j=0}^{d}(-1)^j q_{i,j} x^j Y^{i+j}$.
3. *Return:* Q_x.

Algorithm 1: reverse_iso

Proof. Let $Q_\theta = \sum_{i=1}^{r}\left(\sum_{j=1}^{d} q_{i,j}\theta^j + O(\theta^{d+1})\right)\Phi^i \in A_p[\theta^p - \theta][Y]$. Then according to Lemma 2.4.7,

$$Q_\theta(\Phi^p) = \sum_{i=0}^{r}\left(\sum_{j=1}^{d}(-1)^j q_{i,j}(\theta^p - \theta)^i\right)\Phi^{pi}$$

and

$$\begin{aligned}\gamma_p^{-1}(Q_\theta(\Phi^p)) &= \sum_{i=0}^{r}\left(\sum_{j=0}^{d}(-1)^i q_{i,j}(\gamma_p^{-1}(\theta^p - \theta))^j\right)\partial^{pi} \\ &= \sum_{i=0}^{r}\left(\sum_{j=0}^{d}(-1)^i q_{i,j} x^{pj}\partial^{p(i+j)}\right) \text{ using Lemma 2.3.29}\end{aligned}$$

Thus by setting $Q_x = \sum_{i=0}^{r}\sum_{j=0}^{d}(-1)^j q_{i,j} x^j Y^{i+j}$ we have indeed

$$Q_x(x^p, \partial^p) = \gamma_p^{-1}(Q_\theta(\Phi^p)).$$

□

Remark 2.4.9. — In fact we can still compute γ_p^{-1} if $p \leqslant d$ while only knowing the operator modulo θ^{d+1} but this is more tedious since there is no nice formula. In that case, with notation as in Lemma 2.4.7, we have $q'_i = \sum_{k=0}^{\lfloor i/(p-1)\rfloor}(-1)^{i-kp}\binom{i-k(p-1)}{k} q_{i-k(p-1)}$.
This relation is easily invertible since it is given by a triangular matrix with no zero on the diagonal.

2.4.2 Shift before the computation

From the results of the previous subsection, we know that we only need to determine $\Xi_{\theta,\partial}$ modulo a small power of θ. Unfortunately, the companion matrix of an operator in $A_p[\theta]\langle\partial\rangle$, even if the operator has polynomial coefficients, usually has its coefficient in $A_p(\theta)$. In [BCS14], the authors solve this issue by injecting $A_p(\theta)$ in $A_p((\theta))$ and computing modulo a slightly higher power of θ. In order to minimise the degree of the polynomials used in the computation, we take a different approach based on shifting the origin.

Let $a \in A_p$. We denote by $\tau_a : A_p[x] \to A_p[x]$ the shift automorphism $Q \mapsto Q(x+a)$. This automorphism extends into automorphisms of $A_p[x]\langle\partial\rangle$ and $A_p[x,Y]$ by its application coefficient-wise.
In the case of the former ring, this is due to the fact that for any $f \in A_p[x]$, $\tau_a(f)' = \tau_a(f')$.

PROPOSITION 2.4.10. — *Let $a \in A_p$. For any $L \in A_p[x]\langle\partial\rangle$,*

$$\tau_a(\chi(\psi_p^L)) = \chi(\psi_p^{\tau_a(L)})$$

Proof. Let M_L be the companion matrix of L and $M_{\tau_a(L)}$ be the companion matrix of $\tau_a(L)$. Let $(M_{L,n})_{n\in\mathbb{N}}$ (resp. $(M_{\tau_a(L),n})$) be the recursive sequence of matrices defined by $M_{L,0} = \mathrm{Id}$ (resp. $M_{\tau_a(L),0} = \mathrm{Id}$) and $M_{L,n+1} = M'_{L,n} + M_L \cdot M_{L,n}$ (resp. $M_{\tau_a(L),n+1} = M'_{\tau_a(L),n} + M_{\tau_a(L)} \cdot M_{\tau_a(L),n}$.)
Since $\tau_a(L)$ has the same order as L, $\tau_a(M_L) = M_{\tau_a(L)}$. Since τ_a commutes with the derivation we get that

$$\tau_a(M_{L,2}) = \tau_a(M'_L + M_L^2) = M'_{\tau_a(L)} + M^2_{\tau_a(L)} = M_{\tau_a(L),2}.$$

We can extend this relation recursively to all $n \in \mathbb{N}$. According to Lemma 2.3.1, the matrix of the p-curvature of L (resp. $\tau_a(L)$) is given by $M_{L,p}$ (resp. $M_{\tau_a(L),p}$) Since τ_a is an endomorphism we find

$$\tau_a(\chi(\psi_p^L)) = \tau_a(\chi(M_{L,p})) = \chi(\tau_a(M_{L,p})) = \chi(M_{\tau_a(L),p}) = \chi(\psi_p^{\tau_a(L)}).$$

□

From Proposition 2.4.10, we deduce that we can shift an operator before computing the characteristic polynomials of its p-curvatures, and do the opposite translation on those to get the desired result. It is especially useful because of the following lemma.

LEMMA 2.4.11. — *Let $L_x \in A[x]\langle\partial\rangle$ be an operator and denote by $l_x \in A[x]$ its leading coefficient. If $l_x(0) \neq 0$ then $\gamma_0(L_x)$ has $l_x(0) \in A$ as its leading coefficient.*

Proof. A straightforward computation shows that $\gamma_0(x^i\partial^j) = p_i(\theta)\Phi^{j-i}$ with $p_i(\theta)$ being a polynomial only dependent on i (and not on j). Thus the leading coefficient of $\gamma_0(L_x)$ can only come from the constant coefficient of l_x if this one is not 0. □

In our setting, the fact that $\gamma_0(L_x)$ has a constant leading coefficient means that its companion matrix has its coefficients in $\mathrm{Frac}(A)[\theta]$, implying that we can do all the computations modulo θ^{d+1}. Lemma 2.4.11 shows that we can shift our starting operator by $a \in A$ where a is not a root of its leading coefficient to place ourselves in that setting. Doing this shift can be seen as placing the origin in an ordinary point $a \in A$ of the differential equation defined by L_x.
Since translating back all the characteristic polynomials (the P_p in fact, see Remark 2.4.6) at the end of the computation is basically the same as translating a list of $O(Nr)$ univariate polynomials of degree d, it can be done in $\tilde{O}(Ndr)$ operations in A (for example with binary splitting), with r being the order of L_x and d the maximum degree of its coefficients.

2.4.3 Computing a matrix factorial modulo p for a large amount of primes p

Let $M(\theta) \in \mathscr{M}_r(A[\theta])$ be a square matrix of size r with coefficients of degree less than d. In this subsection we review the algorithm of [CGH14, Har14] applied to the computation of the following matrix factorial:

$$M(\theta) \cdot M(\theta+1) \cdots M(\theta+p-1) \mod (p, \theta^{d+1})$$

for all primes $p < N$.

Since the method of [CGH14] computes products of $p-1$ entries modulo some power of p, we will compute $M(\theta+1)\cdots M(\theta+p-1) \mod (p,\theta^d)$ for all p, and then left-multiply by $M(\theta)$.

Let $\eta := \lceil \log_2(N) \rceil$. For all i and j with $0 \leqslant i \leqslant \eta$ and $0 \leqslant j < 2^i$, we denote

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

It follows from the definition that for all $0 \leqslant i < \eta$ and all $0 \leqslant j < 2^i$,

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

Furthermore, for $i = \eta$, the $U_{i,j}$ are either empty or a singleton.

From this, we introduce $T_{i,j} := \prod_{k\in U_{i,j}} M(\theta+k) \mod \theta^d$, with the product being made by sorting elements of $U_{i,j}$ in ascending order, and $S_{i,j} := \prod_{\substack{p\in U_{i,j}\\ p \text{ prime}}} p$. From now on, we consider that the $T_{i,j}$ are elements of $\mathscr{M}_m(A[\theta]/\theta^{d+1})$. From the properties of $U_{i,j}$, we deduce that $T_{i,j} = T_{i+1,2j}T_{i+1,2j+1}$ and $S_{i,j} = S_{i+1,2j}S_{i+1,2j+1}$.

These relations allow us to fill binary trees containing the $T_{i,j}$ and $S_{i,j}$ as their nodes from the bottom. Furthermore, filling those trees is nothing more than computing a factorial by binary splitting, and keeping the intermediate steps in memory.

To see how to apply this to our problem we suppose that $p \in U_{\eta,j}$ for a certain j. A direct computation gives:

$$\begin{aligned} M(\theta+1)\cdot M(\theta+2)\cdots M(\theta+p-1) &\mod (p,\theta^{d+1}) \\ = T_{\eta,0}T_{\eta,1}\cdots T_{\eta,j-1} &\mod S_{\eta,j}. \end{aligned}$$

This motivates the following definition: for all i,j with $0 \leqslant i \leqslant \eta$ and $0 \leqslant j < 2^i$, we set $W_{i,j} := \prod_{k=0}^{j-1} T_{i,k} \mod S_{i,j}$. The following lemma is easily checked.

Lemma 2.4.12. — *For all i and j such that the following quantities are well defined, $W_{i+1,2j} = W_{i,j} \mod S_{i+1,2j}$ and $W_{i+1,2j+1} = W_{i,j}T_{i+1,2j} \mod S_{i+1,2j+1}$.*

Thus we can compute the $W_{\eta,j}$ by filling a binary tree from the top starting from $W_{0,0} = 1$. This proves the correctness of Algorithm 2, while its complexity is addressed in the next proposition.

Input: $M(\theta) \in M_r(A[\theta])$ with coefficients of degree less than d, $\mathcal{P}$ a list of primes smaller than N.
Output: A list containing $M(\theta)M(\theta+1)\cdots M(\theta+p-1) \mod (p, \theta^d)$ for all p in $\mathcal{P}$.

1. $\eta \leftarrow \lceil \log_2(N) \rceil$.
2. Fill $T_{\eta,\_}$ and $S_{\eta,\_}$.
3. Compute the binary trees T and S.
4. $W_{0,0} \leftarrow 1$.
5. For i going from 0 to $\eta - 1$:
   (a) For j going from 0 to $2^i - 1$:
      i. $W_{i+1,2j} \leftarrow W_{i,j} \mod S_{i+1,2j}$.
      ii. $W_{i+1,2j+1} \leftarrow W_{i,j}T_{i+1,2j} \mod S_{i+1,2j+1}$.
6. Construct $\prod$ the list of $W_{\eta,j}$ where $S_{\eta,j} \in \mathcal{P}$.
7. Do the left multiplication by $M(\theta)$ on the elements of $\prod$.
8. Return: $\prod$.

Algorithm 2: matrix_factorial

PROPOSITION 2.4.13. — *This algorithm has a cost of $\tilde{O}(r^\omega dN)$ operations in A.*

Proof. The computation of the binary tree S is less costly than that of T, so we do not consider it. Let us evaluate the complexity of the computation of T, which we denote $C_1(N)$. Since T is filled by binary splitting we have

$$C_1(N) = r^\omega d + 2C_1(\lceil N/2 \rceil).$$

It follows that T can be computed in $\tilde{O}(r^\omega dN)$ operations in A.

The cost of computing W is the same as that of reducing $T_{i,j} \mod S_{i,j+1}$ whenever both quantities are well defined, and then of computing recursively the $W_{i,j}$. The first step can be done in $\tilde{O}(Nr^2d)$ operations in A, while the second requires $\tilde{O}(r^\omega dN)$ operations in A. □

REMARK 2.4.14. — This step is where counting the cost of the algorithm in operations in A can be a bit misleading. Indeed, since A is a ring of characteristic 0, in particular, it contains $\mathbb{Z}$. Thus operations in A do not have a constant cost in bit operations. This cost is especially not constant when computing a factorial where the size of integers essentially doubles on each level of the trees T and S. In [Pag21], we showed an analog result when $A = \mathbb{Z}$ which we reproduce below.

If $A = B[t]$ is a ring of polynomials however then we expect this algorithm to finish in $\tilde{O}(r^\omega d_1 d_2 N^2)$ operations in B (where the coefficients of $M(\theta)$ are of bidegree maximal d_1, d_2), since each matrix factorial would have coefficients in $B[t]$ of degree $\tilde{O}(d_1 N)$.

We give an analog of the result in the case $A = \mathbb{Z}$:

Proposition 2.4.15. — *For $A = \mathbb{Z}$, Algorithm 2 has a cost of*

$$\tilde{O}(r^\omega dN(n + d\log(N) + \log(r)))$$

bit operations, where n is the maximum bit size of the integers in the matrix $M(\theta)$.

Proof. The computation of the binary tree S is less costly than that of T, so we do not consider it. Let us evaluate the complexity of the computation of T. We need to know the bit size of the integers at each level of T. We use the following lemma.

Lemma 2.4.16. — *For any $a \leqslant N$, all the integers appearing in $M(\theta + a)$ have bit size at most $n + d(1 + \log_2(N))$.*

Proof. Let $Q \in \mathbb{Z}[\theta]$ of degree less than d appearing in $M(\theta)$. Then we can write

$$Q(\theta + a) = \sum_{j=0}^{d-1} \left(\sum_{i=j}^{d-1} \binom{i}{j} q_i a^{i-j} \right) \theta^j$$

where the q_i are the coefficients of Q. Moreover, we know that all the q_i are at most 2^n. Thus the coefficients of $Q(\theta + a)$ are less than $2^n N^{d-1} \sum_{i=j}^{d-1} \binom{i}{j} \leqslant 2^{n+d} N^d$. □

We now resume the proof of Proposition 2.4.13. If Δ_1 and Δ_2 are matrices in $\mathscr{M}_m\left(\mathbb{Z}[\theta]/\theta^d\right)$ with integers of bit size at most n_1, then $\Delta_1\Delta_2$ has integers of bit size at most $2n_1 + \log_2(dm)$. It follows that the integers in the matrices $A_{i,j}$ are of bit size at most:

$$\begin{aligned} &2^{\eta-i}(n + d(1 + \log_2(N))) + (2^{\eta-i} - 1)\log_2(dm) \\ &\quad = O(2^{\eta-i}(n + d\log_2(N) + \log_2(m))). \end{aligned}$$

The computation of T is reduced to the computation of its two sub-trees, followed by a multiplication of two square matrices of size m with polynomial coefficients of degree d and integers of bit size $O(2^{\eta-1}(n + d\log_2(N) + \log_2(m)))$. Since the bit size of the integers is halved at each level, we finally find, using that $2^\eta \leqslant 2N$, that the computation of T can be done in $\tilde{O}(m^\omega dN(n + d\log_2(N) + \log_2(m))$ bit operations.

The cost of computing W is the same as that of reducing $T_{i,j} \mod S_{i,j+1}$ whenever both quantities are well defined, and then of computing recursively the $W_{i,j}$ using only integers smaller than $S_{i,j}$. The first step can be done in $\tilde{O}(Nm^2d(n+d))$ bit operations, while the second requires $\tilde{O}(m^\omega dN)$ bit operations. □

2.4.4 Final algorithm

The most important pieces of our main algorithm are now in place, we are almost ready to write down its final version. Before doing this, we analyze the cost of converting an operator in $A[x]\langle\partial\rangle$ to its counterpart in $A[\theta]\langle\Phi^{\pm 1}\rangle$.

Proposition 2.4.17 (Section 4.1 [BCS14]). — *For any operator $L \in A[x]\langle\partial\rangle$, of order r with coefficients of degree at most d, the computation of $\gamma_0(L)$, can be done in $\tilde{O}(d(r+d))$ operations in A.*

Note that for an operator $L \in A[x]\langle\partial\rangle$ of order r with coefficients of degree at most d, $\gamma_0(L)$ has nonzero coefficients for powers of ∂ varying from $-d$ to r, making the square matrices used in Algorithm 3 of size at most $r+d$.

Before presenting the final algorithm in Algorithm 3, we give the analog result for the case $A = \mathbb{Z}$.

PROPOSITION 2.4.18 (Proposition 3.12 [Pag21]). — *For any operator $L \in \mathbb{Z}[x]\langle\partial\rangle$, of order m with coefficients of degree at most d, with integer coefficients of bit size at most n, the computation of $\gamma_0(L)$, can be done in $\tilde{O}(d(m+d)(n+d))$ bit operations.*
Furthermore the resulting operator in the variable θ has its integer coefficients of bit size $O(n + d\log_2(d))$.

Proof. From [BCS14, Section 4.1] we get that this computation over a ring R can be done in $\tilde{O}((m+d)d)$ algebraic operations in R. Following their algorithm, we can show that, when $R = \mathbb{Z}$, intermediate computations do not produce integers larger than those of the final result. Moreover, if

$$\gamma_0\Big(\sum_{\substack{0\leqslant i\leqslant d\\ 0\leqslant j\leqslant m}} l_{i,j}x^i\partial^j\Big) = \sum_{\substack{0\leqslant i\leqslant d\\ -d\leqslant j\leqslant m}} l'_{i,j}\theta^i\partial^j$$

the estimation $|l_{i,j}| \leqslant 2^n$ implies $|l'_{i,j}| \leqslant 2^{n+d+1}d^d$. Putting all together, we get the announced result. □

THEOREM 2.4.19. — *For any operator $L \in A[x]\langle\partial\rangle$, Algorithm 3 computes a list of polynomials $P_p \in \mathbb{Q}[x,Y]$ for all primes $p < N$ except a finite number not depending on N, such that $P_p(x^p, Y) = \chi(\psi_p^L)$ in*

$$\tilde{O}(Nd((r+d)^\omega + (r+d)^{\Omega_1}))$$

operations in A, where r is the order of the operator, d is the maximum degree of its coefficients.

If $A = \mathbb{Z}$ and in addition n is the maximal bit size of the integers appearing in L then Algorithm 3 has a cost of

$$\tilde{O}(Nd((n+d)(r+d)^\omega + (r+d)^{\Omega_1}))$$

bit operations.

Proof. This is easily seen by summing the cost of each step of Algorithm 3. □

REMARK 2.4.20. — Again, counting the complexity of algorithm 3 in operations in A can be misleading, for the same reasons as in remark 2.4.14.
When $A = B[t]$ is a polynomial ring we expect algorithm 3 to cost $\tilde{O}(N^2d_1d_2(r+d_2)^\omega + (r+d_2)^{\Omega_1})$ operations in B, where L has coefficients of bidegree d_1, d_2.

As we have seen, Algorithm 3 does not compute the characteristic polynomial of the p-curvature for every $p < N$, as we have to remove all primes dividing $l_x(0)$, where l_x is the leading coefficient of the operator (provided of course that $l_x(0) \neq 0$). Primes less than the maximum degree of the coefficients of the operator are also not included; however, it is possible to remedy these with minor tweaks using Remark 2.4.9.

Input: $L_x \in A[x]\langle\partial\rangle$ of order r, with coefficients of degree at most d, $N \in \mathbb{N}$.
If $A = \mathbb{Z}$: Suppose that the integers in L_x are of maximal bit size n.

Output: A list of polynomials $P_p \in A_p[x, Y]$ such that $P_p(x^p, Y) = \chi(\psi_p^{L_x})$ for all primes $p < N$, except a finite number not depending on N.

1. $l_x \leftarrow$ the leading coefficient of L_x.
2. $a \leftarrow 0$.
3. If $l_x(0) = 0$ do:
   (a) Shift L_x by b with $b \in \mathbb{Z}$ not a root of l_x.
   (b) $a \leftarrow b$.

   Cost: $\tilde{O}(rd)$ *operations in* A.
   Cost when $A = \mathbb{Z}$**:** $\tilde{O}(rd(n + d))$ *bit operations.*
4. Compute $L_\theta \partial^{-k} := \gamma_0(L_x)$ with `x_d_to_theta_d` from [BCS14, Section 4].
   Cost: $\tilde{O}((r + d)d)$ *operations in* A.
   Cost when $A = \mathbb{Z}$**:** $\tilde{O}((r + d)(n + d)d)$ *bit operations.*
5. $d \leftarrow$ the maximum degree of the coefficients of L_θ.
6. $l_\theta \leftarrow$ the leading coefficient of L_θ.
   It has been made to belong in A.
7. Construct $M(\theta) = l_\theta \cdot B(\theta)$ where $B(\theta)$ is the companion matrix of L_θ.
8. Compute the list $\mathcal{P}$ of all primes p that do not divide l_θ with $d + 1 \leqslant p < N$.
   Cost: $\tilde{O}(N)$ *bit operations (see [CGH14, Proposition 2.1]).*
9. Compute the list $\mathcal{L}$ of $M(\theta) \cdots M(\theta + p - 1) \bmod (\theta^{d+1}, p)$ for all p in $\mathcal{P}$ using *matrix_factorial*.
   Cost: $\tilde{O}((r + d)^\omega dN)$ *operations in* A.
   Cost when $A = \mathbb{Z}$**:** $\tilde{O}((r + d)^\omega (n + d)dN)$ *bit operations.*

From this point, all computations are done in some A_p. *Thus for* $A = \mathbb{Z}$ *the cost in bit operations is the cost in operations in* A *times* $\log(N)$.

10. Divide all elements of $\mathcal{L}$ by l_θ^p.
    Cost: $\tilde{O}(N(r + d)^2 d)$ *operations in* A.
11. Compute the list $\mathcal{C}$ of the characteristic polynomials of elements of $\mathcal{L}$.
    Cost: $\tilde{O}(N(r + d)^{\Omega_1} d)$ *operations in* A.
12. Multiply the elements of $\mathcal{C}$ by l_θ^p.
    Cost: $\tilde{O}(N(r + d)d)$ *operations in* A.
13. Compute the image by γ_p^{-1} of elements of $\mathcal{C}$ using *reverse_iso*.
    Cost: $\tilde{O}(Nd(r + d))$ *bit operations.*
14. Divide the polynomials obtained by l_x and Y^{-k}.
    Cost: $\tilde{O}(\mathrm{Nrd})$ *bit operations.*
15. If $a \neq 0$, shift the polynomials obtained by $-a$.
    Cost: $\tilde{O}(\mathrm{Nrd})$ *bit operations.*

Algorithm 3: charpoly_p_curv

PROPOSITION 2.4.21. — *It is possible to compute all characteristic polynomials of the p-curvatures of an operator $L \in A[x]\langle\partial\rangle$ of order m and maximum degree of the coefficients d, for all primes p less than N, in an asymptotically quasilinear in N number of operations in A.*

Proof. The computation for primes dividing $l_x(0)$ (with l_x being the leading coefficient of L) can be done using the main algorithm from [BCS14]. All other primes can be addressed using our new Algorithm 3.
As primes which cannot be computed using our algorithm only depend on the operator itself, the result immediately follows. □

2.5 Implementation and timings

We have implemented Algorithm 3 in the Computer Algebra software *SageMath* and tested it for $A = \mathbb{Z}$. The source code can be downloaded from the following URL: https://github.com/raphitek/p_curvatures. In this section we present the result of our tests on the ring of integers.

As mentioned earlier, the computation of the characteristic polynomial of a matrix of size m with coefficients in a ring can be performed in theory using $\tilde{O}(m^{\Omega_1})$ ring operations, with $\Omega_1 \simeq 2.697263$, see [KV05]. However, we did not implement the algorithm from [KV05], and instead used an algorithm computing a Hessenberg form of the matrix in $O(m^3)$ operations [CRV17]. Indeed, the latter algorithm is easier to implement and the computation of the characteristic polynomials is usually not the bottleneck and does not hinder the quasi-linear nature of our algorithm. Furthermore, experiments, as well as Theorem 2.4.19, showed that most of the running time is spent on the computation of trees T and W when the order of the operator is of the same magnitude as the degrees of its coefficients. We expect this trend to improve when the ratio of these two factors grows in favor of the order of the operator, but all experiments conducted so far showed that the computation of the characteristic polynomials is never the bottleneck by a wide margin. It is still more than six times faster on an operator of order 50 with coefficients of degree 2, for $N = 100$.

REMARK 2.5.1. — In our experiments we do not consider cases where the degree d of the coefficients is higher than the order m of the operator because the complexity in d is worse than in m. As in [BBvdH12, Section IV], the general case reduces to this one using the transformation $x \mapsto -\partial$, $\partial \mapsto x$ which exchanges the roles of ∂ and x.

2.5.1 Timings on random operators

Quasilinear as expected. Figure 2.1 shows computation timings of our implementation for operators in $\mathbb{Z}[x]\langle\partial\rangle$ of varying sizes on *SageMath* version 9.3.rc4 on an Intel(R) Core(TM) i3-40050 machine at 1.7Ghz, running ArchLinux. As expected, it does appear that our algorithm finishes in quasi-linear time in N. We can also see a floor phenomenon, with computation time varying very little between two powers of 2, and then doubling. This is an expected effect of the use of the complete binary tree structure in our algorithm. This effect however seems less visible, even if it is still perceptible, as the operator size increases. This is probably due to the fact that for operators of small sizes, the cost of manipulating empty nodes is non-negligible.

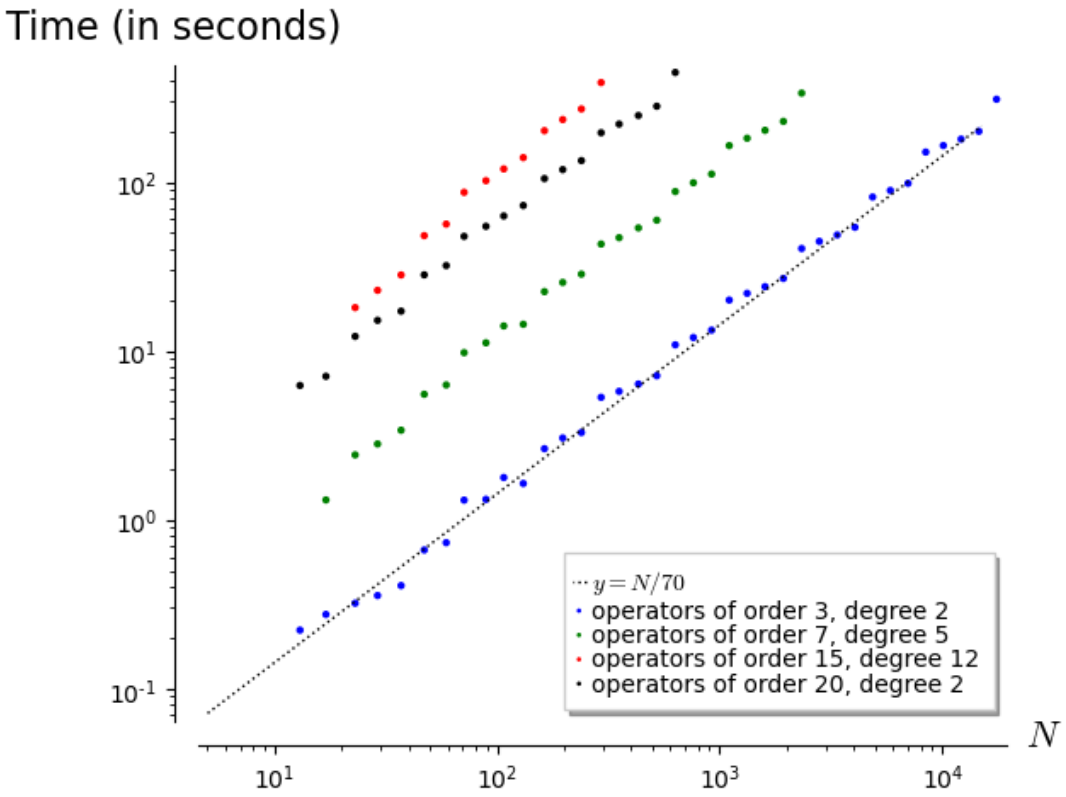


Figure 2.1: Computation time for random operators of varying orders and degrees

Comparison with the previous algorithm. We have compared the timings between our algorithm and the iteration of that of [BCS14] for an operator of order 3 and degree 2. Results are displayed on Figure 2.2 and show that the work presented in this paper is indeed a concrete progress for the considered task, compared to previous state of the art: experiments have shown that our algorithm was already more than twice as fast (on the same machine) than the algorithm of [BCS14] [1] for $N \sim 10^4$. Figure 2.3 shows the ratio of computation times for operators of varying sizes. Results tend to indicate that the good performances of our algorithm compared to the iteration of [BCS14] appear earlier when the order of the operator grows. Further experiments should be conducted to determine the influence of the degree of the coefficients.

2.5.2 Execution on special operators

Our algorithm was also tested on various "special" operators. One example is an operator proven in [BK10] to annihilate the generating function $G(t; 1, 0)$ of Gessel walks in the quarter plane ending on the horizontal axis. The result of this test indicates that this operator has a nilpotent p-curvature for all primes $p < 200$. This was of course expected since the generating function of Gessel walks is algebraic [BK10], hence the p-curvatures of its minimal-order differential operator are all zero. A similar test was performed on an operator proved in [BKV21] to annihilate the generating function of Kreweras walks with interacting boundaries, which is not algebraic. Once again, the result of this test indicates that this operator has a nilpotent p-curvature for all primes

[1] The implementation of the algorithm from [BCS14] used can be found at https://github.com/raphitek/p_curvatures/blob/main/p_curvature_single.sage

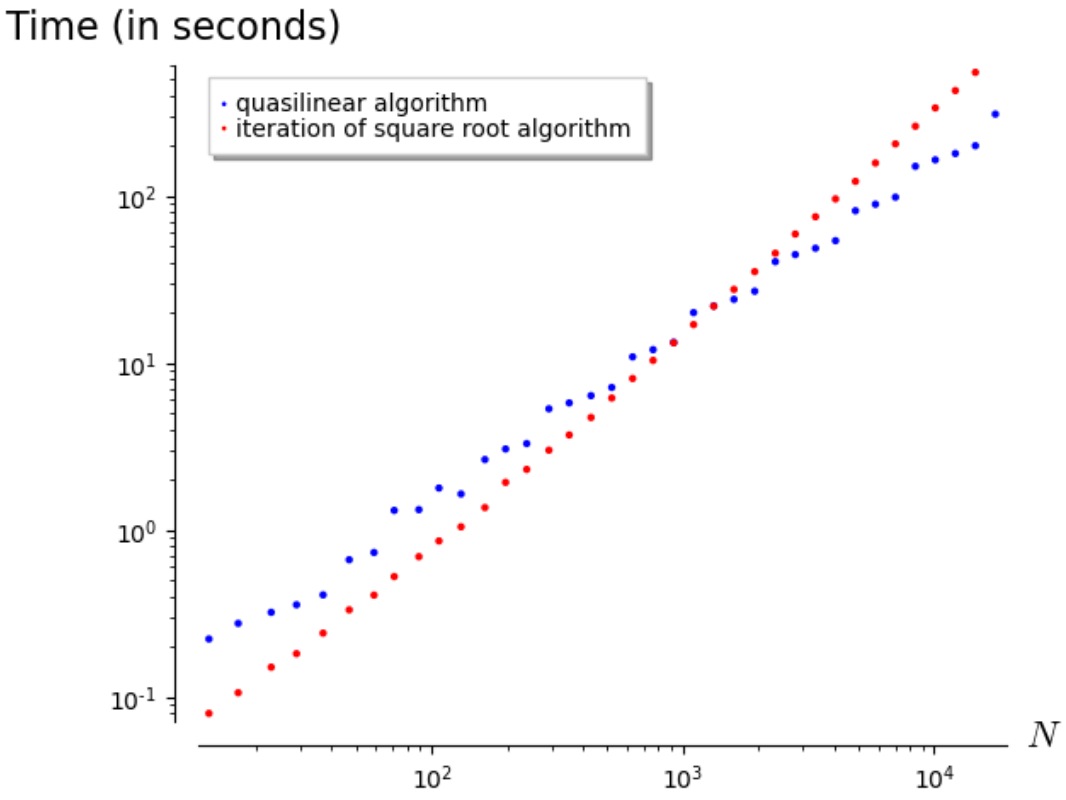


Figure 2.2: Comparison between iteration of [BCS14]'s algorithm and our algorithmtimes for operators of order 3 and degree 2

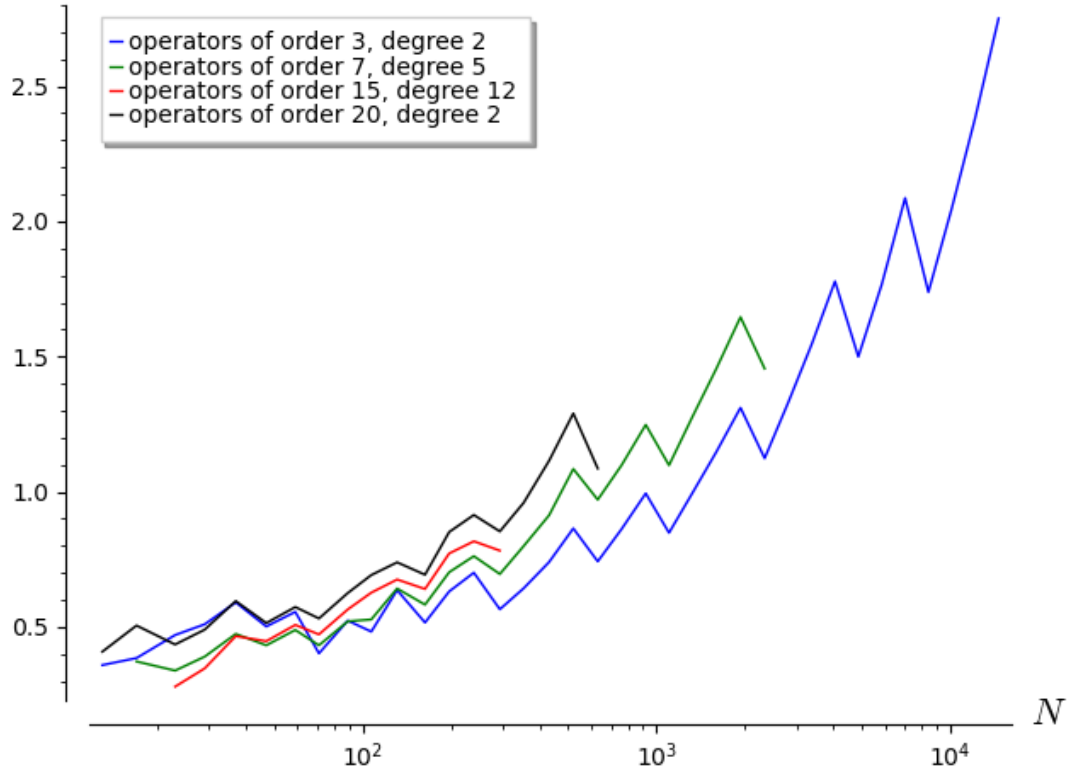


Figure 2.3: Ratio of computation times for operators of varying sizes

$p < 200$[2]. Further testing was conducted on all the 76 operators for (specializations of) the D-finite generating functions for lattice walks classified in [BCvH+17] with $p < 200$, with yet again similar results[3]. All those results were already predicted by Chudnovsky's theorem and make us quite confident in the accuracy of our implementation.

[2]The program running the above mentioned tests can be found at
https://github.com/raphitek/p_curvatures/blob/main/test_p_curvature.sage

[3]The precise list of operators we considered can be found at https://specfun.inria.fr/chyzak/ssw/ct-P.mpl and the testing file can be found at https://github.com/raphitek/p_curvatures/blob/main/ct-P.sage

Chapter 3

Factorisation and p-Riccati equation

From this point forward, we restrict our study to when $\mathcal{A}$ is a finite separable extension K of the field of rational functions $\mathbb{F}_p(x)$ and the derivation ∂ is $\frac{\mathrm{d}}{\mathrm{d}x}$. It was already established in Example 2.1.38 that such a field K verifies Hypothesis 2.1.37. We reuse the notations of Example 2.1.38. In particular, we will denote by C the field of constant of K.
In the previous chapter, we showed (Theorem 2.2.11) that by using the characteristic polynomial of the p-curvature of an operator $L \in K\langle\partial\rangle$, we could reduce the problem of finding a factorisation of L to the case when $\chi_{min}(L)$ is an irreducible polynomial N over C. The goal of this chapter is to develop factorisation method for such operators which may or may not be irreducible. To that end we are going to make great use of the central simple algebra structure of $\mathcal{D}_{N(\partial^p)}$ (see Notation 2.1.26). Indeed, $C[\partial^p]N(\partial^p)$ is a maximal ideal of $C[\partial^p]$. In particular ${}^{C[\partial^p]}/_{N(\partial^p)}$ is a field and it is easy to show that $\mathcal{D}_{N(\partial^p)} \simeq K\langle\partial\rangle \otimes_{C[\partial^p]} {}^{C[\partial^p]}/_{N(\partial^p)}$. It was established in Theorem 2.1.45 that $K\langle\partial\rangle \otimes_{C[\partial^p]} {}^{C[\partial^p]}/_{N(\partial^p)}$ is a central simple ${}^{C[\partial^p]}/_{N(\partial^p)}$-algebra. In the first section of this chapter we explain how the central simple algebra structure of $\mathcal{D}_{N(\partial^p)}$ strongly determines the structure of L's factorisation. We then explain how finding such factorisations is equivalent to solving a particular equation in a separable finite extension of K. We will call the particular equation the p-Riccati equation and the following sections will be dedicated to its effective resolution which will finally allow us to design a complete factorisation algorithm.

3.1 Central simple algebra structure and Morita's equivalence

Notation 3.1.1. We recall that K is a finite separable field extension of $\mathbb{F}_p(x)$ equipped with the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$. Its field of constants is denoted $C := \{f^p | f \in K\}$. We recall that according to Example 2.1.38, K verifies Hypothesis 2.1.37.
Let $N \in C[Y]$ be an irreducible polynomial. We denote by $C_N := {}^{C[Y]}/_{N(Y)}$ the extension of C generated by a root of N.
We recall that $\mathcal{D}_{N(\partial^p)}$ denotes the quotient ${}^{K\langle\partial\rangle}/_{N(\partial^p)}$. Since $N(\partial^p)$ is central in $K\langle\partial\rangle$ this is a ring.
Throughout this section, unless otherwise specified, $L \in K\langle\partial\rangle$ will always denote a divisor of $N(\partial^p)$.

Lemma 3.1.2. — *We have an isomorphism*

$$\mathcal{D}_{N(\partial^p)} \simeq K\langle\partial\rangle \otimes_{C[\partial^p]} {}^{C[\partial^p]}/_{N(\partial^p)}.$$

It follows that $\mathcal{D}_{N(\partial^p)}$ is a central simple C_N-algebra of dimension p^2.

Proof. There are canonical morphisms $K\langle\partial\rangle \to \mathcal{D}_{N(\partial^p)}$ and ${}^{C[\partial^p]}/_{N(\partial^p)} \to \mathcal{D}_{N(\partial^p)}$ which generates a natural morphism of C_N-algebras $K\langle\partial\rangle \otimes_{C[\partial^p]} {}^{C[\partial^p]}/_{N(\partial^p)} \to \mathcal{D}_{N(\partial^p)}$. Furthermore, since $K\langle\partial\rangle$ is a free $C[\partial^p]$ algebra of dimension p^2, $K\langle\partial\rangle \otimes_{C[\partial^p]} {}^{C[\partial^p]}/_{N(\partial^p)}$ is a free ${}^{C[\partial^p]}/_{N(\partial^p)}$-algebra of dimension p^2 of which a basis is given by $(x^i\partial^j \otimes 1)_{(i,j)\in[\![0;p-1]\!]^2}$. We check that the image of this basis in $\mathcal{D}_{N(\partial^p)}$, $(x^i\partial^j)_{(i,j)\in[\![0;p-1]\!]^2}$ is free. Since it is also a $C[\partial^p]$ generating family of $\mathcal{D}_{N(\partial^p)}$ we do have an isomorphism.

The fact that $\mathcal{D}_{N(\partial^p)}$ is a central simple C_N-algebra of dimension p^2 is a direct consequence of Theorem 2.1.45 (when identifying C_N with ${}^{C[\partial^p]}/_{N(\partial^p)}$ through $Y \mapsto \partial^p$). □

If L is a divisor of $N(\partial^p)$, then $\mathcal{D}_L$ has a structure of $\mathcal{D}_{N(\partial^p)}$-module which explains the interest in studying the structure of $\mathcal{D}_{N(\partial^p)}$. We will in fact later reduce the factorisation of L entirely to that of $N(\partial^p)$.

We recall the Artin-Wedderburn theorem [AF92, Thm. 2.1.3] about the structure of finite dimensional central simple algebras:

THEOREM 3.1.3 (Artin-Wedderburn). — *Let k be a field and $\mathcal{A}$ be a central simple k-algebra. Then there exists a central k-division algebra D and $n \in \mathbb{N}^*$ such that $\mathcal{A} \simeq M_n(D)$.*

With the notations of the previous theorem we then find $\dim_k \mathcal{A} = n^2 \dim_k D$. Since $\mathcal{D}_{N(\partial^p)}$ is of dimension p^2 over C_N we deduce the following statement about its structure:

COROLLARY 3.1.4. — *$\mathcal{D}_{N(\partial^p)}$ is either a division algebra, or isomorphic to $M_p(C_N)$.*

In [vdP95] this result is the origin of a discussion about division algebras of dimension p^2 over C_N. For our work, it will be enough to be able to determine whether $\mathcal{D}_{N(\partial^p)}$ is a division algebra or not. Of course this is easy to tell if $L \neq N(\partial^p)$. Indeed, in this case L is a nontrivial zero divisor in $\mathcal{D}_{N(\partial^p)}$. This means that $\mathcal{D}_{N(\partial^p)}$ cannot be a division algebra and is thus isomorphic to $M_p(C_N)$.

REMARK 3.1.5. — If N is not separable over C then $\mathcal{D}_{N(\partial^p)}$ is isomorphic to a matrix ring. Indeed, in this case there exists $P \in K[Y]$ such that $N(Y) = P^p(Y)$. Thus $N(\partial^p) = (P(\partial^p))^p$ since $K[\partial^p]$ is commutative, and $\mathcal{D}_{N(\partial^p)}$ has non trivial zero divisors.

Conversely, when $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ cannot have any nontrivial divisor. Thus we would have $L = N(\partial^p)$ and the factorisation would be done, provided that we are able to prove that $\mathcal{D}_{N(\partial^p)}$ is a division algebra. However, all previous works on factorisation left this problem unsolved in the case where no nontrivial divisor of $N(\partial^p)$ is known. In section 3.3.3, we will present a polynomial time algorithm testing the irreducibility of $N(\partial^p)$ (and thus whether $\mathcal{D}_{N(\partial^p)}$ is a division algebra or not). For now, we focus on the case where $\mathcal{D}_{N(\partial^p)} \simeq M_p(C_N)$. Then $\mathcal{D}_L$ is a $M_p(C_N)$-module. Morita's theorem [AF92, Corollary 22.6], which we recall below, states that $\mathcal{D}_L$ corresponds uniquely to a finite dimensional C_N-vector space.

THEOREM 3.1.6 (Morita's equivalence). — *Let R be a ring (not necessarily commutative). There exists a functor*
$\mathcal{M}\mathrm{or}_N : \mathrm{Mod}^l_R \to \mathrm{Mod}^l_{M_n(R)}$ which realises a categorical equivalence between the left-R-modules and the left-$M_n(R)$-modules. Furthermore:

1. *If R is a finite dimensional k-algebra with k a field, then for all finitely generated left-R-module M,*
$$\dim_k(\mathcal{M}\mathrm{or}_N(M)) = n\dim_k(M).$$
2. *If R is a field then two finite dimensional (over R) left-$M_n(R)$-modules are isomorphic if and only if their dimensions over R are equal.*

Proof. See appendix A. □

This result yields a some significant corollaries.

Corollary 3.1.7. — *Let $L \in K\langle\partial\rangle$ be a divisor of some $N(\partial^p)$ where $N \in C[Y]$ is an irreducible polynomial. This is equivalent to saying that $\chi_{min}(L) = N(\partial^p)$. Then*

i) $\mathcal{D}_L$ is a direct sum of simple differential modules.

If we suppose in addition that $\mathcal{D}_{N(\partial^p)} \simeq M_p(C_N)$ then:

ii) $\mathrm{ord}(L)$ *is a multiple of* $\deg(N)$. *More precisely* $\mathrm{ord}(L) = \deg(N)\cdot\dim_{C_N}\mathcal{M}\mathrm{or}_N(\mathcal{D}_L)$.

iii) L is irreducible if and only if $\mathrm{ord}(L) = \deg(N)$.

Proof. We denote $\mathcal{M}\mathrm{or}_N^{-1}$ the quasi-inverse functor of the functor $\mathcal{M}\mathrm{or}_N$ defined in Theorem 3.1.6. We begin by proving that if $\mathcal{D}_{N(\partial^p)} \simeq M_p(C_N)$ then a finite dimensional (over C_N) $\mathcal{D}_{N(\partial^p)}$-module M is simple if and only $\mathcal{M}\mathrm{or}_N^{-1}(M)$ is a C_N-line. Indeed, if $\mathcal{M}\mathrm{or}_N^{-1}(M)$ is a C_N-line, then from Theorem 3.1.6 (2), we know that $\dim_{C_N}(M) = p$. But we also know that if $M' \subset M$ is a submodule of M then $\dim_{C_N}(M') \leqslant \dim_{C_N} M$. But from Theorem 3.1.6 (2) we know that $\dim_{C_N}(M')$ is a multiple of p so we either have $M' = \{0\}$ or $M' = M$.
Conversely, if $\mathcal{M}\mathrm{or}_N^{-1}(M)$ is not a C_N-line then $\mathcal{M}\mathrm{or}_N^{-1}(M)$ (which is a C_N-vector space) can be written as a direct sum of two nontrivial subspaces. Since direct sums are a categorical construct, M can also be written as a direct sum of two nontrivial differential modules. In particular it has nontrivial submodules and is not simple.

i) If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $L = N(\partial^p)$ and $\mathcal{D}_L$ is already irreducible. Suppose now that $\mathcal{D}_{N(\partial^p)} \simeq M_p(C_N)$. Then $\mathcal{M}\mathrm{or}_N^{-1}(\mathcal{D}_L)$ is a finite dimensional C_N-vector space. Thus it is a finite direct sum of C_N-lines. Moreover C_N-lines correspond to irreducible $\mathcal{D}_{N(\partial^p)}$-modules and since direct sums are a categorical construction, $\mathcal{D}_L$ is isomorphic to a direct sum of irreducible modules.

ii) We recall that a left Euclidean division exists over $K\langle\partial\rangle$, thus for any $L \in K\langle\partial\rangle$ a K-basis of the quotient module $\mathcal{D}_L$ is $(1, \partial, \ldots, \partial^{r-1})$ where r is the order of L. It follows that we have:

$$\begin{aligned}
\mathrm{ord}(L) &= \dim_K \mathcal{D}_L \\
&= \frac{1}{p}\dim_C \mathcal{D}_L \\
&= \frac{[C_N : C]}{p}\dim_{C_N} \mathcal{D}_L \\
&= \frac{\deg(N)}{p}\cdot p\dim_{C_N}\mathcal{M}\mathrm{or}_N(\mathcal{D}_L) \\
&= \deg(N)\cdot\dim_{C_N}\mathcal{M}\mathrm{or}_N(\mathcal{D}_L)
\end{aligned}$$

iii) L is irreducible if and only if $\mathcal{D}_L$ is an irreducible differential $\mathcal{D}_{N(\partial^p)}$-module. This is equivalent to $\mathcal{M}\mathrm{or}_N(\mathcal{D}_L)$ being an irreducible C_N vector space that is to say that $\dim_{C_N} \mathcal{M}\mathrm{or}_N(\mathcal{D}_L) = 1$. Doing the computation of the previous point again this yields

$$\mathrm{ord}(L) = \deg(N).$$

□

REMARK 3.1.8. — *i)* means that L can be written as the least common left multiple of irreducible operators which is a particular case of van der Put's classification of differential modules. This fact was used by Giesbrecht and Zhang in [GZ03, Theorem 3.6] to link nontrivial zero divisors of the ring of endomorphism of $\mathcal{D}_L$ to nontrivial divisors of L.

A few interesting results can be deduced from this, although they won't have much use for the factorisation in itself. The first is a refinement of 2.2.8(iii).

PROPOSITION 3.1.9. — *Let $L \in K\langle\partial\rangle \backslash C[\partial^p]$. L is irreducible if and only if $\chi(\psi_p^L)$ is irreducible in $C[Y]$.*

Proof. We write $N := \chi(\psi_p^L)$. Suppose that N is irreducible over C. Then $L|N(\partial^p)$ and since $\deg(N) = \mathrm{ord}(L)$, L is irreducible (see Corollary 3.1.7 (iii)).
If now we know that L is irreducible then we know from Proposition 2.2.8(iii) that there exist $N \in C[Y]$ irreducible and $\nu \in \mathbb{N}$ such that $\chi(\psi_p^L) = N^\nu$. Since L is irreducible, $L = \mathrm{gcrd}(L, N(\partial^p))$, thus $L|N(\partial^p)$. Since L is not central, $L \neq N(\partial^p)$ thus $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$ and $\mathrm{ord}(L) = \deg(N)$ since L is irreducible. Moreover, since $\mathrm{ord}(L) = \deg(\chi(\psi_p^L))$ it follows that $\nu = 1$. Thus $\chi(\psi_p^L)$ is irreducible over C. □

The second is the foretold criterium on the finiteness of factorisations of a given $L \in K\langle\partial\rangle$.

THEOREM 3.1.10. — *Let $L \in K\langle\partial\rangle$. If ψ_p^L (defined in (2.2)) is cyclic then L has a finite number of factorisations. If K is a separably closed field then it is a equivalence.*

Proof. Let $\chi_{min}(L) = N_1^{\nu_1} \cdots N_n^{\nu_n}$ with the N_i being pairwise distinct irreducible polynomials over C. Let L_1 be an irreducible right divisor of L. Then $\chi_{min}(L_1)$ is irreducible (otherwise the gcrd of L_1 and an irreducible component of $\chi_{min}(L_1)$ applied to ∂^p would be a nontrivial factor of L_1) and divides $\chi_{min}(L)$. Thus there exists $j \in [\![1; n]\!]$ such that L_1 is a right divisor of $\mathrm{gcrd}(L, N_j(\partial^p))$.
We can deduce that L has a finite number of irreducible right divisors if and only if for all $j \in [\![1; n]\!]$, $\mathrm{gcrd}(L, N_j(\partial^p))$ has a finite number of right divisors. Suppose that $\mathcal{D}_{N_j(\partial^p)}$ is isomorphic to $M_p(C_{N_j})$. Then irreducible divisors of $\mathrm{gcrd}(L, N_j(\partial^p))$ are in bijection with vectorial lines in $\mathcal{M}\mathrm{or}_{N_j}(\mathcal{D}_{\mathrm{gcrd}(L,N_j(\partial^p))})$ which are finite in number if and only if $\mathrm{gcrd}(L, N_j(\partial^p))$ is irreducible which, according to Corollary 3.1.7, is to say that

$$\mathrm{ord}(\mathrm{gcrd}(L, N_j(\partial^p))) = \deg(N_j).$$

Let us suppose that ψ_p^L is cyclic. We claim that for any pair $L', R \in K\langle\partial\rangle$ such that $L'R = L$, $\psi_p^{L'}$ and ψ_p^R are also cyclic. Indeed we have $\chi_{min}(L)|\chi_{min}(L')\chi_{min}(R)$. Thus

$$\deg(\chi_{min}(L)) \leqslant \deg(\chi_{min}(L')) + \deg(\chi_{min}(R)) \leqslant \deg(\chi(\psi_p^{L'}) + \deg(\chi(\psi_p^R)) = \deg(\chi(\psi_p^L)).$$

If ψ_p^L is cyclic then all the previous inequalities become equalities. In particular we find $\chi_{min}(R) = \chi(\psi_p^R))$ and $\chi_{min}(L') = \chi(\psi_p^{L'})$ which shows that ψ_p^R and $\psi_p^{L'}$ are indeed cyclic.
In particular for $R := \operatorname{gcrd}(L, N_j(\partial^p)$ we have

$$\chi_{min}(R) = \chi(\psi_p^R).$$

But since $\chi_{min}(R) = N_j$ and $\deg(\chi(\psi_p^R)) = \operatorname{ord}(R)$ we have $\operatorname{ord}(R) = \deg(N_j)$ and $R = \operatorname{gcrd}(L, N_j(\partial^p))$ is irreducible.

Thus we have shown that if ψ_p^L is cyclic then L has a finite number of irreducible right divisor and any divisor L' of L also has a cyclic p-curvature, thus by recurrence, L has a finite number of factorisation.

We suppose now that K is separably closed and that L has a finite number of factorisations. In particular we have

$$\operatorname{ord}(\operatorname{gcrd}(L, N_j(\partial^p)) = \deg(N_j)$$

for all $j \in [\![1; n]\!]$. Since all central simple C_{N_j}-algebras split over a separable extension of C_{N_j}, all $\mathcal{D}_{N_j(\partial^p)}$ are isomorphic to a matrix ring. Indeed since K is separably closed, so is C. Either C_{N_j} is inseparable over C which means that $\mathcal{D}_{N_j}$ is split, or $C = C_{N_j}$ and $\mathcal{D}_{N_j(\partial^p)}$ is split because there are no nontrivial separable extension of C.

We consider $L_n = \operatorname{gcrd}(L, N_n^{\nu_n}(\partial^p))$ and set $L_{n,k} = \operatorname{gcrd}(L_n, N_n^k(\partial^p))$. Thus $L_{n,\nu_n} = L_n$ and $\mathcal{D}_L L_{n,k} = \operatorname{Im}(N_n^k(\psi_p^L))$. Finally $\mathcal{D}_{L_{n,k}} \simeq \ker(N_n^k(\psi_p^L))$. It follows that

$$\begin{aligned}\operatorname{ord}(L_n) &= \dim_K \mathcal{D}_{L_n} \\ &= \sum_{k=1}^{\nu_n} \dim_K \left({}^{\ker(N_n^k(\psi_p^L))}/_{\ker(N_n^{k-1}(\psi_p^L))}\right)\end{aligned}$$

But $\dim_K \left({}^{\ker(N_n^k(\psi_p^L))}/_{\ker(N_n^{k-1}(\psi_p^L))}\right) = \operatorname{ord}(L_{n,k}) - \operatorname{ord}(L_{n,k-1})$. By their definition, $L_{n,k}$ and $L_{n,k-1}$ differ by a factor which is a divisor of $N_n(\partial^p)$ so we have $\operatorname{ord}(L_{n,k}) - \operatorname{ord}(L_{n,k-1}) \geqslant \deg(N_n)$. But we also know that $\dim_K \left({}^{\ker(N_n^k(\psi_p^L))}/_{\ker(N_n^{k-1}(\psi_p^L))}\right) \leqslant \dim_K \ker(N_n(\psi_p^L)) = \operatorname{ord}(L_{n,1})$.
It follows that $\operatorname{ord}(L_n) = \nu_n \deg(N_n)$ if and only if $\operatorname{ord}(\operatorname{gcrd}(L, N_n(\partial^p))) = \deg(N_n)$.
Since the valuation of $\chi(\psi_p^L)$ in N_n is also the valuation of $\chi(\psi_p^{L_n})$ in N_n and since $\deg(\chi(\psi_p^{L_n})) = \operatorname{ord}(L_n)$, it follows that $\operatorname{ord}(\operatorname{gcrd}(L, N_n(\partial^p))) = \deg(N_n)$ if and only if $\chi_{min}(L)$ and $\chi(\psi_p^L)$ have the same valuation in N_n. Since the proof is symmetric for the other factors we find that L has a finite number of irreducible right divisors if and only if $\chi_{min}(L) = \chi(\psi_p^L)$ that is to say that ψ_p^L is cyclic.

□

Finally one last important irreducibility criterion is the following:

Lemma 3.1.11. — *Let N be an irreducible polynomial in $C[Y]$ such that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$. Then $L \in K\langle\partial\rangle$ is an irreducible divisor of $N(\partial^p)$ if and only if $\chi(\psi_p^L) = N$.*

Proof. Let $L \in K\langle\partial\rangle$. If $\chi(\psi_p^L) = N$ then $\chi(\psi_p^L)$ is irreducible. Since $\operatorname{ord}(L) = \deg(N) < \operatorname{ord}(N(\partial^p))$, $L \neq N(\partial^p)$ and in particular $L \notin C[\partial^p]$ so L is also irreducible (Proposition 3.1.9).
If now L is an irreducible divisor of $N(\partial^p)$ then we know that $\operatorname{ord}(L) = \deg(N)$ (Corollary 3.1.7).
Since N is irreducible we have $\chi_{min}(L) = N$ and $N|\chi(\psi_p^L)$. But since $\deg(\chi(\psi_p^L)) = \operatorname{ord}(L) = \deg(N)$ it follows that $\chi(\psi_p^L) = N$. □

We now present a way to reduce the factorisation of L to the factorisation of $N(\partial^p)$. We have seen that $\mathcal{D}_L$ is equivalent to a C_N-vector space through Morita's equivalence. We introduce a notion of hyperplane of $\mathcal{D}_L$ mimicking the usual notion of hyperplane through Morita's equivalence.

DEFINITION-PROPOSITION 3.1.12. — *Let M be a finite dimensional differential K-module. A hyperplane of M is a maximal proper submodule of M.*

i) Suppose $M = \mathcal{D}_L$. Let L' be a right divisor of L. The submodule $\mathcal{D}_L L'$ is a hyperplane of $\mathcal{D}_L$ if and only if L' is irreducible.

ii) Suppose that M is a $\mathcal{D}_{N(\partial^p)}$-module. A submodule $M' \subset M$ is a hyperplane of M if and only if $\mathcal{M}\mathrm{or}_N(M')$ is a hyperplane of $\mathcal{M}\mathrm{or}_N(M)$.

Proof. i) $\mathcal{D}_L L'$ is a hyperplane if and only if $\mathcal{D}'_L \simeq {}^{\mathcal{D}_L}/_{\mathcal{D}_L L'}$ is a simple differential K-module which is to say that L' has no nontrivial right divisor. Thus L' is irreducible.

ii) The submodule $M' \subset M$ is a maximal proper submodule of M if and only if $\mathcal{M}\mathrm{or}_N(M')$ is a maximal proper subspace of $\mathcal{M}\mathrm{or}_N(M)$.

□

Hyperplanes are convenient objects to consider since the intersection of a subspace with a hyperplane is usually a hyperplane itself. This is very useful since $\mathcal{D}_L$ can be seen as a submodule of $\mathcal{D}_{N(\partial^p)}$. Indeed let $R \in K\langle\partial\rangle$ such that $LR = N(\partial^p)$. Then

$$\begin{array}{rccc} \iota_L : & \mathcal{D}_L & \to & \mathcal{D}_{N(\partial^p)}R \\ & M \mod L & \mapsto & MR \mod N(\partial^p) \end{array}$$

is an isomorphism. A consequence is that irreducible factors of L can be "easily" recovered from the knowledge of irreducible factors of $N(\partial^p)$.

THEOREM 3.1.13. — *Let $L \in K\langle\partial\rangle$ be a divisor of $N(\partial^p)$ and $R \in K\langle\partial\rangle$ be such that $LR = N(\partial^p)$. Let $(H_i)_{i\in[\![1;p]\!]}$ be a family of irreducible divisors of $N(\partial^p)$ such that $N(\partial^p) = \mathrm{lclm}_{i=1}^p H_i$. Then there exists $I \subset [\![1;p]\!]$ of cardinality $\frac{\mathrm{ord}(L)}{\deg(N)}$ such that:*

i) for all $i \in I$, $L_i := \mathrm{lclm}(R, H_i) \cdot R^{-1}$ is an irreducible right divisor of L.

ii) $L = \mathrm{lclm}_{i\in I} L_i$.

REMARK 3.1.14. — The expression $\mathrm{lclm}(R, H_i) \cdot R^{-1}$ is valid as it can be seen as a division in the right ring of fractions of $K\langle\partial\rangle$ which can be seen as $K\langle\partial\rangle \otimes_{C[\partial^p]} C(\partial^p)$.
In practice however, algorithms computing $\mathrm{lclm}(R, H_i)$ compute a cofactor $Q \in K\langle\partial\rangle$ such that $QR = \mathrm{lclm}(R, H_i)$. It follows that $Q = \mathrm{lclm}(R, H_i) \cdot R^{-1}$ and that its computation does not require any additional operation.

Proof of Theorem 3.1.13. We know that $\mathcal{D}_L$ is embedded in $\mathcal{D}_{N(\partial^p)}$ as $\mathcal{D}_{N(\partial^p)}R$.
Since $\mathrm{lclm}_{i=1}^p(H_i) = N(\partial^p)$, we know that

$$\bigcap_{i=1}^{p} \mathcal{D}_{N(\partial^p)} H_i = \{0\}.$$

Since the H_i are irreducible, $\mathcal{D}_{N(\partial^p)}H_i$ is a hyperplane of $\mathcal{D}_{N(\partial^p)}$. For any $i \in [\![1;p]\!]$ such that $\mathcal{D}_{N(\partial^p)}H_i$ does not contain $\mathcal{D}_{N(\partial^p)}R$, the module $\mathcal{D}_{N(\partial^p)}H_i \cap \mathcal{D}_{N(\partial^p)}R = \mathcal{D}_{N(\partial^p)}\mathrm{lclm}(H_i, R)$ is an hyperplane of $\mathcal{D}_{N(\partial^p)}R$. Furthermore such H_i necessarily exist, since the intersection of the $\mathcal{D}_{N(\partial^p)}H_i$ is reduced to 0.
According to Corollary 3.1.7 (ii), the C_N vector space $V := \mathcal{M}\mathrm{or}_N(\mathcal{D}_L)$ is of dimension $n = \frac{\mathrm{ord}(L)}{\deg(N)}$. From any family of hyperplanes of V of intersection reduced to zero we can extract a family of n hyperplanes whose intersection is reduced to zero.
Thus from the family $(\mathcal{D}_{N(\partial^p)}\mathrm{lclm}(H_i, R))_{i\in[\![1;p]\!]}$, one can extract a family I of n hyperplanes of intersection reduced to zero.

Now we notice that $\mathcal{D}_{N(\partial^p)}\mathrm{lclm}(H_i, R) = \iota_L(\mathcal{D}_L\mathrm{lclm}(H_i, R) \cdot R^{-1})$. It follows that:

i) For i in I, $\mathcal{D}_L\mathrm{lclm}(H_i, R) \cdot R^{-1}$ is a hyperplane of $\mathcal{D}_L$. Since $\mathrm{lclm}(H_i, R)$ is both a multiple of R and a divisor of $N(\partial^p)$, we have $\mathrm{lclm}(H_i, R) = L'R$ and $N(\partial^p) = L''L'R$. Besides $N(\partial^p) = LR$ so $L''L' = L$ and L' is a divisor of L. Thus $\mathrm{lclm}(H_i, R) \cdot R^{-1}$ is an irreducible divisor of L.

ii) We know that $\bigcap_{i\in I} \mathcal{D}_L\mathrm{lclm}(H_i, R) \cdot R^{-1} = \{0\}$ which is precisely to say that

$$L = \mathrm{lclm}_{i\in I}\mathrm{lclm}(H_i, R) \cdot R^{-1}.$$

□

The question of finding such a family of irreducible operators will be discussed in the next section. Before we first mention the case where N is not separable over C.

Factorisation when N is not separable

Proposition 3.1.15. — *If N is not separable over C then $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.*

Proof. If N is not separable over C, then we can write $N = \sum_{i=1}^n c_i Y^{pi}$. Since $C = \{f^p | f \in K\}$, there exists $a_i \in K$ such that $a_i^p = c_i$. We write $Q = \sum_{i=1}^n a_i Y^i$. Then $N = Q^p$ and $N(\partial^p) = (Q(\partial^p))^p$. Since $N(\partial^p)$ is reducible in $K\langle\partial\rangle$, $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$. □

This means that unlike the general case, determining whether or not $N(\partial^p)$ is irreducible is very easy in the inseparable case. The proof even shows that finding an irreducible divisor of $N(\partial^p)$ is much easier in this case.

Lemma 3.1.16. — *If N is not separable over C then there exists $Q \in K[Y]$ such that $N = Q^p$. Then $Q(\partial^p)$ is an irreducible divisor of $N(\partial^p)$.*

Proof. The existence of Q in shown in the proof of Proposition 3.1.15. Then we see that $\mathrm{ord}(Q(\partial^p)) = p\deg(Q) = \deg(N)$. We deduce that $Q(\partial^p)$ is irreducible. □

If L is a divisor of $N(\partial^p)$ we could still try to compute a family H_i as in Theorem 3.1.13 by "twisting" the irreducible divisor $Q(\partial^p)$ of Lemma 3.1.16. This means taking random operators $H_i \in K\langle\partial\rangle$ coprime with $N(\partial^p)$ and computing $\mathrm{gcrd}(Q(\partial^p)H_i, N(\partial^p))$. Doing this p times yields a good family of irreducible operators with good probability. A deterministic way of computing an irreducible divisor of L is given by the following theorem.

THEOREM 3.1.17. — *Let $LR = N(\partial^p)$.*
If N is not separable and $Q \in K[Y]$ is such that $Q^p = N$ then there exists $i \in [\![1; p-1]\!]$ such that

$$\operatorname{lclm}(R, Q^i(\partial^p)) \cdot R^{-1}$$

is an irreducible right factor of L.

Proof. We know that the right multiplication by R embeds $\mathcal{D}_L$ in $\mathcal{D}_{N(\partial^p)}$ as $\mathcal{D}_{N(\partial^p)}R$ which corresponds to a subspace V of C_N^p by Morita equivalence. Similarly $(\mathcal{D}_{N(\partial^p)}Q^i(\partial^p))_{i\in[\![1;p]\!]}$ corresponds to a family $(U_i)_{i\in[\![0;p]\!]}$ of subspaces of C_N^p such that $U_i \subsetneq U_{i-1}$ for all $i \in [\![1; p]\!]$ and $U_0 = C_N^p$ and $U_p = \{0\}$. Thus there exists $i \in [\![1 : p]\!]$ such that $V \cap U_i$ is an hyperplane of V.
This means that $\mathcal{D}_{N(\partial^p)}R \cap \mathcal{D}_{N(\partial^p)}Q^i(\partial^p) = \mathcal{D}_{N(\partial^p)}\operatorname{lclm}(R, Q^i(\partial^p))$ is an hyperplane of $\mathcal{D}_{N(\partial^p)}R$. We deduce that $\mathcal{D}_L\operatorname{lclm}(Q^i(\partial^p), R) \cdot R^{-1}$ is an hyperplane of $\mathcal{D}_L$. Thus $\operatorname{lclm}(Q^i(\partial^p), R) \cdot R^{-1}$ is an irreducible divisor of L. □

3.2 The p-Riccati equation

In this section we discuss ways of finding irreducible right factors of L for different values of the minimal polynomial of its p-curvature. We begin by the most specific case and progress towards the most general.

3.2.1 When $\chi_{min}(L)(Y) = Y$

We suppose that $\chi_{min}(L)(Y) = Y$, which is to say that $\psi_p^L = 0$ or, equivalently, that L is a divisor of ∂^p. According to [vdPS03, Lemma 13.2] this means that L has a basis of solutions in K. In this case, irreducible divisors of L can be deduced from those solutions as we show in the following lemma.

LEMMA 3.2.1. — *Let $L \in K\langle\partial\rangle$ be such that $\chi_{min}(L)(Y) = Y$ and $f \in K^\times$ such that $L(f) = 0$. Then $\partial - \frac{f'}{f}$ is an irreducible right factor of L. Furthermore, all of the monic irreducible right factors of L are of this form.*

Proof. It is easy to see that $(\partial - \frac{f'}{f})(f) = 0$. Let $Q \in K\langle\partial\rangle$ and $a \in K$ be such that $L = Q(\partial - \frac{f'}{f}) + a$. Then

$$\begin{aligned} L(f) &= 0 \\ &= Q\left(\partial - \frac{f'}{f}\right)(f) + af \\ &= af \end{aligned}$$

It follows that $a = 0$ and $\partial - \frac{f'}{f}$ is a right factor of L. Since it is of order 1 it is irreducible.

If now N_1 is an irreducible right factor of L then in particular N_1 is an irreducible divisor of ∂^p. Since ∂^p is obviously not irreducible, we must have $\operatorname{ord}(N_1) = 1$. Since $\psi_p^{N_1} = 0$, N_1 has a solution, say f, in K. We can suppose that the leading coefficient of N_1 is 1. Then we can set $N_1 = \partial - g$ and $N_1(f) = f' - gf = 0$.
Thus $g = \frac{f'}{f}$. Finally if f is a solution of N_1 then it is also a solution of L since N_1 is a right factor of L. □

One way of factoring L is thus to compute a solution of L. When $K = \mathbb{F}_p(x)$ this can be done by solving a $p \times p$ linear system over $C = \mathbb{F}_p(x^p)$. From the dimension of this system it follows that the solutions found are usually of size at least linear in p. Another way is to use Theorem 3.1.13. Let $R \in K\langle\partial\rangle$ be such that $LR = \partial^p$.

Theorem 3.2.2. — *Let $(f_i)_{i\in[\![1;p]\!]}$ be a C-basis of K. Then there exists $I \subset [\![1;p]\!]$ of cardinality* $\mathrm{ord}(L)$ *such that:*

i) for all $i \in I$, $L_i := \mathrm{lclm}(R, \partial - \frac{f_i'}{f_i}) \cdot R^{-1}$ is an irreducible right divisor of L.

ii) $L = \mathrm{lclm}_{i\in I} L_i$.

Proof. It is enough to show that $\partial^p = \mathrm{lclm}_{i=1}^p \left(\partial - \frac{f_i'}{f_i}\right)$ according to Theorem 3.1.13. But since $\partial - \frac{f_i'}{f_i}$ is a factor of ∂^p for all i, $\mathrm{lclm}_{i=1}^p \left(\partial - \frac{f_i'}{f_i}\right)$ is a divisor of ∂^p. Furthermore $\mathrm{lclm}_{i=1}^p \left(\partial - \frac{f_i'}{f_i}\right)$ has p-linearly independent solutions so it is at least of order p. Thus $\mathrm{lclm}_{i=1}^p \left(\partial - \frac{f_i'}{f_i}\right) = \partial^p$. □

A C-basis of K is always given by the family $(x^i)_{i\in[\![0;p-1]\!]}$, from which we deduce the following corollary:

Corollary 3.2.3. — *There exists a family $I \subset [\![0; p-1]\!]$ of cardinal* $\mathrm{ord}(L)$ *such that*

i) for all $i \in I$, $L_i := \mathrm{lclm}(R, \partial - \frac{i}{x}) \cdot R^{-1}$ is an irreducible right divisor of L.

ii) $L = \mathrm{lclm}_{i\in I} L_i$.

3.2.2 When $\chi_{min}(L)(Y) = Y - a$ with $a \in C$

We now suppose that there exists $a \in C$ such that $\chi_{min}(L)(Y) = Y - a$. Let L_* be an irreducible factor of L. Then L_* is in particular an irreducible factor of $\partial^p - a$. If $\mathcal{D}_{\partial^p - a}$ is isomorphic to a matrix algebra then it follows that L_* is an operator of order 1 verifying $\chi(\psi_p^{L_*}) = Y - a$ (Corollary 3.1.11). Furthermore, up to a multiplicative constant, we can suppose that L_* is monic and of the form $N_1 = \partial - b$ with $b \in K$.

Lemma 3.2.4 (Lemma 1.3.2(1) [vdP95]). — *Let K be any differential field of positive characteristic p verifying Hypothesis 2.1.37. Then for any $b \in K$,*

$$\chi(\psi_p^{\partial - b}) = Y - b^{(p-1)} - b^p.$$

Proof. We give an alternative proof of this result. It is enough to show that $\psi_p^{\partial-b} = b^{(p-1)} + b^p$. We consider the application

$$\begin{array}{rccc} \tau : & K & \to & C \\ & b & \mapsto & \psi_p^{\partial - b} \end{array}.$$

The first step is to show that τ is additive. Let b_1 and $b_2 \in K$.
Then $\mathcal{D}_{\partial - b_1} \otimes_K \mathcal{D}_{\partial - b_2}$ is provided with the connexion

$$\tilde{\partial}(a_1 \otimes a_2) = \overline{\partial \cdot a_1} \otimes a_2 + a_1 \otimes \overline{\partial \cdot a_2}.$$

Furthermore, $\mathcal{D}_{\partial - b_1} \otimes_K \mathcal{D}_{\partial - b_2}$ is a K-vector space of dimension one generated by $e = 1 \otimes 1$. But then

$$\tilde{\partial}(e) = b_1 \otimes 1 + 1 \otimes b_2 = (b_1 + b_2)e.$$

Thus, as a differential module $\mathcal{D}_{\partial-b_1} \otimes_K \mathcal{D}_{\partial-b_2}$ is isomorphic to $\mathcal{D}_{\partial-b_1-b_2}$. Furthermore by recurrence we see that for any $a_1, a_2 \in K$,

$$\tilde{\partial}^k(a_1 \otimes a_2) = \sum_{i=0}^{k} \binom{k}{i} \overline{\partial^i \cdot a_1} \otimes \overline{\partial^{k-i} \cdot a_2}.$$

Thus by definition

$$\tilde{\partial}^p(a_1 \otimes a_2) = \psi_p^{\partial-b_1}(a_1) \otimes a_2 + a_1 \otimes \psi^{\partial-b_2}(a_2).$$

Finally we see that

$$\tilde{\partial}^p(e) = \tau(b_1+b_2)e = \psi_p^{\partial-b_1}e + \psi_p^{\partial-b_2}e = (\tau(b_1)+\tau(b_2))e.$$

Thus τ is additive.

We now show that for all $b \in K$, $\partial^p - \tau(b) = (\partial - b)^p$. We consider the map

$$\begin{array}{rccc} \mu_b : & K\langle\partial\rangle & \to & K\langle\partial\rangle \\ & \partial & \mapsto & \partial + b \end{array}.$$

It is an automorphism of $K\langle\partial\rangle$ mapping $\partial - b$ to ∂. Since μ_b is an automorphism, it maps central elements to central elements and preserve divisibility. Furthermore, from its definition it preserves the order and leading coefficients. It follows that $\mu_b(\chi(\psi_p^{\partial-b})(\partial^p)) = \mu_b(\partial^p - \tau(b))$ is a monic central multiple of $\mu_b(\partial - b) = \partial$ or order p. Thus $\mu_b(\partial^p - \tau(b)) = \partial^p$. Finally we find that

$$\partial^p - \tau(b) = \mu_{-b}(\partial^p) = (\mu_{-b}(\partial))^p = (\partial - b)^p.$$

Since τ is additive, it is enough to show the result for $b = cx^i$ for $i \in [\![0; p-1]\!]$ and $c \in C$. Since $(\partial - cx^i)^p$ is central we find that

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

where the $p_{i,j}$ are polynomials depending solely on i and j. This can be shown by recurrence as the constant coefficient of $(\partial - cx^i)^k$ is also the value of $(\partial - cx^i)^k$ applied to 1.
But since τ is additive, we must have

$$\sum_{j=1}^{p} p_{i,j}(x)(c+c')^j = \sum_{j=1}^{p} p_{i,j}(x)(c^j + c'^j)$$

which is to say that

$$\sum_{j=2}^{p-1} p_{i,j}(x)(c+c')^j - \sum_{j=2}^{p-1} p_{i,j}(x)(c^j + c'^j) = 0.$$

for all $c, c' \in C$. It follows that the polynomial

$$\sum_{j=2}^{p-1} p_{i,j}(x)Y^j - \left(\sum_{j=2}^{p-1} p_{i,j}(x)\right) Y$$

is of degree smaller than $p-1$ and any $k \in \mathbb{F}_p$ is a root of it. Thus it must be the zero polynomial and except for $j = 1$ and $j = p$, all the $p_{i,j} = 0$.

The only monomial in $(\partial - cx^i)^p$ providing c^p as a factor is $(cx^i)^p$. Thus $p_{i,p}(x) = x^{pi}$.

The products playing a role in $p_{i,1}(x)c$ are the terms of the form $\partial^l cx^i \partial^{p-1-l}$ since the other terms would make higher powers of c appear. Furthermore, if $l \neq p-1$ then any monomial coming from $\partial^l cx^i \partial^{p-1-l}$ is a multiple of ∂ so it does not appear in $\tau(cx^i)$.
If follows that $p_{i,1}(x)c$ is the constant coefficient of $\partial^{p-1} cx^i$ which is equal to $c\left(x^i\right)^{(p-1)}$. We finally have $\tau(cx^i) = c(x^i)^{(p-1)} + c^p x^{ip}$ which concludes the proof. □

An immediate corollary is that

Corollary 3.2.5. — *Let $a \in C$ be such that $\mathcal{D}_{\partial^p - a}$ is isomorphic to a matrix algebra. Then N_1 is a monic irreducible divisor of $\partial^p - a$ if and only if there exists $b \in K$ such that $b^{(p-1)} + b^p = a$ and $N_1 = \partial - b$.*

We call the equation

$$b^{(p-1)} + b^p = a \tag{3.1}$$

of unknown variable b the p-Riccati equation.

Corollary 3.2.6. — *Let $a \in C$. $\mathcal{D}_{\partial^p - a}$ is isomorphic to $M_p(C)$ if and only if (3.1) has a solution in K.*

Proof. If $\mathcal{D}_{\partial^p - a}$ is isomorphic to $M_p(C)$ then $\partial^p - a$ has irreducible monic divisors of order 1 of the form $\partial - b$. According to Corollary 3.2.5, b is a solution of (3.1). Conversely, if b is a solution of (3.1) then $\chi(\psi_p^{\partial - b})(\partial^p) = \partial^p - a$ and $\partial - b$ is a nontrivial divisor of $\partial^p - a$. Thus $\mathcal{D}_{\partial^p - a}$ is isomorphic to $M_p(C)$. □

Methods to solve the p-Riccati equation will be developed in the next section. However finding a solution to (3.1) is a way to find an irreducible divisor of $\partial^p - a$ but is not enough to factorise a divisor L of $\partial^p - a$.

Lemma 3.2.7. — *Let $b \in C$ be a solution of (3.1). We define the map*

$$\begin{array}{rccc} \mu_b : & K\langle\partial\rangle & \to & K\langle\partial\rangle \\ & \partial & \mapsto & \partial + b \end{array}$$

If $L \in K\langle\partial\rangle$ is such that $\chi_{min}(L)(Y) = Y - a$ then $\chi_{min}(\mu_b(L))(Y) = Y$.

Proof. μ_b defines an automorphism of $K\langle\partial\rangle$ which preserves divisibility. Thus $\mu_b(L)$ is a divisor of $\mu_b(\chi_{min}(L)(\partial^p)) = \mu_b(\partial^p - a) = \mu_b(\partial - b)^p = \partial^p$. Thus $\chi_{min}(\mu_b(L))(Y) = Y$. □

Thus we can apply the techniques of Section 3.2.1 to $\mu_b(L)$. This yields the three following corollaries:

Corollary 3.2.8. — *Let $b \in K$ be a solution of (3.1) and $f \in K$ verifying $\mu_b(L)(f) = 0$. Then $\partial - b + \frac{f'}{f}$ is an irreducible divisor of L.*

Proof. Since $\chi_{min}(\mu_b(L))(Y) = Y$ we know from lemma 3.2.1 that $\partial - \frac{f'}{f}$ is an irreducible right divisor of $\mu_b(L)$. Since μ_{-b} is an automorphism it preserves divisibility relations. Thus $\mu_{-b}(\partial - \frac{f'}{f}) = \partial - b - \frac{f'}{f}$ is an irreducible right divisor of $\mu_{-b}(\mu_b(L)) = L$. □

Let R be such that $LR = \partial^p - a$.

COROLLARY 3.2.9. — *Let $b \in K$ be a solution of (3.1) and $(f_i)_{i\in[\![1;p]\!]}$ be a C-basis of K. Then there exists $I \subset [\![1;p]\!]$ of cardinality* $\mathrm{ord}(L)$ *such that:*

i) for all $i \in I$, $L_i := \mathrm{lclm}(R, \partial - b - \frac{f_i'}{f_i}) \cdot R^{-1}$ is an irreducible right divisor of L.

ii) $L = \mathrm{lclm}_{i\in I} L_i$.

Proof. Since $\chi_{min}(\mu_b(L))(Y) = Y$, Theorem 3.2.2 states that there exists $I \subset [\![1;p]\!]$ of cardinality $\mathrm{ord}(\mu_b(L)) = \mathrm{ord}(L)$ such that:

i) for all $i \in I$, $L_i' := \mathrm{lclm}(\mu_b(R), \partial - \frac{f_i'}{f_i}) \cdot \mu_b(R)^{-1}$ is an irreducible right divisor of $\mu_b(L)$.

ii) $\mu_b(L) = \mathrm{lclm}_{i\in I} L_i'$.

Since μ_{-b} is an automorphism of $K\langle\partial\rangle$ it preserves divisibility relations. Furthermore, it maps left ideals to left ideals so it must commutes with lclms. It follows that

i) for all $i \in I$, $L_i := \mu_{-b}(\mathrm{lclm}(\mu_b(R), \partial - \frac{f_i'}{f_i}) \cdot \mu_b(R)^{-1}) = \mathrm{lclm}(R, \partial - b - \frac{f_i'}{f_i}) \cdot R^{-1}$ is an irreducible right divisor of $\mu_{-b}(\mu_b(L)) = L$.

ii) $\mu_{-b}(\mu_b(L)) = L = \mathrm{lclm}_{i\in I} L_i'$.

□

Finally, using the fact that $(x^i)_{i\in[\![0;p-1]\!]}$ is always a C-basis of K we get

COROLLARY 3.2.10. — *Let $b \in K$ be a solution of (3.1). There exists $I \subset [\![1;p]\!]$ of cardinality* $\mathrm{ord}(L)$ *such that:*

i) for all $i \in I$, $L_i := \mathrm{lclm}(R, \partial - b - \frac{i}{x}) \cdot R^{-1}$ is an irreducible right divisor of L.

ii) $L = \mathrm{lclm}_{i\in I} L_i$.

3.2.3 General case

In this section we consider the case where $\chi_{min}(L)$ is a separable irreducible polynomial $N \in C[Y]$. The method to solve the general case where $\chi_{min}(L)$ is any irreducible polynomial in $C[Y]$ of degree greater than 2 is to bring ourselves back to the case $\chi_{min}(L)$ of degree 1 at the price of a scalar extension. This of course implies that we are able to solve the p-Riccati equation in all generality which will be the focus of section 3.4.

Notation 3.2.11. Recall that $C_N = {}^{C[Y]}/_{N(Y)}$ and that K is a separable extension of $\mathbb{F}_p(x)$. We set $K_N = K \cdot C_N$ and we denote by y_N the image of Y in C_N.

Before going further we need to collect somme lemmas about K_N.

LEMMA 3.2.12. — *Let $Q \in K[Y]$ such that $Q^p(Y) = N(Y^p)$ and y_Q a root of Q in an algebraic closure of K.*

i) Q is irreducible and separable.

ii) $C_N = \{f^p | f \in K[y_Q]\}$.

iii) $K[y_Q] \simeq C_N[x]$. *In particular* $[K[y_Q] : C_N] = p$.

iv) $K_N \simeq K[y_Q]$.

Proof. i) The map $\iota_1 : f \mapsto f^p$ is an isomorphism between $K[Y]$ and $C[Y^p]$ and $\iota_2 : Y \mapsto Y^p$ is an isomorphism between $C[Y]$ and $C[Y^p]$. Since $\iota_2^{-1} \circ \iota_1(Q) = N$, Q is irreducible. Q is separable since $\iota_2^{-1} \circ \iota_1$ commutes with $\frac{\mathrm{d}}{\mathrm{d}Y}$.

ii) Since y_Q^p is a root of N and $C \subset \{f^p | f \in K[y_Q]\}$, $C_N \subset \{f^p | f \in K[y_Q]\}$. Furthermore we have

$$\begin{aligned}[K[y_Q] : C] &= [K[y_Q] : K][K : C] = \deg(Q) \cdot p = \deg(N) \cdot p \\ &= [K[y_Q] : C_N][C_N : C] = [K[y_Q] : C_N] \cdot \deg(N)\end{aligned}$$

It follows that $[K[y_Q] : C_N] = p$. Since we know that $K[y_Q]$ is separable over K, it is separable over $\mathbb{F}_p(x)$. From Proposition 2.1.38, we know that $[K[y_Q] : K[y_Q]^p] = p$. Thus $C_N = \{f^p | f \in K[y_Q]\}$.

iii) This is just Proposition 2.1.38.

iv) We have $C_N \subsetneq K_N \subset K[y_Q]$. Since $[K[y_Q] : C_N] = p$, this can only mean that $K_N = K[y_Q]$.

□

With Lemma 3.2.12 in mind we can construct the aforementioned scalar extension the following way:

Proposition 3.2.13. — *The injection $K \hookrightarrow K_N$ induces an injection $K\langle\partial\rangle \hookrightarrow K_N\langle\partial\rangle$. Its composite with the canonical projection $K_N\langle\partial\rangle \twoheadrightarrow {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ factors as follows.*

$$\begin{array}{ccc} K\langle\partial\rangle & \hookrightarrow & K_N\langle\partial\rangle \\ \downarrow & & \downarrow \\ \mathcal{D}_{N(\partial^p)} & \overset{\varphi_N}{\dashrightarrow} & {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)} \end{array}$$

where φ_N is an isomorphism of C_N-algebra.

Proof. The fact that φ_N is well defined is obvious since by definition of y_N, $Y - y_N$ divides N in $C_N[Y]$. We deduce that φ_N is a morphism of C_N-algebra from the fact that the following diagram commutes

$$\begin{array}{ccccc} & & C_N & & \\ & \swarrow^{\sim} & & \searrow_{\sim} & \\ {}^{C[\partial^p]}/_{N(\partial^p)} & & \longrightarrow & & {}^{C_N[\partial^p]}/_{(\partial^p - y_N)} \\ \downarrow & & & & \downarrow \\ \mathcal{D}_{N(\partial^p)} & & \xrightarrow{\varphi_N} & & {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)} \end{array}$$

Let us now show that φ_N is an isomorphism. We first show that φ_N is injective.
Let $L \in \ker(K\langle\partial\rangle \to {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)})$. We can write $L = \sum_{0 \leqslant i,j \leqslant p-1} l_{i,j}(\partial^p) x^i \partial^j$ with the $l_{i,j} \in$

$C[Y]$. From lemma 3.2.12 (iii) we deduce that the family $(x^i\partial^j)_{0\leqslant i,j\leqslant p-1}$ is a C_N-basis of ${}^{K_N\langle\partial\rangle}/_{\partial^p-y_N}$. This means that for all $i,j\in[\![0;p-1]\!]$, $Y-y_N$ divides $l_{i,j}$.
Thus y_N is a root of all $l_{i,j}$. But since the $l_{i,j}$ all have coefficients in C and N is the minimal polynomial of y_N over C, it follows that N divides all $l_{i,j}$.
Thus the ideal generated by $N(\partial^p)$ is precisely the kernel of the considered map. It follows that φ_N is injective. Since

$$\dim_{C_N}(\mathcal{D}_{N(\partial^p)})=p^2$$

and

$$\dim_{C_N}({}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)})=p[K_N:C_N]=p^2$$

we deduce that φ_N is also surjective by dimensional analysis. □

REMARK 3.2.14. — $K_N\langle\partial\rangle$ is well defined precisely because N is separable over C, which makes K_N separable as well and allows the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ to be well defined over K_N.
However, we can notice that in the separable case we have $K_N\simeq {}^{C[T]}/_{T^p-x^p}\otimes_C C_N$. This expression is still well defined even when N is not separable and is also equipped with a natural derivation $\frac{\mathrm{d}}{\mathrm{d}T}\otimes 0$.

For the rest of this thesis we will continue to denote the isomorphism of Proposition 3.2.13 by φ_N. $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$ if and only if this is also the case of ${}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)}$. In particular the theory developed for $\mathcal{D}_{N(\partial^p)}$ in the previous section can be applied here as well.

The two following lemmas on how φ_N affects submodules of $\mathcal{D}_{N(\partial^p)}$ will allow to transfer factorisations of ∂^p-y_N to factorisations of $N(\partial^p)$ and vice-versa.

LEMMA 3.2.15. — *We suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$. The morphisms φ_N and φ_N^{-1}:*

- *map hyperplanes to hyperplanes,*
- *map families of hyperplanes whose intersection is reduced to zero to families of hyperplanes whose intersection is reduced to zero.*

Proof. Since φ_N is an isomorphism (thus surjective), the image of a left ideal of $\mathcal{D}_{N(\partial^p)}$ is a left ideal of ${}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)}$. Furthermore since φ_N is an isomorphism, if H_i is a maximal proper ideal then so is $\varphi_N(H_i)$. Since for any two subsets $I,J\subset\mathcal{D}_{N(\partial^p)}$, $\varphi_N(I\cap J)=\varphi_N(I)\cap\varphi_N(J)$ we get the result. □

LEMMA 3.2.16. — *For all L' divisor of $N(\partial^p)$ in $K\langle\partial\rangle$ and all L'' divisor of ∂^p-y_N in $K_N\langle\partial\rangle$ the following holds true:*

- $\varphi_N(\mathcal{D}_{N(\partial^p)}\cdot L')={}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)}\cdot\operatorname{gcrd}(\varphi_N(L'),\partial^p-y_N)$
- $\varphi_N^{-1}({}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)}\cdot L'')=\mathcal{D}_{N(\partial^p)}\cdot\operatorname{gcrd}(\varphi_N^{-1}(L''),N(\partial^p))$.

Proof. Since L' is a generator of the left ideal $\mathcal{D}_{N(\partial^p)}\cdot L'$ of $\mathcal{D}_{N(\partial^p)}$, $\varphi_N(L')$ is a generator of the left ideal $\varphi_N(\mathcal{D}_{N(\partial^p)}\cdot L')$ of ${}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)}$.
Thus

$$\begin{aligned}\varphi_N(\mathcal{D}_{N(\partial^p)}\cdot L')&=\Big(K_N\langle\partial\rangle\varphi_N(L')+K_N\langle\partial\rangle(\partial^p-y_N)\Big)\Big/_{(\partial^p-y_N)}\\&=K_N\langle\partial\rangle\cdot\operatorname{gcrd}(\varphi_N(L'),\partial^p-y_N)\Big/_{(\partial^p-y_N)}.\end{aligned}$$

Mutatis mutandis, the proof for the second point is the same. □

From those two lemmas we see that the problem of factoring $N(\partial^p)$ in $K\langle\partial\rangle$ is equivalent to the problem of factoring $\partial^p - y_N$ in $K_N\langle\partial\rangle$. We can then apply the results of the previous section. In particular, Corollary 3.2.5 states that the monic irreducible divisors of $\partial^p - y_N$ are all the operators of the form $\partial - b$ with

$$b^{(p-1)} + b^p = y_N$$

Definition 3.2.17. — The equation

$$b^{(p-1)} + b^p = y_N \tag{3.2}$$

of unknown variable b is called the p-Riccati equation relative to N. We denote by $\mathcal{S}_N$ the set of its solutions in K_N

Lemma 3.2.18. — *$\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$ if and only if $\mathcal{S}_N$ is not empty.*

Proof. This is just Corollary 3.2.6 applied to ${}^{K_n\langle\partial\rangle}/_{\partial^p - y_N}$. The result is immediately deduced from it since $\mathcal{D}_{N(\partial^p)} \simeq {}^{K_N\langle\partial\rangle}/_{\partial^p - y_N}$. □

When $\mathcal{S}_N$ is not empty the whole set is easily deduced from one solution of (3.2) as shown in the following lemma:

Lemma 3.2.19. — *Let b be a solution of (3.2) in K_N. Then*

$$\mathcal{S}_N = \left\{ b + \frac{f'}{f} | f \in K_N \right\}.$$

Proof. Let $b_* \in S_N$. Then $(b - b_*)^{(p-1)} + (b - b_*)^p = y_N - y_N = 0$. It follows that $\chi_{min}(\partial - b + b_*)(Y) = Y$. From lemma 3.2.1 it follows that $b - b_*$ is of the form $\frac{f'}{f}$. Conversely, for all $f \in K_N$, $\gamma_b(\partial - b - \frac{f'}{f}) = \partial - \frac{f'}{f}$ is a divisor of ∂^p so $\gamma_{-b}(\gamma_b(\partial - b - \frac{f'}{f})) = \partial - b - \frac{f'}{f}$ is a divisor of $\gamma_{-b}(\partial^p) = \partial^p - y_N$. Thus $b + \frac{f'}{f} \in \mathcal{S}_N$. □

Let us now suppose that an element of S_N is known and see how this translates to a factorisation of L, a divisor of $N(\partial^p)$.

Theorem 3.2.20. — *Let $b \in \mathcal{S}_N$ and $(f_i)_{i\in[\![1;p]\!]}$ be a C_N-basis of K_N.*
Then for all $i \in [\![1;p]\!]$, $\operatorname{gcrd}\left(N(\partial^p), \varphi_N^{-1}\left(\partial - g - \frac{f_i'}{f_i}\right)\right)$ is an irreducible divisor of $N(\partial^p)$ and

$$N(\partial^p) = \operatorname{lclm}_{i=1}^{p} \operatorname{gcrd}\left(N(\partial^p), \varphi_N^{-1}\left(\partial - b - \frac{f_i'}{f_i}\right)\right).$$

Proof. We know by applying Corollary 3.2.9 to $\partial^p - y_N$ that $\partial^p - y_N = \operatorname{lclm}_{i=1}^{p}\left(\partial - b - \frac{f_i'}{f_i}\right)$. From what precedes we deduce that $\left(\partial - g - \frac{f_i'}{f_i}\right)_{i\in[\![1;p]\!]}$ generates a family of hyperplanes of ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ whose intersection is reduced to zero. Thus according to Lemma 3.2.15, φ_N^{-1} maps it to a family of hyperplanes of $\mathcal{D}_N$ whose intersection is reduced to zero. Using Lemma 3.2.16 it follows that $H_i := \operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - b - \frac{f_i'}{f_i}))$ is an irreducible divisor of $N(\partial^p)$ and $\bigcap_{i=1}^{p} \mathcal{D}_{N(\partial^p)} H_i = \{0\}$. Thus $N(\partial^p) = \operatorname{lclm}_{i=1}^{p} H_i$. □

In particular, using the fact that $(x^i)_{i\in[\![0;p-1]\!]}$ is always a C_N basis of K_N:

COROLLARY 3.2.21. — *Let $b \in \mathcal{S}_N$. For all $i \in [\![0;p-1]\!]$, $H_i := \operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - b) - \frac{i}{x})$ is an irreducible divisor of $N(\partial^p)$ and*

$$N(\partial^p) = \operatorname{lclm}_{i=0}^{p-1} H_i.$$

Let $L \in K\langle\partial\rangle$ be a monic divisor of $N(\partial^p)$ and $R \in K\langle\partial\rangle$ such that $LR = N(\partial^p)$. In particular R is monic. For any $g \in K_N$ we set

$$\mathcal{L}_g := \operatorname{lclm}(\operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - g)), R) \cdot R^{-1}.$$

The following Theorem is an analog of Corollary 3.2.9 in the general case.

THEOREM 3.2.22. — *1. If $L = N(\partial^p)$ and $S_N \neq \varnothing$ then $g \mapsto \mathcal{L}_g$ is a bijection between $\mathcal{S}_N$ and the set of monic irreducible right divisors of $N(\partial^p)$.*

2. If $S_N \neq \varnothing$, in general, all monic irreducible right divisors of L are of the form $\mathcal{L}_g$ with $g \in \mathcal{S}_N$.

3. For all $g \in \mathcal{S}_N$, there exists $\{i_1, ..., i_k\} \subset [\![0;p-1]\!]$ with $k = \frac{\operatorname{ord}(L)}{\deg(N)}$ such that

$$L = \operatorname{lclm}_{j=1}^{k} \left(\mathcal{L}_{g+\frac{i_1}{x}}, \mathcal{L}_{g+\frac{i_2}{x}}, \cdots, \mathcal{L}_{g+\frac{i_k}{x}} \right).$$

Proof. 1. In this case, $R = 1$ and $\mathcal{L}_g = \operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - g))$ for all $g \in K_N$. We know from Proposition 2.1.27 and Proposition 3.1.12 that there is a bijection between the set of monic irreducible divisors of $N(\partial^p)$ and hyperplanes of $\mathcal{D}_{N(\partial^p)}$. Similarly, there is a bijection between hyperplanes of ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ and monic irreducible divisors of $\partial^p - y_N$ in $K_N\langle\partial\rangle$. We know that the map $g \mapsto \partial - g$ is a bijection from $\mathcal{S}_N$ to the set of monic irreducible divisors of $\partial^p - y_N$. Since we know that φ_N^{-1} induces a bijection between the hyperplanes of $\mathcal{D}_{N(\partial^p)}$ and the hyperplanes of ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ (see Proposition 3.2.15) given by the formulas of Proposition 3.2.16, we finally deduce that $g \mapsto \mathcal{L}_g$ is a bijection between S_N and the set of monic irreducible divisor of $N(\partial^p)$.

2. If $L = 1$, L has no irreducible divisors. Suppose that $L \neq 1$, and thus that $\mathcal{D}_{N(\partial^p)} \cdot R \neq \{0\}$. Let L_* be a monic irreducible right divisor of L. We know that $\mathcal{D}_L$ is embedded in $\mathcal{D}_{N(\partial^p)}$ as $\mathcal{D}_{N(\partial^p)} \cdot R$ and thus $\mathcal{D}_L \cdot L_*$ is embedded in $\mathcal{D}_{N(\partial^p)}$ as $\mathcal{D}_{N(\partial^p)} \cdot L_*R$. Let H be a monic irreducible divisor of $N(\partial^p)$ such that $\mathcal{D}_{N(\partial^p)} \cdot H$ contains $\mathcal{D}_{N(\partial^p)} \cdot L_*R$ but not $\mathcal{D}_{N(\partial^p)} \cdot R$. Then

$$\mathcal{D}_{N(\partial^p)} \cdot L_*R \subset \mathcal{D}_{N(\partial^p)} \cdot H \cap \mathcal{D}_{N(\partial^p)} \cdot R = \mathcal{D}_{N(\partial^p)} \cdot \operatorname{lclm}(H, R).$$

But since L_* is an irreducible right divisor of L, $\mathcal{D}_{N(\partial^p)} \cdot L_*R$ is an hyperplane of $\mathcal{D}_{N(\partial^p)} \cdot R$, as is $\mathcal{D}_{N(\partial^p)} \cdot \operatorname{lclm}(H, R)$, since $\mathcal{D}_{N(\partial^p)} \cdot H$ does not contain $\mathcal{D}_{N(\partial^p)} \cdot R$.
Thus $\mathcal{D}_{N(\partial^p)} \cdot L_*R = \mathcal{D}_{N(\partial^p)} \cdot \operatorname{lclm}(H, R)$. Since both L_*R and $\operatorname{lclm}(H, R)$ are monic divisors of $N(\partial^p)$, we deduce that $L_*R = \operatorname{lclm}(H, R)$ and $L_* = \operatorname{lclm}(H, R) \cdot R^{-1}$.
Since H is an irreducible divisor of $N(\partial^p)$, according to the previous point it is of the form $\operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - g))$ for some $g \in \mathcal{S}_N$, and we get $L_* = \mathcal{L}_g$.

3. Let $g \in \mathcal{S}_N$. According to Proposition 2.1.38, the family $(x^i)_{i\in[\![0;p-1]\!]}$ is a C_N basis of K_N. Thus it follows from Theorem 3.2.20 that

$$N(\partial^p) = \operatorname{lclm}_{i=0}^{p-1} \operatorname{gcrd}\left(N(\partial^p), \varphi_N^{-1}\left(\partial - g - \frac{i}{x}\right)\right)$$

where each factor is an irreducible divisor of $N(\partial^p)$. The result follows from Theorem 3.1.13.

□

The "only" question that remains to be answered is how to solve the p-Riccati equation in all generality. In [vdP97], M. van der Put presents a way to find an element of $\mathcal{S}_N$ when a nontrivial divisor L of $N(\partial^p)$ is known.

Lemma 3.2.23 (M. van der Put). — *Suppose that L is a nontrivial divisor of $N(\partial^p)$ and set $L_N := \operatorname{gcrd}(\partial^p - y_N, \varphi_N(L))$.*
If $L_N = \partial^m + a_{m-1}\partial^{m-1} + \cdots + a_1\partial + a_0$, then $-\frac{a_{m-1}}{m} \in \mathcal{S}_N$.

Proof. By Proposition 3.2.16, L_N is a nontrivial divisor of $\partial^p - y_N$. Thus there exists $(f_1, \ldots, f_m) \in \mathcal{S}_N^m$ such that

$$L_N = (\partial - f_1)\cdots(\partial - f_m).$$

It follows that $a_{m-1} = -(f_1 + \cdots + f_m)$. Thus $-\frac{a_{m-1}}{m}$ is the barycentre of the f_i. Since $\mathcal{S}_N$ is an $\mathbb{F}_p$-affine space (Corollary 3.2.19), the result follows. □

One issue of this method is that even when the nontrivial divisor L is of "small" size, $\operatorname{gcrd}(L, \partial^p - y_N)$ usually has coefficients of size linear in p. Thus the solution of p-Riccati obtained this way has size linear in p. Furthermore the question of how to solve the p-Riccati equation when we do not know a nontrivial divisor of $N(\partial^p)$ remains open.

3.3 p-Riccati equation for Laurent series

In the previous section we have seen that factoring a differential operator of the form $N(\partial^p)$, with N an irreducible polynomial over C, is equivalent the solving the p-Riccati equation

$$f^{(p-1)} + f^p = y_N$$

over K_N. The relation between the p-Riccati equation and factorisation is not limited to algebraic function fields but appears more generally for any differential field verifying Hypothesis 2.1.37. This section is dedicated to the study of one of those cases, specifically $\mathbb{F}_q((t))$ where q is a power of p. We begin by presenting a criteria for determining whether the p-Riccati equation has a solution over $\mathbb{F}_q((t))$. Then we write explicit algorithms, to test this criteria and compute a solution of the p-Riccati equation in $\mathbb{F}_q((t))$ at arbitrary precision. Finally we use those results to design an irreducibility test for differential operators of the form $N(\partial^p) \in C[\partial^p]$. Unlike the algorithm to exhibit irreducible factors of such operators presented in the next sections, this irreducibility test runs in polynomial time in $\log(p)$. In particular, it runs in polynomials time in the size of its entry.

3.3.1 Resolution over $\mathbb{F}_q((t))$

We recall that $\mathbb{F}_q((t))$ is provided with a valuation $\nu : f \mapsto \max\{k \in \mathbb{Z} | f = O(t^k)\}$ verifying the following properties

- $\nu(f_1 f_2) = \nu(f_1) + \nu(f_2)$ for any $f_1, f_2 \in \mathbb{F}_q((t))$.
- $\nu(f) = \infty \Leftrightarrow f = 0$.
- $\nu(f_1 + f_2) \geqslant \min(\nu(f_1), \nu(f_2))$ with it being an equality if $\nu(f_1) \neq \nu(f_2)$.

We want to solve the equation

$$\partial^{p-1}(f) + f^p = a^p$$

of unknown variable f with $a \in \mathbb{F}_q((t))$, where ∂ is a nonzero derivation on $\mathbb{F}_q((t))$ verifying $\partial^p = 0$.

EXAMPLE 3.3.1. — Let q be a power of some prime number $p \in \mathbb{N}^*$. Then for any $i \in \mathbb{N}$, the derivation $\partial_i = t^i \frac{\mathrm{d}}{\mathrm{d}t}$ over $\mathbb{F}_q((t))$ verifies $\partial_i^p = 0$ if and only if $i \not\equiv 1 \mod p$.

Proof. $\partial_i^p = 0$ if and only if $\partial_i^p(t) = 0$. Let us write $\partial_i^j(t) = \lambda_{i,j} t^{\alpha_{i,j}}$. Then we find that $\partial_i^{j+1}(t) = \alpha_{i,j}\lambda_{i,j} t^{\alpha_{i,j}+(i-1)}$ which proves by induction that such $\lambda_{i,j}$ and $\alpha_{i,j}$ always exists and that $\lambda_{i,j+1} = \lambda_{i,j}\alpha_{i,j}$ and $\alpha_{i,j+1} = \alpha_{i,j} + (i-1)$, with $\lambda_{i,0} = \alpha_{i,0} = 1$. It follows that $\alpha_{i,j} = 1 + j(i-1)$. Then $\partial_i^p = 0$ if and only if $\lambda_{i,p} = 0$. But $\lambda_{i,p} = 0$ if and only if there exists $j \in [\![1; p-1]\!]$ such that $\alpha_{i,j} \equiv 0 \mod p$ which is to say that $j(i-1) \equiv -1 \mod p$. Such a j exists if and only if $i - 1 \not\equiv 0 \mod p$. □

LEMMA 3.3.2. — *The set of derivations over $\mathbb{F}_q((t))$ is $\mathbb{F}_q((t))\frac{\mathrm{d}}{\mathrm{d}t}$.*
In particular if ∂ is a derivation over $\mathbb{F}_q((t))$ then there exists $g \in \mathbb{F}_q((t))$ such that $\partial = g\frac{\mathrm{d}}{\mathrm{d}t}$.

Proof. It is easy to see that each element of $\mathbb{F}_q((t))\frac{\mathrm{d}}{\mathrm{d}t}$ is a derivation. Conversely let ∂ is a derivation over $\mathbb{F}_q((t))$ and set $g = \partial(t)$. For any $h \in \mathbb{F}_q((t))$ we know that $\partial(h^p) = 0$ which means that $\partial(\mathbb{F}_q((t^p))) = \{0\}$. Let $f \in \mathbb{F}_q((t))$. There exists $(f_0, \ldots, f_{p-1}) \in \mathbb{F}_q((t^p))^p$ such that

$$f = \sum_{k=0}^{p-1} f_k t^k.$$

But then

$$\partial(f) = \sum_{k=0}^{p-1} f_k \partial(t^k) = \sum_{k=0}^{p-1} k f_k \partial(t) t^{k-1} = g \sum_{k=0}^{p-1} k f_k t^{k-1} = g\frac{\mathrm{d}}{\mathrm{d}t} f.$$ □

Notation 3.3.3. Let ∂ be a derivation over $\mathbb{F}_q((t))$ and $g \in \mathbb{F}_q((t))$ such that $\partial = g\frac{\mathrm{d}}{\mathrm{d}t}$. We set

$$e(\partial) := 1 - \nu(g)$$

It is easy to see that $(\mathbb{F}_q((t)), \partial)$ verifies Hypothesis 2.1.37. A consequence, true in general but particularly helpful here, is the following:

LEMMA 3.3.4. — *Let ∂ be a nonzero derivation over $\mathbb{F}_q((t))$ such that $\partial^p = 0$. Then*

$$\ker(\partial) = \mathrm{Im}\,(\partial^{p-1}).$$

Proof. The inclusion $\operatorname{Im}(\partial^{p-1}) \subset \ker(\partial)$ is obvious.
We know that $(\mathbb{F}_q((t)), \partial)$ verifies Hypothesis 2.1.37. Let $C = \ker(\partial) = \mathbb{F}_q((t^p))$. We know that $[\mathbb{F}_q((t)) : C] = p$. But furthermore

$$\begin{aligned} p &= \dim_C \mathbb{F}_q((t)) \\ &= \dim_C \ker(\partial^p) \\ &= \sum_{k=1}^{p} \dim_C {}^{\ker(\partial^k)}\!/_{\ker(\partial^{k-1})} \end{aligned}$$

Since $\dim_C {}^{\ker(\partial^k)}\!/_{\ker \partial^{k-1}} \leqslant \dim_C \ker(\partial) = 1$ we can only have the equality if for any $k \in [\![1; p]\!]$, $\ker(\partial^{k-1})$ is an hyperplane of $\ker(\partial^k)$. Thus $\dim_C \ker(\partial^k) = k$ and $\dim_C \operatorname{Im}(\partial^k) = p - \dim_C \ker(\partial^k) = p - k$.
Thus $\dim_C \operatorname{Im}(\partial^{p-1}) = 1 = \dim_C \ker(\partial)$. □

Corollary 3.3.5. — *Let ∂ be a nonzero derivation over $\mathbb{F}_q((t))$ such that $\partial^p = 0$. Then:*

i) For any $f \in \operatorname{Im}(\partial)$ there exists $F \in \mathbb{F}_q((t))$ such that $\partial(F) = f$, p does not divide $\nu(F)$ and $\nu(F) = \nu(f) + e(\partial)$.

ii) The characteristic p does not divide $e(\partial)$.

Proof. i) Since $f \in \operatorname{Im}(\partial)$ there exists $F^* = \sum_{n=\nu(F^*)}^{\infty} F_n t^n$, with $F^*_{\nu(F^*)} \neq 0$ such that $\partial(F^*) = f$. But then

$$f = g \sum_{n=\nu(F)} n F_n t^{n-1}$$

We consider $F = F^* - \sum_{n\in\mathbb{Z}} F_{pn} t^{pn}$. We have $\partial(F) = \partial(F^*) = f$. Moreover by construction, p does not divide $\nu(F)$. By definition of $e(\partial)$, $\nu(f) = \nu(F) - e(\partial)$.

ii) Let $f \in \ker(\partial) = \mathbb{F}_q((t^p))$. From Lemma 3.3.4 we know that $f \in \operatorname{Im}(\partial^{p-1}) \subset \operatorname{Im}(\partial)$. In particular there exists $F \in \mathbb{F}_q((t))$ such that $\partial(F) = f$, p does not divide $\nu(F)$ and $\nu(F) = \nu(f) + e(\partial)$. In particular, $\nu(F) \equiv e(\partial) \mod p$. Since p does not divide $\nu(F)$, it does not divide $e(\partial)$ either.

□

We know that ∂ is of the form $g\frac{\mathrm{d}}{\mathrm{d}t} \in \mathbb{F}_q((t))\frac{\mathrm{d}}{\mathrm{d}t}$. We suppose that $g \neq 0$.

Proposition 3.3.6. — *Let $n \geqslant -e(\partial)$ and $f_0 \in \mathbb{F}_q((t))$ be such that*

$$\partial^{p-1}(f_0) + f_0^p = a^p + O(t^{pn}).$$

There exists an element $\mathcal{I}(f_0) \in (\partial^{p-1})^{-1}(a^p - \partial^{p-1}(f_0) - f_0^p)$ verifying $\nu(\mathcal{I}(f_0)) \geqslant pn + (p-1)e(\partial)$. We set $f_1 := f_0 + \mathcal{I}(f_0)$. Then

$$\begin{aligned} f_1 &= f_0 + O(t^{pn+(p-1)e(\partial)}) \\ \nu(\partial^{p-1}(f_1) + f_1^p - a^p) &\geqslant p(pn + (p-1)e(\partial)). \end{aligned}$$

Proof. We have $\partial(a^p - \partial^{p-1}(f_0) - f_0^p) = 0$ so according to Lemma 3.3.4, there exists $\mathcal{I}(f_0) \in \mathbb{F}_q((t))$ such that $\partial^{p-1}(\mathcal{I}(f_0)) = a^p - \partial^{p-1}(f_0) - f_0^p$. By applying Corollary 3.3.5 (i) recursively we show that we can suppose that $\nu(\mathcal{I}(f_0)) \geqslant pn + (p-1)e(\partial)$. Thus $f_1 = f_0 + \mathcal{I}(f_0) =$

$f_0 + O(t^{pn+(p-1)e(\partial)})$.

Then

$$\begin{aligned}\partial^{p-1}(f_1) + f_1^p &= f_0^p + \partial^{p-1}(f_0) + \partial^{p-1}(\mathcal{I}(f_0)) + \mathcal{I}(f_0)^p \\ &= f_0^p + \partial^{p-1}(f_0) + a^p - \partial^{p-1}(f_0) - f_0^p + \mathcal{I}(f_0)^p \\ &= a^p + \mathcal{I}(f_0)^p.\end{aligned}$$

Thus

$$\partial^{p-1}(f_1) + f_1^p = a^p + O(t^{p(pn+(p-1)e(\partial))}).$$ □

Criteria over power series

For now we suppose that $g \in \mathbb{F}_q[[t]]\backslash\{0\}$; we want to solve in $\mathbb{F}_q[[t]]$ the equation

$$\partial^{p-1}(f) + f^p = a^p$$

with $a \in \mathbb{F}_q[[t]]$.

COROLLARY 3.3.7. — *The equation*

$$\partial^{p-1}(b) + b^p = a^p$$

over $\mathbb{F}_q[[t]]$ *has a solution in* $\mathbb{F}_q[[t]]$ *if and only if there exists* $n > -e(\partial)$ *and* $f \in \mathbb{F}_q[[t]]$ *such that*

$$\partial^{p-1}(f) + f^p = a^p + O(t^{pn}).$$

In this case there exists a solution $f_* \in \mathbb{F}_q[[t]]$ *equal to* f *at precision* n*:*

$$f_* - f = O(t^n).$$

Proof. If the equation has a solution f then in particular for $n = 1 - e(\partial)$ we have

$$\partial^{p-1}(f) + f^p = a^p + O(t^{pn}).$$

Conversely if we have $f \in \mathbb{F}_q[[t]]$ such that

$$\partial^{p-1}(f) + f^p = a^p + O(t^{pn}).$$

with $n > -e(\partial)$ then according to Proposition 3.3.6 we can recursively construct a sequence $(f_k)_{k\in\mathbb{N}} \in \mathbb{F}_q[[t]]^{\mathbb{N}}$ and a sequence $(l_k)_{k\in\mathbb{N}}$ of integers such that

$$\begin{aligned}f_0 &= f \\ l_0 &= n \\ f_{k+1} &= f_k + O(t^{l_k}) \\ l_{k+1} &\geqslant p(pl_k + (p-1)e(\partial)) \\ \partial^{p-1}(f_k) + f_k^p &= a^p + O(t^{pl_k})\end{aligned}$$

Furthermore, since $n > -e(\partial)$, $pn + (p-1)e(\partial) > n$ and we can recursively show that the sequence (l_k) is increasing.
Thus the sequence $(f_k)_{k\in\mathbb{N}}$ converges to $b \in \mathbb{F}_q((t))$ verifying

$$\partial^{p-1}(b) + b^p = a^p.$$ □

Corollary 3.3.7 provides a criteria determining whether a p-Riccati equation has a solution over $\mathbb{F}_q[[t]]$. We now show that testing this criteria is just a matter of solving a $\mathbb{F}_p$-linear system of $(1-e(\partial))$ equations over $(1-e(\partial))$ variables.

Lemma 3.3.8. — *Let ∂ be a nonzero derivation over $\mathbb{F}_q((t))$ such that $\partial^p = 0$ and let $g = \partial(t)$. Then for any $f \in \mathbb{F}_q((t))$,*

$$\partial^{p-1}(f) = \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}(g^{p-1}f).$$

Proof. We consider two rings of differential operators $\mathbb{F}_q((t))\langle\partial_1\rangle := \mathbb{F}_q((t))[\partial_1, \mathrm{Id}, \partial]$ and $\mathbb{F}_q((t))\langle\partial_2\rangle := \mathbb{F}_q((t))[\partial_2, \mathrm{Id}, \frac{\mathrm{d}}{\mathrm{d}t}]$. We know that $\iota : \partial_1 \mapsto g\partial_2$ realises an isomorphism between $\mathbb{F}_q((t))\langle\partial_1\rangle$ and $\mathbb{F}_q((t))\langle\partial_2\rangle$ of reverse morphism $\partial_2 \mapsto \frac{1}{g}\partial_1$.

We want to show that

$$\iota(\partial_1^{p-1}) = (g\partial_2)^{p-1} = \partial_2^{p-1}g^{p-1}.$$

We know that the leading coefficient of $(g\partial_2)^{p-1}$ is g^{p-1}. Furthermore we know that $\partial^p = 0$ which is to say that ∂_1^p is central in $\mathbb{F}_q((t))\langle\partial_1\rangle$. So $\iota(\partial_1^p) = g\partial_2(g\partial_2)^{p-1}$ is also central. In particular, since $(g\partial_2)^p$ is a multiple of ∂_2 and therefore has a zero constant coefficient, it follows that $g\partial_2(g\partial_2)^{p-1}$, and therefore $\partial_2(g\partial_2)^{p-1}$, are multiples of ∂_2^p. Since $\partial_2(g\partial_2)^{p-1}$ is of order p and of leading coefficient g^{p-1} we have $\partial_2(g\partial_2)^{p-1} = g^{p-1}\partial_2^p = \partial_2^p g^{p-1}$. But since $\mathbb{F}_q((t))\langle\partial\rangle$ is integral this means that $(g\partial_2)^{p-1} = \partial_2^{p-1}g^{p-1}$. □

For any $f_1, f_2 \in \mathbb{F}_q[[t]]$, all $k \in \mathbb{N}$ and all $i \in [\![0; p-1]\!]$, if $f_1 = f_2 + O(t^{kp})$ then

$$\frac{\mathrm{d}^i}{\mathrm{d}t^i}f_1 = \frac{\mathrm{d}^i}{\mathrm{d}t^i}f_2 + O(t^{kp}).$$

It follows that if $g := \partial(t)$ and a are formal power series in $\mathbb{F}_q[[t]]$ then the equation

$$\partial^{p-1}(f) + f^p = a^p$$

can be reduced modulo t^{kp} for all $k \in \mathbb{N}$ and yields a $\mathbb{F}_p$-linear system of $\log_p(q)kp$ equations in $\log_p(q)kp$ variables. However, since for any $f \in \mathbb{F}_q((t))$, $\partial^{p-1}(f) \in \ker(\partial) = \mathbb{F}_q((t^p))$ we see that the equations obtained by looking at the coefficients of t^{pl+i} for $l \in \mathbb{N}$ and $i \in [\![1; p-1]\!]$ is always the trivial equation $0 = 0$.

Thus

$$\partial^{p-1}(f) + f^p = a^p + O(t^{kp})$$

is really only a $\mathbb{F}_p$-linear system of $\log_p(q)k$ equations in $\log_p(q)kp$ variables. The following theorem is a refinement of Corollary 3.3.7 which incorporates this idea.

Theorem 3.3.9. — *Let ∂ be a nonzero derivation over $\mathbb{F}_q[[t]]$ such that $\partial^p = 0$ and $a \in \mathbb{F}_q[[t]]$. The equation*

$$\partial^{p-1}(b) + b^p = a^p$$

has a solution in $\mathbb{F}_q[[t]]$ if and only if there exists $(f_0, \dots, f_{-e(\partial)}) \in \mathbb{F}_q^{1-e(\partial)}$ such that $f := \sum_{k=0}^{-e(\partial)} f_k t^k$ verifies

$$\partial^{p-1}(f) + f^p = a^p + O(t^{p(1-e(\partial))}).$$

In this case the $(1-e(\partial))$-tuples verifying this condition are exactly tuples of the $(1-e(\partial))$ first coefficients of a solution of

$$\partial^{p-1}(b)+b^p=a^p$$

Proof. If such $(f_0,\dots,f_{-e(\partial)})$ exists then by Corollary 3.3.7 we know that a solution f_* of

$$\partial^{p-1}(b)+b^p=a^p$$

such that $f_*=\sum_{k=0}^{-e(\partial)} f_k t^k+O(t^{1-e(\partial)})$ exists in $\mathbb{F}_q[[t]]$. Reciprocally let f verify

$$\partial^{p-1}(f)+f^p=a^p.$$

We know that ∂ is of the form $g\frac{\mathrm{d}}{\mathrm{d}t}$. In particular, f verifies

$$f^p+\frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}(g^{p-1}f)=a^p+O(t^{p(1-e(\partial))}).$$

We write $f:=\sum_{n=0}^{\infty} f_n t^n$, $g^{p-1}:=\sum_{n=0}^{\infty} g_n t^n$ and $a:=\sum_{n=0}^{\infty} a_n t^n$.

$$\begin{aligned} f^p+\frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}(g^{p-1}f)&=\sum_{n=0}^{\infty}\left(f_n^p-\sum_{k=0}^{pn+p-1} g_k f_{pn+p-1-k}\right)t^{pn}\\ &=\sum_{n=0}^{\infty} a_n^p t^{pn}\end{aligned}$$

In particular, for any $n\in\mathbb{N}$,

$$f_n^p-\sum_{k=0}^{pn+p-1} g_k f_{pn+p-1-k}=a_n^p.$$

But we know that $\nu(g^{p-1})=(p-1)(1-e(\partial))$ so for all $j<(p-1)(1-e(\partial))$, $g_j=0$. Thus we have

$$f_n^p-\sum_{k=(p-1)(1-e(\partial))}^{pn+p-1} g_k f_{pn+p-1-k}=a_n^p.$$

If we suppose $n\leqslant -e(\partial)$ then $k\geqslant (p-1)(1-e(\partial))$ implies that $pn+p-1-k\leqslant -e(\partial)$.

This means that only the coefficients f_i for $i\leqslant -e(\partial)$ appear in the equation

$$\partial^{p-1}(f)+f^p\equiv a^p \mod (t^{p(1-e(\partial))}).$$

In particular if we set $f_*=\sum_{k=0}^{-e(\partial)} f_k t^k$ then

$$\partial^{p-1}(f_*)+f_*^p=a^p+O(t^{p(1-e(\partial))}).$$

□

Once the $1-e(\partial)$ first coefficients of a solution (if it exists) are determined, then Proposition 3.3.6 provides an efficient algorithmic way to compute a solution at arbitrary precision.

Criteria over $\mathbb{F}_q((t))$

We now no longer require that g or a are formal power series and suppose that they are general Laurent series in $\mathbb{F}_q((t))$ instead.

Lemma 3.3.10. — *If $f \in \mathbb{F}_q((t))$ verifies*

$$\partial^{p-1}(f) + f^p = a^p$$

then

$$\nu(f) \geqslant \min(-e(\partial), \nu(a)).$$

Furthermore there exists $f_* \in \mathbb{F}_q((t))$ verifying the same equation and

$$\nu(f_*) \geqslant \min(1 - e(\partial), \nu(a)).$$

Proof. Let $g \in \mathbb{F}_q((t))$ be such that $\partial = g\frac{\mathrm{d}}{\mathrm{d}t}$. Then for any $h := \sum_{n=\nu(h)}^{\infty} h_n t^n \in \mathbb{F}_q((t))$,

$$\partial(h) = g \sum_{n=\nu(h)}^{\infty} n h_n t^{n-1}.$$

In particular $\nu(\partial(h)) \geqslant \nu(h) - 1 + \nu(g) = \nu(h) - e(\partial)$. Furthermore, this is an equality if and only if p does not divide $\nu(h)$.

It follows that $\nu(\partial^{p-1}(f)) \geqslant \nu(f) - (p-1)e(\partial)$. Besides,

$$\nu(a^p) = p\nu(a) = \nu(\partial^{p-1}(f) + f^p) \geqslant \min(\nu(\partial^{p-1}(f), p\nu(f))$$

with the last inequality being an equality if $\nu(\partial^{p-1}(f)) \neq p\nu(f)$. In particular if $\nu(f) < -e(\partial)$ then

$$p\nu(f) < \nu(f) - (p-1)e(\partial) \leqslant \nu(\partial^{p-1}(f))$$

and we obtain $\nu(f) = \nu(a)$. It follows that

$$\nu(f) \geqslant \min(-e(\partial), \nu(a)).$$

Let us now suppose that $\nu(a) > -e(\partial)$ and that $\nu(f) = -e(\partial)$. Let $g_{\nu(g)}$ be the coefficient of $t^{\nu(g)}$ in g and $f_{-e(\partial)}$ be the coefficient of $t^{-e(\partial)}$ in f. Those are the first nonzero coefficients of f and g respectively. According to Corollary 3.3.5 (ii) we know that p does not divide $e(\partial)$. For any $h \in \mathbb{F}_q((t))$ we know that if p does not divide $\nu(h)$ then $\nu(\partial(h)) = \nu(h) - e(\partial)$. Thus $\nu(\partial^{p-1}(f)) = \nu(f) - (p-1)e(\partial) = -pe(\partial)$ and its first non zero coefficient is $-g_{\nu(g)}^{p-1} f_{-e(\partial)}$ while $\nu(f^p) = -pe(\partial)$ and its first nonzero coefficient is $f_{-e(\partial)}^p$. Since $\nu(\partial^{p-1}(f)+f^p) = \nu(a^p) > -pe(\partial)$ it follows that

$$f_{-e(\partial)}^p - g_{\nu(g)}^{p-1} f_{-e(\partial)} = 0$$

which is to say that

$$\frac{f_{-e(\partial)}}{g_{\nu(g)}} \in \mathbb{F}_p^\times.$$

Thus

$$f_* = f - \frac{f_{-e(\partial)}}{g_{\nu(g)}} \frac{g}{t}$$

verifies $\nu(f_*) \geqslant 1 - e(\partial)$. We claim that it also verifies

$$\partial^{p-1}(f_*) + f_*^p = a^p.$$

This is because

$$\partial^{p-1}\left(\frac{g}{t}\right) + \left(\frac{g}{t}\right)^p = 0.$$

Indeed according to Lemma 3.3.4 we have

$$\partial^{p-1}\left(\frac{g}{t}\right) = \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}\left(\frac{g^p}{t}\right) = g^p \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}\left(\frac{1}{t}\right) = \frac{(-1)^{p-1}(p-1)!g^p}{t^p} = -\left(\frac{g}{t}\right)^p. \qquad \square$$

With this in mind we can prove the main theorem of this subsection. This theorem is an analog of Theorem 3.3.9 for Laurent series.

THEOREM 3.3.11. — *Let ∂ be a nonzero derivation over $\mathbb{F}_q((t))$ such that $\partial^p = 0$ and $a \in \mathbb{F}_q((t))$. Set $\eta := \min(1 - e(\partial), \nu(a))$. The equation*

$$\partial^{p-1}(b) + b^p = a^p$$

has a solution in $\mathbb{F}_q((t))$ if and only if there exists $(f_\eta, f_{\eta+1}, \ldots, f_{-e(\partial)}) \in \mathbb{F}_q^{1-(\eta+e(\partial))}$ such that $f := \sum_{k=\eta}^{-e(\partial)} f_k t^k$ verifies

$$\partial^{p-1}(f) + f^p = a^p + O(t^{p(1-e(\partial))}).$$

Proof. Let $k \in \mathbb{Z}$ be such that $-pk \leqslant \eta$.

Let us suppose that there exists $(f_\eta, \ldots, f_{-e(\partial)})$ such that $f := \sum_{k=\eta}^{-e(\partial)} f_k t^k$ verifies

$$\partial^{p-1}(f) + f^p = a^p + O(t^{p(1-e(\partial))}).$$

Then

$$\begin{aligned} t^{kp^2}(\partial^{p-1}(f) + f^p) &= (t^{kp}\partial)^{p-1}(t^{kp}f) + (t^{kp}f)^p \\ &= t^{kp^2}a^p + O(t^{p(1-e(\partial)+pk)}) \\ &= (t^{kp}a)^p + O(t^{p(1-e(\partial)+pk)}) \end{aligned}$$

Thus $t^{kp}f$ is a solution of

$$(t^{kp}\partial)^{p-1}(b) + b^p = (t^{kp}a)^p + O(t^{p(1-e(\partial)+pk)}).$$

Since $e(t^{pk}\partial) = e(\partial) - pk$, $\nu(t^{pk}\partial(t)) = pk + 1 - e(\partial) \geqslant 0$ and $\nu(t^{pk}a) = pk + \nu(a) \geqslant 0$, Corollary 3.3.7 then guarantees the existence of $f_* \in \mathbb{F}_q[[t]]$ verifying

$$(t^{kp}\partial)^{p-1}(f_*) + f_*^p = (t^{kp}a)^p.$$

Then $t^{-pk}f_*$ is a solution of the equation

$$\partial^{p-1}(b) + b^p = a^p$$

of unknown variable b.

Conversely, if $f \in \mathbb{F}_q((t))$ verifies $\partial^{p-1}(f) + f^p = a^p$ then there exists $f_* \in \mathbb{F}_q((t))$ another solution such that $\nu(f_*) \geqslant \eta$. $t^{pk} f_*$ is then a solution of the equation $(t^{kp}\partial)^{p-1}(b) + b^p = (t^{kp}a)^p$ of unknown variable b. Let $\tilde{f} := \sum_{k=0}^{pk-e(\partial)} f_{*,k} t^k$ such that $t^{pk} f_* = \tilde{f} + O(t^{pk+1-e(\partial)})$. Since $e(\partial) - pk = e(t^{pk}\partial)$, according to Theorem 3.3.9,

$$(t^{kp}\partial)^{p-1}(\tilde{f}) + \tilde{f}^p = (t^{kp}a)^p + O(t^{p(pk+1-e(\partial))})$$

and thus

$$\partial^{p-1}(t^{-pk}\tilde{f}) + (t^{-pk}\tilde{f})^p = a^p + O(t^{p(1-e(\partial))}).$$

Since $\tilde{f} = t^{pk} f_* + O(t^{pk+1-e(\partial)})$, $t^{-pk}\tilde{f} = \sum_{i=-pk}^{-e(\partial)} f_{*,pk+i} t^i = f_* + O(t^{1-e(\partial)})$. In particular, for $i < \eta$, $f_{*,pk+i} = 0$. Thus $t^{-pk}\tilde{f} = \sum_{i=\eta}^{-e(\partial)} f_{*,pk+i} t^i$ which concludes the proof. □

Corollary 3.3.12. — *Let ∂ be a nonzero derivation of $\mathbb{F}_q((t))$ such that $\partial^p = 0$ and $a \in \mathbb{F}_q((t))$. If $\nu(a) > -e(\partial)$ then*

$$\partial^{p-1}(b) + b^p = a^p$$

has a solution in $\mathbb{F}_q((t))$.

Proof. If $\nu(a) > -e(\partial)$ then $a^p = O(t^{1-e(\partial)})$. It follows that $\partial^{p-1}(0) + 0^p = a^p + O(t^{p(1-e(\partial))})$ and according to the previous theorem,

$$\partial^{p-1}(b) + b^p = a^p$$

has a solution in $\mathbb{F}_q((t))$. □

Those results will actually enable us to build an algorithm for an efficient deterministic irreducibility test on differential operators in section 3.3.3.

3.3.2 Computing a solution to p-Riccati in $\mathbb{F}_q((t))$

Let q be a power of some prime number p. We present algorithms resulting from the work of Section 3.3.1 to solve equations of the form

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(b) + b^p = a^p \tag{3.3}$$

over $\mathbb{F}_q((t))$ at arbitrary precision, where g, a are elements of $\mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^p = 0$. As in section 3.3.1 we denote by ν the unique valuation on $\mathbb{F}_q((t))$.

We recall from Theorem 3.3.11 that (3.3) has a solution in $\mathbb{F}_q((t))$ if and only if there exists $(f_{\nu(a)}, f_{\nu(a)+1}, \ldots, f_{\nu(g)-1}) \in \mathbb{F}_q^{\nu(g)-\nu(a)}$ such that $f := \sum_{k=\nu(a)}^{\nu(g)-1} f_k t^k$ verifies

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p + O(t^{p\nu(g)}).$$

We call such a $(\nu(g)-\nu(a))$-tuple of elements $(f_{\nu(a)}, \ldots, f_{\nu(g)-1})$ a seed of the p-Riccati equation relative to g and a. The first question we need to tackle is how to compute a seed of the p-Riccati equation.

DEFINITION 3.3.13. — Let $h \in \mathbb{F}_q((t))$. We say that h is known at relative precision $n \in \mathbb{N}$ if and only if we know $(h_0, \dots, h_{n-1}) \in \mathbb{F}_q^n$ such that

$$h = \sum_{k=0}^{n-1} h_k t^{k+\nu(g)} + O(t^{n+\nu(g)}).$$

We say that $(h_0, \dots, h_{n-1})$ is the approximation of h at relative precision n.

REMARK 3.3.14. — A seed of the p-Riccati equation relative to g and a is the approximation at relative precision $\nu(g) - \nu(a)$ of a solution.

We recall from Lemma 3.3.8 that for any $f \in \mathbb{F}_q((t))$.

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) = \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}(g^{p-1}f).$$

We suppose that (3.3) has a solution in $\mathbb{F}_q((t))$ and that $\nu(a) < \nu(g)$. Let $(f_{\nu(a)}, \dots, f_{\nu(g)-1})$ be a seed of the p-Riccati equation relative to g and a. We know that

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}\left(\sum_{k=\nu(a)}^{\nu(g)} f_k t^k\right) + \sum_{k=\nu(a)}^{\nu(g)} f_k^p t^{pk} = a^p + O(t^{p\nu(g)}).$$

As in the proof of Theorem 3.3.11 we show that for any $n \in \mathbb{N}$:

$$\left(t^{pn}g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}\left(\sum_{k=\nu(a)}^{\nu(g)} f_k t^{k+pn}\right) + \sum_{k=\nu(a)}^{\nu(g)} f_k^p t^{p(k+pn)} = a^p + O(t^{p(\nu(g)+pn)}).$$

which is to say that $(f_{\nu(a)}, \dots, f_{\nu(g)-1})$ is also a seed of the p-Riccati equation with respect to $t^{pn}g$ and $t^{pn}a$. Thus we can suppose that $(g, a) \in \mathbb{F}_q[[t]]$. Let us write $g^{p-1} = \sum_{n=(p-1)\nu(g)}^{\infty} g_{n-(p-1)\nu(g)} t^n$. For any $h := \sum_{n=0}^{\infty} h_n t^n$ we have

$$\begin{aligned}\frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}(g^{p-1}h) &= -\sum_{n=0}^{\infty}\left(\sum_{k=0}^{pn+p-1} g_{k-(p-1)\nu(g)} h_{pn+p-1-k}\right) t^{pn} \\ &= -\sum_{n=0}^{\infty}\left(\sum_{k=(p-1)\nu(g)}^{pn+p-1} g_{k-(p-1)\nu(g)} h_{pn+p-1-k}\right) t^{pn}\end{aligned} \tag{3.4}$$

REMARK 3.3.15. — We consider that $g_k = 0$ for $k < 0$.

Applying this to $h = \sum_{k=\nu(a)}^{\nu(g)-1} f_k t^k$ ensures that for all $i \in [\![1; \nu(g) - \nu(a)]\!]$ the coefficient of $t^{p(\nu(g)-i)}$ in $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(h)$ is given by

$$\begin{aligned}-\sum_{k=(p-1)\nu(g)}^{p(\nu(g)-i)+p-1} g_{k-(p-1)\nu(g)} f_{p(\nu(g)-i)+p-1-k} &= -\sum_{k=0}^{\nu(g)-pi+p-1} g_k f_{\nu(g)-pi+p-1-k} \\ &= -\sum_{k=0}^{\nu(g)-\nu(a)-1-p(i-1)} g_k f_{\nu(g)-1-p(i-1)-k}\end{aligned}$$

Remark 3.3.16. — The last line comes from the fact that $\nu(h) \geqslant \nu(a)$. In particular if $\nu(g)-1-p(i-1)-k < \nu(a)$, which is to say that $k \geqslant \nu(g)-\nu(a)-p(i-1)$, then $f_{\nu(g)-1-p(i-1)-k} = 0$

We deduce the following result:

Proposition 3.3.17. — *Let $g \in \mathbb{F}_q((t))$ be such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^p = 0$ and $a \in \mathbb{F}_q((t))$ such that $\nu(a) < \nu(g)$. Let $\eta = \nu(g) - \nu(a)$ and $D_g^{p-1} \in M_\eta(\mathbb{F}_q)$ be a matrix such that for any $(f_{\nu(a)}, \ldots, f_{\nu(g)-1}) \in \mathbb{F}_q^\eta$,*

$$D_g^{p-1} \begin{pmatrix} f_{\nu(a)} \\ \vdots \\ f_{\nu(g)-1} \end{pmatrix}$$

is the vector whose entries are the coefficients of $t^{p\nu(a)}, \ldots, t^{p(\nu(g)-1)}$ in $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}\left(\sum_{k=\nu(a)}^{\nu(g)-1} f_k t^k\right)$. Finally let $(g_0, \ldots, g_{\eta-1})$ be the approximation at relative precision η of g^{p-1} and r be the remainder in the Euclidean division of $\eta - 1$ by p. Then

$$D_g^{p-1} = -\begin{pmatrix} & & & \mathbf{0} & & & \\ & & & & & & \\ g_r & \cdots & g_0 & & & & \\ \vdots & & & \ddots & & & \\ g_{\eta-1-p} & & \cdots & & g_0 & 0 & \cdots & 0 \\ g_{\eta-1} & & \cdots & & g_p & g_{p-1} & \cdots & g_0 \end{pmatrix}$$

Notation 3.3.18. We fix a $\mathbb{F}_p$-basis $\mathcal{B}$ of $\mathbb{F}_q$ with $q = p^d$. Let $a \in \mathbb{F}_q$. We denote by $M(a) \in M_n(\mathbb{F}_p)$ the matrix in the basis $\mathcal{B}$ of the multiplication by a on $\mathbb{F}_q$ seen as a $\mathbb{F}_p$-vector space. The map $a \in \mathbb{F}_q \mapsto M(a) \in M_d(\mathbb{F}_p)$ is a ring homomorphism which induces a morphism

$$\begin{array}{rccc} M: & M_k(\mathbb{F}_q) & \to & M_{kd}(\mathbb{F}_p) \\ & (a_{i,j})_{i,j} & \mapsto & (M(a_{i,j}))_{i,j} \end{array}.$$

Theorem 3.3.19. — *Let $g \in \mathbb{F}_q((t))$ be such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^p = 0$ and $a \in \mathbb{F}_q((t))$. Let $\eta := \nu(g) - \nu(a)$ and $q = p^d$. Algorithm 4 determines whether the p-Riccati equation relative to g and a has a solution and computes a seed of it in*

$$\tilde{O}\left(\left(\frac{\eta}{p} d\log(p) + \eta + \frac{\eta^2}{p} + d^{\omega-1}\right) d\log(p)\right)$$

bit operations.

Proof. Let $\Phi_p \in M_d(\mathbb{F}_p)$ be the matrix of the Frobenius endomorphism on $\mathbb{F}_q$. Let also $(a_0, \ldots, a_{\eta-1})$ and $(g_0, \ldots, g_{\eta-1})$ be the respective approximations of a and g^{p-1} at relative

Input: $g, a \in \mathbb{F}_q((t))$ known at relative precision $\eta := \nu(g) - \nu(a)$
Output: $(f_0, \ldots, f_{\eta-1})$ a seed of the p-Riccati equation relative to g and a if it exists.

1. Set $(a_0, \ldots, a_{\eta-1})$ the approximation of a at relative precision η.
2. Set $d := \log_p(q)$.
3. Compute $(g_0, \ldots, g_{\eta-1}) \in \mathbb{F}_q((t))$ an approximation of g^{p-1} at relative precision η.
   Cost: $\tilde{O}(\eta d \log^2(p))$ bit operations.
4. Compute $A = \Phi_p - M(g_0)$, with Φ_p the matrix of the Frobenius endomorphism of $\mathbb{F}_q$.
   Cost: $\tilde{O}((d\log(p))^2)$ bit operations.
5. Set $l := \left\lceil \frac{\eta}{p} \right\rceil$
6. For i from 0 to $\eta - l$ do:
   - Set $f_i := a_i$.

   Cost: $O(\eta d \log(p))$ bit operations.
7. For i from $\eta - l + 1$ to $\eta - 2$ do:
   - Set $f_i := a_i + \left(\sum_{k=0}^{\eta-1-p(\eta-i-1)} g_k f_{\eta-1-p(\eta-i-1)-k}\right)^{p^{d-1}}$

   Cost: $\tilde{O}((\frac{\eta^2}{p} + \eta + \frac{\eta}{p} d\log(p))d\log(p))$ bit operations.
8. Set $Y = a_{\eta-1}^p + \sum_{k=1}^{\eta-1} g_k f_{\eta-1-k}$.
   Cost: $\tilde{O}((\eta + \log(p))d\log(p))$ bit operations.
9. If $AX = Y$ has a solution $f_{\eta-1}$:
   - Return $(f_0, \ldots, f_{\eta-1})$.

   Else:
   - The p-Riccati equation relative to g and a has no solution.

   Cost: $\tilde{O}(d^\omega \log(p))$ bit operations.

Algorithm 4: p-Riccati_seed

precision η. From Proposition 3.3.17 we know that $(f_0, \dots, f_{\eta-1})$ is a seed of the p-Riccati equation relative to g and a if and only if

$$(M(D_g^{p-1}) + \operatorname{diag}(\Phi_p)) \begin{pmatrix} f_0 \\ \vdots \\ f_{\eta-1} \end{pmatrix} = \begin{pmatrix} \Phi_p(a_0) \\ \vdots \\ \Phi_p(a_{\eta-1}) \end{pmatrix}.$$

Let $l = \left\lceil \frac{\eta}{p} \right\rceil$. From the form of D_g^{p-1} we know that $M(D_g^{p-1}) + \operatorname{diag}(\Phi_p)$ is a lower triangular matrix. Furthermore for $i \leqslant \eta - l + 1$, the only nonzero coefficient of the i-th row is the diagonal coefficient which is Φ_p. Thus $f_{i-1} = a_{i-1}$.
Then for $i \in [\![\eta - l + 2 : \eta - 1]\!]$, the diagonal coefficient of the i-th row is still Φ_p which proves the correctness of step (7).
Finally the diagonal coefficient of the η-th row is $\Phi_p - M(g_0)$ so we have $(\Phi_p - M(g_0))f_{\eta-1} = a_{\eta-1}^p + \sum_{k=1}^{\eta-1} g_k f_{\eta-1-k}$ as in step (8).
This proves the correctness of the algorithm.

To proves the cost of Algorithm 4 it suffices to bound the cost of each step of the algorithm. Step (3) can be done by computing the $(p-1)$-th power of the truncated power series of g in $\mathbb{F}_q[t]/t^\eta$. By using a fast exponentiation method this can be done in $O(\log(p))$ multiplications in $\mathbb{F}_q[t]/t^\eta$. FFT algorithms can do multiplications in $\mathbb{F}_q[t]/t^\eta$ in $\tilde{O}(\eta)$ operations $\mathbb{F}_q$. Again, FFT algorithms allow to do computations in $\mathbb{F}_q$ in $\tilde{O}(d)$ operations in $\mathbb{F}_p$, or $\tilde{O}(d\log(p))$ bit operations.

Next step (4) can be accomplished by computing the p-th powers of an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. Similarly to the previous point, each p-th power can be computed in $\tilde{O}(d\log^2(p))$ bit operations and the cost follows from the fact that $[\mathbb{F}_q : \mathbb{F}_p] = d$. The cost of computing $M(g_0)$ is d multiplication in $\mathbb{F}_q$ which is to say $\tilde{O}(d^2\log(p))$ bit operations, which is also to cost of computing the difference $\Phi_p - M(g_0)$. The cost follows.

Step (6) is just a matter of reading $\eta - l + 1$ elements of $\mathbb{F}_q$ which can be done in $O((\eta - l + 1)d\log(p)) = O(\eta d\log(p))$ bit operations.

Step (7) consist in doing $\sum_{k=0}^{l-1} r + kp = O(lr + l^2p) = O(lp + l^2p)$ multiplications in $\mathbb{F}_q$ and computing l p^{d-1}-power in $\mathbb{F}_q$. Since $l \sim \frac{\eta}{p}$ the multiplications correspond to a cost of $\tilde{O}((\eta + \frac{\eta^2}{p})d\log(p))$ bit operations while the computation of the p^{d-1} powers has a cost of $O(ld\log(p))$ multiplications in $\mathbb{F}_q$ or $\tilde{O}(\frac{\eta}{p}d^2\log^2(p))$ bit operations. Step (8) has the cost of $O(\eta)$ operations in $\mathbb{F}_q$ and computing one p-th power in $\mathbb{F}_q$ which yields the cost. Finally step (9) is the cost of solving a linear system of d equations in d variables in $\mathbb{F}_p$ which can be done in d^ω operations in $\mathbb{F}_p$. □

We now tackle the question of computing a solution of the p-Riccati equation at a chosen precision. Let's precise our goal. Given $g \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^p = 0$, $a \in \mathbb{F}_q((t))$ and $N \in \mathbb{N}$ we want to compute $f \in \mathbb{F}_q((t))$ such that

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p + O(t^{pN}).$$

If $N \geqslant \nu(g)$ this also implies that there exists a solution f_* of the p-Riccati equation relative to g and a verifying $f = f_* + O(t^{pN+(p-1)(1-\nu(g))})$.

For this purpose we are going to use Proposition 3.3.6. This requires first to compute a seed of the p-Riccati equation relative to g and a. This can be done using Algorithm 4. Then we need for a given $f \in \mathbb{F}_q((t))$ to compute $F \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(F) = f^p$. This is the content of the proposition below.

Notation 3.3.20. Let $f \in \mathbb{F}_q((t))$. For $m \in \mathbb{N}$ We denote by $\lceil f \rceil^m$ the truncated series such that $f = \lceil f \rceil^m + O(t^m)$.

Input: $N \in \mathbb{N}$, $a \in \mathbb{F}_q((t))$ known at absolute precision N and $g \in \mathbb{F}_q((t))$ known at absolute precision $pN + (p-2)(1-\nu(g)) + 1 - \min(\nu(g), \nu(a))$.
Output: $f \in \mathbb{F}_q[t^{\pm 1}]$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p + O(t^{pN})$.

1. Set $\eta := \min(\nu(g), \nu(a))$.
2. Compute $g_* := \lceil g^{p-1} \rceil^{pN+(p-1)-\eta}$ and $h_* = \lceil g^{1-p} \rceil^{pN+(p-1)(1-\nu(g))-\eta}$.
3. Compute $(f_{\nu(a)}, \dots, f_{\nu(g)-1})$ a seed of the p-Riccati equation relative to g and a.
4. Set $f_0 := \sum_{k=\nu(a)}^{\nu(g)-1} f_k t^k$.
5. Set $N_0 := \nu(g)$.
6. While $N_0 < N$ do:
   (a) If $pN_0 + (p-1)(1-\nu(g)) \leqslant N$ do:
   - Set $N_1 := p(pN_0 + (p-1)(1-\nu(g)))$.

   Else
   - Set $N_1 := pN$.

   (b) Set
   - $N_2 := N_1 - pN_0 + (p-1)(1-\nu(g))$.
   - $N_3 := N_1 + p - 1 - \eta$.
   - $N_4 := N_1 + (p-1)(1-\nu(g))$.

   (c) Set $f_1 := \left\lceil \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}} \left(\lceil g_* \rceil^{N_3} f_0 \right) \right\rceil^{N_1}$.
   (d) Set $f_2 := \lceil a^p - f_0^p \rceil^{N_1} - f_1$.
   (e) Set $f_3 := \left\lceil -t^{p-1} \lceil h_* \rceil^{N_2} f_2 \right\rceil^{N_4}$
   (f) Set $f_0 := f_0 + f_3$.
   (g) Set $N_0 = N_1/p$.
7. return $\lceil f_0 \rceil^{pN}$

Algorithm 5: p-Riccati_$\mathbb{F}_q((t))$

THEOREM 3.3.21. — *Let $g, a \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^p = 0$ and $N \in \mathbb{N}$. Suppose $q = p^d$.*

Then Algorithm 5 computes $f \in \mathbb{F}_q((t))$ such that

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = a^p + O(t^{pN}).$$

in asymptotically $\tilde{O}(p(N-\nu(g))d + C(g,a))$ bit operations where $C(g,a)$ is the cost of computing a seed of the p-Riccati equation relative to g and a.

Proof. We know that at the end of step (2), f_0 is such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1} + f_0^p = a^p + O(t^{p\nu(g)})$. We claim that at each iteration of the loop of step (6), if f_0 at the start of the iteration is such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1} + f_0^p = a^p + O(t^{pN_0})$, then at the end of the iteration we have $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1} + f_0^p = a^p + O(t^{N_1})$ (or N if $N_1 \geqslant N$). Furthermore, $\nu(f_0)$ is constant from step (4) and greater or equal to $\min(\nu(a), \nu(g))$.

Indeed, suppose that at step (6a), $\nu(f_0) \geqslant \min(\nu(a), \nu(g))$. Then at step (6b) we have

$$\begin{aligned} f_1 &= \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}((g^{p-1} + O(t^{N_1+p-1-\nu(f_0)}))f_0) + O(t^{N_1}) \\ &= \frac{\mathrm{d}^{p-1}}{\mathrm{d}t^{p-1}}(g^{p-1}f_0) + O(t^{N_1}) \end{aligned}$$

And at step (6c),

$$f_2 = a^p - f_0^p - \left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0) + O(t^{N_1}).$$

In particular since $N_0 \geqslant \nu(g)$, $N_1 = p(pN_0 + (p-1)(1-\nu(g))) > pN_0$. Thus $\nu(f_2) \geqslant pN_0$. Finally at step (6d), we have

$$\begin{aligned} f_3 &= -t^{p-1}\left(g^{1-p} + O(t^{(p-1)(pN_0+(p+1)(1-\nu(g))-1)})\right)(f_2) + O(t^{N_1+(p-1)(1-\nu(g))}) \\ &= -t^{p-1}g^{1-p}(a^p - f_0^p - \left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0)) + O(t^{n_*}) + O(t^{N_1+(p-1)(1-\nu(g))}) \end{aligned}$$

where

$$n_* := \min\left(N_1 - pN_0, (p-1)(pN_0 + (p+1)(1-\nu(g)) - 1) + (p-1)\nu(g)\right) + pN_0 + (p-1)(1-\nu(g)).$$

But

$$\begin{aligned} N_1 - pN_0 - (p-1)(pN_0 + (p+1)(1-\nu(g)) - 1) - (p-1)\nu(g)) \\ = N_1 - p^2N_0 - (p-1)p(1-\nu(g)) \\ = N_1 - N_1 = 0 \end{aligned}$$

Thus we have

$$\begin{aligned} n_* &= N_1 - pN_0 + pN_0 + (p-1)(1-\nu(g)) \\ &= N_1 + (p-1)(1-\nu(g)) \end{aligned}$$

It follows that

$$f_3 = -t^{p-1}g^{1-p}(a^p - f_0^p - \left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0)) + O(t^{N_1+(p-1)(1-\nu(g))})$$

Then according to Lemma 3.3.8 we have that

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_3) = a^p - f_0^p - \left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0) + O(t^{N_1})$$

and $\nu(f_3) \geqslant pN_0 + (p-1)(1-\nu(g))$.

At the end of step (6e), f_0 is updated to a function $f_{0*} := f_0 + f_3$. We have

$$\begin{aligned} a^p - f_{0*}^p - \left(g\tfrac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_{0*}) \\ &= a^p - f_0^p - f_3^p - \left(g\tfrac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0) - \left(g\tfrac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_3) \\ &= a^p - f_0^p - \left(g\tfrac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0) - a^p - f_0^p - \left(g\tfrac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_0) + O(t^{N_1}) + f_3^p = O(t^{N_1}) \end{aligned}$$

This proves the correctness of Algorithm 5.

To bound the complexity of the algorithm it is enough to show that step (6) can be done in $p(N-\tilde{\nu}(g)d$ bit operations. Each iteration of the loop consists in $O(1)$ operations (multiplications and additions) of power series at precision $O(p(N-\nu(g)))$. Thus each iteration of the loop can be done in $\tilde{O}(p(N-\nu(g)))$ operations in $\mathbb{F}_q$, that is $\tilde{O}(p(N-\nu(g)))$ bit operations.

Let $n_0 = \nu(g)$ and $n_{k+1} = pn_k + (p-1)(1-\nu(g))$. We have

$$n_k = p^k n_0 + (p-1)(1-\nu(g))\sum_{i=0}^{k-1} p^i = p^k n_0 + \frac{p^k-1}{p-1}(1-\nu(g))$$

In particular $n_k \geqslant N$ if and only if $k \geqslant \log_p(N-\nu(g)+1)$. Thus the number of iteration of the loop at step (6) is $O(\log_p(N-\nu(g)))$ which gives the result. □

3.3.3 Application: an irreducibility test on $K\langle\partial\rangle$

Before moving on to solving the p-Riccati equation over a global field, we describe here an irreducibility test for $N(\partial^p) \in C[\partial^p]$, where N is an irreducible polynomial over C. The core objects of this test are the completions of K_N over their different places (see Notation 3.2.11).

Any field F equipped with a valuation $\nu : F \to \mathbb{Z}\cup\{\infty\}$ (that is to say that ν verify (i), (ii) and (iii) of Definition B.1.11) is a metric space for the distance $d_\nu(x,y) := 2^{-\nu(x-y)}$ in which the addition, the multiplication and the division are continuous. We say that (F,ν) is a valued field.

DEFINITION 3.3.22. — Let (F,ν) be a valued field. For a valued field $(\tilde{F},\tilde{\nu})$ we say that

- $(\tilde{F},\tilde{\nu})$ is a valued field extension of (F,ν) if $\tilde{F}$ is a field extension of F and $\tilde{\nu}_{|F} = \nu$.
- That $(\tilde{F},\tilde{\nu})$ is the completion of (F,ν) if it is a valued field extension of (F,ν), complete for $d_{\tilde{\nu}}$ such that F is dense in $\tilde{F}$.

Any valued field admits a unique (up to a unique isomorphism of valued field) completion [Sti08, Proposition 4.2.3].

Notation 3.3.23. Let N be an irreducible polynomial over C. For any place $\mathfrak{P}$ of K_N we denote by $K_{N,\mathfrak{P}}$ the completion of $(K_N,\nu_{\mathfrak{P}})$.
For any place of $\mathfrak{P}$ of C_N, we denote by $C_{N,\mathfrak{P}}$ the completion of $(C_N,\nu_{\mathfrak{P}})$.
For any algebraic function field F we denote by $\mathbb{P}_F$ the set of places of F as defined in Definition B.1.10. For more details on places in algebraic function fields, we refer to the Appendix B.
Throughout this section, for any place $\mathfrak{P} \in \mathbb{P}_{K_N}$, we denote $h' := \frac{\mathrm{d}}{\mathrm{d}x}(h)$ for any $h \in K_{N,\mathfrak{P}}$, and $K_{N,\mathfrak{P}}\langle\partial\rangle := K_{N,\mathfrak{P}}[\partial, \mathrm{Id}, \frac{\mathrm{d}}{\mathrm{d}x}]$.

Proposition 3.3.24. — *Let $\mathfrak{P}$ be a place of K_N, $\mathcal{G}_\mathfrak{P}$ be the residue class field of K_N in $\mathfrak{P}$ and $t_\mathfrak{P}$ be a prime element of $\mathfrak{P}$. Then*

$$K_{N,\mathfrak{P}} = \mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$$

where $\mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$ is equipped with the usual valuation of Laurent series fields.

Proof. Let $\tilde{k}$ be the subfield of elements of K_N that are algebraic over $\mathbb{F}_p$. If $[\mathcal{G}_\mathfrak{P} : \tilde{k}] = 1$ then the result is just [Sti08, Theorem 4.2.6].
If $[\mathcal{G}_\mathfrak{P} : \tilde{k}] > 1$ then we consider the constant field extension $F := K_N\mathcal{G}_\mathfrak{P}/\mathcal{G}_\mathfrak{P}$ of $K_N/\mathbb{F}_p$. Let $\mathfrak{P}'$ be a place of F above $\mathfrak{P}$. $\mathfrak{P}'$ is unramified ([Sti08, Theorem 3.6.3(a)]), so $t_\mathfrak{P}$ is a prime element of $\mathfrak{P}'$. Furthermore $\mathcal{G}_\mathfrak{P}$ is the residue class field of F in $\mathfrak{P}'$ ([Sti08, Theorem 3.6.3(g)]). Thus from what precedes, the completion of F in $\mathfrak{P}'$ is precisely $\mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$. Thus we have a continuous (for $\nu_\mathfrak{P}$) injection

$$K_N \to F \to \mathcal{G}_\mathfrak{P}((t_\mathfrak{P})).$$

Let $a_0 \in \mathcal{G}_\mathfrak{P}$. There exists $a_0' \in \mathcal{O}_\mathfrak{P}$ such that $a_0'(\mathfrak{P}) = a_0$. Thus $a_0 - a_0' \in t_\mathfrak{P}\mathcal{G}_\mathfrak{P}[[t_\mathfrak{P}]]$. Let a_1 be the constant coefficient in $\mathcal{G}_\mathfrak{P}$ of $\frac{a_0 - a_0'}{t}$.
By induction we construct a sequence $(a_n')_{n\in\mathbb{N}} \in K_N^\mathbb{N}$ such that

$$\nu\left(a_0 - \sum_{k=0}^{n} a_k t_\mathfrak{P}^k\right) > n.$$

Thus $a_0 \in \overline{K_N}$ the (topological) closure of K_N in $\mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$. Since $\overline{K_N}$ contains $\mathcal{G}_\mathfrak{P}$ and all powers of $t_\mathfrak{P}$, it is equal to $\mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$ which is thus the completion of K_N. □

From this we see that $\frac{\mathrm{d}}{\mathrm{d}x}$ has a unique prolongation to $K_{N,\mathfrak{P}}$ for any $\mathfrak{P} \in \mathbb{P}_{K_N}$. Indeed from Proposition B.2.8 we know that $\frac{\mathrm{d}}{\mathrm{d}x}$ is a continuous map on K_N for any place $\mathfrak{P} \in \mathbb{P}_{K_N}$ thus it can be extended to a continuous map over $K_{N,\mathfrak{P}}$ which we easily verify is a derivation. Furthermore from Lemma 3.3.2 we see that if a derivation prolongs $\frac{\mathrm{d}}{\mathrm{d}x}$ it is of the form $g\frac{\mathrm{d}}{\mathrm{d}t_\mathfrak{P}}$ with $g = \frac{\mathrm{d}}{\mathrm{d}x}(t_\mathfrak{P})$ thus it is unique.

It follows that we have an injection

$$K_N\langle\partial\rangle \to K_{N,\mathfrak{P}}\langle\partial\rangle$$

for all $\mathfrak{P} \in \mathbb{P}_{K_N}$. Furthermore $f \mapsto f^p$ is an isomorphism between K_N and C_N so and induces a one-to-one correspondence $\kappa : \mathbb{P}_{K_N} \to \mathbb{P}_{C_N}$. Then $f \mapsto f^p$ is also an isomorphism between $K_{N,\mathfrak{P}}$ and $C_{N,\kappa(\mathfrak{P})}$ for any $\mathfrak{P} \in \mathbb{P}_{K_N}$. In particular $K_{N,\mathfrak{P}} = C_{N,\kappa(\mathfrak{P})}[t_\mathfrak{P}]$ and is of dimension p over $C_{N,\kappa(\mathfrak{P})}$ which is the field of constants of $K_{N,\mathfrak{P}}$ for $\frac{\mathrm{d}}{\mathrm{d}x}$.

Proposition 3.3.25. — *Let $P \in C_N[Y]$ and $\mathfrak{P} \in \mathbb{P}_{K_N}$.*

$$K_N\langle\partial\rangle/P(\partial^p) \otimes_{C_N} C_{N,\kappa(\mathfrak{P})} \simeq K_{N,\mathfrak{P}}\langle\partial\rangle/P(\partial^p).$$

Proof. From the above discussion we know that we have two natural injections $\iota_1 : K_N\langle\partial\rangle/P(\partial^p) \to K_{N,\mathfrak{P}}\langle\partial\rangle/P(\partial^p)$ equal over C_N and $\iota_2 : C_{N,\kappa(\mathfrak{P})} \to K_{N,\mathfrak{P}}$. Furthermore since $C_{N,\kappa(\mathfrak{P})}$ is the subfield of constants in $K_{N,\mathfrak{P}}$ we see that $\iota_1(h)\iota_2(c) = \iota_2(c)\iota_1(h)$ for any h and c in the domains of ι_1 and ι_2 respectively.

Let B be a C_N-algebra and $\varphi_1 : {}^{K_N\langle\partial\rangle}/_{P(\partial^p)} \to B$ and $\varphi_2 : C_{N,\kappa(\mathfrak{P})} \to B$ be C_N-algebras homomorphism such that $\varphi_1(h)\varphi_2(c) = \varphi_2(c)\varphi_1(h)$ for any h and c in the domains of ι_1 and ι_2 respectively. Let us show that there exists a unique C_N-algebra homomorphism

$$\varphi : {}^{K_{N,\mathfrak{P}}\langle\partial\rangle}/_{P(\partial^p)} \to B$$

such that $\varphi \circ \iota_i = \varphi_i$ for $i \in \{1, 2\}$.

We know that $K_{N,\mathfrak{P}} = C_{N,\kappa(\mathfrak{P})}[t_{\mathfrak{P}}]$ so such a morphism is uniquely determined over $K_{N,\mathfrak{P}}$ and exists if and only if $\varphi_1(t_{\mathfrak{P}})^p = \varphi_2(t_{\mathfrak{P}}^p)$, which turns out to be true because φ_1 and φ_2 are morphisms of C_N-algebras. Then we know that there exists a unique morphism $\varphi : K_{N,\mathfrak{P}}\langle\partial\rangle \to B$ extending φ on $K_{N,\mathfrak{P}}$ and sending ∂ to $\varphi_1(\partial)$. We only have to verify that

$$\varphi_1(\partial)\varphi(f) = \varphi(f)\varphi_1(\partial) + \varphi(\frac{\mathrm{d}}{\mathrm{d}t}f)$$

for all $f \in K_{N,\mathfrak{P}}$, but this is easy since it is true on $C_{N,\kappa(\mathfrak{P})}$ and for $(t_{\mathfrak{P}})^i \in K_N$.
Since $\varphi(P(\partial^p)) = 0$ we get the desired morphism by factoring.

Thus ${}^{K_{N,\mathfrak{P}}\langle\partial\rangle}/_{P(\partial^p)}$ verifies the universal property of the tensor product and we get the desired result. □

The basis for our irreducibility test is the following proposition

PROPOSITION 3.3.26. — *Let N be an irreducible polynomial over C. $N(\partial^p)$ is reducible in $K\langle\partial\rangle$ if and only if the p-Riccati equation*

$$f^{(p-1)} + f^p = y_N$$

has a solution in $K_{N,\mathfrak{P}}$ for all $\mathfrak{P} \in \mathbb{P}_{K_N}$.

Proof. We know that $N(\partial^p)$ is reducible in $K\langle\partial\rangle$ if and only if $\mathcal{D}_{N(\partial^p)} \simeq {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$. That is to say that ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ is equal to zero in the Brauer group of C_N, $\mathrm{Br}(C_N)$. We know that $D \mapsto \bigoplus_{\mathfrak{P}\in\mathbb{P}_{C_N}} D \otimes_{C_N} C_{N,\mathfrak{P}}$ induces an injective group morphism [GS06, Corollary 6.5.4]

$$\mathrm{Br}(C_N) \hookrightarrow \bigoplus_{\mathfrak{P}\in\mathbb{P}_{C_N}} \mathrm{Br}(C_{N,\mathfrak{P}}).$$

In particular this means that ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$ if and only if

$${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)} \otimes_{C_N} C_{N,\mathfrak{P}}$$

is isomorphic to $M_p(C_{N,\mathfrak{P}})$ for all $\mathfrak{P} \in \mathbb{P}_{C_N}$.

Besides we know that ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)} \otimes_{C_N} C_{N,\mathfrak{P}}$ is isomorphic to ${}^{K_{N,\kappa^{-1}(\mathfrak{P})}\langle\partial\rangle}/_{(\partial^p - y_N)}$. Thus ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$ if and only if ${}^{K_{N,\mathfrak{P}}\langle\partial\rangle}/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_{N,\kappa(\mathfrak{P})}$ for all $\mathfrak{P} \in \mathbb{P}_{K_N}$.

Lastly $K_{N,\mathfrak{P}}$ is of the form $\mathbb{F}_q((t_{\mathfrak{P}}))$ for q some power of p. In particular it is a field verifying Hypothesis 2.1.37. Thus ${}^{K_{N,\mathfrak{P}}\langle\partial\rangle}/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_{N,\mathfrak{P}})$ if and only if the equation

$$f^{(p-1)} + f^p = y_N$$

has a solution in $K_{N,\mathfrak{P}}$ (see Lemma 3.2.6). □

If $\mathfrak{P} \in \mathbb{P}_{K_N}$ is a place in K_N, it follows from from Corollary 3.3.12 that if $\nu_{\mathfrak{P}}(y_N) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ then

$$f^{(p-1)} + f^p = y_N$$

always has a solution in $K_{N,\mathfrak{P}}$. But if $\mathfrak{P}$ is not a place over $\mathfrak{P}_\infty$, we know from Proposition B.2.8 that $\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) \leqslant 0$. In particular, if $\mathfrak{P}$ is not a pole of y_N then the equation has a solution in $K_{N,\mathfrak{P}}$. Thus the set of places $\mathfrak{P}$ of K_N such that $\nu_{\mathfrak{P}}(y_N) < p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ is a finite set included in places at infinity and poles of y_N.

Theorem 3.3.27. — *Let $N \in C[Y]$ be a separable irreducible polynomial. Let*

$$S := \{\mathfrak{P} \in \mathbb{P}_{K_N} | \nu_{\mathfrak{P}}(y_N) < p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})\}.$$

Then $N(\partial^p)$ is irreducible if and only if there exists $\mathfrak{P} \in S$ such that the $\mathbb{F}_p$-linear system

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}\left(\sum_{k=\eta_{\mathfrak{P}}}^{\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})-1} f_k t^k\right) + \sum_{k=\eta_{\mathfrak{P}}}^{\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})-1} f_k^p t^{pk} = y_N + O(t_{\mathfrak{P}}^{p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})})$$

has no solution in $\mathcal{G}_{\mathfrak{P}}^{\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})-\eta_{\mathfrak{P}}}$ where

$$\eta_{\mathfrak{P}} := \min(\nu_{\mathfrak{P}}(y_N), \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})).$$

Proof. This is a direct consequence of the above discussion and Theorem 3.3.11. □

We can now write an algorithm for testing the irreducibility of an operator $N(\partial^p)$ where N is an irreducible polynomial over C. From Lemma 3.2.12 we know that we can take $Q \in K[Y]$ such that $Q^p(Y) = N(Y^p)$ and $K_N \simeq {}^{K[Y]}/_{Q}$. If we denote by a the image of Y in K_N then $y_N = a^p$. This representation is easier to manipulate (because smaller by a factor p in all generality) so we consider that the entry of our algorithm is the polynomial Q. Thus the goal of the algorithm can be stated as such: Given a separable irreducible polynomial $N \in K[Y]$, is $N^p(\partial)$ irreducible in $K\langle\partial\rangle$?

Evaluating the complexity of Algorithm 6

The correctness of Algorithm 6 is easily deduced from the discussion that precedes. Evaluating its complexity is difficult without specifying the algorithm used to choose primes elements because the sole property of being a prime element does not bound the size of said element.

Example 3.3.28. — In the rational function field $\mathbb{F}_q(x)$, x is a prime element of the place 0, as are the elements $x(x+1)^n$ for $n \in \mathbb{N}$.

We leave aside this question for the time being and will circle back to it later. To simplify the complexity evaluation of this algorithm, we assume that $K = \mathbb{F}_q(x)$ with $q = p^b$ and that $N \in \mathbb{F}_q[x, y]$ with $d_x = \deg_x N$ and $d_y = \deg_y N$. It follows that K_N is a field extension of $\mathbb{F}_q(x)$ of degree d_y. As such, any $f \in K_N$ can be represented by d rational functions in $\mathbb{F}_q(x)$. For any element $f = \frac{1}{D_f}\sum_{i=0}^{d_y-1} f_i a^i \in K_N$ such that $D_f, f_0, \ldots, f_{d_y-1} \in \mathbb{F}_q[x]$ with $\gcd(D_f, f_0, \ldots, f_{d_y-1}) = 1$ we write

$$\deg f := \max(\deg D_f, \deg f_0, \ldots, \deg f_{d_y-1}).$$

Input: $N_* \in K[Y]$ a separable irreducible polynomial.
Output: Whether or not $N_*^p(\partial)$ in irreducible in $K\langle\partial\rangle$

1. Set $K_N := K[a] = {}^{K[Y]}/_{N_*}$ where a is a root of N_*.
2. Compute $\mathbb{S} := \mathrm{Supp}(a)_- \cup \mathrm{Supp}(x)_-$.
3. For $\mathfrak{P}$ in $\mathbb{S}$ do:
   (a) Compute $t_\mathfrak{P}$ a prime element of $\mathfrak{P}$.
   (b) Compute $t'_\mathfrak{P}$ and set $\eta := \nu_\mathfrak{P}(t'_\mathfrak{P}) - \nu_\mathfrak{P}(a)$.
   (c) If $\eta > 0$ do:
      i. Compute $g_\mathfrak{P}$, the Taylor expansion of $t'_\mathfrak{P}$ in $t_\mathfrak{P}$ at relative precision η.
      ii. Compute $a_\mathfrak{P}$ the Taylor expansion of a in $t_\mathfrak{P}$ at relative precision η.
      iii. Check if a seed of the p-Riccati equation relative to $g_\mathfrak{P}$ and $a_\mathfrak{P}$ exists using Algorithm 4.
      iv. If it doesn't, return **False** and stop the algorithm.
4. return **True**

Algorithm 6: irreducibility_test

The concept of Algorithm 6 is to transform a global problem (meaning a problem on a global field) to several local problems that can be solved using "small" precisions. As such the cost of this irreducibility test can be divided in two distinct categories:

- Doing the conversion from global to local. Those are step (1) to step $(3)(c)(ii)$.
- Solving the local problems. Those are steps $(3)(c)(iii)$ and $(3)(c)(iv)$.

This separation is particularly relevant since, while the size of the local prime elements $t_\mathfrak{P}$ influences the cost of computing $t'_\mathfrak{P}$ and the cost of computing the Taylor expansions, once those step are done it does not influence the complexities of solving the local problems.

THEOREM 3.3.29. — *When applying Algorithm 6 to N, solving the local problems can be done in $\tilde{O}(b^\omega(d_x + d_y)^\omega \log^2(p))$ bit operations.*

Proof. First, let $\mathfrak{P} \in \mathrm{Supp}(a)_- \setminus \mathrm{Supp}(x)_-$ and let $\eta_\mathfrak{P} = \nu_\mathfrak{P}(t'_\mathfrak{P}) - \nu_\mathfrak{P}(a)$. We can suppose that $\eta_\mathfrak{P} > 0$. Since $\mathfrak{P} \notin \mathrm{Supp}(x)_-$, $\nu_\mathfrak{P}(t'_\mathfrak{P}) \leqslant 0$. Thus $\eta_\mathfrak{P} \leqslant \nu_\mathfrak{P}(a)$. Theorem 3.3.19 states that step $(3)(c)(iii)$ relative to $\mathfrak{P}$ can be done in

$$\tilde{O}\left(\left(\frac{\eta_\mathfrak{P}}{p} b\deg(\mathfrak{P})\log(p) + \eta_\mathfrak{P} + \frac{\eta_\mathfrak{P}^2}{p} + (b\deg(\mathfrak{P}))^{\omega-1}\right) b\deg(\mathfrak{P})\log^2(p)\right)$$

bit operations or, less precisely, in $\tilde{O}((\eta_\mathfrak{P} b\deg(\mathfrak{P}))^\omega \log(p))$ bit operations. It follows that step $(3)(c)(iii)$ over all the places of $\mathrm{Supp}(a)_- \setminus \mathrm{Supp}(x)_-$ can be done in

$$\tilde{O}\left(\sum_{\mathfrak{P}\in\mathrm{Supp}(a)_-} (-b\nu_\mathfrak{P}(a)\deg(\mathfrak{P}))^\omega \log^2(p)\right) \subset \tilde{O}(b^\omega \deg\,(a)_-^\omega)\log^2(p))$$

bit operations. According to Proposition B.3.7, $\deg\,(a)_- = [K_N : \mathbb{F}_q(a)] \leqslant d_x$. Thus step $(3)(c)(iii)$ over all the places of $\mathrm{Supp}(a)_- \setminus \mathrm{Supp}(x)_-$ can be done in $\tilde{O}((bd_x)^\omega \log^2(p))$ bit operations.

We do the same reasoning for the places $\mathfrak{P} \in \mathrm{Supp}(x)_-$. We find that $\eta_\mathfrak{P} = \nu_\mathfrak{P}(t'_\mathfrak{P}) - \nu_\mathfrak{P}(a) \leqslant e(\mathfrak{P}|\mathfrak{P}_\infty) - \nu_\mathfrak{P}(a)$ and that step $(3)(c)(iii)$ can be done in

$$\tilde{O}((b(\deg\,(x)_- + \deg\,(a)_-))^\omega \log^2(p))$$

bit operations, or

$$\tilde{O}(b^\omega (d_y + d_x)^\omega \log^2(p))$$

bit operations, according to Proposition B.3.7. The result immediately follows. □

Evaluating the complexity of the first part of the algorithm is a harder task. We begin by the cost of computing the Taylor expansions. Let $\mathfrak{P} \in \mathbb{P}_{K_N}$ and $t_\mathfrak{P} \in K_N$ be a prime element of $\mathfrak{P}$. We set $d_t := \deg t_\mathfrak{P}$ as defined earlier.

Lemma 3.3.30. — *Let $f, g \in K_N$ of respective degrees d_f and d_g. Then*

- $\deg fg \leqslant d_f + d_g + O(d_x d_y)$.
- $\deg f^{-1} = O((d_f + d_x)d_y)$.
- *If $f = F(x, a)$ with $F \in \mathbb{F}_q[x, Y]$, then* $\deg f' \leqslant d_f + O(d_x d_y)$.

Proof.

- Let $f = F(x, a)$ and $g = G(x, a)$ with $F, G \in \mathbb{F}_q(x)[Y]$. We have $\deg_x(FG) = d_f + d_g$ and $\deg_Y(FG) \leqslant 2(d_y - 1)$. Then fg can be represented by $R(x, a)$ where R is the remainder of the Euclidean division of FG by N. It is easy to see that each step of the naive Euclidean division algorithm only makes the degree in x grow by d_x. Since there are at most $d_y - 1$ steps we have

$$\deg fg \leqslant d_f + d_g + d_x d_y.$$

- Let $f = F(x, a)$ with $F \in \mathbb{F}_q(x)[Y]$. Then the coefficients of f^{-1} can be expressed as minors of the Sylvester matrix of F and N. The minors of the Sylvester matrix have a degree in x which is $O((d_f + d_x)d_y)$.

- Let $f = F(x, a)$ with $F \in \mathbb{F}_q[x, Y]$. Then

$$f' = \partial_x F(x, a) + a' \partial_y F(x, a).$$

But we also have

$$a' = -\frac{\partial_x N(x, a)}{\partial_y N(x, a)}.$$

From the previous points we see that $\deg a' = O(d_x d_y)$. But then

$$\deg(f') \leqslant d_f + O(d_x d_y).$$

□

Input: $f \in K_N$, $\mathfrak{P} \in \mathbb{P}_{K_N}$, $t_{\mathfrak{P}}$ a prime element of $\mathfrak{P}$, $N \in \mathbb{N}$
Output: The list of coefficients of the Taylor expansion of f in $t_{\mathfrak{P}}$ at relative precision N

1. **If** $\nu_{\mathfrak{P}}(f) < 0$, set $f_* = t_{\mathfrak{P}}^{-\nu_{\mathfrak{P}}(f)} f$.
2. **Else** set $f_* = f$.
3. Set $L = [\,]$ an empty list.
4. **For** k **from** 1 **to** N **do**:
   (a) Compute $v := f_*(\mathfrak{P})$.
   (b) Set $f_* \leftarrow (f_* - v)t_{\mathfrak{P}}^{-1}$.
   (c) Append v to L.
5. return L.

Algorithm 7: Naive_Taylor_expansion

We can now evaluate the cost of computing the Taylor expansions in steps $(3)(c)(i)$ and $(3)(c)(ii)$ in terms of bit operations and evaluations in K_N. We use a naive algorithm

REMARK 3.3.31. — If $\mathfrak{P}$ is not of degree 1, this algorithm requires to compute the constant field extension $K_N \cdot \mathcal{G}_{\mathfrak{P}}$ of K_N, where $\mathcal{G}_{\mathfrak{P}}$ is the residue class field of K_N in $\mathfrak{P}$.

LEMMA 3.3.32. — *Let $f \in K_N$ be of degree d_f. Algorithm 7 computes the Taylor expansion of f at order N in N evaluations of functions of degree $O(d_f + N(d_t + d_x)d_y)$ and $\tilde{O}(Nd_y(d_f + N(d_t + d_x)d_y))$ operations in $K_{N,\mathfrak{P}}$.*

Proof. The result comes from the fact that if f_* is of degree d_{f_*} then at step $(4)(b)$, f_* is updated to a function of degree $d_{f_*} + O((d_t + d_x)d_y)$. Since step (4) is repeated N times we see that Algorithm 7 manipulates functions of degree $O(d_f + N(d_t + d_x)d_y)$. Now the algorithm does N multiplications of those functions. Each of these can be realised in $\tilde{O}(d_y(d_f + N(d_t + d_x)d_y)$ operations in $K_{N,\mathfrak{P}}$ which yields the desired result. □

The final cost of steps $(3)(c)(i)$ and $(3)(c)(ii)$ thus depends on the "size" of the prime elements $t_{\mathfrak{P}}$.

Computing local uniformisers In 2011, Jordi Guardia, Jesús Montes and Enric Nart presented in [GMN11] an algorithm designed for number fields called *Montes algorithm*. This algorithm takes in input a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ which defines a number field $K = \mathbb{Q}[\theta]$, where θ is a root of f, and a prime number $p \in \mathbb{Z}$.
The algorithm returns a full factorisation $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ of the ideal $p\mathbb{Z}_K$ as a product of prime ideals of $\mathbb{Z}_K$, where $\mathbb{Z}_K$ is the subring of elements of K which are integral over $\mathbb{Z}$, as well as generators $\alpha_1, \dots, \alpha_g$ verifying $\mathfrak{p}_i = p\mathbb{Z}_K + \alpha_i\mathbb{Z}_K$.

The settings of number fields and algebraic function fields are actually very similar and *Montes algorithm* can be easily adapted to this last one. The analogous algorithm would take

in input a monic irreducible polynomial $f(x,y) \in \mathbb{F}_q[x][y]$ generating an algebraic function field of positive characteristic $F \simeq {}^{\mathbb{F}_q(x)[y]}/_{f(x,y)}$, and an irreducible polynomial $P \in \mathbb{F}_q[x]$.
It would return the divisor $(P) = e(\mathfrak{P}_1|P) \cdot \mathfrak{P}_1 + \ldots + e(\mathfrak{P}_g|P) \cdot \mathfrak{P}_g$ as well as prime elements $t_{\mathfrak{P}_i}$ for all the places in $\mathrm{Supp}(P)$.

Montes algorithm is the basis of a lot of algorithms to work in number fields or algebraic function fields. Among other things, in [BNS13], a version of *Montes algorithm* where the generators α_i are not computed is used as a key element to compute *OM-representations* (see for example [Nar11]), of the ideals dividing p, from which the generators can be obtained as a byproduct.
In [PW22, section 6], Adrien Poteaux and Martin Weimann stated that for a number field $\mathbb{K} = {}^{\mathbb{Q}[x]}/_{(F)}$, where F is a monic integral polynomial, and a prime $p \in \mathbb{Z}$, an *OM-representation* of the prime ideals dividing p can be computed in $\tilde{O}_\varepsilon(\deg_y(f)\delta)$ operations in $\mathbb{F}_p$, where δ is the valuation of $\mathrm{Disc}(F)$ in p, if $p > \deg_y(f)$ or $O_\varepsilon(\deg_y(f)\delta + \delta^2)$ operations in $\mathbb{F}_p$ otherwise.
The analogous result for algebraic functions fields is that for an algebraic function field $\mathbb{F} = {}^{\mathbb{F}_q(x)[y]}/_{f(x,y)}$, where f is a monic integral polynomial, and an irreducible polynomial $P \in \mathbb{F}_q[x]$, an *OM-factorisation* of the prime ideals dividing P can be computed in $O_\varepsilon(\deg(P)\deg_y(f)\delta)$ operations in $\mathbb{F}_q$ if $\mathrm{char}(\mathbb{F}_q) > \deg_y(f)$, and $O_\varepsilon(\deg(P)(\deg_y(f)\delta + \delta^2))$ operations in $\mathbb{F}_q$ otherwise, where δ is the valuation of $\mathrm{Disc}(F)$ in P.

In a personal communication, Martin Weimann explained to us, as a consequence of [GMN11, Proposition 4.28] and of results of a paper in preparation [PWed], that a prime element $t_{\mathfrak{P}}$ of a place $\mathfrak{P} \in \mathrm{Supp}(P)$ can be computed with $\deg t_{\mathfrak{P}} = O(\deg(P)\frac{\delta}{\deg_y(f)})$ at the cost of an *OM-factorisation* and $O(\deg(P)\delta)$ operations in $\mathbb{F}_q$.

Lemma 3.3.33. — *Steps* (3)(*c*)(*i*) *and* (3)(*c*)(*ii*) *of Algorithm 6 can be done in* $O(d_x + d_y)$ *evaluations of algebraic functions in* K_N *of degree* $O(d_x^2 d_y + d_x d_y^2)$ *and* $\tilde{O}((d_x^3 d_y^2 + d_x^2 d_y^3)b\log(p))$ *bit operations.*

Proof. To apply the results previously mentioned we must first bring ourselves back to the case where K_N is generated by an integral element over $\mathbb{F}_q[x]$. Let us denote l_c the leading coefficient of N. If a is not integral then $l_c a$ is integral, of minimal polynomial over $\mathbb{F}_q[x]$

$$N_{int} = l_c^{d_y - 1} N(Y/l_c).$$

Furthermore we have

$$\mathrm{Disc}(N_{int}) = l_c^{d_y - 1}\mathrm{Disc}(N).$$

Let $\mathfrak{P} \in \mathrm{Supp}(a)_- \setminus \mathrm{Supp}(x)_-$. Applying Lemma 3.3.32 to $f = t'_{\mathfrak{P}}$ and $d_t = O(\deg(P)\delta/d_y)$ yields that the Taylor expansion of $t'_{\mathfrak{P}}$ and a in $t_{\mathfrak{P}}$ at precision $-\nu_{\mathfrak{P}}(a)$ can be computed in $-\nu_{\mathfrak{P}}(a)$ evaluation of algebraic functions in K_N of degree $O(-\nu_{\mathfrak{P}}(a)(\deg(P)\delta + d_x d_y))$ where $\mathfrak{P}|P$ and δ is the valuation of $\mathrm{Disc}(N_{int})$ in P, and $\tilde{O}(-d_y\nu_{\mathfrak{P}}(a)^2(\deg(P)\delta + d_x d_y))$ operations in $K_{N,\mathfrak{P}}$.
We know that $\deg(P)\delta \leqslant \deg \mathrm{Disc}(N_{int}) = O(d_x d_y)$.

Remark 3.3.34. — We could also have $\delta = 0$ in which case $\deg t_{\mathfrak{P}}$ would still verify $\deg t_{\mathfrak{P}} = O(\deg(P))$. But since $\mathfrak{P}$ is a pole of a this means that P is a zero of l_c. In particular this means that $\deg(P) \leqslant d_x$.

Furthermore since $-\nu_{\mathfrak{P}}(a) \leqslant d_x$ we find that the Taylor expansion of $t'_{\mathfrak{P}}$ and a in $t_{\mathfrak{P}}$ at precision $-\nu_{\mathfrak{P}}(a)$ can be computed in $-\nu_{\mathfrak{P}}(a)$ evaluations of functions in K_N of functions of degree $O(d_x^2 d_y)$ and $\tilde{O}(-\nu_{\mathfrak{P}}(a)^2 d_x d_y^2)$ operations in $K_{N,\mathfrak{P}}$, which is to say $\tilde{O}(-\nu_{\mathfrak{P}}(a)^2 \deg(\mathfrak{P}) d_x d_y^2 b \log(p)$ bit operations. We make the summation of those for $\mathfrak{P} \in \mathrm{Supp}(a)_-$ and get that steps $(3)(c)(i)$ and $(3)(c)(ii)$ can be for all those places can be done in $O(d_x)$ evaluations of functions in K_N of degree $O(d_x^2 d_y)$ and $\tilde{O}(d_x^3 d_y^2 b \log(p))$ bit operations.

The symmetrical reasoning for places in $\mathrm{Supp}(x)_-$ (we just exchange the roles of d_x and d_y) yields the final result.

REMARK 3.3.35. — We have skipped places in $\mathrm{Supp}(a)_- \cap \mathrm{Supp}(x)_-$. The reasoning is the same but one has to replace $-\nu_{\mathfrak{P}}(a)$ by $e(\mathfrak{P}) - \nu_{\mathfrak{P}}(a)$. Then we have

$$\sum_{\mathfrak{P} \in \mathrm{Supp}(a) \cap \mathrm{Supp}(x)_-} (e(\mathfrak{P}) - \nu_{\mathfrak{P}}(a)) \deg(\mathfrak{P}) \leqslant \sum_{\mathfrak{P} \in \mathrm{Supp}(x)_-} e(\mathfrak{P}) \deg(\mathfrak{P}) - \sum_{\mathfrak{P} \in \mathrm{Supp}(a)_-} \nu_{\mathfrak{P}}(a) \deg(\mathfrak{P})$$
$$\leqslant d_y + d_x$$

and this doesn't modify the final result.

□

Now we can give an upper bound on the cost of doing the conversion from global to local in Algorithm 6.

THEOREM 3.3.36. — *Steps* (1) *to* $(3)(c)(ii)$ *in Algorithm 6 can be done at the cost of computing* $(a)_-$ *and* $(x)_-$ *as well as* $O_\varepsilon(d_x d_y b \log(p))$ *bit operations from computing* OM-representations *and prime elements,* $O(d_x + d_y)$ *evaluation of functions in* K_N *of degree* $O(d_x^2 d_y + d_x d_y^2)$ *and* $\tilde{O}((d_x^3 d_y^2 + d_x^2 d_y^3) b \log(p))$ *bit operations.*

REMARK 3.3.37. — In particular, testing the irreducibility of $N(\partial^p)$ with N an irreducible polynomial $C[Y]$ can be done in polynomial time in $\log(p)$

3.4 A factorisation algorithm on algebraic function fields

The goal of this section is to write a complete factorisation algorithm over $K\langle\partial\rangle$. Our work in Section 3.2.3 teaches us that we first need to solve (3.2). We begin this section by presenting a method to solve the p-Riccati equation. To this end we use algebraic geometry tools such as Riemann-Roch spaces and the Picard group of K_N.
Solving the p-Riccati equation is somewhat easy to do when $K = \mathbb{F}_q(x)$, where q is a power of p, and $\chi_{min}(L)(Y) = Y - a$ with $a \in K$. In [vdPS03, §13.2.1], van der Put and Singer presented a method to find a solution when it exists. We recall briefly their method as it will serve as a guideline for the techniques we shall develop afterwards in the general case.

We suppose that $K = \mathbb{F}_q(x)$. In this case the p-Riccati equation can be written as

$$b^{(p-1)} + b^p = g^p$$

with $g \in \mathbb{F}_q(x)$. We write $g = \frac{P_1}{P_2}$ with $P_1, P_2 \in \mathbb{F}_q[x]$ coprime. Let $P_2 = \prod_{i\in I} N_i^{\nu_i}$ where the N_i are pairwise distinct irreducible polynomials and let $f \in \mathbb{F}_p(x)$ verify

$$f^{(p-1)} + f^p = g^p.$$

For all irreducible polynomial P we find:

$$\begin{aligned}\nu_P(g^p) &= p\nu_P(g)\\ &= \nu_P(f^{(p-1)} + f^p)\\ &\geqslant \min(\nu_P(f^{(p-1)}), p\nu_P(f))\\ &\geqslant \min(\nu_P(f) - (p-1), p\nu_P(f)).\end{aligned}$$

Furthermore we have an equality if $\nu_P(f^{(p-1)}) \neq p\nu_P(f)$. In particular we find $\nu_P(g) = \nu_P(f)$ if $\nu_P(f) \leqslant -2$. This implies that if f has a pole that is not a pole of g, then it is a simple pole.
Let us suppose that P is a pole of f which is not a pole of g. We write $f = f_1 + f_2$ with $f_2 = \frac{Q}{P}$, $\nu_P(f_1) \geqslant 0$ and $\deg(Q) < \deg(P)$. The fact that we are able to do such a decomposition is a consequence of partial fraction decomposition. Since $\nu_P(g^p) \geqslant 0$ and $\nu_P(f_1^{(p-1)} + f_1^p) \geqslant 0$ it follows that $\nu_P(f_2^{(p-1)} + f_2^p) \geqslant 0$. Moreover, since $\nu_\infty(f_2) > 0$, we also have $\nu_\infty(f_2^{(p-1)} + f_2^p) > 0$. Since $f_2^{(p-1)} + f_2^p$ has no poles outside of P, this means that $f_2^{(p-1)} + f_2^p$ has no poles but has at least one zero (at ∞). Thus $f_2^{(p-1)} + f_2^p = 0$.
Thus f_1 is also a solution of the p-Riccati equation with no pole in P and no poles outside of those of f.

We deduce that there is a solution f_* of the p-Riccati equation whose denominator divides P_2. We write $f_* = \frac{R}{P_2}$. Then

$$f_*^{(p-1)} + f_*^p = \frac{(RP_2^{p-1})^{(p-1)} + R^p}{P_2^p} = \frac{P_1^p}{P_2^p}.$$

Thus

$$p\deg(P_1) \leqslant \max(p\deg(R), \deg(R) + (p-1)(\deg(P_2) - 1))$$

and equality holds if $p\deg(R) \neq \deg(R) + (p-1)(\deg(P_2) - 1)$. Thus

$$\deg(R) \leqslant \max(\deg(P_1), \deg(P_2) - 1).$$

Finding R is now just a matter of solving a finite dimensional $\mathbb{F}_p$-linear system since $R \mapsto (RP_2^{p-1})^{(p-1)} + R^p$ is an $\mathbb{F}_p$-linear map.
An important part of our work on the structure of factorisations of L (and $N(\partial^p)$) is made under the assumption that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to a matrix algebra. A consequence of the above discussion is the following:

The idea for solving the p-Riccati equation in all generality over algebraic function fields is the same as the one developed above for rational functions, that is to say to look at the poles of a solution and show that another solution has "few" poles outside those of y_N. The situation is more complicated than in the rational case because we do not have an equivalent to the partial fraction decomposition. In other words, in the rational case we remove unwanted poles P of a

solution by adding a multiple of $\frac{P'}{P}$ to our solution. This method works because it is always possible to create rational functions of chosen numerators and denominators. That is to say, that it is always possible to choose exactly the zeros and poles of a rational function.
Such a thing is not true for algebraic functions and we will have to measure "how far" a certain combination of zeros and poles is from being represented by an algebraic function. The object measuring this obstruction is called the Picard group of K_N and is a finite commutative group. This analysis will allow us to restrain our search for solutions to a finite dimensional $\mathbb{F}_p$-vector space of algebraic functions in K_N whose poles can only appear in a finite number of places and are of bounded multiplicity. Such spaces are called Riemann-Roch spaces and are a classical tool in algebraic geometry. A number of algorithms to compute them have been developed [ABCL22, ACL22, LGS20, BCL22].

3.4.1 p-Riccati equation over algebraic function fields and Picard group

We now present our theorical results from which we will deduce an algorithm to solve the p-Riccati equation. As we will see, a fully deterministic approach to solving this equation would require one to compute the cokernel of the multiplication by p on the Picard group of K_N with relations which is a notoriously difficult task. Although algorithms polynomial in the genus of K_N and in the characteristic exist for computing l-torsion subgroups as well as the cokernel of the multiplication by l (see for example [EC11, Theorem 13.6.2]), they only work for primes l coprime with the characteristic. To our knowledge there is no algorithm computing the cokernel of the multiplication by p on the Picard group of K_N in polynomial time in the genus of K_N and in p.

This is why the actual algorithm will take a more probabilistic approach which cannot on its own guarantee the irreducibility of $N(\partial^p)$ if no solution is found, and combine it with the irreducibility test presented in the previous section.
The methods presented in this section will work to find irreducible divisors of operators with coefficients in any algebraic function field K. However, for the sake of simplicity, we will limit our complexity analysis to $K = \mathbb{F}_q(x)$ where q is a power of p.

As previously mentioned, the idea behind this method is the same as for the method over $\mathbb{F}_q(t)$ which is to say that we study the poles of a given solution. Before we begin let us fix some notation.

Notation 3.4.1. We continue to use Notation 3.2.11. We also recall that if $N \in C[Y]$ is a separable irreducible polynomial then we denote by $S_N := \{f \in K_N | f^{(p-1)} + f^p = y_N\}$.
We also use the notations of Appendix B to which we refer for more details on the objects used in this section. From now on we will often denote places of K_N by $\mathfrak{P}$. The valuation associated with $\mathfrak{P}$ will be denoted $\nu_{\mathfrak{P}}$ and $t_{\mathfrak{P}}$ will always be a prime element of the place $\mathfrak{P}$, which is to say that $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}) = 1$. If $f \in K_N$ verifies $\nu_{\mathfrak{P}}(f) \geqslant 0$ we will denote by $f(\mathfrak{P})$ the image of f in the residue field of $\mathfrak{P}$.
As we did earlier, the set of places over an algebraic function field F will be denoted $\mathbb{P}_F$. The group of divisors of F will be denoted by $\mathrm{Div}(F)$ and its divisor class group (or Picard group) by $\mathrm{Cl}(F)$. For $f \in K_N$ we denote by (f) its principal divisor, $(f)_+$ its zero divisor and $(f)_-$ the divisor of its poles. We will designate by $\mathrm{Diff}(K_N)$ the different divisor of K_N.

Finally, if $D \in \mathrm{Div}(F)$ we will denote by $\mathcal{L}(D)$ the associated Riemann-Roch space.

We begin by proving some results, analog to Lemma 3.3.10 for algebraic functions.

PROPOSITION 3.4.2. — *Let $N \in C[Y]$ be a separable irreducible polynomial. Let $\mathfrak{P}$ be a place of K_N, $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$ and $f \in S_N$. Then*

$$\nu_{\mathfrak{P}}(f) \geqslant \min(p^{-1}\nu_{\mathfrak{P}}(y_N), \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1).$$

Proof. Let $f \in K_N$ be a solution of the p-Riccati equation over K_N (3.2). Then we have

$$\begin{aligned}\nu_{\mathfrak{P}}(y_N) &= \nu_{\mathfrak{P}}(f^{(p-1)} + f^p)\\ &\geqslant \min(\nu_{\mathfrak{P}}(f^{(p-1)}, p\nu_{\mathfrak{P}}(f))\end{aligned}$$

Furthermore we have an equality if $\nu_{\mathfrak{P}}(f^{(p-1)}) \neq p\nu_{\mathfrak{P}}(f)$.
In particular if $\nu_{\mathfrak{P}}(f) < \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$ then, according to Proposition B.2.8,

$$p\nu_{\mathfrak{P}}(f) < \nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1) \leqslant \nu_{\mathfrak{P}}(f^{(p-1)})$$

and

$$\nu_{\mathfrak{P}}(y_N) = p\nu_{\mathfrak{P}}(f).$$

□

When solving the p-Riccati equation over $\mathbb{F}_q((t))$ we showed that we could find another solution verifying a slightly better bound. The same principle applies here locally.

DEFINITION-PROPOSITION 3.4.3. — *Let $f \in S_N$ and $\mathfrak{P}$ be a place of K_N verifying $\nu_{\mathfrak{P}}(y_N) \geqslant p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. Then there exists a unique $k \in \mathbb{F}_p$ such that for all $g \in K_N$, if $\nu_{\mathfrak{P}}(g) \equiv k \mod p$ then $f - \frac{g'}{g} \in S_N$ and $\nu_{\mathfrak{P}}\left(f - \frac{g'}{g}\right) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. We call k the ramified residue of f in $\mathfrak{P}$ and write*

$$\mathfrak{Re}_{\mathfrak{P}}(f) := k.$$

Proof. The fact that for any $g \in K_N^{\times}$, $f - \frac{g'}{g} \in S_N$ is a direct consequence of Lemma 3.2.19.

If $\nu_{\mathfrak{P}}(f) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ then we can take $k = 0$. Indeed in this case if $\nu_{\mathfrak{P}}(g) \equiv 0 \mod p$ then there exists $l \in \mathbb{N}$ such that $g = t_{\mathfrak{P}}^{pl}u$ with $\nu_{\mathfrak{P}}(u) = 0$. Then

$$\frac{g'}{g} = \frac{u'}{u} + pl\frac{t'_{\mathfrak{P}}}{t_{\mathfrak{P}}} = \frac{u'}{u}.$$

Since $\nu_{\mathfrak{P}}(u) = 0$, we can write $u = \sum_{n=0}^{\infty} u_n t_{\mathfrak{P}}^n$ and $u' = t'_{\mathfrak{P}} \sum_{k=0}^{\infty}(n+1)u_{n+1}t_{\mathfrak{P}}^n$. Thus $\nu_{\mathfrak{P}}(u') \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ and $\nu_{\mathfrak{P}}\left(\frac{g'}{g}\right) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ which yields the result.

Suppose now that $\nu_{\mathfrak{P}}(f) < \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. From Proposition 3.4.2, this means that $\nu_{\mathfrak{P}}(f) = \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$. We set $e = 1 - \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$, $a := (t_{\mathfrak{P}}^{e-1}t'_{\mathfrak{P}})(\mathfrak{P})$ and $c := (t_{\mathfrak{P}}^e f)(\mathfrak{P})$. Let us show that $c \in \mathbb{F}_p^{\times}a$. Since we know that p does not divide e (see Proposition B.2.8), we know that $\nu_{\mathfrak{P}}(f^{(p-1)}) = -pe$. Furthermore we know (Proposition 3.3.8) that

$$f^{(p-1)} := \frac{\mathrm{d}^{p-1}}{\mathrm{d}t_{\mathfrak{P}}^{p-1}}(t_{\mathfrak{P}}^{p-1}f).$$

It follows that

$$(t_{\mathfrak{P}}^{pe} f^{(p-1)})(\mathfrak{P}) = -a^{p-1}c$$

and

$$(t_{\mathfrak{P}}^{pe} f^{p})(\mathfrak{P}) = c^{p}.$$

But

$$t_{\mathfrak{P}}^{pe}(f^{(p-1)} + f^{p})(\mathfrak{P}) = (t_{\mathfrak{P}}^{pe} y_N)(\mathfrak{P}) = 0$$

since $\nu_{\mathfrak{P}}(y_N) > -pe$.
It follows that

$$\begin{aligned} t_{\mathfrak{P}}^{pe}(f^{(p-1)} + f^{p})(\mathfrak{P}) &= c^{p} - a^{p-1}c \\ &= 0. \end{aligned}$$

Thus $c^{p-1} = a^{p-1}$ and $c \in \mathbb{F}_p^{\times} a$. We set $k := c \cdot a^{-1}$. Let $g \in K_N$ be such that $\nu_{\mathfrak{P}}(g) \equiv k \mod p$. There exists $l \in \mathbb{Z}$ and $u \in K_N$ such that $\nu_{\mathfrak{P}}(u) = 0$ and $g = t_{\mathfrak{P}}^{pl+k} u$. Then

$$\frac{g'}{g} = k\frac{t_{\mathfrak{P}}}{t_{\mathfrak{P}}} + \frac{u'}{u}.$$

Since $\nu_{\mathfrak{P}}(u) = 0$, $\nu_{\mathfrak{P}}(u') > -e$ and $\nu_{\mathfrak{P}}\left(\frac{g'}{g}\right) = -e$. Then

$$\left(t_{\mathfrak{P}}^{e}\frac{g'}{g}\right)(\mathfrak{P}) = k(t_{\mathfrak{P}}^{e-1}t'_{\mathfrak{P}})(\mathfrak{P}) = ka = c.$$

Thus

$$\left(t_{\mathfrak{P}}^{e}\left(f - \frac{g'}{g}\right)\right)(\mathfrak{P}) = 0$$

which is to say that

$$\nu_{\mathfrak{P}}\left(f - \frac{g'}{g}\right) \geqslant 1 - e = \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}).$$

□

Thus we see that if S_N is not empty and if $\mathfrak{P} \in \mathbb{P}_{K_N}$ is such that y_N has no pole of greater multiplicity than $-p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$, then S_N contains an element with no pole in $\mathfrak{P}$ of multiplicity greater than $-\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. This is also the valuation of the divisor $\mathrm{Diff}(K_N) - 2(x)_-$ in $\mathfrak{P}$(see Proposition B.4.17). In particular if $\mathfrak{P}$ is neither ramified nor a pole of y_N then S_N contains an element with no pole in $\mathfrak{P}$. This local improvement on the bound provided in Proposition 3.4.2 is accomplished by adding an element of the form $\frac{g'}{g}$. Unfortunately adding such an element makes new poles appear in general so we cannot proceed as we did over $\mathbb{F}_q(t)$. Instead we take a more global approach.

THEOREM 3.4.4. — *Let $f \in S_N$ and $V := \{\mathfrak{P} \in \mathbb{P}_{K_N} | \nu_{\mathfrak{P}}(y_N) < p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})\}$. Set*

$$\mathfrak{Re}(f) := \sum_{\substack{\mathfrak{P} \in \mathbb{P}_{K_N} \\ \mathfrak{P} \notin V}} \mathfrak{Re}_{\mathfrak{P}}(f) \cdot \mathfrak{P}.$$

Let $D', D_p \in \mathrm{Div}(F)$ be such that

$$\mathfrak{Re}(f) \sim D' + pD_p.$$

There exists $f_* \in S_N$ verifying $\nu_{\mathfrak{P}}(f_*) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ for all places $\mathfrak{P}$ outside $V \cup \mathrm{supp}(D')$.

Proof. Since $\mathfrak{Re}(f) \sim D' + pD_p$, there exists $g \in K_N$ such that $\mathfrak{Re}(f) - D' - pD_p = (g)$. From Lemma 3.2.19, we deduce that $f - \frac{g'}{g} \in S_N$. Let $\mathfrak{P} \in \mathbb{P}_{K_N} \backslash (S \cup \operatorname{supp}(D'))$. Then we find

$$\begin{aligned} \nu_{\mathfrak{P}}(g) &= \nu_{\mathfrak{P}}(\mathfrak{Re}(f)) - \nu_{\mathfrak{P}}(D') - p\nu_{\mathfrak{P}}(D_p) \\ &= \nu_{\mathfrak{P}}(\mathfrak{Re}(f)) - 0 - p\nu_{\mathfrak{P}}(D_p) \\ &\equiv \nu_{\mathfrak{P}}(\mathfrak{Re}(f)) \mod p \\ &\equiv \mathfrak{Re}_{\mathfrak{P}}(f) \mod p \end{aligned}$$

By definition of $\mathfrak{Re}_{\mathfrak{P}}(f)$, $f - \frac{g'}{g}$ is an element of S_N verifying for any place $\mathfrak{P}$ outside $V \cup \operatorname{Supp}(D')$ that

$$\nu_{\mathfrak{P}}(f - \frac{g'}{g}) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}).$$

□

We consider $\mathfrak{G}_N^p = {}^{\mathrm{Cl}(K_N)}\!/_{p\mathrm{Cl}(K_N)}$. According to Proposition B.3.10, $\mathfrak{G}_N^p$ is a finite commutative group of the form $\mathfrak{G}_N^p \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$ for some $n \in \mathbb{N}^*$.

DEFINITION 3.4.5. — Let $D_1, D_2 \in \operatorname{Div}(K_N)$. We define the maximum of D_1 and D_2 as

$$\max(D_1, D_2) := \sum_{\mathfrak{P} \in \mathbb{P}(K_N)} \max(\nu_{\mathfrak{P}}(D_1), \nu_{\mathfrak{P}}(D_2)) \cdot \mathfrak{P}.$$

COROLLARY 3.4.6. — *For each place $\mathfrak{P} \in \mathbb{P}_{K_N}$ we denote by $t_{\mathfrak{P}}$ a prime element of $\mathfrak{P}$.*
Let $(D_1, \ldots, D_n) \in \operatorname{Div}(K_N)^n$ be a lifting of a generating family of $\mathfrak{G}_N^p$ viewed as a $\mathbb{F}_p$-vector space.
Let $S = \bigcup_{i=1}^n \operatorname{Supp} D_i$ and set

$$A := \max\left(\sum_{\mathfrak{P} \in S} \mathfrak{P} + \operatorname{Diff}(K_N) - 2(x)_-, \frac{(y_N)_-}{p}\right).$$

If S_N is not empty then it contains an element of $\mathcal{L}(A)$.

Proof. Let $f \in S_N$ and let $\mathfrak{Re}(f)$ be defined similarly as in Theorem 3.4.4. Since $D_1, \ldots, D_n$ is a basis of $\mathfrak{G}_N^p$ there exists a linear combination $D' = a_1 D_1 + \ldots + a_n D_n$ such that $\mathfrak{Re}(f) \equiv D'$ mod $p\operatorname{Div}(K_N)$. Thus there exists $D_p \in \operatorname{Div}(K_N)$ such that

$$\mathfrak{Re}(f) \sim D' + pD_p.$$

But $\operatorname{Supp}(D') \subset \bigcup_{i=1}^n \operatorname{Supp}(D_i) = S$.
According to Theorem 3.4.4, S_N contains an element f^* verifying for all places outside of $\operatorname{Supp}(D')$ (in particular for all places outside of S) that $\nu_{\mathfrak{P}}(f^*) \geqslant \min(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}), p^{-1}\nu_{\mathfrak{P}}(y_N))$.
The result follows from Proposition 3.4.2 and Proposition B.4.17. □

DEFINITION 3.4.7. — For any effective divisor D (see Definition B.3.2) over K_N, we define

$$A(D) := \max\left(\sum_{\mathfrak{P} \in \operatorname{Supp} D} \mathfrak{P} + \operatorname{Diff}(K_N) - 2(x)_-, \frac{(y_N)_-}{p}\right).$$

We say that D is a generating divisor of $\mathfrak{G}_N^p$ if $(\mathfrak{P})_{\mathfrak{P}\in\operatorname{Supp} D}$ is a generating family of $\mathfrak{G}_N^p$. In this case

$$S_N = \varnothing \Leftrightarrow S_N \cap \mathcal{L}(A(D)) = \varnothing.$$

For a family of effective divisors $(D_1, \dots, D_n)$ we define

$$A(D_1, \dots, D_n) = A(D_1 + \dots + D_n).$$

Notation 3.4.8. We denote $\mathrm{Cl}^0(K_N)$ the subgroup of $\mathrm{Cl}(K_N)$ generated by the divisors of degree 0 and $\mathfrak{G}_N^{p,0} = {}^{\mathrm{Cl}^0(K_N)}\!/_{p\mathrm{Cl}^0(K_N)}$.

According to Proposition B.3.10, $\mathfrak{G}_N^p \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times \mathfrak{G}_N^{p,0}$. Furthermore if $D_1, \dots, D_N$ is a generating family of $\mathfrak{G}_N^{p,0}$ then $(\mathfrak{P})_{\mathfrak{P}\in\bigcup_{i\in[\![1;n]\!]}\operatorname{Supp} D_i}$ is a generating family of $\mathfrak{G}_N^p$ if at least one place of $\bigcup_{i=1}^n \operatorname{Supp} D_i$ is of degree coprime with p. This is very likely to happen and since this latter family of divisor is really the one we work with, in most cases we only need to care about $\mathfrak{G}_N^{p,0}$.

As we mentioned earlier, from now on we will limit our complexity analysis to the case $K = \mathbb{F}_q(x)$ with $q = p^b$. With no loss of generality, we can suppose that $N \in \mathbb{F}_q[x^p, Y]$. As we did in Algorithm 6, the input we take is not N itself, but an irreducible polynomial $N_* \in \mathbb{F}_q[x, Y]$ such that $N_*^p(Y) = N(Y^p)$. Let a be a root of N_* in K_N. We have $K_N = K[a]$.

REMARK 3.4.9. — Such a N_* is always uniquely defined. In order to simplify the notations, we extend the notations depending on N to N_*. That is to say:

- $C_{N_*} := C_N$.
- $K_{N_*} := K_N$.
- $\varphi_{N_*} := \varphi_N$.
- $S_{N_*} := S_N$.
- $\mathfrak{G}_{N_*}^p := \mathfrak{G}_N^p$.
- $\mathfrak{G}_{N_*}^{p,0} := \mathfrak{G}_N^{p,0}$.

Similarly we refer to the p-Riccati equation relative to N_* to mean the p-Riccati equation relative to N.
This convention poses a small conflict of notation when $N_* \in C[Y]$. However in this case, this means that y_N is a p-th power of an element in C_N which is a trivial solution to the p-Riccati equation relative to N. Thus we can suppose that N_* is not a polynomial with coefficients in C.

We write $d_x := \deg_x N_*$ and $d_y := \deg_Y N_*$.
Let

$$\begin{array}{rccc} \tau : & K_N & \to & K_N \\ & f & \mapsto & f^{(p-1)} + f^p \end{array}.$$

For any $P \in \mathbb{F}_q(x)$, and any integers $r, m \in \mathbb{N}$ we denote

$$\frac{\mathbb{F}_q[x,a]_{\leqslant r,<m}}{P} := \{P^{-1} \cdot f(x,a) | f \in \mathbb{F}_q[x,Y],\ \deg_x(f) \leqslant r \text{ and } \deg_Y(f) < m\}.$$

For a finite family of functions $\mathcal{B} \subset K_N$ there exists $P \in \mathbb{F}_q[x]$ and an integer $r \in \mathbb{N}$ such that

$$\tau(\mathcal{B}) \subset \frac{\mathbb{F}_q[x,a]_{\leqslant r,<d_y}}{P}.$$

Notation 3.4.10. Let $\mathcal{B} \subset K_N$ be a finite family of functions in K_N and $(\nu_1,\dots,\nu_b)$ an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. If $r \in \mathbb{N}$ and $P \in \mathbb{F}_q[x]$ are such that

$$\tau(\mathcal{B}) \subset \frac{\mathbb{F}_q[x,a]_{\leqslant r,<d_y}}{P}$$

then we denote by $\mathcal{T}_{P,r}(\mathcal{B})$ the matrix whose columns are the images of the elements of $\mathcal{B}$ by τ written in the basis

$$\left(\frac{\nu_k x^i a^j}{P}\right)_{\substack{k\in[\![1,n]\!]\\ i\in[\![0,r]\!]\\ j\in[\![0,d_y[\![}}.$$

Input: $N_* \in K[Y]$ an irreducible separable polynomial.
Output: $f_S \in S_{N_*}$ a solution (if it exists) of the p-Riccati equation relative to N_*.

1. Set $d_y := \deg_Y N_*$ and $K_{N_*} := K[a] = {}^{K[Y]}/_{N_*}$.
2. Compute $(a)_-$ and $(x)_-$.
3. Compute $D_1,\dots,D_n$ a lift of a basis of $\mathfrak{G}^p_{N_*}$ as defined in Corollary 3.4.6
4. Set $A := \mathrm{Diff}(K_N) - 2(x)_-$.
5. **For** $\mathfrak{P} \in \bigcup_{i=1}^n \mathrm{Supp}(D_i)$ **do**:
   - $A \leftarrow A + \mathfrak{P}$.
6. $A \leftarrow \max((a)_-, A)$.
7. Compute $\mathcal{B}$ a basis of $\mathcal{L}(A)$
8. Compute $\mathcal{T}_{P,r}(\mathcal{B})$ (see Notation 3.4.10) and $v = P \cdot a^p$.
9. **If** $v \in \mathbb{F}_q[x,a]_{\leqslant r,<d_y}$ **do**:
   - Set V the vector whose coordinates are those of v in the basis $(\nu_k x^i a^j)$.
10. **Else**:
    - The p-Riccati equation relative to N_* has no solution.
11. Solve $\mathcal{T}_{P,r}(\mathcal{B})X = V$.
12. If a solution exists, reconstruct it from X and return it.

Algorithm 8: p-Riccati: a first attempt

We present a first version of our algorithm in Algorithm 8. Written as such, this algorithm is "semi-recursive" in the sense that while we do not precise how the choices of the divisors D_i or

the choice of the returned solution is made, it is sure to find a solution to the p-Riccati solution relative to N if such a solution exists. As such, it also serves as an irreducibility test for $N(\partial^p)$. However it necessitates to compute a family of divisor whose classes constitute a basis of $\mathfrak{G}^p_{N_*}$. To our knowledge, there is no easier way of doing this than by computing the whole divisor class group of K_{N_*}. While operations in the divisor class group can be computed in polynomial time in the genus of K_N [KM07], it appears that computing lattices of relations of divisors in $\mathrm{Cl}^0(K_{N_*})$ can only be done in exponential time[1].
This is why we prefer to use a probabilistic approach for our algorithm and pick divisors randomly, hoping to pick a generating family of $\mathfrak{G}^{p,0}_N$ without actually verifying if it is indeed one. Since such a technique cannot on its own confirm or rebut the existence of a solution to the p-Riccati equation, we test the irreducibility of $N(\partial^p)$ beforehand using Algorithm 6 presented in Section 3.3.3. This approach will be treated in Subsection 3.4.2.

REMARK 3.4.11. — An algorithm testing the irreducibility and computing a solution to the p-Riccati equation at the same time in polynomial time in the genus of K_N and the characteristic p could still be found if one was able to test whether a randomly chosen family of divisors generates $\mathfrak{G}^p_N$ or not in polynomial time in the aforementioned datas.

Another option would be to compute the $\mathbb{F}_p$-dimension of $\mathfrak{G}^{p,0}_N$ beforehand to know approximately how many divisors to pick. We say a few words of how this could be done though this is not the option we chose. Recall that $\mathrm{Cl}^0(K_N)$ is a finite commutative group. As such it can be written as a product

$$\mathrm{Cl}^0(K_N) \simeq \prod_{i=1}^{\eta} \mathbb{Z}/p^{\nu_i}\mathbb{Z} \times G.$$

where G is a finite commutative group of order coprime with p, and $\nu_i \in \mathbb{N}^*$. Since the multiplication by p in G is surjective, $\mathfrak{G}^{p,0}_N$ is isomorphic to the product of the cokernels of the multiplication by p in the $\mathbb{Z}/p^{\nu_i}\mathbb{Z}$ which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.
Thus

$$\mathfrak{G}^{p,0}_N \simeq \mathbb{F}_p^{\eta}.$$

Similarly, G contains no p-torsion element so the p-torsion subgroup $\mathrm{Cl}^0(K_N)_{T_p}$ of $\mathrm{Cl}^0(K_N)$ is isomorphic to the product of the p-torsion subgroups of the $\mathbb{Z}/p^{\nu_i}\mathbb{Z}$. Again those are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. This proves that

$$\mathrm{Cl}^0(K_N)_{T_p} \simeq \mathbb{F}_p^{\eta}$$

and the following result:

LEMMA 3.4.12. — *There exists an isomorphism of $\mathbb{F}_p$-vector spaces*

$$\mathfrak{G}^{p,0}_N \simeq \mathrm{Cl}^0(K_N)_{T_p}.$$

REMARK 3.4.13. — This isomorphism is not canonical in general and depends on the choice of basis of $\mathfrak{G}^{p,0}_N$ and $\mathrm{Cl}^0(K_N)_{T_p}$.

To our knowledge, this isomorphism cannot be used to compute a basis of $\mathfrak{G}^{p,0}_N$. However, it can be used to compute its dimension by cohomological means as illustrated in [Ser03, Proposition 10]. It also shows as a direct consequence in the same paper that $\mathrm{Cl}^0(K_N)_{T_p}$ cannot be

[1] Based on a draft from F . Hess Computing relations in divisor class groups of algebraic curves over finite fields

of a dimension higher than the genus g of K_N which, as a consequence is also the case for $\mathfrak{G}_N^{p,0}$. Computing the dimension of $\mathrm{Cl}^0(K_N)_{T_p}$ is doable in time polynomial in d_x and d_y and linear in p.

Thus we could conceive an algorithm taking in input N_* and a probability ρ which would compute the dimension of $\mathfrak{G}_N^{p,0}$ and select enough randomly chosen divisors that the probability of N not being irreducible if a solution is not found is smaller than ρ.

3.4.2 A polynomial time algorithm in degrees and characteristic.

We now develop our approach which consists in testing whether or not $N(\partial^p)$ is irreducible beforehand using Algorithm 6. If it is not the case we pick enough randomly chosen divisors to have a good enough probability of generating $\mathfrak{G}_N^p$. We actually need to explicit the method used to pick randomly chosen divisors in $\mathrm{Div}(K_N)$.

We refer to [Bru13, Section 3.5] in which the author present an algorithm to select uniformly random elements in $\mathrm{Cl}^0(K_N)$. If K_N is seen as the regular function field of a curve $\mathcal{C}$, [Bru13, Algorithm 3.7] presupposes the choice of a line bundle $\mathcal{L}$ over $\mathcal{C}$ of degree at least $2g+1$. Since we are working over finite fields, line bundles of arbitrary degrees exist and we can choose a line bundle of degree exactly $2g+1$. Then we can use [Bru13, Algorithm 3.7] to pick uniformly random elements in $\mathrm{Cl}^0(K_N)$ represented by uniformly random effective divisors of degree $2g+1$ in polynomial time in g and $\log(q)$. However, [Bru13, Algorithm 3.7] also suppose that the zeta function of $\mathcal{C}$ is known in order to ensure the uniform distribution of the divisors. The computation of the zeta function can be done in time polynomial in g and linear in b and p (precisely $\tilde{O}(pbd_x^6d_y^4)$ bit operations [Tui17]). This is not really a problem for us as other parts of our algorithm work in polynomial time in p, such as the computation of reduced norms and p-curvatures, or the computation of the linear system representing the p-Riccati equation as we will see later.
However, if one wishes to avoid computing the zeta function, they could also refer to [EC11, section 13.2] in which the authors present a method to pick random elements in the Picard group with a distribution close enough to the random distribution. We suspect the problem pointed out by the authors about only being able to generate a big subgroup of $\mathrm{Cl}^0(K_N)$ arises because, unlike $\mathfrak{G}_N^{p,0}$, $\mathrm{Cl}^0(K_N)$ is only a $\mathbb{Z}$-module and not a vector space. While we would have to pick ($O(d_y)$ times) more divisors, using this algorithm ensures that picking enough divisors can be done polynomial time in g and $\log(q)$.

Remark 3.4.14. — In [EC11, section 13.2] the authors also state that $\mathrm{Cl}^0(K_N)$ is generated by the places of degree less than $1+2\log_q(4g-2)$. This in turns guarantees the existence of a generating divisor D of $\mathfrak{G}_{N_*}^p$ of degree $\tilde{O}(d_xd_y)$. However the probability of generating $\mathfrak{G}_N^p$ with $O(g)$ uniformly chosen effective divisors of degree less than $1+\log_q(4g-2)$ could be very low which is why we do not use it for our algorithm.

From now on we will assume that we are able to pick uniformly random elements in $\mathrm{Cl}^0(K_N)$. We recall the following classical result:

Lemma 3.4.15. — *Let $(\nu_1,\dots,\nu_d)$ be a family of d vectors in $\mathbb{F}_p^r$ with $r\in\mathbb{N}$ and $d\geqslant r$. The probability that $(\nu_1,\dots,\nu_d)$ is not a generating family of $\mathbb{F}_p^r$ is smaller than $p^{-d\frac{p^r-1}{p-1}}$.*

Proof. Let us consider the event E: $(\nu_1, \dots, \nu_d)$ is not a generating family of $\mathbb{F}_p^r$. Then there exists an hyperplane H of $\mathbb{F}_p^r$ such that $(\nu_1, \dots, \nu_d)$ are all vectors of H. For a given hyperplane H, the probability that $(\nu_1, \dots, \nu_d)$ randomly chosen in $\mathbb{F}_p^r$ would all be elements of H is $\frac{p^{d(r-1)}}{p^{rd}} = p^{-d}$. Thus

$$\mathbb{P}(E) \leqslant \sum_{H \text{ hyperplane}} p^{-d}.$$

The set of hyperplanes of $\mathbb{F}_p^r$ is in bijection with $\mathbb{P}^{r-1}(\mathbb{F}_p)$ of cardinality $\frac{p^r-1}{p-1}$. Thus we find

$$\mathbb{P}(E) \leqslant \frac{1}{p^d}\frac{p^r-1}{p-1}.$$

□

Since we know that $\dim_{\mathbb{F}_p} \mathfrak{G}_N^{p,0} \leqslant g$, it follows that in all generality, by picking $g+1$ uniformly random elements in $\mathrm{Cl}^0(K_N)$, the probability of generating $\mathfrak{G}_N^p$ is greater than $1 - \frac{1}{p(p-1)} \geqslant \frac{1}{2}$, ensuring that we only have to pick random divisors $O(1)$ times.

PROPOSITION 3.4.16. — *Let $(V_N)_{n\in\mathbb{N}} \in (\mathbb{F}_p^r)^{\mathbb{N}}$ be a sequence of uniformly random vectors and $T = \min\{n \in \mathbb{N} | \mathbb{F}_p^r = \mathrm{Vect}(V_1, \dots, V_n)\}$. Then*

$$\mathbb{E}(T) \leqslant r\left(1 + O\left(\frac{1}{p^2}\right)\right) + O\left(\frac{1}{p^3}\right)$$

Proof. We have

$$\begin{aligned}
\mathbb{E}(T) &= \sum_{d=r}^{\infty} d\mathbb{P}(T = d) \\
&= \sum_{d=r}^{\infty} d\mathbb{P}(\dim \mathrm{Vect}(V_1, \dots, V_{d-1}) = r-1 \wedge V_d \notin \mathrm{Vect}(V_1, \dots, V_{d-1})) \\
&= \sum_{d=r}^{\infty} d\mathbb{P}(\dim \mathrm{Vect}(V_1, \dots, V_{d-1}) = r-1)\mathbb{P}(V_d \notin \mathrm{Vect}(V_1, \dots, V_{d-1}) | \dim \mathrm{Vect}(V_1, \dots, V_{d-1}) = r-1) \\
&= \sum_{d=r}^{\infty} d\mathbb{P}(\dim \mathrm{Vect}(V_1, \dots, V_{d-1}) = r-1)\frac{p-1}{p} \\
&\leqslant \frac{p-1}{p}\left(r\prod_{k=0}^{r-2}\frac{p^r-p^k}{p^r} + \sum_{d=r+1}^{\infty} d\mathbb{P}(\mathbb{F}_p^r \neq \mathrm{Vect}(V_1, \dots, V_{d-1}))\right) \\
&\leqslant r\prod_{k=1}^{r}\frac{p^k-1}{p^k} + \frac{p-1}{p}\sum_{d=r+1}^{\infty}\frac{d}{p^d}\frac{p^r-1}{p-1} \\
&= r\prod_{k=1}^{r}\frac{p^k-1}{p^k} + \frac{p^r-1}{p^2}\sum_{d=r+1}^{\infty}\frac{d}{p^{d-1}} \\
&= r\prod_{k=1}^{r}\frac{p^k-1}{p^k} + \frac{p^r-1}{p^2}\left(\frac{(r+1)p^{-r}}{1-p^{-1}} + \frac{p^{-r-1}}{(1-p^{-1})^2}\right) \\
&\leqslant r + \frac{r+1}{p(p-1)} + \frac{1}{p(p-1)^2}.
\end{aligned}$$

The result follows. □

This result states that if $\mathfrak{G}_N^{p,0}$ is of dimension r over $\mathbb{F}_p$ then, provided that we are able to choose uniformly random elements in $\mathfrak{G}_N^{p,0}$, we would only need on average to select $O(r)$ elements to generate $\mathfrak{G}_N^{p,0}$.

We now discuss in more details the computation of $\mathcal{T}_{P,r}(\mathcal{B})$ (and in more generality of the linear system representing the p-Riccati equation over some $\mathcal{L}(A(D))$), where $\mathcal{B}$ is a basis of $\mathcal{L}(A(D))$ for some effective divisor D. We recall that $\mathcal{T}_{P,r}(\mathcal{B})$ is defined in Notation 3.4.8 and is the matrix of the application $\tau : f \mapsto f^{(p-1)} + f^p$ over $\mathcal{L}(A(D))$. A naive algorithm is to compute $f^{(p-1)} + f^p$ in the form $\frac{1}{Q_f}\sum_{i=0}^{d_y-1} f_i a^i$ where $Q_f, f_0, \dots, f_{d_y-1}$ is a family of globally coprime polynomials in $\mathbb{F}_q[x]$. Then we compute a common denominator $Q_{\mathcal{B}} = \operatorname{lclm}_{f\in\mathcal{B}} P_f$ and compute $Q_{\mathcal{B}}(f^{(p-1)} + f^p)$ for every $f \in \mathcal{B}$, which can be represented by a bivariate polynomial $P_f(x, y) \in \mathbb{F}_q[x, y]$ for every $f \in \mathcal{B}$. We can then set $r = \max_{f\in\mathcal{B}} \deg_x P_f$.

Let us assume for now that elements of $\mathcal{B}$ can be represented by $d+1$ polynomials in $\mathbb{F}_q[x]$ (one denominator and d coefficients of powers of a) of degree $O(1)$. Lemma 3.3.30 states that $f^{(p-1)} + f^p$ has coefficients of degree $O(pd_xd_y)$. Thus $\mathcal{T}_{P,r}(\mathcal{B})$ is a matrix of size linear in p. A first simplification of the algorithm follows from the observation that for any $f \in K_N$, $f^{(p-1)} + f^p \in C_N$ which is to say that it belongs in the image the Frobenius endomorphism of K_N.

Notation 3.4.17. We denote

$$\begin{array}{rccc} \Phi_N : & K_N & \xrightarrow{\sim} & C_N \\ & f & \mapsto & f^p \end{array}$$

Thus instead of computing $f^{(p-1)} + f^p$ for every $f \in \mathcal{B}$, we can compute $\Phi_N^{-1}(f^{(p-1)} + f^p)$ and instead look for a solution of the equation

$$\Phi_N^{-1}(f^{(p-1)} + f^p) = a.$$

PROPOSITION 3.4.18. — *Let $D \in \operatorname{Div}(K_N)$ and let $f \in \mathcal{L}(A(D))$ (see Definition 3.4.7). Then $\Phi_N^{-1}(f^{(p-1)} + f^p) \in \mathcal{L}(A(D))$.*

Proof. Let $\mathfrak{P} \in \mathbb{P}_{K_N}$. If $\mathfrak{P} \notin \operatorname{Supp}(A(D))$ then by definition of $A(D)$, f is not a ramified place and f has no poles in $\mathfrak{P}$. Thus neither $f^{(p-1)}$ nor f^p has a pole in $\mathfrak{P}$. Thus $\Phi_N^{-1}(f^{(p-1)} + f^p)$ has no pole in $\mathfrak{P}$.

For $\mathfrak{P} \in \operatorname{Supp}(A(D))$, we let $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$. We know that

$$\nu_{\mathfrak{P}}(\Phi_N^{-1}(f^{(p-1)} + f^p)) \geqslant \min(p^{-1} \cdot (\nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)), \nu_{\mathfrak{P}}(f))$$

Besides we know that if $\nu_{\mathfrak{P}}(f) \leqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$ then $p^{-1} \cdot (\nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)) \geqslant \nu_{\mathfrak{P}}(f)$ so in that case we get that

$$\nu_{\mathfrak{P}}(\Phi_N^{-1}(f^{(p-1)} + f^p)) \geqslant \nu_{\mathfrak{P}}(f)$$

which implies the desired result since $f \in \mathcal{L}(A(D))$.
If now we have $\nu_{\mathfrak{P}}(f) > \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$ then $p^{-1} \cdot (\nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)) > \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$. Since valuations have to be integers we deduce that

$$\nu_{\mathfrak{P}}(\Phi_N^{-1}(f^{(p-1)} + f^p)) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) \geqslant -\nu_{\mathfrak{P}}(A(D)).$$

Thus $\Phi_N^{-1}(f^{(p-1)} + f^p) \in \mathcal{L}(A(D))$. □

Proposition 3.4.18 ensures that for a function f in $\mathcal{L}(A(D))$, $\Phi_N^{-1}(f^{(p-1)}+f^p)$ and f have a common bound on the size of their coefficients which should allow to drop the factor p in the size of $\mathcal{T}_{p,r}(\mathcal{B})$. However, naively computing $\Phi_N^{-1}(f^{(p-1)}+f^p)$ still requires to derive a function $p-1$ times. According to Lemma 3.3.30, if a function f has coefficients of size $O(1)$, the coefficients of $f^{(i)}$ are of size $O(id_xd_y)$. It follows that computing the $p-1$ derivative of f will take at least $O(p^2d_xd_y^2)$ operations in $\mathbb{F}_q$. Our goal is to reduce to the complexity of our algorithm with regard to p.

DEFINITION 3.4.19. — Let $f \in K_N$. There exist unique $f_0, \dots, f_{p-1} \in K_N$ such that

$$f = \sum_{i=0}^{p-1} f_i^p x^i.$$

For all $i \in [\![0; p-1]\!]$ We denote by $S_i(f) := f_i$ the i-th section of f.

Although we define sections for all $i \in [\![0; p-1]\!]$, we will really only be interested in S_{p-1} as shown in the following lemma:

LEMMA 3.4.20. — *For any $f \in K_N$,*

$$\Phi_N^{-1}(f^{(p-1)}) = -S_{p-1}(f).$$

Proof. Let $f := \sum_{i=0}^{p-1} f_i^p x^i$. It suffices to show that $f^{(p-1)} = -f_{p-1}^p$. But this is obvious since $f^{(p-1)} = (p-1)!f_{p-1}^p$ and $(p-1)! = -1 \mod p$. □

Thus another way of writing p-Riccati equation is

$$b - S_{p-1}(b) = a.$$

We now use the fact that Lemma 3.4.20 also holds over $K_{N,\mathfrak{P}}$ for any $\mathfrak{P} \in \mathbb{P}_{K_N}$. Let $\mathfrak{P}$ be a place over K_N that does not belong in $\mathrm{Supp}(A(D))$. Then the injective homomorphism from K_N to its $\mathfrak{P}$-completion induces an injective homomorphism of $\mathbb{F}_q$-vector spaces

$$\mathcal{L}(A(D)) \hookrightarrow \mathcal{G}_{\mathfrak{P}}[[t_{\mathfrak{P}}]].$$

It follows that there exists a constant $N \in \mathbb{N}$ such that for all $f \in \mathcal{L}(A(D))$, $f = 0$ if and only if $\nu_{\mathfrak{P}}(f) \geqslant N$.

LEMMA 3.4.21. — *Let $\mathfrak{P} \in \mathrm{Div}(K_N) \setminus \mathrm{Supp}(A(D))$ and let $d := \deg(A(D))$. For any $f \in \mathcal{L}(A(D))$,*

$$f = 0 \Leftrightarrow \nu_{\mathfrak{P}}(f) > \frac{d}{\deg(\mathfrak{P})}.$$

Proof. Since $f \in \mathcal{L}(A(D))$, if $f \neq 0$ then we know that $\deg(f)_- \leqslant d$. But since $\deg(f)_- = \deg(f)_+$ we know that $\deg(f)_+ \leqslant d$. But since $\mathfrak{P} \notin \mathrm{Supp}(A(D))$ we know that f has no pole in $\mathfrak{P}$ and $\deg(f)_+ \geqslant \nu_{\mathfrak{P}}(f)\deg(\mathfrak{P})$ which yields the result. □

Thus it suffices for a function $f \in \mathcal{B}$ (where $\mathcal{B}$ is a basis of $\mathcal{L}(A(D))$) to compute the image of $f - S_{p-1}(f)$ modulo $t_{\mathfrak{P}}^{\left\lfloor \frac{\deg(A(D))}{\deg \mathfrak{P}} \right\rfloor + 1}$ in $\mathcal{G}_{\mathfrak{P}}[[t_{\mathfrak{P}}]]$. If one writes $f = \sum_{k=0}^{\infty} f_i t_{\mathfrak{P}}^i$ then $S_{p-1}(f) \mod t_{\mathfrak{P}}^{\left\lfloor \frac{\deg(A(D))}{\deg \mathfrak{P}} \right\rfloor + 1}$ can be deduced from knowing the coefficients f_{pk+p-1} for $k \leqslant \frac{\deg(A(D))}{\deg \mathfrak{P}}$.

To that end we can compute the full Taylor expansion of f up to its $p\left\lfloor\frac{\deg(A(D))}{\deg\mathfrak{P}}\right\rfloor+p-1$ coefficient. To that end we first compute the Taylor expansion of a in $t_{\mathfrak{P}}$ up to the desired precision (by definition of $A(D)$, $a\in\mathcal{L}(A(D))$) with a Newton iteration in $\tilde{O}(p\deg(A(D))d_y)$ operations in $\mathbb{F}_q$ (we can suppose that $d_x=O(\deg(A(D)))$ as we will show later. Then, knowing that elements of $\mathcal{L}(A)$ are given by polynomials $F(x,a)$ we get their Taylor expansions by composition for an additional cost of $\tilde{O}(p\deg(A)d_y)$ operations in $\mathbb{F}_q$.

Note that this method requires that the coefficients of elements of $\mathcal{B}$ must have no pole in $\mathfrak{P}$ (otherwise we would have to compute the Taylor expansion of a up to a higher precision). For that purpose, just choosing $\mathfrak{P}\notin\mathrm{Supp}(A(D))$ is insufficient. Let us discuss the poles of the coefficients of the elements of $\mathcal{B}$.

PROPOSITION 3.4.22. — *Let $K_{N_*}=\mathbb{F}_q(x)[a]$ where $N_*\in\mathbb{F}_q(x)[Y]$ is an irreducible polynomial and a is a root of N_*. We denote $d_y:=\deg_Y N_*$.*
Let Q_i be the quotient of the Euclidean division of $N_*(x,Y)$ by Y^{i+1} for any $i\in\mathbb{N}$. Then for any $f:=\sum_{k=0}^{d_y-1}f_ka^k\in K_{N_*}$ and any $i\in[\![0;d_y-1]\!]$,

$$f_i=Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{Q_i(x,a)f}{\partial_Y N_*(x,a)}\right).$$

Proof. Let us fix $N_*(x,Y)=\sum_{k=0}^{d_y}\eta_k(x)Y^k$. From [Ser04, Lemma 2 section III. 6] we know that $\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{a^i}{\partial_Y N_*(x,a)}\right)=\frac{1}{\eta_{d_y}}\delta_{i,d_y-1}$, for all $i\leqslant d_y-1$. Thus the result holds for $i=d_y-1$, since $Q_{d_y-1}=\eta_{d_y}$. Then for all i we have $Q_i=Q_{i+1}Y+\eta_{i+1}$. We assume the Proposition to be true for $i+1$. Then

$$Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{Q_i(x,a)f}{\partial_Y N_*(x,a)}\right)=Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{Q_{i+1}(x,a)af}{\partial_Y N_*(x,a)}\right)+\eta_{i+1}Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{f}{\partial_Y N_*(x,a)}\right)$$

and by hypothesis $Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{Q_{i+1}(x,a)af}{\partial_Y N_*(x,a)}\right)$ is the coefficient of a^{i+1} in af, which is given by $f_i-\frac{f_{d_y-1}\eta_{i+1}}{\eta_{d_y}}$, while $Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{f}{\partial_Y N_*(x,a)}\right)$ is the coefficient of a^{d_y-1} of $\frac{f}{\eta_{d_y}}$.

$$Tr_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{Q_i(x,a)f}{\partial_Y N_*(x,a)}\right)=f_i-\frac{f_{d_y-1}\eta_{i+1}}{\eta_{d_y}}+\eta_{i+1}\frac{f_{d_y-1}}{\eta_{d_y}}=f_i.$$

□

COROLLARY 3.4.23. — *Assume that $N_*\in\mathbb{F}_q[x,Y]$. Let $D\in\mathrm{Div}(K_{N_*})$ and P be an irreducible polynomial in $\mathbb{F}_q[x]$ coprime with $\mathrm{Disc}(N_*)$ and the leading coefficient of N_*. If $\mathrm{Supp}(A(D))$ does not contain any place above P then for $f\in\mathcal{L}(A(D))$, none of the coefficients of f in the basis $(1,a,\dots,a^{d_y-1})$ have a pole in P.*

Proof. Let l_c be the leading coefficient of N_*. The function l_ca is integral and its minimal polynomial is $N_*'=l_c^{d_y-1}N_*(x,Y/l_c)$. Hence $\partial_Y N_*'=l_c^{d_y-2}\partial_Y N_*(x,Y/l_c)$. If x_1 is such that $N_*'(x_1,Y)$ and $\partial_Y N_*'(x_1,Y)$ have a common root then x_1 is either such that $N_*(x_1,Y)$ and $\partial_Y N_*(x_1,Y)$ have a common root, or it is a root of l_c. In the latter case, $N_*'(x_1,Y)=Y^{d_y}$ and $\partial_Y N_*'(x_1,Y)=d_yY^{d_y-1}$, therefore $N_*'(x_1,Y)$ and $\partial_Y N_*'(x_1,Y)$ have a unique common root of multiplicity d_y-1. Thus $\mathrm{Disc}(N_*')=l_c^{d_y-1}\mathrm{Disc}(N_*)$.

We have

$$(\partial_Y N_*(x,a))_+ \leqslant (\partial_Y N'_*(x,l_c a))_+ \leqslant (d_y-1)(l_c)_+ + (\mathrm{Disc}(N_*))_+.$$

Let $\mathrm{Diff}(K_{N_*})_0$ be the different divisor of K_{N_*} outside of the places at infinity. Since $l_c a$ is integral we know from Corollary B.4.16 that

$$\mathrm{Diff}(K_{N_*})_0 \leqslant (\partial_Y N'_*(x,l_c a))_+.$$

Let $\mathcal{O}_P$ be the valuation ring associated to P in $\mathbb{F}_q(x)$ and $\mathcal{O}'_P$ its integral closure in K_{N_*}. Let Q_i be the quotient of the Euclidean division of N_* by Y^{i+1}.
By construction, P is such that if for some i, $\mathfrak{P}$ was a pole of $\frac{Q_i(x,a)f}{\partial_Y N_*(x,a)}$ for some $f \in \mathcal{L}(A(D))$ then $\mathfrak{P} \nmid P$. Indeed

$$\begin{aligned}\mathfrak{P} &\in \mathrm{Supp}(Q_i(x,a))_- \cup \mathrm{Supp}(f)_- \cup \mathrm{Supp}(\partial_Y N_*(x,a))_+ \\ &\subset (\mathrm{Supp}(x)_- \cup \mathrm{Supp}(a)_-) \cup \mathrm{Supp}(A(D)) \cup \mathrm{Supp}(\mathrm{Disc}(N_*)_+).\end{aligned}$$

We have $\mathrm{Supp}(a)_- \subset \mathrm{Supp}(A(D))$ and P is not the infinity place thus, by construction, $\mathfrak{P} \nmid P$ and neither does its conjugates. This means that

$$\frac{Q_i(x,a)f}{\partial_Y N_*(x,a)} \in \mathcal{O}'_P.$$

By virtue of [Sti08, Corollary 3.3.2] this means that

$$\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}\left(\frac{Q_i(x,a)f}{\partial_Y N_*(x,a)}\right) \in \mathcal{O}_P.$$

After Corollary 3.4.22, we conclude that for all i, the coefficient of a^i in f has no pole in P. □

Notation 3.4.24. Let $\mathcal{B}$ be a basis of $\mathcal{L}(A(D))$ with $D \in \mathrm{Div}(K_N)$, and $P \in \mathbb{F}_q[x]$ an irreducible polynomial verifying the hypothesis of Corollary 3.4.23. Let $\mathfrak{P} \in \mathbb{P}(K_N)$ be lying over P, $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$ and B_0 be an $\mathbb{F}_p$-basis of $\mathcal{G}_{\mathfrak{P}}$.

We denote by $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})$ the matrix with coefficient in $\mathbb{F}_p$ whose columns are the Taylor expansion of the images of the elements of $\mathcal{B}$ by the map $f \mapsto f - S_{p-1}(f)$, at precision $\left\lfloor \frac{\deg A(D)}{\deg \mathfrak{P}} \right\rfloor + 1$ written in the basis $\mathcal{B}_0 \times (t^i_{\mathfrak{P}})_{i \deg(\mathfrak{P}) \leqslant \deg(A(D))}$.

When knowing the Taylor expansion of a up to the desired precision, computing the Taylor expansion of an element f of $\mathcal{L}(A(D))$ by composition requires to compute the Taylor expansion of its coefficients. This can be done in $\tilde{O}(p \max(\eta, \deg A(D)) d_y)$ operations in $\mathbb{F}_q$ where η is the degree of the coefficients of f. As we show now, by construction of $A(D)$, η and $\deg(A(D))$ have the same order of magnitude.

PROPOSITION 3.4.25. — *Let $D \in \mathrm{Div}(K_N)$ and $f = \frac{1}{f_{-1}} \sum_{i=0}^{d_y-1} f_i a^i \in \mathcal{L}(A(D))$ where $f_{-1}, f_0, \ldots, f_{d_y-1} \in \mathbb{F}_q[x]$ are globally coprime polynomials.*
Then for any $i \in [\![-1; d_y - 1]\!]$, both $\deg(f_i)$ and $\deg(A(D))$ are in $O(\deg(D) + d_x d_y)$.

We begin by proving an intermediary result.

LEMMA 3.4.26. — *Let $f \in K_N$ and $\mathfrak{P} \in \mathbb{P}_{\mathbb{F}_q(x)}$.*

$$\nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(f)) \geqslant \min\left(0, \min_{\mathfrak{P}'|\mathfrak{P}} \left\lfloor \frac{\nu_{\mathfrak{P}'}(f)}{e(\mathfrak{P}'|\mathfrak{P})} \right\rfloor\right).$$

Proof. Let $\mathcal{O}_{\mathfrak{P}}$ be the valuation ring associated to the place $\mathfrak{P}$ and $\mathcal{O}'_{\mathfrak{P}}$ be its integral closure in K_N. For any $f \in K_N$, if $f \in \mathcal{O}'_{\mathfrak{P}}$ then $\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(f) \in \mathcal{O}_{\mathfrak{P}}$ [Sti08, Corollary 3.3.2].
It follows that if $\mathfrak{P}$ is a pole of $\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(f)$, then at least one of the places lying under $\mathfrak{P}$ is a pole of f. Let $\mathfrak{P}^*$ above $\mathfrak{P}$ be such that

$$\left\lfloor \frac{\nu_{\mathfrak{P}^*}(f)}{e(\mathfrak{P}^*|\mathfrak{P})} \right\rfloor = \min_{\mathfrak{P}'|\mathfrak{P}} \left\lfloor \frac{\nu_{\mathfrak{P}'}(f)}{e(\mathfrak{P}'|\mathfrak{P})} \right\rfloor.$$

Set $k = \left\lceil \frac{-\nu_{\mathfrak{P}^*}(f)}{e(\mathfrak{P}^*|\mathfrak{P})} \right\rceil$ and $P \in \mathbb{F}_q(x)$ a prime element of $\mathfrak{P}$. Then for any $\mathfrak{P}'$ above $\mathfrak{P}$ we have

$$\nu_{\mathfrak{P}'}(P^k f) = k e(\mathfrak{P}'|\mathfrak{P}) + \nu_{\mathfrak{P}'}(f).$$

By definition $k \geqslant -\frac{\nu_{\mathfrak{P}'}(f)}{e(\mathfrak{P}'|\mathfrak{P})}$ thus $\nu_{\mathfrak{P}'}(P^k f) \geqslant 0$.

It follows that

$$\begin{aligned} \nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(P^k f)) &= \nu_{\mathfrak{P}}(P^k \,\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(f)) \\ &= k + \nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(f)) \\ &\geqslant 0 \\ \nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_q(x)}(f)) &\geqslant -k \end{aligned}$$

which is the desired result.

□

Proof of Proposition 3.4.25. Let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial and let Q_i denote the quotient of the Euclidean division of N_* by Y^{i+1} applied to x and a. If P is a pole of $\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f)$:

$$\begin{aligned} \nu_P(\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f))\deg(P) &\geqslant \min_{\mathfrak{P}|P} \left\lfloor \frac{\nu_{\mathfrak{P}}(Q_i) + \nu_{\mathfrak{P}}(f)}{e(\mathfrak{P}|P)} \right\rfloor \deg(P) \\ &\geqslant \sum_{\mathfrak{P}|P} (\nu_{\mathfrak{P}}(Q_i) + \nu_{\mathfrak{P}}(f))\deg(\mathfrak{P}) \\ &\geqslant \sum_{\mathfrak{P}|P} (\nu_{\mathfrak{P}}(Q_i) - \nu_{\mathfrak{P}}(A(D)))\deg(\mathfrak{P}) \end{aligned}$$

It follows that

$$\deg(\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f))_- \leqslant \deg(Q_i)_- + \deg(A(D)).$$

But

$$A(D) \leqslant D + \mathrm{Diff}(K_N) - 2(x)_- + (a)_-$$

thus, according to Proposition B.4.18

$$\deg A(D) \leqslant \deg(D) + d_x + 2g - 2.$$

Since $g \leqslant (d_x - 1)(d_y - 1)$ (see [Bee09, Corollary 2.6]), it follows that $\deg(A(D)) = O(\deg(D) + d_x d_y)$ and

$$\deg(\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f))_- = O(d_x d_y + \deg(D)).$$

Thus, according to Corollary 3.4.22, $\partial_y N_*(x, a) f$ has coefficients of degree $O(d_x d_y + \deg(D))$. Since $(\partial_y N_*(x, a) f)^{-1}$ has coefficients of size $d_x d_y$, the result follows. □

Thus, knowing that $\dim \mathcal{L}(A) = O(\deg A(D))$. This justify the following result.

LEMMA 3.4.27. — *Let $D \in \mathrm{Div}(K_N)$ and let $\mathcal{B}$ be a basis of $\mathcal{L}(A(D))$. Let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial verifying the hypothesis of Corollary 3.4.23 and $\mathfrak{P}$ be a place above P. Recall that $q = p^b$. Under the assumption that neither the zeros of the leading coefficient of N, nor the places at infinity are wildly ramified, the matrix $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})$ can be computed in*

$$\tilde{O}(bpd_y(d_x d_y + \deg(D))^2 + (b(d_x d_y + \deg(D)))^2)$$

bit operations.

Proof. We know that both $\deg(\mathcal{L}(A(D))$ and the degree of the coefficients of elements of $\mathcal{L}(A(D))$ can be bounded by $O(d_x d_y + \deg(D))$.

Moreover $\dim_{\mathbb{F}_q}(\mathcal{L}(A(D)) = O(\deg A(D)) = O(d_x d_y + \deg(D))$ and the cost of computing the Taylor expansion of a to the desired precision is $\tilde{O}(pd_y(\deg(A(D))) = \tilde{O}(pd_y(d_x d_y + \deg(D)))$ operations in $\mathbb{F}_q$. The latter is also the cost of computing (by composition) the Taylor expansion of any element of $\mathcal{L}(A(D))$. We can thus compute the Taylor expansion of the $O(d_x d_y + \deg(D))$ elements of the basis of $\mathcal{L}(A(D))$ at the required precision in $\tilde{O}(pd_y(d_x d_y + \deg(D))^2)$ operations in $\mathbb{F}_q$ or $\tilde{O}(pbd_y(d_x d_y + \deg(D))^2)$ bit operations.

To get the result for an $\mathbb{F}_p$-basis of $\mathcal{L}(A(D))$ one only needs to multiply the Taylor expansion of an $\mathbb{F}_q$-basis by an $\mathbb{F}_p$-basis of $\mathbb{F}_q$ which can be done in $\tilde{O}(b^2(d_x d_y + \deg(D))^2)$ operations in $\mathbb{F}_p$ which yields the result. □

REMARK 3.4.28. — In fact we only need to know the coefficients of $pk + p - 1$-th powers of $t_{\mathfrak{P}}$ of elements of $\mathcal{L}(A(D))$ and not their full Taylor expansion. Using [BCCD19, Theorem 4.1] we should be able to compute those coefficients in time polynomial in d_x, d_y and $\deg(D)$ as well as quasi-linear in $\sqrt{p}$, provided that their result extends nicely to other denominators.

We can now write the final version of our algorithm the solve the p-Riccati equation in Algorithm 9.

THEOREM 3.4.29. — *Algorithm 9 returns if it exists a solution of the p-Riccati equation relative to N_* whose coefficients are of degree $O((d_x d_y)^2)$ at the cost of*

- *testing the irreducibility of $N_*^p(\partial)$ using Algorithm 6*
- *factoring the divisors $(a)_-$ and $(x)_-$*

Input: $N_* \in K[Y]$ an irreducible separable polynomial.
Output: $f_S \in S_{N_*}$ a solution (if it exists) of the p-Riccati equation relative to N_*.

1. Test if $N_*^p(\partial)$ is irreducible using Algorithm 6.
2. **If** $N_*^p(\partial)$ is irreducible **return**.
3. Set $d_y := \deg_Y N_*$ and $K_{N_*} := K[a] = {}^{K[Y]}/_{N_*}$.
4. Compute $(a)_-$.
5. Set $A := \mathrm{Diff}(K_{N_*}) - 2(x)_-$.
6. Select $(D_1, \ldots, D_{g+1}) \in \mathrm{Div}(K_{N_*})^{g+1}$ a family of $g+1$ randomly chosen divisors of degrees $2g+1$
7. Set $A(D_1, \ldots, D_{g+1}) := A$.
8. **For** $\mathfrak{P} \in \mathrm{Supp}\,\mathfrak{O} \cup \bigcup_{i=1}^{g+1} \mathrm{Supp}\,D_i$ **do:**
   - $A(D_1, \ldots, D_{g+1}) \leftarrow A(D_1, \ldots, D_{g+1}) + \mathfrak{P}$
9. $A(D_1, \ldots, D_{g+1}) \leftarrow \max((a)_-, A(D_1, \ldots, D_{g+1}))$.
10. Compute a basis $\mathcal{B}$ of $\mathcal{L}(A(D_1, \ldots, D_{g+1}))$
11. Select $P \in \mathbb{F}_q[x]$ an irreducible polynomial verifying the hypothesis of Corollary 3.4.23 and $\mathfrak{P}|P$.
12. Compute the Taylor expansion V of a in $t_{\mathfrak{P}}$ at precision $\left\lfloor \frac{\deg A(D_1,\ldots,D_{g+1})}{\deg P} \right\rfloor + 1$
13. Compute $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})$ (see Notation 3.4.24).
14. Solve $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})X = V$.
15. **If** a solution X exists reconstruct a solution to the p-Riccati equation from it and **return** it.
16. **Else** redo from step 6

Algorithm 9: p-Riccati_with_irreducibility

- *computing the different divisor of* K_{N_*}
- *selecting* $O(d_x d_y)$ *uniformely random elements of* $\mathrm{Div}(K_{N_*})$ *of degree* $2g+1$
- *computing a basis of a Riemann-Roch space of dimension* $O((d_x d_y)^2)$
- $\tilde{O}(bpd_y(d_x d_y)^4 + b^\omega (d_x d_y)^{2\omega})$ *bit operations.*

The total complexity of the computation is polynomial in $\log_p(q)$, d_x *and* d_y *and linear in* p.

Proof. The cost of steps (1) to (3) in Algorithm 9 is the cost of using Algorithm 6. The cost of step (4) is the cost of computing $(a)_-$, $(x)_-$ and $\mathrm{Diff}(K_{N_*})$. The cost of step (6) to (9) is essentially the cost of selecting uniformely random divisors of degree $2g+1$. By definition of $A(D_1, \dots, D_{g+1})$, it is of degree $O(d_x d_y + g^2)$. Since $g = O(d_x d_y)$ we find that $A(D_1, \dots, D_{g+1})$ is of degree $O((d_x d_y)^2)$.
Since we know that the solution of the p-Riccati equation constructed by Algorithm 9 is an element of $\mathcal{L}(A(D_1, \dots, D_{g+1}))$, Proposition 3.4.25 states that this solution has coefficients of degree $O((d_x d_y)^2)$.
The cost of step (10) is thus the cost of computing a basis of $\mathcal{L}(A(D_1, \dots, D_{g+1}))$ which is of dimension $O(\deg(A(D_1, \dots, D_{g+1}))$ (Theorem B.3.13) that is to say $O((d_x d_y)^2)$.
Step (11) requires the computation of $\mathrm{Disc}(N_*)$ whose cost is negligible in regard of the final result.
Applying Lemma 3.4.27 we know that step (12) and (13) can be done in $\tilde{O}(bpd_y(d_x d_y)^4 + b^2(d_x d_y)^4)$ binary operations.
Finally, step (14) is a matter of solving a $\mathbb{F}_p$-linear system of size $O(b(d_x d_y)^2) \times O(b(d_x d_y)^2)$ which can be done in $\tilde{O}(b^\omega (d_x d_y)^{2\omega})$ operations in $\mathbb{F}_p$.
Reconstructing the solution to the p-Riccati equation is a matter of summing $O(d_y(d_x d_y)^2)$ polynomial coefficients in $\mathbb{F}_q[x]$ of degree $O((d_x d_y)^2)$ which can be done in $\tilde{O}(bd_y(d_x d_y)^4)$ binary operations.

The sum of those cost yield the final result. □

REMARK 3.4.30. — While the divisor class group of K_N is generally not trivial, $\mathfrak{G}_N^{p,0}$ is usually much smaller and has a much nicer structure. Indeed, if, for example, $\mathrm{Cl}^0(K_N)$ is of the form $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$, which happens often on randomly chosen N, then $\mathfrak{G}_N^{p,0}$ is either 0 or equal to a $\mathbb{F}_p$-vector space of dimension 1. In this case, a basis of $\mathfrak{G}_N^{p,0}$ is just a divisor which is not a multiple of p in $\mathrm{Cl}^0(K_N)$. For a randomly chosen divisor, the probability that this happens is $\frac{p-1}{p}$.

As such, there is a good chance that

$$S_N = \varnothing \Leftrightarrow S_N \cap \mathcal{L}(A(0)) = \varnothing.$$

This is why in practice we prefer picking increasingly more divisors D_i and try to solve the p-Riccati equation on increasingly larger Riemann-Roch spaces. Precisely, at each step we want to double the amount of divisors selected and redo Algorithm 9 from step 7 to step 15.

When $\dim_{\mathbb{F}_p} \mathfrak{G}_{N_*}^p = O(1)$ this allows us to find a solution to the p-Riccati equation whose coefficients are of degrees $O(d_x d_y)$ and with sufficiently good assumptions on the ramifications of K_{N_*} (see Lemme 3.4.27), this can be done instead in $\tilde{O} = (bpd_y(d_x d_y)^2 + b^\omega (d_x d_y)^\omega)$.

More generally if $\dim_{\mathbb{F}_p} \mathfrak{G}^p_{N_*} = r$ then by will yield a solution whose coefficients are of degrees $O(rd_xd_y)$ in $\tilde{O}(bpd_y(rd_xd_y)^2 + b^\omega(rd_xd_y)^\omega)$ bit operations.

The overall cost of this technique could be further reduced (although only by a multiplicative or logarithmic factor and not an order of magnitude) by using iterative techniques, allowing to reuse the work of each step for the next one. Indeed, if A and D are two effective divisors of sufficiently large degrees ($2g$ and $2g+1$ respectively) then ([Mum11, Theorem 6])

$$\mathcal{L}(A+D) = \mathcal{L}(A)\mathcal{L}(D).$$

Heuristics, possible improvements

In [BCCD19], the authors improved the complexity in secondary parameters of a previously established approach to computing the N^{th} coefficient of an algebraic power series $f \in \mathbb{F}_q[[t]]$ in $\tilde{O}(\log(N))$ bit operations. The approach relied on the fact that there existed a finite dimensional $\mathbb{F}_q$-vector space containing f which, much like the spaces $\mathcal{L}(A(D))$, are stable under the sections operators. As a matter of fact, if $F := \mathbb{F}_q(x)[f]$ then the Riemann-Roch space $\mathcal{L}(\max(\mathrm{Diff}(F) - 2(x)_-, (f)_-))$ can be shown to be such a space.
The improvement brought by the paper stems for the choice by the authors of another space, of a higher dimension but conceptually simpler, which they prove to also be stable under the section operators. Let $\varphi \in \mathbb{F}_q[x,y]$ be the minimal polynomial of f, $h := \deg_x \varphi$ and $d := \deg_y \varphi$. The authors show that the spaces

$$\frac{\mathbb{F}_q[x,f]_{<r,<d}}{\partial_y\varphi(x,f)}$$

with $r \geqslant h$ are also finite dimensional vector spaces stable under the section operators.

We conjecture that a similar idea could be used to simplify the computation of solutions to the p-Riccati. We keep the same notations as the previous sections.

HEURISTIC 3.4.31. — Let $N_* \in \mathbb{F}_q[x,y]$ be a separable irreducible polynomial and let $d_x := \deg_x N_*$ and $d_y := \deg_y N_*$. Let a be a root of N_* in K_{N_*}. Remember that by definition

$$A(0) = \max(\mathrm{Diff}(K_{N_*}) - 2(x)_-, (a)_-).$$

Then

$$\mathcal{L}(A(0)) \subset \frac{\mathbb{F}_q[x,a]_{\leqslant d_x, <d_y}}{\partial_y N_*(x,a)}.$$

This conjecture was verified on all generic examples and randomly chosen N_* against which it was tested, however results like Corollary 3.4.22 are not enough to prove it. In the case where $\mathfrak{G}^{p,0}_{N_*} = \{0\}$ this conjecture would allow us to use a simpler algorithm which does not require to compute any Riemann-Roch space. Instead we can use the fact that $\frac{\mathbb{F}_q[x,a]_{\leqslant d_x,<d_y}}{\partial_y N_*(x,a)}$ is stable by the section operators [BCCD19, Lemma 3.3] which bound the precision to which computing the Taylor expansion of its elements to solve

$$b - S_{p-1}(b) = a.$$

While this approach will not lower the cost of steps 11 to 14 of Algorithm 9 by any order of magnitude, it is in practice much faster since we do not need to compute a Riemann-Roch space,

or to compute the divisors $(a)_-$, $(x)_-$ and $\mathrm{Diff}(K_{N_*})$ (which depending on the chosen algorithm may require to compute an integral basis which for small values of p is usually the bottleneck of the algorithm).

In the case where $\mathfrak{G}^p_{N_*}$ is not reduced to 0, we conjecture that a similar approach could be developed.

HEURISTIC 3.4.32. — With the same notations as in Conjecture 3.4.31, let D be a generating divisor for $\mathfrak{G}^p_{N_*}$ and let $Q(x,a) \in \mathbb{F}_q[x,a]\backslash\{0\}$ be such that for any place $\mathfrak{P}$ outside infinity,

$$\nu_{\mathfrak{P}}(Q(x,a)) \geqslant \nu_{\mathfrak{P}}(D).$$

Denote $l_x := \deg_x Q$ and $l_y := \deg_y Q$. Then

$$\mathcal{L}(A(D)) \subset \frac{\mathbb{F}_q[x,a]_{\leqslant d_x+l_x,<d_y+l_y}}{Q(x,a)\partial_y N_*(x,a)}.$$

This second conjecture has not yet been tested, nor were its applications to the computation of solutions to the p-Riccati equation, as constructing testing polynomials N_* verifying both that $N^p_*(\partial)$ is reducible in $\mathbb{F}_q(x)\langle\partial\rangle$ and that $\mathfrak{G}^{p,0}_{N_*}$ is not trivial is hard.

The proof of [BCCD19, Theorem 2.2] can be easily adapted to show that the spaces

$$\frac{\mathbb{F}_q[x,a]_{\leqslant d_x+l_x,<d_y+l_y}}{Q(x,a)\partial_y N_*(x,a)}$$

are also stable under the section operators, and we expect an analog of [BCCD19, Lemma 3.3] to be true there as well.

If that conjecture was verified, we could also replace the selection of random divisors by the choice of successive random polynomials $Q(x,a) \in \mathbb{F}_q[x,a]$. The exact parameters of these choice remain to be determined. The fact that Algorithm 9 select random divisor of degree $2g+1$ suggest that we could take $l_x = d_x$ and $l_y = d_y$. There is however no guarantee that a uniform distribution of polynomials $Q(x,a)$ corresponds to a uniform distribution in $\mathfrak{G}^{p,0}_{N_*}$.

Similarly, it could be argued that one could limit their selection to $l_x = d_x$ and $l_y = 0$, meaning polynomials $P(x) \in \mathbb{F}_q[x]$ of degree d_x. Such polynomials verify in general that $\deg(P(x))_+ = d_x d_y$, however it is unknown how efficiently the selection of random polynomials would allow a selection of a generating divisor for $\mathfrak{G}^p_{N_*}$.

3.4.3 Factorisation algorithm

Now that we have a working algorithm to solve p-Riccati equations and degree bounds for the solutions, we discuss how it fits in the broader context of differential operators factorisation. We begin by discussing how to go from a solution of the p-Riccati equation relative to N, to the corresponding irreducible divisor of $N(\partial^p)$. From Theorem 3.2.22 we know that when $N(\partial^p)$ is reducible,

$$f \mapsto \mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$$

is a bijection between the set of solutions to the p-Riccati equation relative to N, and the set of irreducible divisors of $N(\partial^p)$. While this formula is technically also an algorithm, it is not efficient and does not reflect the actual size of the irreducible factors. Indeed, φ_N^{-1} is given by a matrix $\Phi_N \in M_{pd_y}(K)$ whose coefficients are of size linear in p. Combined with the computation of a gcrd with an operator of order $d_y p$, a naive approach states that the size of the coefficients of the irreducible divisor of $N(\partial^p)$ is at least linearly dependent in p^2. However we now show they are of size independent from p.

PROPOSITION 3.4.33. — *Let $N \in C[Y]$ be a separable irreducible polynomial and $f \in K_N$ be a solution to the p-Riccati equation relative to N. Then $\operatorname{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$ is a generator of the kernel of the canonical K-linear map*

$$K\langle\partial\rangle \to {}^{K_N\langle\partial\rangle}\big/_{K_N\langle\partial\rangle(\partial - f)}.$$

Proof. By construction of φ_N, the following diagram commutes:

$$\begin{array}{ccc} K\langle\partial\rangle & \xrightarrow{\pi_{N(\partial^p)}} & \mathcal{D}_{N(\partial^p)} \\ \downarrow & \swarrow^{\varphi_N} & \downarrow{\scriptstyle \pi'_f} \\ K_N\langle\partial\rangle/_{(\partial^p - y_N)} & \xrightarrow{\pi_f} & K_N\langle\partial\rangle/_{K_N\langle\partial\rangle(\partial - f)} \end{array}$$

Thus, $\ker(\pi'_f) = \varphi_N^{-1}(\ker(\pi_f)) = \varphi_N^{-1}({}^{K_N\langle\partial\rangle(\partial-f)}/_{(\partial^p - y_N)}) = \mathcal{D}_{N(\partial^p)}\varphi_N^{-1}(\partial - f)$.
Finally $\ker(\pi'_f \circ \pi_{N(\partial^p)}) = \pi_{N(\partial^p)}^{-1}(\mathcal{D}_{N(\partial^p)}\varphi^{-1}(\partial - f)) = K\langle\partial\rangle\operatorname{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$. □

Furthermore, we now any solution $f \in K_N$ of the p-Riccati equation relative to N satisfies $\operatorname{ord}(\operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))) = d_y$ (as a consequence of Corollary 3.1.7(iii), since it is an irreducible divisor of $N(\partial^p)$). Thus the kernel of the K-linear map $K\langle\partial\rangle_{\leqslant d_y} \to {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ is a K-vector space of dimension 1 and any element of it is equal to $\operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$ up to a multiplicative element of K.

COROLLARY 3.4.34. — *Let $N \in C[Y]$ be an irreducible polynomial and $f \in K_N$ be a solution to the p-Riccati equation relative to N. Set $d_y = \deg(N)$.*
Let $a_0 = 1$ and for all $i \in [\![0; d_y - 1]\!]$, $a_{i+1} = a_i f + a_i'$. Consider the matrix $M(f)$ in $M_{d_y, d_y+1}(K)$ whose columns are the coefficients of the a_i (in some fixed K basis of K_N). Then all $v \in \ker(M(f))$ is K-collinear with the vector of K^{d_y+1} whose coordinates are the coefficients of $\operatorname{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$.

Proof. By Proposition 3.4.33 we know that $L := \operatorname{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$ is a generator of the kernel of the morphism $\pi_f : K\langle\partial\rangle \to {}^{K_N\langle\partial\rangle}/_{K_N\langle\partial\rangle(\partial - f)}$. Since we also know that it is of order d, it follows that the restriction of π_f to the K-vector space of operators of order at most d is a K-linear map with a 1-dimensional kernel containing L.
We claim that the matrix $M(f)$ is the matrix of this restriction from the basis $(1, \partial, \cdots, \partial^d)$ to the K-basis of $K_N \simeq {}^{K_N\langle\partial\rangle}/_{K_N\langle\partial\rangle(\partial - f)}$ we have fixed.
Indeed let $L' = \partial^k l_k + \partial^{k-1} l_{k-1} + \cdots + l_0$ be any differential operator in $K_N\langle\partial\rangle$. Then there exists an operator $B = \partial^{k-1} b_{k-1} + \cdots + \partial b_1 + b_0 \in K_N\langle\partial\rangle$ and $b_{-1} \in K_N$ such that

$$L' = B(\partial - f) + b_{-1}.$$

Then

$$L' = \sum_{i=0}^{k-1} \partial^{i+1} b_i - \sum_{i=0}^{k-1} \partial^i (b_i' + fbi) + b_{-1}$$
$$= \partial^k b_{k-1} + \sum_{i=0}^{k-1} \partial^i (b_{i-1} - b_i' - f b_i)$$

and we find that $l_i = b_{i-1} - b_i' - f b_i$ or equivalently $b_{i-1} = l_i + b_i' + f b_i$ and $b_{k-1} = l_k$. We apply this result to $L' = \partial^k$. It immediately follows that the corresponding b_{-1} is the k-th term of the recursive sequence defined by $a_0 = 1$, $a_{i+1} = a_i f + a_i'$.
We have shown that $a_k = \pi_f(\partial^k)$. It follows that if $v = {}^t(v_0, \ldots, v_{d_y}) \in \mathrm{Ker}(M(f))$ then $\pi_f(v_{d_y}\partial^{d_y} + \ldots + v_0) = 0$. Thus there exists $\mu \in K$ such that $\mu \cdot L = v_{d_y}\partial^{d_y} + \ldots + v_0$. □

It is now easy to see that the coefficients of $\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$ are of size independent from p as long as its also the case of the coefficients of f, which we know to be the case from Theorem 3.4.29.

LEMMA 3.4.35. — *We keep the notation of Corollary 3.4.34 with the additional hypothesis that $f \in \mathcal{L}(A(D))$ where $D \in \mathrm{Div}(K_N)$ is a generating divisor of $\mathfrak{G}_N^p$. Then for all $i \in [\![1; d_y]\!]$,*

$$a_i \in \mathcal{L}(iA(D) + (i-1)\max(\mathrm{Diff}(K_N) - 2(x)_-), 0).$$

Proof. We know that $a_1 = f \in \mathcal{L}(A(D))$ so the proposition is verified here. Now suppose established the fact that $a_i \in \mathcal{L}(iA(D) + (i-1)\max(\mathrm{Diff}(K_N) - 2(x)_-), 0)$ for a given i. Let $\mathfrak{P} \in \mathbb{P}(K_N)$. Then we know that

$$\begin{aligned}\nu_{\mathfrak{P}}(a_{i+1}) &\geqslant \min(\nu_{\mathfrak{P}}(a_i'), \nu_{\mathfrak{P}}(a_i f)) \\ &\geqslant \nu_{\mathfrak{P}}(a_i) + \min(\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') - 1, \nu_{\mathfrak{P}}(A(D))).\end{aligned}$$

Furthermore if $p | \nu_{\mathfrak{P}}(a_i)$ then we have

$$\nu_{\mathfrak{P}}(a_{i+1}) \geqslant \nu_{\mathfrak{P}}(a_i) + \min(\nu_{\mathfrak{P}}(t_{\mathfrak{P}}'), \nu_{\mathfrak{P}}(A(D)))$$

in which case we trivially have

$$\nu_{\mathfrak{P}}(a_{i+1}) \geqslant -(i+1)\nu_{\mathfrak{P}}(A(D)) - i\nu_{\mathfrak{P}}(\mathrm{Diff}(K_N) - 2(x)_-).$$

Thus let us assume that p does not divide $\nu_{\mathfrak{P}}(a_i)$. Furthermore we can assume that

$$\nu_{\mathfrak{P}}(a_i) = -i\nu_{\mathfrak{P}}(A(D)) - (i-1)\max(\nu_{\mathfrak{P}}(\mathrm{Diff}(K_N) - 2(x)_-), 0)$$

otherwise the result is trivial. If $\nu_{\mathfrak{P}}(A(D)) > -\nu_{\mathfrak{P}}(t_{\mathfrak{P}}')$ then we find that $\nu_{\mathfrak{P}}(a_{i+1}) \geqslant \nu_{\mathfrak{P}}(a_i) - \nu_{\mathfrak{P}}(A(D))$ which yields the result. Thus let us assume that $\nu_{\mathfrak{P}}(A(D)) \leqslant -\nu_{\mathfrak{P}}(t_{\mathfrak{P}}')$. By definition of $A(D)$, $\nu_{\mathfrak{P}}(A(D)) \geqslant -\nu_{\mathfrak{P}}(t_{\mathfrak{P}}')$. Thus $\nu_{\mathfrak{P}}(A(D)) = -\nu_{\mathfrak{P}}(t_{\mathfrak{P}}')$. Furthermore, by definition the divisor $(i+1)A(D) + i\max(\mathrm{Diff}(K_N) - 2(x)_-, 0)$ is effective so we can assume that $\mathfrak{P}$ is a pole of a_{i+1}. This is only possible if $\mathfrak{P}$ is a zero of $A(D)$ or is such that $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') \leqslant 0$. Since we showed that we could assume $\nu_{\mathfrak{P}}(A(D)) = -\nu_{\mathfrak{P}}(t_{\mathfrak{p}}')$, this means that $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') \leqslant 0$.
We claim that $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') < 0$. Indeed, if it was not the case then $\mathfrak{P}$ could only be a pole of a_i' if it was a pole of a_i. Since $\mathfrak{P}$ is a pole of a_{i+1}, this means that $\mathfrak{P}$ would be a zero of $A(D)$, which could not be the case since we supposed that $\nu_{\mathfrak{P}}(A(D)) = -\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') = 0$.
We have shown that $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') < 0$. Then $\nu_{\mathfrak{P}}(A(D)) \geqslant 1$ and $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}') - 1 \geqslant -\max(\nu_{\mathfrak{P}}(\mathrm{Diff}(K_N) - 2(x)_-), 0) - \nu_{\mathfrak{P}}(A(D))$. The result follows. □

Input: $N_* \in \mathbb{F}_q(x)[Y]$ an irreducible separable polynomial, f a solution of the p-Riccati equation relative to N_*.
Output: $L \in K\langle\partial\rangle$ the smallest monic multiple of $\partial - f$ with coefficients in K.

1. Set $K_{N_*} = \mathbb{F}_q(x)[a]$ with a a root of N_*.
2. Set $d_y := \deg N_*$.
3. Set $a_0 := 1$.
4. **For** i going from 1 to d_y **do**:
   - Set $a_i := a'_{i-1} + f a_{i-1}$
5. Set $M \in M_{d,d+1}(\mathbb{F}_q(x))$ the matrix whose columns are the a_i written in the $\mathbb{F}_q(x)$-basis $(1, a, \dots, a^{d_y-1})$ of K_{N_*}.
6. Solve $MX = 0$.
7. Reconstruct L from a solution and return it.

Algorithm 10: Irreducible_factors

THEOREM 3.4.36. — *Let $N_* \in \mathbb{F}_q(x)[Y]$ be a separable irreducible polynomial. Keeping the notations of the previous sections, we suppose that $\dim_{\mathbb{F}_p} \mathfrak{G}^p_{N_*} = r$. Using Remark 3.4.30 we can compute a solution f of the p-Riccati equation relative to N_* whose coefficients are of degrees $O(rd_xd_y)$. Then Algorithm 10 computes an irreducible divisor of $N^p_*(\partial)$ whose coefficients are of degree $O(rd_xd_y^3)$ in $\tilde{O}(rd_xd_y^{\omega+2})$ operations in $\mathbb{F}_q$.*

Proof. The coefficients of the irreducible divisor returned by Algorithm 10 can be expressed using the minors of the matrix M whose columns are the a_i written in the basis $(1, a, \dots, a^{d_y-1})$. Since we know that f has coefficients of degree $O(rd_xd_y)$, by immediate recurrence we get that a_i has coefficients of degree $O(rd_xd_y^2)$. Thus the minors of M are of degree $O(d_y^2rd_xd_y)$ since M is a matrix of size $d \times (d+1)$. Furthermore, the coefficients a_i can all be computed in $\tilde{O}(rd_xd_y^3)$ operations in $\mathbb{F}_q$. It finally remains to solve a linear system of size $d \times (d+1)$ with coefficients in $\mathbb{F}_q(x)$ of degree $O(rd_xd_y^2)$. This can be done in in $\tilde{O}(rd_xd_y^{\omega+2})$ operations in $\mathbb{F}_q$ [Sto03]. □

PROPOSITION 3.4.37. — *Let $N_* \in \mathbb{F}_q[x, Y]$ be a separable irreducible polynomial. We keep the notations of the previous sections and set $N \in \mathbb{F}_q[x^p, Y]$ such that $N^p_*(Y) = N(Y^p)$.*
Let f be a solution of the p-Riccati equation relative to N whose coefficients are of degree $O(rd_xd_y)$ with $r = \dim_{\mathbb{F}_p} \mathfrak{G}^p_N$ and let $N_i = \operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f + \frac{i}{x}))$ and $L_i = \operatorname{lclm}^i_{k=0} N_k / \operatorname{lclm}^{i-1}_{k=0} N_k$. Then each L_i is irreducible and

$$N(\partial^p) = L_{p-1}L_{p-2}\dots L_1L_0.$$

Furthermore L_i has coefficients of degree $O(i^2rd_xd_y^5)$.

Proof. The fact that $N(\partial^p) = L_{p-1}L_{p-2}\dots L_1L_0$ is obvious as each successive terms telescopes so it is the same as saying that $N(\partial^p) = \operatorname{lclm}^{p-1}_{i=0} N_i$ which we know to be the case from Theorem 3.2.22 applied to $L = N(\partial^p)$. Moreover the L_i are well defined operators as $\operatorname{lclm}^i_{k=0} N_k$ is in particular a multiple of all N_k for $k \leqslant i-1$, so $\operatorname{lclm}^{i-1}_{k=0} N_k$ is a right divisor of $\operatorname{lclm}^i_{k=0} N_k$.

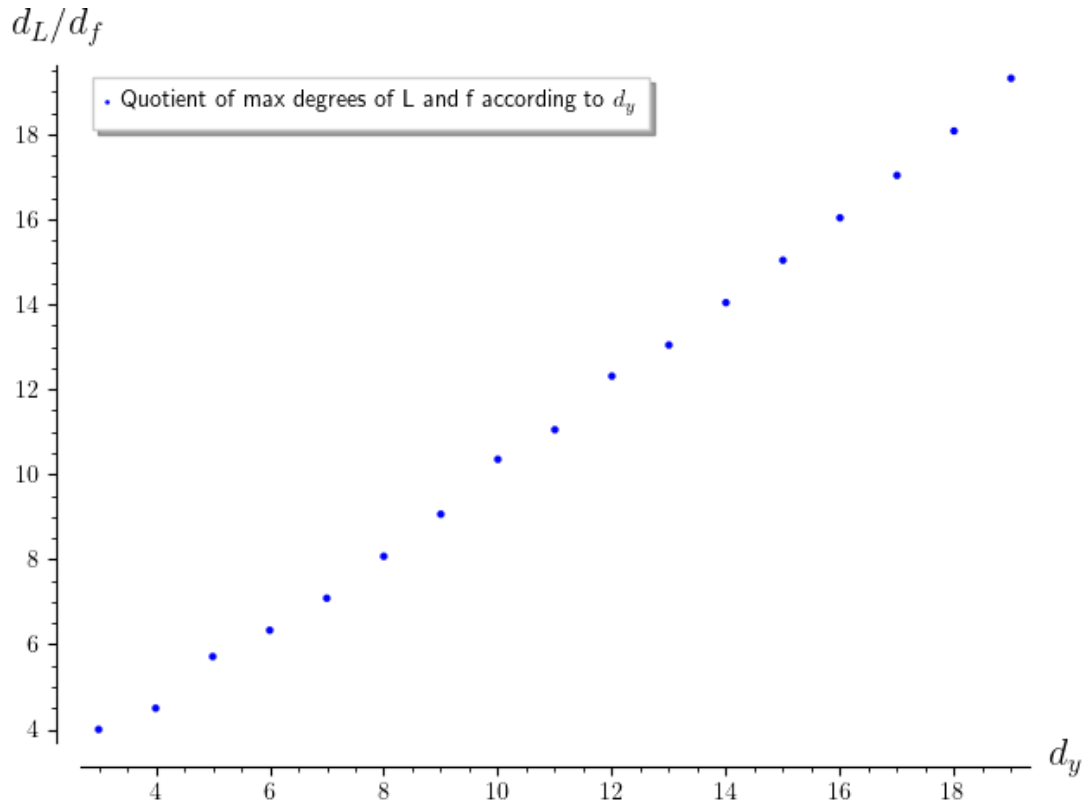


Figure 3.1: Linear growth of the relative size of an irreducible factor compared to its associated solution with regards to d_y

Furthermore, since the N_i are a fully coprime family of divisors, $\operatorname{ord}(L_i) = id_y - (i-1)d_y = d_y = \deg_y(N)$ so L_i is irreducible.
Now we know from [BCSL12, Theorem 1] that $\operatorname{lclm}_{k=0}^{i} N_k$ is of order id_y and has coefficients of degree at most $rd_xd_y^3i(d_y(i-1)+1) = O(i^2rd_xd_y^4)$. Similarly $\operatorname{lclm}_{k=0}^{i-1} N_k$ also has coefficients of size $O(i^2rd_xd_y^4)$. Since $\operatorname{ord}(\operatorname{lclm}_{k=0}^{i} N_K) - \operatorname{ord}(\operatorname{lclm}_{k=0}^{i-1} N_k) = d_y$ the result follows. □

REMARK 3.4.38. — In practice, experiments have shown that the irreducible factors returned by Algorithm 10 had coefficients of degree closer to $\tilde{O}(rd_xd_y^2)$. This also suggests that the bound on the degree of the coefficients of L_i in Proposition 3.4.37 could be improved by a factor d_y. This phenomenon is illustrated by Figure 3.1. This figure was obtained on randomly generated separable irreducible polynomials N_* in $\mathbb{F}_{41}[x,y]$ of degree 2 in the variable x, all verifying that

$$S_N \cap \mathcal{L}(A(0)) \neq \varnothing$$

and the solution to the p-Riccati equation relative to N_* was taken in $\frac{\mathbb{F}_{41}[x,a]_{\leqslant 2,<d_y}}{\partial_Y N_*(x,a)}$. A possible explanation for this phenomenon stems from the following discussion.

LEMMA 3.4.39. — *Let L/k be a separable differential field extension and let $\partial : L \to L$ be the derivation over L. Then for any $\sigma \in \operatorname{Gal}(L/k)$,*

$$\sigma \circ \partial = \partial \circ \sigma.$$

Proof. Let $\nu \in L$ and let $P_\nu(X) \in k[X]$ be its minimal polynomial. Since L/k is separable, so is P_ν. In particular, $\partial_X P_\nu(\nu) \neq 0$. Thus we know that

$$\partial(\nu) = -\frac{\partial(P_\nu)(\nu)}{\partial_X P_\nu(\nu)}.$$

But since L/k is a differential field extension, $\partial(P_\nu) \in k[X]$ since $\partial(k) \subset k$. Thus we have

$$\begin{aligned}\sigma \circ \partial(\nu) &= \sigma\left(-\frac{\partial(P_\nu)(\nu)}{\partial_X P_\nu(\nu)}\right)\\ &= -\frac{\sigma(\partial(P_\nu))(\sigma(\nu))}{\sigma(\partial_X P_\nu)(\sigma(\nu))}\\ &= -\frac{\partial(P_\nu)(\sigma(\nu))}{\partial_X P_\nu(\sigma(\nu))}\end{aligned}$$

and since P_ν is also the minimal polynomial of $\sigma(\nu)$

$$\partial(\sigma(\nu)) = -\frac{\partial(P_\nu)(\sigma(\nu))}{\partial_X P_\nu(\sigma(\nu))}$$

and thus

$$\sigma \circ \partial(\nu) = \partial \circ \sigma(\nu).$$

□

It follows from Lemma 3.4.39 that if K'/K is a separable field extension, then any $\sigma \in \mathrm{Gal}(K'/K)$ extends in an automorphism

$$\begin{array}{rccc}\sigma: & K'\langle\partial\rangle & \to & K'\langle\partial\rangle\\ & \partial & \mapsto & \partial\\ & f & \mapsto & \sigma(f)\end{array}$$

PROPOSITION 3.4.40. — *Let $N \in C[Y]$ be a separable irreducible polynomial and L/K_N be the splitting field of N over K. Let $f \in K_N$ be a solution of the p-Riccati equation relative to N. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\partial - \sigma(f)$ is a right divisor of* $\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$.

Proof. We know that σ is an automorphism of $L\langle\partial\rangle$, so it preserves divisibility and $\partial - \sigma(f) = \sigma(\partial - f)$ must thus be a right divisor of $\sigma(\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))) = \mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$ □

COROLLARY 3.4.41. — *Let $N \in C[Y]$ be a separable irreducible polynomial and K'_N be the splitting field of N over K. Let also f be a solution of the p-Riccati equation relative to N. Then*

$$\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f)) = \mathrm{lclm}_{\sigma \in \mathrm{Gal}(K'_N/K)}(\partial - \sigma(f))$$

Proof. We know that $\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$ is a common left multiple of the $\partial - \sigma(f)$. Furthermore, since the action of $\mathrm{Gal}(K'_N/K)$ preserves divisibility and acts transitively the conjugates of f, for any $\sigma' \in \mathrm{Gal}(K'_N/K_N)$,

$$\sigma'(\mathrm{lclm}_{\sigma \in \mathrm{Gal}(K'_N/K)}(\partial - \sigma(f))) = \mathrm{lclm}_{\sigma \in \mathrm{Gal}(K'_N/K)}(\partial - \sigma(f)).$$

Since K'_N/K is a Galois extension (as the splitting field of a separable polynomial), it follows that $\mathrm{lclm}_{\sigma\in\mathrm{Gal}(K'_N/K)}(\partial-\sigma(f))$ has coefficients in K.
Since $\mathrm{gcrd}(N(\partial^p),\varphi_N^{-1}(\partial-f))$ is the smallest left multiple of $\partial-f$ in $K\langle\partial\rangle$ the result follows. □

This result states that if $N\in C[Y]$ has degree d_y, then an irreducible divisor of $N(\partial^p)$ can be found as a lclm of d_y conjugate operators of order 1. This formula is not effective as the $\sigma(f)$ generally lie in a non trivial field extension of K_N. Even if it were, it would not necessarily yield better bounds ([BCSL12, Theorem 1]). It highlights however that the situation is similar to the problem of finding vanishing operators for algebraic function given by a bivariate polynomial $f(x,a)\in K_N$. Indeed in this case, the minimal polynomial of f is also given by $P_f=\mathrm{lclm}_{\sigma\in\mathrm{Gal}(K_N/\mathbb{F}_q(x))}(Y-\sigma(f))$. And similarly, one could find P_f, or a multiple of it, by computing nontrivial element of the right kernel of the matrix $M_f\in M_{d_y,d_y+1}(\mathbb{F}_q(x))$ whose vector columns are the elements f^i for $i\in[\![1;d_y]\!]$ written in any basis of K_N. This technique yields a polynomial whose coefficients are bounded by $O(d_y^2(d_f+d_x))$ where d_f is the maximal degree of the coefficients of f in the chosen basis. However such a polynomial is also given by $\mathrm{res}_T(Y-f(x,T),N(x,T))$ whose degree in x is bounded by $O(d_y(d_x+d_f))$. A similar method may perhaps exist for our problem.

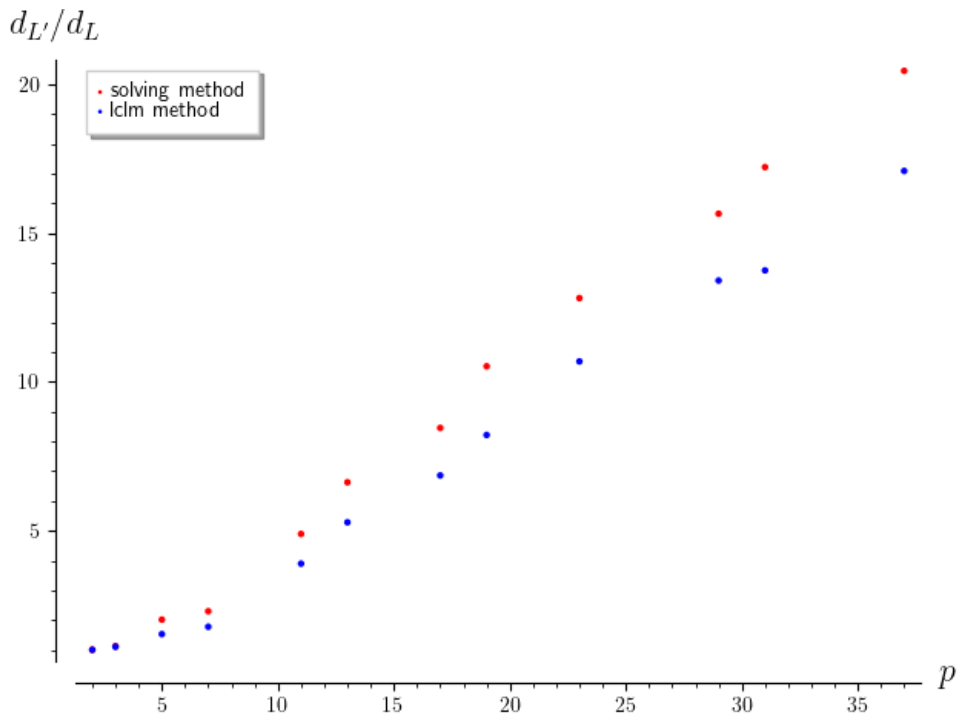


Figure 3.2: Variation with p of the relative size of the coefficients of a computed irreducible factor compared with original operators of order 2 generated with **Method 1**.

Let us now say a word of the size of a factorisation of an operator in general. Let $L\in K\langle\partial\rangle$ be a divisor of $N(\partial^p)$ and $R\in K\langle\partial\rangle$ such that $LR=N(\partial^p)$. With the notations of Proposition 3.4.37, we know that for at least $\frac{\mathrm{ord}(L)}{d_y}$ of the N_i, $\mathrm{lclm}(N_i,R)\cdot R^{-1}$ is an irreducible right factor of L (Theorem 3.2.22).

PROPOSITION 3.4.42. — *We keep the notations of Proposition 3.4.37. Let d be the maximum degree of the coefficients of R and $k := \frac{\mathrm{ord}(R)}{d_y}$. Then* $\mathrm{lclm}(N_i, R) \cdot R^{-1}$ *has coefficients of degree* $O(d_y(rkd_xd_y^3 + d))$

Proof. If $\mathrm{lclm}(N_i, R) \cdot R^{-1} \neq 1$ then it is an irreducible polynomial of order d_y and $\mathrm{lclm}(N_i, R)$ is of order $kd_y + d_y$.
We consider the map

$$\begin{array}{rccc} \mathrm{Syl}: & K\langle\partial\rangle_{\leqslant kd_y} \times K\langle\partial\rangle_{\leqslant d_y} & \to & K\langle\partial\rangle_{\leqslant d_y(k+1)} \\ & (U, V) & \mapsto & UN_i + VR \end{array}$$

Since $\mathrm{lclm}(N_i, R)$ is exactly of order $d_y(k+1)$ it follows that this map has a kernel of dimension exactly 1 and there exists $U \in K\langle\partial\rangle_{\leqslant k}$ such that $(U, \mathrm{lclm}(N_i, R) \cdot R^{-1})$ is a non trivial element of it.
Since gcrd is defined up to a multiplicative coefficient in $\mathbb{F}_q(x)$, we can suppose that N_i has polynomial coefficients. Furthermore for all $h \in \mathbb{F}_q(x)^\times$, a common left multiple of hR and N_i is a common left multiple of R and N_i. Thus $\mathrm{lclm}(hR, N_i) = \mathrm{lclm}(R, N_i)$. It follows that if h is the smallest common denominator of the coefficients of R, then $\mathrm{lclm}(N_i, R) \cdot R^{-1} = \mathrm{lclm}(N_i, R) \cdot (hR)^{-1} \cdot h$. With no loss of generality, we can suppose that R has polynomial coefficients. polynomial coefficients in which case the coefficients of the matrix Syl in the canonical basis has kd_y column vectors with polynomial coefficients of degree at most $rd_xd_y^3$ and d_y of degree at most d. Since the coefficients of $\mathrm{lclm}(N_i, R) \cdot R^{-1}$ can be expressed as quotient of minors of this matrix, it follows that they are of degree at most

$$kd_yrd_xd_y^3 + d_yd = d_y(krd_xd_y^3 + d).$$

□

REMARK 3.4.43. — Again, this result could be improved if Remark 3.4.38 was proven.

The real degree of the coefficients found with this method is hidden in the innocuous notations d and k. Indeed, if L is of small order compared to pd_y then in general both k and d are linearly dependent of p. Conversely if L is of order of the same magnitude as pd_y then k will be small but the coefficient of L, and thus of R which is obtained by Euclidean division of $N(\partial^p)$ and L, will often also be of size linearly dependent of p. Thus in all generality the result of Proposition 3.4.42 hides a linear dependance in p.

REMARK 3.4.44. — Although we are not able to avoid the dependency in p, it should be noted that being able to find "small" divisor of $N(\partial^p)$ gains us a factor p for operators of small order compared with using Lemma 3.2.23.

We recall that another way of finding an irreducible right factor of L is by computing a solution $b \in K_N$ of the operator $L(\partial + f)$. Then $\partial - f - \frac{b'}{b}$ is a right factor of L, and the corresponding irreducible right factor of L can be recovered using Algorithm 10. We have compared the two methods for divisors of ∂^p in $\mathbb{F}_p(x)\langle\partial\rangle$ for varying p and present the results in the Figures 3.2 to 3.7

Generating random non irreducible divisors of ∂^p is in general not a trivial task, as a random product of m operators of the form $\partial - \frac{b'}{b}$ has more chances of being an indecomposable factor

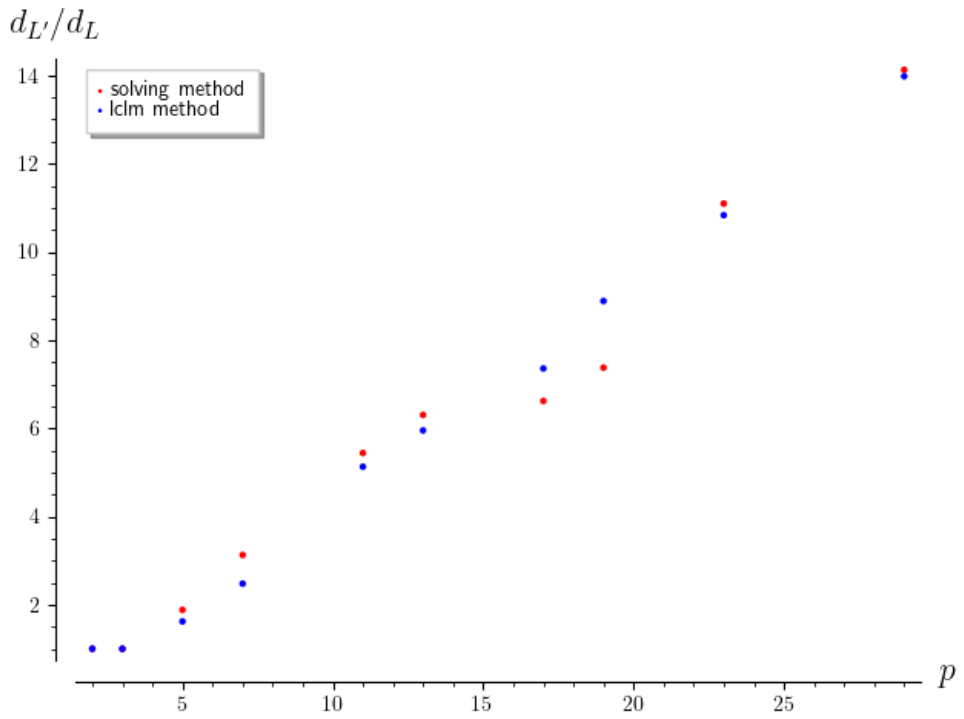


Figure 3.3: Variation with p of the relative size of the coefficients of a computed irreducible factor compared with original operators of order $\frac{p-1}{2}$ generated with **Method 1**.

of ∂^{mp} than a divisor of ∂^p. We construct our testing operators as follows:

- **Method 1:** For a specified order $1 < m < p$, we select m random functions $b_1, \ldots, b_m \in \mathbb{F}_q[x]$ of degree 2 and return $\mathrm{lclm}_{i=1}^{m}(\partial - \frac{b_i'}{b_i})$.
- **Method 2:** For a specified order $1 < m < p$ we use the first method to generate an operator L of order $p - m$ and return $\partial^p \cdot L^{-1}$.

Then, to find a solution of a given operators we can use the proof of [Clu03, Theorem 3.8].

Figure 3.2 presents the quotient of the maximal degree of the coefficient of a computed irreducible operators L' of L, divided by the maximal degree of a coefficient of L, for $L \in \mathbb{F}_p(x)\langle\partial\rangle$ an operators of order 2 generated with Method 1.
We clearly see that both methods yield a result of size linearly dependent in p, despite the relative small size of the operators L which was expected, at least for the lclm method. Indeed, applying Proposition 3.4.42 to this particular case would yield $k = p - 2$ and $d = O((p-2)d_L)$ where d_L is the maximum degree of the coefficients of L and so we predicted this linear growth in p.
The specific parameters chosen for the comparison show that the lclm-method is slightly better here for small operators, but this may not be true anymore for operators of bigger starting degrees. All in all, both method seem sensibly equivalent in this case.

Figure 3.3 presents similar data, but for operators of order $\frac{p-1}{2}$. Again we see a linear dependence in p arise which is again expected for the lclm-method as by applying Proposition 3.4.42

we now have $k = \frac{p+1}{2}$ and $d = O(\frac{p+1}{2} d_L)$.

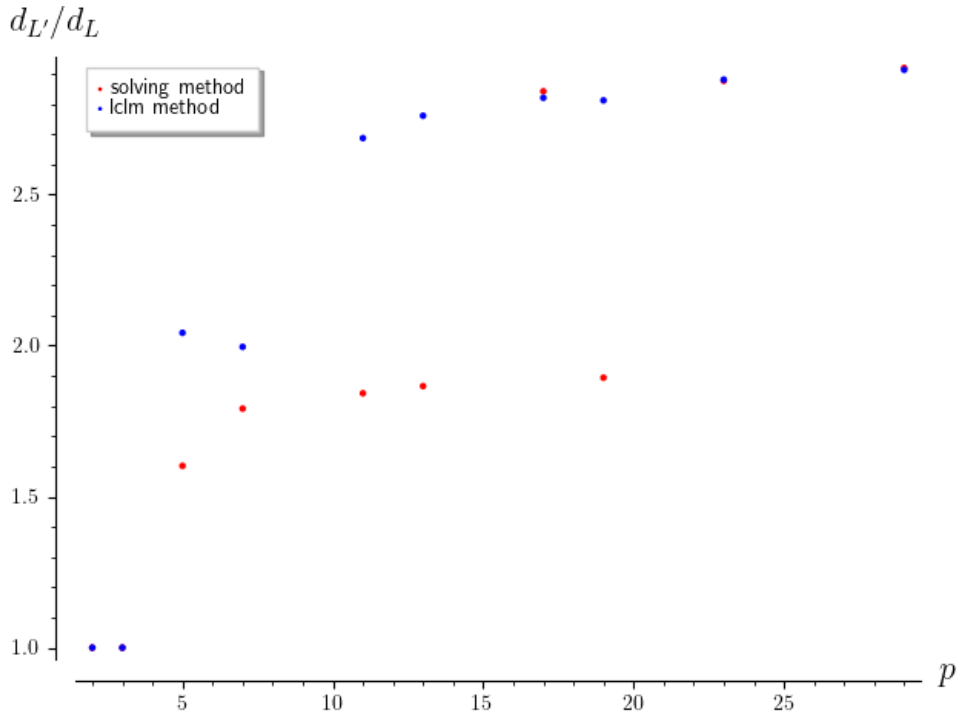


Figure 3.4: Variation with p of the relative size of the coefficients of a computed irreducible factor compared with original operators of order $\max(1, p-2)$ generated with **Method 1**.

In Figure 3.4 we once again do a similar comparison for operators of order $\max(1, p-2)$. This time both curves seem to converge to a finite bound. That is not to say that the solution obtained has a size independent from p, however this dependence is hidden in the size of the coefficients of the operator L. The figure also suggests that the lclm-method yields bigger operators for operators of high order (although only by a constant factor).

Since the lclm-method works by computing a cofactor of L to $N(\partial^p)$ it is also interesting to see what happens for operators generated with **method 2**.

On Figure 3.5 we see that whereas the resolution method still yields operators of size linear in p and d_L, the lclm-method always returns an irreducible operators whose coefficients are of a size similar to that of L.

REMARK 3.4.45. — This again does not mean that the result has a size independent from p but that this dependence is hidden in the size of L itself.

In Figures 3.6 and 3.7 we repeat the comparison tests for operators L of order $\frac{p-1}{2}$ and $\max(1, p-2)$, constructed this time with **Method 2**. This time while the coefficients of the irreducible factors computed by resolution seems to grow only by a constant factor compared to the coefficients from L, for the irreducible factors found with the lclm-method, the curve seem to follow an expression of the form $y = a/p$ for some coefficient $a > 0$. This last phenomenon is actually expected since in those case, by construction, L has actually coefficients of size $O(p)$

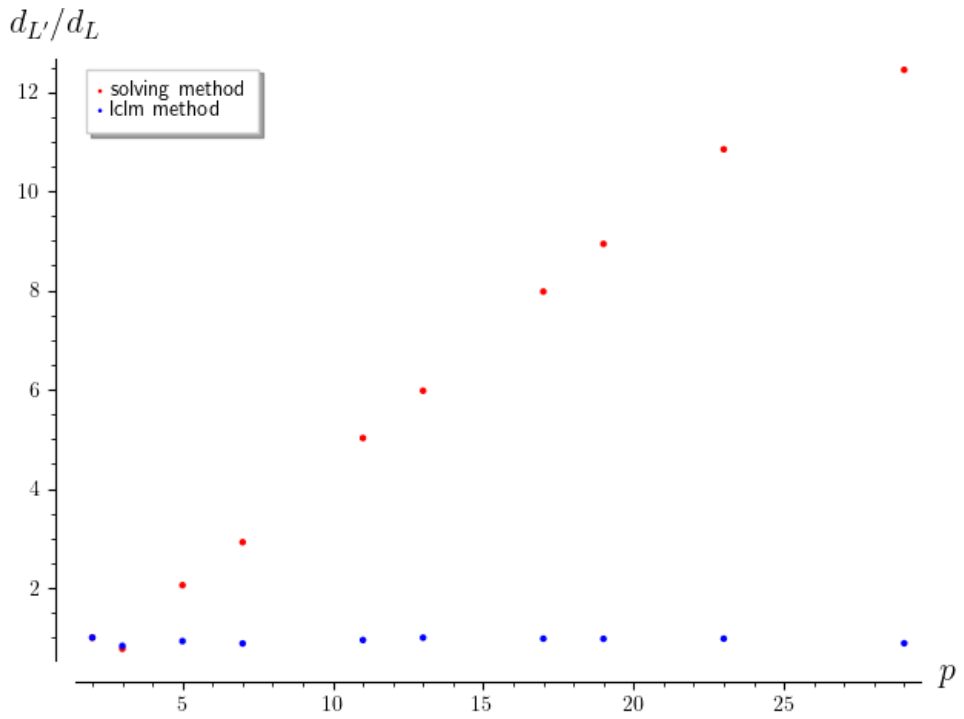


Figure 3.5: Variation with p of the relative size of the coefficients of a computed irreducible factor compared with original operators of order 2 generated with **Method 2**.

times those of its cofactor.

The results from this experiment suggest that the lclm-method is at worst as good (or not much worse) than the resolution method, while it is much better (by a factor p) for cofactors of classic operators, at least for the complexity with regard to p.

For both of these methods, we are able to compute an irreducible right factor of L in quasi-linear time in p^2 at worst. However for the special case of finding rational solutions for operators in $\mathbb{F}_q(x)\langle\partial\rangle$, Alin Bostan and Eric Schost described in [BS09, Proposition 2] to compute a basis of solution of a given operator in quasilinear time in p making it much faster for this specific task.

PROPOSITION 3.4.46. — *Let $L \in \mathbb{F}_q(x)\langle\partial\rangle$ be a right divisor of $N(\partial^p)$. Let $N_i = \operatorname{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f + \frac{i}{x}))$. Let $R \in \mathbb{F}_q(x)\langle\partial\rangle$ be such that $RL = 0$. There exists $\{i_1, \dots, i_l\} \subset [\![0; p-1]\!]$ with $l = \frac{\operatorname{ord}(L)}{d_y}$ such that we can take*

$$L_k = \operatorname{lclm}(N_{i_1}, \dots, N_{i_k}, R)/\operatorname{lclm}(N_{i_1}, \dots, N_{i_{k-1}}, R)$$

and have

$$L = L_l L_{l-1} \dots L_1.$$

Proof. This products simplifies and we only have to show that $L = \operatorname{lclm}(N_{i_1}, \dots, N_{i_r}, R) \cdot R^{-1}$. But from Theorem 3.2.22 we know that there exists a subfamily $\{i_1, \dots, i_l\}$ such that

$$L = \operatorname{lclm}_{k=1}^{l}(\operatorname{lclm}(N_{i_k}, R) \cdot R^{-1}).$$

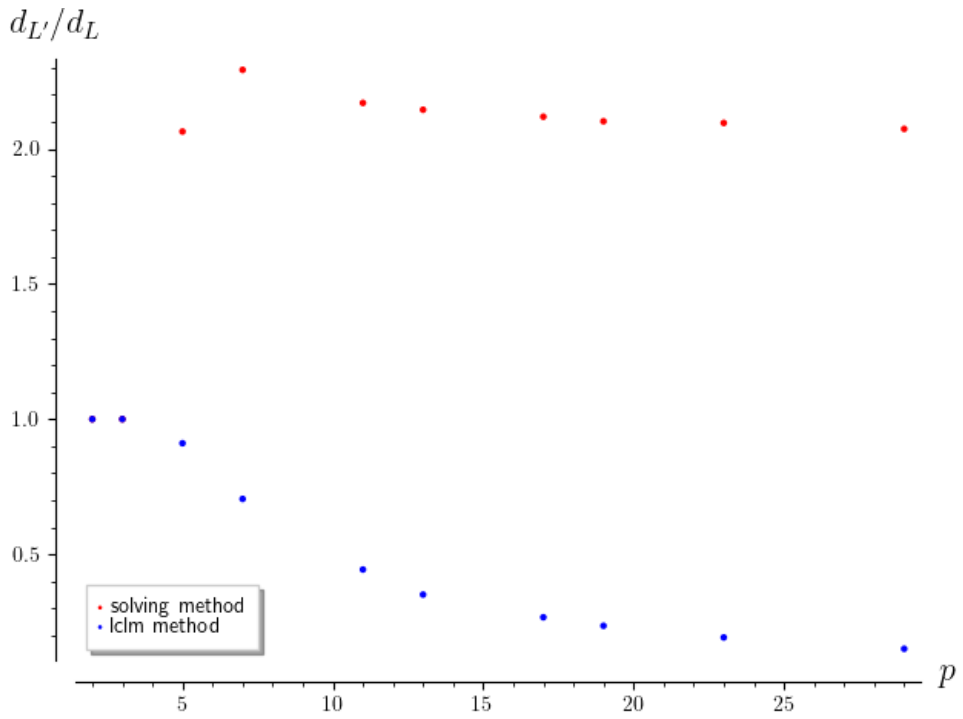


Figure 3.6: Variation with p of the relative size of the coefficients of a computed irreducible factor compared with original operators of order $\frac{p-1}{2}$ generated with **Method 2**.

We claim that $LR = N(\partial^p)$ is the least common left multiple of the $\mathrm{lclm}(N_{i_k}, R)$. Indeed if is wasn't then by dividing by R we would find a common multiple of the $\mathrm{lclm}(N_{i_k}, R) \cdot R^{-1})$ of smaller order than L which is impossible.

Thus we have $N(\partial^p) = \mathrm{lclm}_{k=1}^{l} \mathrm{lclm}(N_{i_k}, R) = \mathrm{lclm}(N_{i_1}, N_{i_2}, \ldots, N_{i_l}, R)$ and

$$N(\partial^p) \cdot R^{-1} = L = \mathrm{lclm}(N_{i_l}, \ldots, N_{i_1}, R) \cdot R^{-1}.$$

□

We can show similarly as what we have done for the factorisation of $N(\partial^p)$, that the size of the factors of L will have a size linearly dependant of p^2, which for operators of order m yields a factorisation of size at least linearly dependant of mp^2. Thus in terms of size of a classical factorisation of an operator there is no fundamental difference between factoring $N(\partial^p)$ and factoring one of its factors.
However while we are able to find "small" factors of $N(\partial^p)$, this is not the case for its divisors in general.

THEOREM 3.4.47. — *Algorithm 11 always returns a non trivial factor of L whose coefficients are of degree $O(pd^2r^5)$ in polynomial time in d and r and linear time in p^2.*

Proof. From [BCS16, Proposition 3.6], we know that N_* in step 1 can be accomplished in $\tilde{O}((d+r)^\omega \sqrt{dp})$ operations in $\mathbb{F}_q$.
Then [BCS15] states that D in step 2 can computed in $\tilde{O}(pdr^\omega)$ operations in $\mathbb{F}_q$.

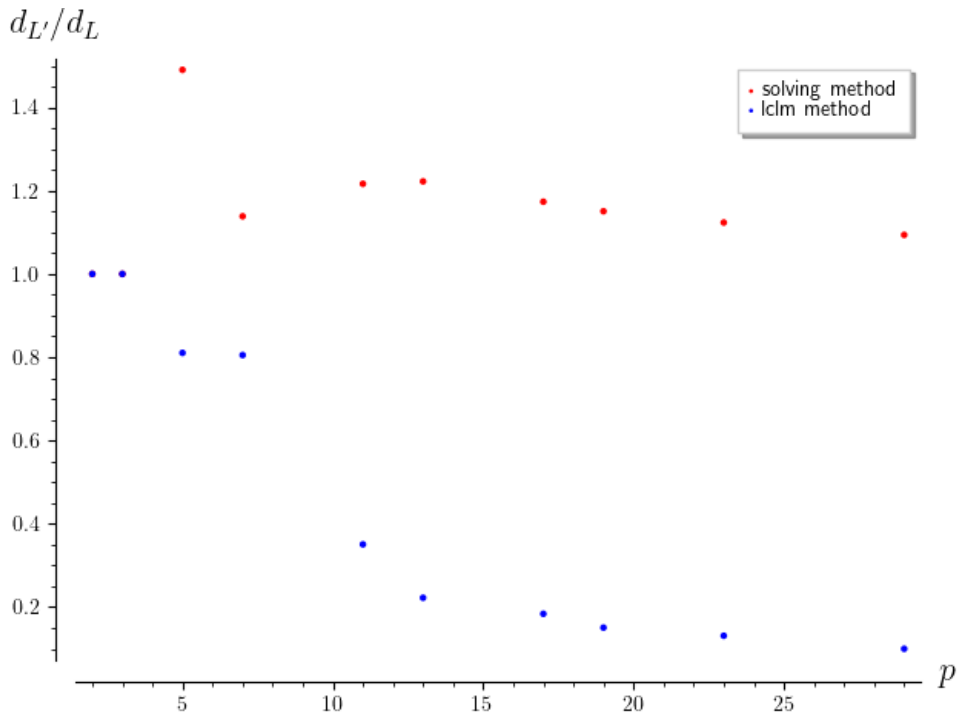


Figure 3.7: Variation with p of the relative size of the coefficients of a computed irreducible factor compared with original operators of order $\max(1, p-2)$ generated with **Method 2**.

Then $\chi_{min}(L)(D)$ is an operator of order $O(r^2)$ and of coefficients of degree at most pd. R is then an operator of order $O(pr)$ with coefficients of size $O(pd)$ and can be computed in quasi-linear time in p^2 and polynomial time in r and d.
N_* is a polynomial in $\mathbb{F}_q[x, Y]$ of bidegree (d, r) and can be factored in polynomial time in d and r and yields $N_1 \in \mathbb{F}_q[x, Y]$ of bidegree smaller than (d, r). Then computing a solution to the p-Riccati equation relative to N_1 can be done quasi-linear time in p and polynomial time in r and d according to Theorem 3.4.29 and yields f_1 whose coefficients are of size $O((rd)^2)$ if a solution exists. If it doesn't exists then the algorithm returns $N_1^p(\partial)$ whose coefficients are of size $O(pd)$.
Computing $H_0(\partial)$ using Algorithm 10 is done in polynomial time in d and r and yields an operator whose coefficients are of degree $O(r^2d^4)$ according to Theorem 3.4.36. This bound is also true for the H_i as they are also the smallest multiple of $\partial - f + \frac{i}{x}$ in $\mathbb{F}_q(x)\langle\partial\rangle$ so the same result can be applied.
We claim that at least one of the H_i does not divide R. Indeed we know that $\text{lclm}_{i=0}^{p-1}(H_i) = N_1^p(\partial)$. If all the H_i divided R then it follows that R would be a multiple of $N_1^p(\partial)$. So we could write $R = R'N_1^p(\partial)$ and $\chi_{min}(L)(\partial^p) = \chi'(\partial^p)N_1^p(\partial)$.
Then it would follow that

$$LR' = \chi'(\partial^p)$$

which contradicts the minimality of $\chi_{min}(L)$. Thus at least one of the H_i does not divide R (in practice we will often found that none of them do as H_i dividing R can be seen as the hyperplane defined by H_i containing the space defined by R, which happens rarely for randomly chosen vector spaces.) Then for this H_i we find that $\text{lclm}(R, H_i) \cdot R^{-1}$ is an operator of order

Input: $L \in \mathbb{F}_q[x]\langle\partial\rangle$.
Output: $L' \in \mathbb{F}_q[x]\langle\partial\rangle$ an irreducible divisor of L.

1. Compute $N_* \in \mathbb{F}_q(x)[Y]$ such that $N_*^p(Y) = \chi_{min}(L)(Y^p)$ using [BCS16, Proposition 3.6].
2. Compute $R \in \mathbb{F}_q(x)\langle\partial\rangle$ such that $LR = \chi_{min}(L)(\partial^p)$.
3. Compute N_1 an irreducible factor of N_*.
4. Compute $f_1 \in K_{N_1}$ a solution of the p-Riccati equation with respect to N_1 using Algorithm 9.
5. **If** no solution is found, **end** the algorithm and **return** $L' := N_1^p(\partial)$.
6. Set $H_0(\partial) := \text{gcrd}(N_1^p(\partial), \varphi_{N_1}^{-1}(\partial - f))$ using Algorithm 10
7. **For** i going from 0 to $p-1$ **do**:
   (a) Compute $H_i := H_0(\partial + \frac{i}{x})$.
   (b) **If** H_i is not a right divisor of R **do:**
      i. Compute the remainder R_* of the Euclidean division of R by H_i.
      ii. **Return** $L' := \text{lclm}(R_*, H_i) \cdot R_*^{-1}$.

Algorithm 11: Irreducible_factor_general

$\text{ord}(H_i) = \deg(N_1)$ and is a divisor of $N_1^p(\partial)$ so it has to be irreducible. Furthermore, it is a divisor of L. Indeed, $\chi_{min}(L)(\partial^p)$ is a common multiple of R and H_i so we there exists L'' such that

$$L''L'R = \chi_{min}(L).$$

But since

$$LR = \chi_{min}(L)$$

it follows that $L''L' = L$ and L' is an irreducible right factor of L.
According to Proposition 3.4.42, L' has coefficients of size $O(pd^2r^5)$ since R is of order $O(pr)$ and has coefficients of degree $O(pd)$.

Let $R = QH_i + R_*$. Since R and H_i are coprime, so too are R_* and H_i. Thus $\text{ord}(\text{lclm}(R_*, H_i)) = \text{ord}(R_*) + \text{ord}(H_i)$. It follows that there exists $U, V \in \mathbb{F}_q(x)\langle\partial\rangle$ with $\text{ord}(U) = \text{ord}(H_i)$ such that

$$UR_* + VH_i = 0.$$

By definition, $U = \text{lclm}(R_*, H_i) \cdot R_*^{-1}$. We have

$$UR + N_i(V - Q) = 0.$$

Thus we also have $U = \text{lclm}(R, H_i) \cdot R^{-1}$.

In order to compute R_*, we can compute $\partial^k \mod H_i$ for $k \leqslant \mathrm{ord}(R)$ in $\tilde{O}(p^2)$ bit operations (and in polynomial complexity in r and d). R_* has coefficients of degree linear in p and polynomial in r and d. $\mathrm{lclm}(R_*, H_i) \cdot R_*^{-1}$ can then be computed in quasilinear time in p and polynomial time in r and d. □

REMARK 3.4.48. — It should be possible to compute a right factor of a given operator L in quasi-linear time in p, provided that an analog of [BS09, Proposition 2] could be found for seeking algebraic solutions in K_N of a given operator in $K_N\langle\partial\rangle$. The method would then not require to compute a cofactor L. Instead, once a solution to the p-Riccati equation f relative to N_1 is found, we can compute the operator $L(\partial + f)$. Since we know $\partial^p - f^{(p-1)} - f^p$ divides $\chi(\psi_p^L)(\partial^p)$, it follows that ∂^p divides $\chi(\psi_p^{l(\partial+f)})(\partial^p)$ which means that $L(\partial + f)$ has solutions in K_N. If g is such a solution then we know that $\partial - \frac{g'}{g}$ is a right factor of $L(\partial + f)$ which means that $\partial - f - \frac{g'}{g}$ is a right factor of L.
To find the corresponding right factor of L with coefficient in $\mathbb{F}_q(x)$ we would once again use Algorithm 10

3.5 On computing lclm decomposition

The goal of this section is to present some potential ways to compute a lclm decomposition of a given differential operator. lclm decompositions of differential operators are often more interesting than classical factorisations as a product of irreducible differential operators because the space of solutions of a differential operators is the sum of the spaces of solutions of its right factors. In particular if we have a decomposition $L = \mathrm{lclm}(L_1, L_2)$ with $\mathrm{gcrd}(L_1, L_2) = 1$ then the space of solutions of L is the direct sum of the spaces of solutions of L_1 and L_2. We can generalise this type of decomposition, already mentioned in Corollary 2.1.31, to one where each factor is in a sense indecomposable. As we will see later on, indecomposable operators are not the same as irreducible operators.
In classical factorisation, being able to find a right factor L' of L is enough since we can then apply recursively the algorithm to L' and $L \cdot L'^{-1}$. This is not the case for lclm decompositions since finding what we will call a direct factor does not automatically yields its complementary factors. This is the main difficulty of the lclm decomposition. This work has not yet lead to a complete lclm decomposition algorithm and only present some results in that direction.

DEFINITION 3.5.1. — Let $L \in K\langle\partial\rangle$. We say that L is indecomposable if and only if L can not be written as a lclm of of two coprime smaller operators.
Through Corollary 2.1.31, this is equivalent to saying that $\mathcal{D}_L$ is indecomposable as a $K\langle\partial\rangle$-module.

The notion of indecomposability in positive characteristic p is tightly linked to the p-curvature.

LEMMA 3.5.2. — *Let $L \in K\langle\partial\rangle$. L is indecomposable if $(\mathcal{D}_L, \psi_p^L)$ is an indecomposable $K[T]$-module.*

Proof. If L is decomposable then there exists L_1 and $L_2 \in K\langle\partial\rangle$ non invertible such that $\mathcal{D}_L = \mathcal{D}_{L_1} \oplus \mathcal{D}_{L_2}$. Then $\mathcal{D}_{L_1}$ and $\mathcal{D}_{L_2}$ are stable for ψ_L^p. □

This is in fact an equivalence but the reverse implication is more complicated and will be a consequence of a later result. The reason is that subspaces of $\mathcal{D}_L$ stable for ψ_p^L are not necessarily stable $K\langle\partial\rangle$-submodules.

Definition 3.5.3. — We say that a finite family F of differential operators are fully coprime if it verifies one of the equivalent property below:

i) $\forall f \in F, \operatorname{gcrd}(f, \operatorname{lclm}_{s\in F\setminus\{f\}}(s)) = 1$.

ii) $\operatorname{ord}(\operatorname{lclm}_{f\in F} f) = \sum_{f\in F} \operatorname{ord}(f)$.

iii) There exists a bijection $u : [\![1; \operatorname{Card}(F)]\!] \to F$ such that for all $k \in [\![1; \operatorname{Card}(F) - 1]\!]$, $\operatorname{gcrd}(u(k+1), \operatorname{lclm}_{i=1}^{k}(u(i))) = 1$.

iv) For all bijection $u : [\![1; \operatorname{Card}(F)]\!] \to F$, and for all $k \in [\![1; \operatorname{Card}(F) - 1]\!]$, $\operatorname{gcrd}(u(k+1), \operatorname{lclm}_{i=1}^{k}(u(i))) = 1$.

Proof. Let's show that those are indeed equivalent properties.

i ⇒ iv Let u be a bijection $[\![1; \operatorname{Card}(S)]\!] \to S$. Then for all $k \in [\![1; \operatorname{Card}(S) - 1]\!]$, $\operatorname{lclm}_{i=1}^{k}(u(i))$ is a right divisor of $\operatorname{lclm}_{f\in S\setminus\{u(k+1)\}} f$. Since $u(k+1)$ and $\operatorname{lclm}_{f\in S\setminus\{u(k+1)\}} f$ are coprime, this is also the case for $u(k+1)$ and $\operatorname{lclm}_{i=1}^{k} u(i)$.

iv ⇒ iii is obvious.

iii ⇒ ii is an obvious induction.

ii ⇒ i Let $f \in F$. We know (Lemma 2.1.32) that $\operatorname{ord}(\operatorname{lclm}_{s\in F\setminus\{f\}} s) \leqslant \sum_{s\in F\setminus\{f\}} \operatorname{ord}(s)$.
Since $\operatorname{lclm}_{s\in F} s = \operatorname{lclm}(f, \operatorname{lclm}_{s\in F\setminus\{f\}} s)$ it follows that

$$\operatorname{ord}(\operatorname{lclm}_{s\in F}(s)) \leqslant \operatorname{ord}(f) + \operatorname{ord}(\operatorname{lclm}_{s\in F\setminus\{f\}} s)$$

with an equality if and only if $\operatorname{gcrd}(f, \operatorname{ord}(\operatorname{lclm}_{s\in F\setminus\{f\}} s)) = 1$.
Furthermore we know that $\operatorname{ord}(\operatorname{lclm}_{f\in F} f) = \sum_{f\in F} \operatorname{ord}(f) \geqslant \operatorname{ord}(f) + \operatorname{ord}(\operatorname{lclm}_{s\in F\setminus\{f\}} s)$.
Thus we have an equality and the result.

□

Remark 3.5.4. — While the two notions are equivalent in the commutative case, this notion is stronger than the simple notion of pairwise coprimality. For example the family $(\partial, \partial - \frac{1}{x}, \dots, \partial - \frac{p-1}{x}, \partial - \frac{1}{x+1})$ is pairwise coprime but not fully coprime in $\mathbb{F}_p(x)\langle\partial\rangle$. This is because $\operatorname{lclm}_{i=1}^{p}(\partial - \frac{i}{x}) = \partial^p$ and

$$\operatorname{gcrd}(\partial^p, \partial - \frac{1}{x+1}) = \partial - \frac{1}{x+1}.$$

Example 3.5.5. — The family $(\partial - \frac{i}{x})_{i\in[\![1;p]\!]}$ is fully coprime in $\mathbb{F}_p(x)\langle\partial\rangle$.

Example 3.5.6. — Let $L \in K\langle\partial\rangle$. If we write $\chi(\psi_p^L) := N_1^{\nu_1} \dots N_n^{\nu_n}$ with the N_i being pairwise coprime irreducible polynomials in $C[Y]$, then $(\operatorname{gcrd}(L, N_i^{\nu_i}(\partial^p))_{i\in[\![1;n]\!]}$ is a fully coprime family and

$$L = \operatorname{lclm}_{i=1}^{n} \operatorname{gcrd}(L, N_i^{\nu_i}(\partial^p)).$$

Proof. Since the N_i are pairwise coprime, the family $(N_i^{\nu_i}(\partial^p))_{i\in[\![1;n]\!]}$ is fully coprime. Furthermore for any $k \in [\![1;n]\!]$ and any $i \neq k$, $\mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p))$ is a right divisor of $N_i^{\nu_i}(\partial^p)$ so it is a right divisor of $\mathrm{lclm}_{i\neq k} N_i^{\nu_i}(\partial^p)$. It follows that $\mathrm{lclm}_{i\neq k}\mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p)$ is a right divisor of $\mathrm{lclm}_{i\neq k} N_i^{\nu_i}(\partial^p)$. Thus a common right divisor of $\mathrm{gcrd}(L, N_k^{\nu_k}(\partial^p)$ and $\mathrm{lclm}_{i\neq k}\mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p))$ would also be a common right divisor of $N_k^{\nu_i}(\partial^p)$ and $\mathrm{lclm}_{i\neq k} N_i^{\nu_i}(\partial^p)$.
Since the family $(N_i^{\nu_i}(\partial^p))_{i\in[\![1;n]\!]}$ is fully coprime, it must be equal to 1. Thus we conclude that the family $(\mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p)))_{i\in[\![1;n]\!]}$ is fully coprime.
As in the proof of Theorem 2.2.9, we know that $\mathrm{ord}(\mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p)) = \nu_i \deg(N_i)$. Thus

$$\mathrm{ord}(\mathrm{lclm}_{i=1}^n \mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p))) = \sum_{i=1}^n \nu_i \deg(N_i) = \deg(N) = \mathrm{ord}(L).$$

Thus $L = \mathrm{lclm}_{i=1}^n \mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p))$. □

DEFINITION 3.5.7. — Let $L \in K\langle\partial\rangle$ and $F \subset K\langle\partial\rangle$ a finite family of operators such that $L = \mathrm{lclm}_{f\in F}(f)$. We say that this identity is a lclm decomposition of L if F is a family of fully coprime indecomposable operators.

DEFINITION 3.5.8. — Let $L \in K\langle\partial\rangle$ and L_1 be a right divisor of L. We say that L_1 is a direct right factor of L is there exists a right divisor L_2 of L coprime with L_1 such that $L = \mathrm{lclm}(L_1, L_2)$. We call L_2 a complementary direct right factor of L_1.

As previously said, being able to find a direct right factor of L is not enough to conceive a full decomposition algorithm since it does not enables us to find a complementary direct right factor.

From Exemple 3.5.6 we know that one can find a first decomposition of L as a lclm of a family of fully coprime differential operators by computing its gcrd with the full irreducible components of the characteristic polynomial of its p-curvature.
Thus in this section we make the following hypothesis

HYPOTHESIS 3.5.9. — There exists $N \in C[Y]$ irreducible such that $\chi(\psi_p^L) = N^m$ for some $m \in \mathbb{N}^*$.

It follows that $\mathcal{D}_L$ has a structure of $\mathcal{D}_{N(\partial^p)^m}$-module. Let us first evacuate the case where $\mathcal{D}_{N(\partial^p)}$ is a division algebra. In this case $N(\partial^p)$ is irreducible and L is a multiple of $N(\partial^p)$, since $\mathrm{gcrd}(L, N(\partial^p))$ is a divisor of L and $N(\partial^p)$ which is not 1. It follows that L is a power of $N(\partial^p)$ (otherwise dividing L by the highest power of $N(\partial^p)$ which divides it would provide a nontrivial factor of $N(\partial^p)$ which is impossible). Furthermore, the same reasoning can be applied to any divisor of L. Thus no nontrivial divisor of L is a direct factor of L and it follows that L is already indecomposable.
Thus we will suppose from now on that $\mathcal{D}_{N(\partial^p)}$ is a matrix algebra.
From now on, we make the assumption that N is separable and keep the notations C_N, y_N and K_N of the previous sections.

REMARK 3.5.10. — The results of this section could probably be extended to the inseparable case by setting instead

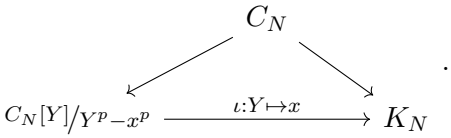
$$K_N = {}^{C_N[Y]}\!/_{Y^p - x^p}.$$

This definition coincides with the usual definition of K_N as the smallest extension of K containing both C_N and K in the separable case as we illustrate in Proposition 3.5.11. In the inseparable case we can equip this K_N with the derivation

$$\begin{array}{rccc} \frac{\mathrm{d}}{\mathrm{d}Y}: & K_N & \to & K_N \\ & \sum_{k=0}^{p-1} f_n Y^k & \mapsto & \sum_{k=1}^{p-1} k f_n Y^{k-1} \end{array}$$

We should then verify that the results of Subsection 3.2.3 extend to this new setting. This is not completely trivial because K_N is not a field, or even an integral domain in the inseparable case.

Proposition 3.5.11. — *Let K_N be the smallest extension of K containing C_N. We have a commutative diagram*



ι is an isomorphism if and only if for all $f \in K \backslash C$, C_N does not contain a p-th root of f^p.

Proof. We know that $K = C[x] \simeq {}^{C[Y]}/_{Y^p-x^p}$. Then ${}^{C_N[Y]}/_{Y^p-x^p} \simeq K \otimes_C C_N$. Let us suppose that C_N does not contain a p-th root of an element of C. Then in particular, C_N does not contain x. It follows that $[C_N[x] : C_N] = p$. Furthermore $C_N[x]$ contains C_N and K so $K_N \subset C_N[x]$. Thus we either have $K_N = C_N$ or $K_N = C_N[x]$. Since C_N does not contain x, $K_N = C_N[x] \simeq {}^{C_N[Y]}/_{Y^p-x^p}$.

Let us now suppose that $K_N \simeq {}^{C_N[Y]}/_{Y^p-x^p}$. Then in particular ${}^{C_N[Y]}/_{Y^p-x^p}$ is a field so $Y^p - x^p$ is irreducible over C_N so C_N does not contain a p-th root of x^p. Let $f \in K \backslash C$. Then $f^p \in C$. Thus $[C[f] : C] = p$ and $K = C[f]$. But if C_N contained a p-th root of f^p then we would have an injection $K \hookrightarrow C_N$ mapping C to C. Thus $K_N = C_N$ and $C_N \to K_N$ is the identity. But this is impossible since $\dim_{C_N} {}^{C_N[Y]}/_{Y^p-x^p} = p$ and ι is an isomorphism. Thus C_N does not contain a p-th root of f^p. □

With the assumption that N is separable, we now give a generalization of Proposition 3.2.13.

Lemma 3.5.12. — *There is an isomorphism of C-algebras*

$$\varphi_{N,m} : \mathcal{D}_{N(\partial^p)^m} \xrightarrow{\sim} {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)^m}.$$

Proof. There is a natural map $\varphi : K\langle\partial\rangle \to {}^{K_N\langle\partial\rangle}/_{(\partial^p-y_N)^m}$. Let $L \in \ker\varphi$. We can write $L = \sum_{i,j \in [\![0;p-1]\!]} l_{i,j}(\partial^p) x^i \partial^j$ with $l_{i,j} \in C[Y]$. Since $L \in \ker\varphi$, it follows that $(\partial^p - y_N)^m$ divides all of the $l_{i,j}(\partial^p)$. Thus y_N is a root of multiplicity at least m of all the $l_{i,j}$. Since N is irreducible, it is the minimal polynomial of y_N over C, thus N^m divides the $l_{i,j}$.
Thus $\ker\varphi = K\langle\partial\rangle N(\partial^p)^m$. We conclude by equality of dimensions over C_N. □

This lemma allows us to reduce the case where N is separable to the case N is of degree one.

Lemma 3.5.13. — *Let $L \in K_N[\partial^p]$. We can write $L = \sum_{i=0}^{p-1} l_i x^i$ with $l_i \in C_N[\partial^p]$. Then*

$$(\partial - L)^p = \partial^p - L^p + l_i$$

Proof. We consider the ring of differential operators $K_N[T]\langle\partial\rangle$ where ∂ acts on $K_N[T]$ as $\frac{\mathrm{d}}{\mathrm{d}x}$. The differential field $(K_N(T), \frac{\mathrm{d}}{\mathrm{d}x})$ verifies Hypothesis 2.1.37. The we can consider the p-curvature of elements of $K_N[T]\langle\partial\rangle \subset K_N(T)\langle\partial\rangle$.
Furthermore for any $g \in K_N(T)$, $\mu_g : \partial \mapsto \partial - g$ induces an automorphism of $K_N(T)\langle\partial\rangle$. It follows that $\chi(\psi_p^{\partial-g})(\partial^p) = (\partial - g)^p$. Indeed since μ_g is an automorphism, we know that $(\partial - g)^p = \mu_g(\partial^p)$ is a central element, of order p which is a multiple of $\partial - g$. It can only be the reduced norm of $\partial - g$, that is to say $\chi(\psi_p^{\partial-g})(\partial^p)$.
We can apply Lemma 3.2.4. It follows that for any $g \in K_N[T]$,

$$(\partial - g)^p = \partial^p - \frac{\mathrm{d}^{p-1}g}{\mathrm{d}x^{p-1}} - g^p.$$

Evaluating this equality in $T = \partial^p$ yields the result. □

THEOREM 3.5.14. — *We have an isomorphism of C-algebras:*

$$\mathcal{D}_{N(\partial^p)^m} \simeq \mathcal{D}_{N(\partial^p)}{}^{[T]}/_{T^m}.$$

Proof. Using Lemma 3.5.12 we can assume that N is of degree 1 of the form $N = Y - r$ with $r \in C$. We set $\xi_1 = 0$. We construct a sequence $(\xi_n)_{n\in\mathbb{N}} \in C[\partial^p]^{\mathbb{N}}$ such that

- $\xi_{n+1} \equiv \xi_n \mod N^n$.
- $N(\partial + x^{p-1}\xi_n) \equiv 0 \mod N(\partial^p)^n$

Suppose that we have constructed ξ_n verifying the second condition. Then we seek ξ_{n+1} of the form $\xi_n + PN(\partial^p)^n$ with $P \in C[\partial^p]$. Then we have

$$\begin{aligned} N(\partial + x^{p-1}\xi_{n+1}) &= (\partial + x^{p-1}\xi_{n+1})^p - r^p \\ &= \partial^p - \xi_{n+1} + x^{p(p-1)}\xi_{n+1}^p - r^p \\ &= \partial^p - \xi_n - PN(\partial^p)^n + x^{p(p-1)}\xi_n^p + x^{p(p-1)}P^pN(\partial^p)^{np} - r^p \\ &\equiv N(\partial + x^{p-1}\xi_n) - PN(\partial^p)^n \mod N(\partial^p)^{n+1} \end{aligned}$$

Since by hypothesis, $N(\partial^p)^n$ divides $N(\partial+x^{p-1}\xi_n)$, we can choose P such that $N(\partial+x^{p-1}\xi_{n+1}) \equiv 0 \mod N(\partial^p)^{n+1}$.

We deduce a morphism

$$\begin{array}{rccc} \varphi_m : & \mathcal{D}_{N(\partial^p)} & \to & \mathcal{D}_{N(\partial^p)^m} \\ & \partial & \mapsto & \partial + x^{p-1}\xi_m \end{array}.$$

Since $\mathcal{D}_{N(\partial^p)}$ is either a division algebra or a matrix ring over a field, it has no nontrivial two-sided ideal. Thus φ_m is injective.
Note that since for all $k \in [\![0, p-1]\!]$, $\mathrm{ord}((\partial+x^{p-1}\xi_m)) \equiv k \mod p$, the family $((\partial+x^{p-1}\xi_m)^k)_{0\leqslant k\leqslant p-1}$ is a $K[\partial^p]$-basis of $K\langle\partial\rangle$.

Mapping T to $N(\partial^p)$ allows us to define a morphism

$$\overline{\varphi} : \mathcal{D}_{N(\partial^p)}{}^{[T]}/_{T^m} \to \mathcal{D}_{N(\partial^p)^m}.$$

Furthermore a sum

$$\sum_{k=0}^{p-1}\sum_{l=0}^{m-1} f_{k,l}(\partial + x^{p-1}\xi_m)^k N(\partial^p)^l$$

with $f_{k,l} \in K$ is only divided by $N(\partial^p)^m$ if all $f_{k,l} = 0$.
Thus $\overline{\varphi}$ is injective, and bijective by equality of dimensions over C. □

It follows that if N is separable over C then $\mathcal{D}_L$ is a $\mathcal{D}_{N(\partial^p)}{}^{[T]}/_{T^m}$-module. Remember that we suppose here that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to a matrix algebra.

Theorem 3.5.15. — *Let $N^{m_1}|N^{m_2}|\cdots|N^{m_k}$ be the Frobenius invariants of ψ_p^L. Then there exists $L_1, \ldots, L_k \in K\langle\partial\rangle$ indecomposable such that*

- $L = \mathrm{lclm}(L_1, \ldots, L_k)$ *is a* lclm *decomposition of L.*
- $\mathrm{ord}(L_i) = m_i \deg(N)$.

Proof. We know that $\mathcal{D}_L$ is a $\mathcal{D}_{N(\partial^p)}{}^{[T]}/_{T^m}$-module. Since $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$ it follows that $\mathcal{D}_L$ is a $M_p(C_N)^{[T]}/_{T^m}$-module. It is important to note that for any L' in $\mathcal{D}_L$, $T \cdot L' = N(\partial^p)L'$ by construction.
Then $\mathcal{D}_L$ corresponds to some ${C_N}^{[T]}/_{T^m}$-module M through Morita's equivalence. Then there exists a unique decomposition

$$M = {C_N}^{[T]}/_{T_1^m} \oplus \cdots \oplus {C_N}^{[T]}/_{T_k^m}$$

which corresponds to a decomposition

$$\mathcal{D}_L = M_1 \oplus \cdots \oplus M_k$$

of indecomposable $K\langle\partial\rangle$-modules. Furthermore T^{m_i} is the minimal polynomial of the multiplication by T over M_i. Thus the minimal polynomial of $\psi_p^{M_i}$ is $\mu(\psi_p^{M_i}) = N^{m_i}$. Moreover

$$\dim_K(M_i) = p^{-1}\dim_C(M_i) = \dim_C {C_N}^{[T]}/_{T_i^m} = m_i \deg(N).$$

Then $\chi(\psi_p^{M_i}) = \mu(\psi_p^{M_i}) = N^{m_i}$ and the M_i fits the criteria of the Frobenius decomposition of ψ_p^L and is a decomposition of $\mathcal{D}_L$ as a direct sum of indecomposable $K\langle\partial\rangle$-modules. The result immediately follows. □

Although this result allows to compute the form of a lclm factorisation of L from the Frobenius decomposition of ψ_p^L, we can't directly compute such a factorisation from it. This is because we have no guarantee the sub-K-vector spaces of $\mathcal{D}_L$ that would come with a Frobenius decomposition of ψ_p^L would be $K\langle\partial\rangle$-modules.
It should be noted that being able to compute a solution to the p-Riccati equation relative to N allows us to explicitly compute Morita's equivalence.

Lemma 3.5.16. — *Let L be an indecomposable divisor of $N(\partial^p)^m$ or order $m\deg(N)$. Then $\mathcal{D}_L$ is a free ${C[\partial^p]}/_{N(\partial^p)^m}$-module of dimension p.*

Proof. Since L is indecomposable, it corresponds through Morita's equivalence to ${C_N}^{[T]}/_{T^m} \simeq {C[\partial^p]}/_{N(\partial^p)^m}$ so it must be isomorphic to $({C[\partial^p]}/_{N(\partial^p)^m})^p$ as a ${C[\partial^p]}/_{N(\partial^p)^m}$-module. □

THEOREM 3.5.17. — *Let L be an indecomposable divisor of $N(\partial^p)^m$ or order $m\deg(N)$.*

$$\begin{array}{rccl} \iota_L : & \mathcal{D}_{N(\partial^p)^m} & \to & \mathrm{End}_{C[\partial^p]/\partial^p}(\mathcal{D}_L) \\ & M & \mapsto & (L' \mapsto ML' \mod L) \end{array}$$

is an isomorphism of ${}^{C[\partial^p]}/_{N(\partial^p)^m}$-algebras.

Proof. Let us show that ι is injective which will yield the result by dimension equality. Let $M \in \ker(\iota)$. Then for any $L' \in K\langle\partial\rangle$, ML' is a left multiple of L. In particular M is a left multiple of L. But L is similar to all the direct indecomposable factors of $N(\partial^p)^m$. Thus for any direct indecomposable factor L_b of $N(\partial^p)^m$ we have an isomorphism of $K\langle\partial\rangle$-module $\varphi : \mathcal{D}_L \to \mathcal{D}_{L_b}$. Furthermore since φ is a morphism of $K\langle\partial\rangle$-module it follows that $\varphi \circ \iota_L(M) \circ \varphi^{-1} = \iota_{L_b}(M)$. Thus we find that any direct indecomposable factor of $N(\partial^p)^*$ is a right factor of M. It follows that $N(\partial^p)^m$ is a right divisor of M. □

Theorem 3.5.17 allows us to write an explicit isomorphism between $\mathcal{D}_{N(\partial^p)^m}$ and a matrix algebra. This in turn would allow us to explicitly compute the Morita equivalence to find a lclm decomposition.

LEMMA 3.5.18. — *For all $n \in \mathbb{N}$, the operator $\partial(x\partial)^n$ is indecomposable of order $n+1$.*

Proof. By multiplicativity of the reduced norm, we know that the characteristic polynomial of the p-curvature of $\partial(x\partial)^n$ is Y^{n+1} so the p-curvature of $\partial(x\partial)^n$ is nilpotent. We want to show that $\chi_{min}(L) = Y^{n+1}$ which will prove that $\partial(x\partial)^n$ is indecomposable according to Theorem 3.5.17. It is enough to show that $\ker(\psi_p^{\partial(x\partial)^n})$ is 1-dimensional over K which is to say that the space of solutions of $\partial(x\partial)^n$ is 1-dimensional over C.

Let $f = \sum_{i=0}^{p-1} f_i x^i$ with the $f_i \in C$. We find

$$\partial(x\partial)^n = \sum_{i=0}^{p-2} (i+1)^{n+1} f_{i+1} x^i.$$

Thus f is a solution of $\partial(x\partial)^n$ if and only if $f \in C$ and $\partial(x\partial)^n$ is indecomposable. □

COROLLARY 3.5.19. — *For any $f \in K_N$, $(\partial - f)(x(\partial - f))^n$ is indecomposable of order $n+1$.*

Proof. We consider the automorphism of $K_N\langle\partial\rangle$, $\tau_f : \partial \mapsto \partial + f$. Then $(\partial - f)(x(\partial - f))^n$ is indecomposable if and only if $\tau_f((\partial - f)(x(\partial - f))^n)$ is indecomposable. But $\tau_f((\partial - f)(x(\partial - f))^n) = \partial(x\partial)^n$ which is indecomposable by Lemma 3.5.18. □

LEMMA 3.5.20. — *Let $f \in S_N$. If $L \in K\langle\partial\rangle$ is a left multiple of order $m\deg(N)$ of $(\partial - f)(x(\partial - f))^{m-1}$ then L is indecomposable.*

Proof. We claim that $\varphi_{N,m}(\mathcal{D}_{N(\partial^p)^m} L)$ is the submodule of ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)^m}$ generated by $(\partial - f)(x(\partial - f))^{m-1}$, which we denote M. Indeed we know that $\varphi_{N,m}(\mathcal{D}_{N(\partial^p)^m} L)$ is the submodule generated by $\mathrm{gcrd}(L, (\partial^p - y_N)^m)$. Since L is a multiple of $(\partial - f)(x(\partial - f))^{m-1}$,

$$\varphi_{N,m}(\mathcal{D}_{N(\partial^p)^m} L) \subset M.$$

Then by equality of the dimensions over C we get the result.
It follows that $\mathcal{D}_L$ is isomorphic to the quotient module of $K_N\langle\partial\rangle$ by the left ideal generated by $(\partial - f)(x(\partial - f))^{m-1}$ and is thus indecomposable. □

We can use Lemma 3.5.20 to compute direct factors of $N(\partial^p)^m$ whose coefficients are of degrees independent from p and use it to explicitly compute Morita's equivalence.

We fear that this method may not be very efficient since to compute Morita's equivalence we to view K_N as a C_N-vector space which induces a heavy dependence in p. The rest of this section is a collection of results that we hope could lead to an analog expression of a lclm decomposition to Theorem 1.3.2 in the case $m = 1$.

Lemma 3.5.21. — *Let $N \in C[Y]$ irreducible and separable such that $N(\partial^p)$ is not irreducible. Then for all $m \in \mathbb{N}^*$, there exists $L_{1,m}, \dots, L_{p,m}$ fully coprime indecomposable operators of order $m \deg(N)$ such that*

$$N(\partial^p)^m = \operatorname{lclm}(L_{1,m}, \cdots, L_{p,m})$$

Proof. $\mathcal{D}_{N(\partial^p)^m}$ is isomorphic to $M_p({C_N}^{[T]}/_{T^m})$ and is thus mapped through Morita's equivalence to $({C_N}^{[T]}/_{T^m})^p$, which is to say that there exists a decomposition $\mathcal{D}_{N(\partial^p)^m} = M_1 \oplus \cdots \oplus M_p$ with $\dim_K(M_i) = m \deg(N)$ which yields the result. □

Example 3.5.22. — Let $f \in S_N$ and let $(g_i)_{i\in[\![1;p]\!]}$ be a C-basis of K. We set $L_i = (\partial - f - \frac{g_i'}{g_i})(x(\partial - f - \frac{g_i'}{g_i}))^{m-1}$. Then

$$(\partial^p - y_N)^m = \operatorname{lclm}_{i=0}^{p-1}(L_i).$$

Proof. We know that each L_i is an indecomposable factor of $(\partial^p - y_N)^m$. We only have to show that the family $(L_i)_{i\in[\![0;p-1]\!]}$ is fully coprime. By using the shift $\partial \mapsto \partial + f$ we can assume that $f = 0$. By reccurence, we show that $\operatorname{gcrd}(L_k, \operatorname{lclm}_{i=0}^{k-1} L_i) = 1$ for all $k \in [\![0; p-1]\!]$. Let us assume that we have shown that the family $(L_i)_{i<k}$ is fully coprime. Let L_* be a divisor of both L_K and $\operatorname{lclm}_{i=0}^{k-1} L_i$. If $L_* \notin K$ then we can assume that L_* is irreducible and thus is equal to $\partial - \frac{g_k'}{g_k}$. Thus g_k is a solution of $\operatorname{lclm}_{i=0}^{k-1} L_i$ in K.
Since $(L_i)_{i<k}$ is fully coprime by hypothesis, the quotient module by $\operatorname{lclm}_{i=0}^{k-1} L_i$ is isomorphic with $\bigoplus_{i=0}^{k-1} \mathcal{D}_{L_i}$. In particular the dimension of the kernel of its p-curvature is

$$\sum_{i=0}^{k-1} \dim_K \ker(\psi_p^{L_i}).$$

But we know that the space of solutions of L_i in K is 1-dimensional over C and generated by g_i. Thus

$$\sum_{i=0}^{k-1} \dim_K \ker(\psi_p^{L_i}) = \sum_{i=0}^{k-1} 1 = k.$$

It follows that the space of solutions of $\operatorname{lclm}_{i=0}^{k-1} L_i$ in K is $\bigoplus_{i=0}^{k-1} g_i C$. But this space does not contain g_k.
Thus $\operatorname{gcrd}(L_k, \operatorname{lclm}_{i=0}^{k-1} L_i) = 1$. □

Lemma 3.5.23. — *Let $N(\partial^p)^m = \operatorname{lclm}(N_1, \cdots, N_p)$ be a* lclm *decomposition. Then for all $m' \leqslant m$ we have*

$$N(\partial^p)^{m'} = \operatorname{lclm}_{i=1}^{p}(\operatorname{gcrd}(N_i, N(\partial^p)^{m'}))$$

which is also a lclm *decomposition.*

Proof. It is enough that we show this result for $m' = m-1$ and then conclude by finite induction.

Let $N_i' := \mathrm{gcrd}(N_i, N(\partial^p)^{m'})$ for all i. It is easy to see that the N_i' are fully coprime. Indeed for any $i \in [\![1;p]\!]$, $\mathrm{lclm}_{j\neq i}(N_j')$ is a right divisor of $\mathrm{lclm}_{j\neq i}(N_j)$ and N_i' is a right divisor of N_i. Thus if they were not coprime then N_i and $\mathrm{lclm}_{j\neq i}(N_j)$ would have a non trivial common right divisor which is impossible since the N_i are supposed fully coprime.

We want to show that

$$\mathcal{D}_{N(\partial^p)^m} N(\partial^p)^{m-1} = \bigcap_{i=1}^{p} \mathcal{D}_{N(\partial^p)^m} N_i'.$$

The "$\subset$" direction is trivial since

$$\bigcap_{i=1}^{p} \mathcal{D}_{N(\partial^p)^m} N_i' = \bigcap_{i=1}^{p} (\mathcal{D}_{N(\partial^p)^m} N_i + \mathcal{D}_{N(\partial^p)^m} N(\partial^p)^{m-1}).$$

To conclude we show that we have an equality of codimension.

Since the N_i' are fully coprime we have

$$\mathrm{codim}_K \bigcap_{i=1}^{p} \mathcal{D}^m_{N(\partial^p} = \mathrm{ord}(\mathrm{lclm}_{i=1}^{p} N_i') = \sum_{i=1}^{p} \mathrm{ord}(N_i').$$

To conclude it is enough to show that for all i, $\mathrm{ord}(N_i') = (m-1)\deg(N)$.

We have $\mathrm{ord}(N_i') \leqslant (m-1)\deg(N)$. Indeed if such was not the case then N_i' would be of order $m\deg(N)$ and be equal to N_i. But then $N(\partial^p)^{m-1}$ would have an indecomposable factor of order strictly more than $(m-1)\deg(N)$ which is impossible.

We now want to show that $\deg(N_i') \geqslant (m-1)\deg(N)$ which is equivalent to

$$\begin{aligned}\mathrm{ord}(\mathrm{lclm}(N_i, N(\partial^p)^{m-1})) &\leqslant m\deg(N) + (m-1)p\deg(N) - (m-1)\deg(N)\\ &= ((m-1)p-1)\deg(N).\end{aligned}$$

This again is equivalent to saying that

$$\begin{aligned}\dim_K(\mathcal{D}_{N(\partial^p)^m} N_i \cap \mathcal{D}_{N(\partial^p)^m} N(\partial^p)^{m-1}) &\geqslant mp\deg(N) - ((m-1)p-1)\deg(N)\\ &= (p-1)\deg(N)\end{aligned}$$

But $\mathcal{D}_{N(\partial^p)^m} N_i \cap \mathcal{D}_{N(\partial^p)^m} N(\partial^p)^{m-1}$ is the kernel of the multiplication by $N(\partial^p)$ in $\mathcal{D}_{N(\partial^p)^m} N_i$. It follows that

$$\begin{aligned}\dim_K(\mathcal{D}_{N(\partial^p)^m} N_i) &= \dim_K(\ker \times N(\partial^p)^m)\\ &\leqslant m\dim_K(\ker \times N(\partial^p))\end{aligned}$$

which translates to

$$m(p-1)\deg(N) \leqslant m\dim_K(\mathcal{D}_{N(\partial^p)^m} N_i \cap \mathcal{D}_{N(\partial^p)^m} N(\partial^p)^{m-1})$$

and finally to

$$\dim_K(\mathcal{D}_{N(\partial^p)^m}N_i \cap \mathcal{D}_{N(\partial^p)^m}N(\partial^p)^{m-1}) \geqslant (p-1)\deg(N)$$

which is the desired result. □

Lemma 3.5.24. — *Let L be a right divisor of some $N(\partial^p)^m$. If L_* is a right indecomposable factor of L of maximal order then it is also a direct factor.*

Proof. $\mathcal{D}_L \cdot L^*$ is a submodule of $\mathcal{D}_L$ whose quotient is indecomposable and of maximal order. Morita's equivalence maps $\mathcal{D}_L$ to a C_N-vector space E provided with an endomorphism $u \in \mathcal{L}(E)$, and $\mathcal{D}_L \cdot L_*$ to a subspace V of E stable by u such that $({}^{E}/_{V},\bar{u})$ is cyclic with $\dim(V) = \dim(E) - \deg(\pi_u)$ (where π_u is the minimal polynomial of u). Let E^* be the dual of E and $u^* : l \mapsto l \circ u$ be the dual endomorphism of u. V is the dual of a cyclic stable (for u^*) subspace of E^* of maximal dimension. Thus, it admits a complementary subspace stable by u. Thus there exists L_* a right divisor of L such that $\mathcal{D}_L L^* \oplus \mathcal{D}_L L_* = \mathcal{D}_L$ which gives the result. □

Theorem 3.5.25. — *Let $L \in K\langle\partial\rangle$ be a divisor of $N(\partial^p)^m$ with m minimal, and $R \in K\langle\partial\rangle$ such that $LR = N(\partial^p)^m$. Let*

$$N(\partial^p)^m = \mathrm{lclm}(L_1^*, \cdots, L_p^*)$$

be an lclm *factorisation of $N(\partial^p)$. Then there exists $i \in [\![1;p]\!]$ such that*

$$\mathrm{lclm}(R, L_i^*) \cdot R^{-1}.$$

is a direct right indecomposable factor of L of maximal order.

Proof. We show that for at least one $i \in [\![1;p]\!]$, $\mathrm{gcrd}(L_i^*, R) = 1$. Indeed if such was not the case then for each $i[\![1;p]\!]$ there would exists N_i an irreducible factor of $N(\partial^p)$ which would be a right divisor of both L_i^* and L. But then for all $k \in \mathbb{N}$, $\mathrm{lclm}_{i=1}^k(N_i)$ is a right divisor of $\mathrm{lclm}_{i=1}^k(L_i^*)$. Since $\mathrm{gcrd}(L_{k+1}^*, \mathrm{lclm}_{i=1}^k(L_i^*)) = 1$ it follows that $\mathrm{gcrd}(N_{k+1}, \mathrm{lclm}_{i=1}^k(N_i)) = 1$, thus

$$N(\partial^p) = \mathrm{lclm}_{i=1}^p(N_i)$$

by checking the orders. It follows that $N(\partial^p)$ would be a right divisor of R. Let us then write $R = R'N(\partial^p)$. Then $LR' = N(\partial^p)^{m-1}$ which contradicts the minimality of m.
Thus there exists $i \in [\![1;p]\!]$ such that $\mathrm{gcrd}(R, L_i^*) = 1$.
It follows that $\mathcal{D}_{N(\partial^p)^m}R \cap \mathcal{D}_{N(\partial^p)^m}L_i^*$ is of K-codimension $m\deg(N)$ in $\mathcal{D}_{N(\partial^p)^m}R$. Furthermore the injection $\mathcal{D}_{N(\partial^p)^m}R \hookrightarrow \mathcal{D}_{N(\partial^p)^m}$ induces an injection

$${}^{\mathcal{D}_{N(\partial^p)^m}R}/_{\mathcal{D}_{N(\partial^p)^m}R \cap \mathcal{D}_{N(\partial^p)^m}L_i^*} \hookrightarrow \mathcal{D}_{L_i^*}$$

and by dimension equality we deduce that the two spaces are isomorphic as $K\langle\partial\rangle$-modules.
Thus $\mathcal{D}_{\mathrm{lclm}(R,L_i^*)\cdot R^{-1}} \simeq {}^{\mathcal{D}_{N(\partial^p)^m}R}/_{\mathcal{D}_{N(\partial^p)^m}R \cap \mathcal{D}_{N(\partial^p)^m}L_i^*}$ is indecomposable and $\mathrm{lclm}(R, L_i^*) \cdot R^{-1}$ is an indecomposable right factor of L.
We still have to show that it is a direct factor. This stems from Lemma 3.5.24 and that we have shown that it is a maximal indecomposable right factor. □

Theorem 3.5.25 gives us a way to compute the first direct factor of a lclm decomposition of L by knowing a lclm decomposition of $N(\partial^p)^m$. We know that decompositions of this last operator are not hard to find (meaning not harder than finding a solution to the p-Riccati equation with

respect to N). However, lclm decompositions are not as simple as classical factorisations in the sense that knowing a first factor does automatically allow one to compute a cofactor upon which one could reccursively use his algorithm.
The following result states that if we are able to find several then indecomposable factors, provided some conditions are verified, they will still constitute direct factors.

LEMMA 3.5.26. — *Let L be a divisor of $N(\partial^p)^m$ and let $N^{m_d}|N^{m_{d-1}}|\cdots|N^{m_1}$ be the Frobenius invariants of its p-curvature. Let $L_1,\cdots,L_k$ be a family of indecomposable factors of L such that $\mathrm{ord}(L_i)=m_i\deg(N)$. If the L_i are fully coprime, then $\mathrm{lclm}(L_1,\cdots,L_k)$ is a direct factor of L.*

Proof. We begin by showing that

$$\mathcal{D}_{\mathrm{lclm}_{i=1}^k(L_i)}=\bigoplus_{i=1}^k\mathcal{D}_{L_i}$$

. We proceed by recurrence on k. The result is obviously true for $k=1$. We write $L_*=\mathrm{lclm}_{i=1}^{k-1}(L_i)$. Since $(L_1,\ldots,L_k)$ is a family of fully coprime operators, it follows that $\mathrm{gcrd}(L_*,L_k)=1$ which is to say that

$$\mathcal{D}_L L_* + \mathcal{D}_L L_k = \mathcal{D}_L.$$

Then

$$\begin{array}{ccc} {}^{\mathcal{D}_L L_*}/_{\mathcal{D}_L L_*\cap\mathcal{D}_L L_k}\oplus {}^{\mathcal{D}_L L_k}/_{\mathcal{D}_L L_*\cap\mathcal{D}_L L_k} & \to & {}^{\mathcal{D}_L}/_{\mathcal{D}_L L_*\cap\mathcal{D}_L L_k} \\ (M_1,M_2) & \mapsto & M_1+M_2 \end{array}$$

is an isomorphism.
Since ${}^{\mathcal{D}L_*}/_{\mathcal{D}_L L_*\cap\mathcal{D}_L L_k}\simeq {}^{\mathcal{D}_L}/_{\mathcal{D}_L L_k}\simeq\mathcal{D}_{L_k}$ and ${}^{\mathcal{D}L_k}/_{\mathcal{D}_L L_*\cap\mathcal{D}_L L_k}\simeq {}^{\mathcal{D}_L}/_{\mathcal{D}_L L_*}\simeq\mathcal{D}_{L_*}$ we have the result by immediate recurrence.

Let E be the $C_N[T]$-module corresponding to $\mathcal{D}_L$ through Morita's equivalence and V be the submodule corresponding to $\mathcal{D}_L\mathrm{lclm}_{i=1}^k(L_i)$. From the hypothesis we get that $E\simeq\bigoplus_{i=1}^d {}^{C_N[T]}/_{T^{m_i}}$ and ${}^E/_V\simeq\bigoplus_{i=1}^k {}^{C_N[T]}/_{T^{m_i}}$. It is well known that such a V admits a supplementary $C_N[T]$-submodule. □

We have seen that we have ways of finding indecomposable factors of a given L. They can be interpreted as computing the intersection of $\mathcal{D}_L$ and a generic indecomposable submodule of $\mathcal{D}_{N(\partial^p)}$ of the right dimension, under a dimension condition. Our hope is that by taking randomly constructed indecomposable submodule of $\mathcal{D}_{N(\partial^p)}$, the intersection of $\mathcal{D}_L$ and those submodule would most often be of generic dimension (meaning that the intersection of two submodules of respective codimensions l and n would be of codimension $l+n$). However it would be better here to think of our submodules not as vector spaces but as stables subspaces for a nilpotent endomorphism, and the intersection might not generically behave as it does for vector spaces.

However if it did then we could design an iterative algorithm based on Lemma 3.5.26 and Theorem 3.5.25 to compute lclm decompositions of L.
We also note that through Lemma 3.5.20, we know of a way to find many indecomposable factors of $N(\partial^p)^m$ of maximal order. Not all indecomposable factors of $N(\partial^p)^m$ are of this form however. We conjecture that a classical product of m random irreducible divisors of $N(\partial^p)$ will most often

end up being an indecomposable factor of $N(\partial^p)^m$. We see this as the probability of picking a nilpotent endomorphism of C_N^m of nilpotence order m among the nilpotent endomorphisms of C_N^m. Note however that C_N does not naturally come with a probability measure so this is just a heuristic.

Appendix A

Morita's theorem

A.1 Noncommutative tensor product

In this appendix, we study the construction and universal properties of the tensor product of non necessarily commutative rings.

Definition A.1.1. — Let R and S be two (non necessarily commutative) rings and M be an abelian group. We say that M is a $R-S$-bimodule if and only if M is provided with a left R-module structure and a right S-module structure and if for all $(r,s) \in R \times S$ and all $m \in M$:

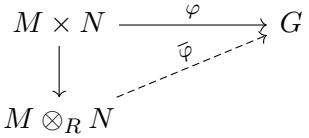
$$(rm)s = r(ms).$$

An $R-R$-bimodule is called an R-bimodule.

Definition A.1.2. — Let R be a ring and M be a left R-module and N a right R-module. Let G be an abelian group and $f : M \times N \to G$ be a biadditive map.
f is said to be R-associative if for any $(r,m,n) \in R \times M \times N$

$$f(mr,n) = f(m,rn).$$

Let R be a ring, M be a right R-module and N a left R-module.
There exists an abelian group $M \otimes_R N$, unique up to unique isomorphism, and a unique biadditive R-associative map $M \times N \to M \otimes_R N$ such that for all abelian group G and biadditive R-associative map $\varphi : M \times N \to G$ there exists a unique group morphism $\overline{\varphi}$ such that the following diagram commutes:



Indeed the quotient of the free $\mathbb{Z}$-module generated by $M \times N$ by the sub-group generated by the $(m+m') \otimes n - m \otimes n - m' \otimes n$, $m \otimes (n+n') - m \otimes n - m \otimes n'$, $mr \otimes n - m \otimes rn$ is such a group.

Proposition A.1.3. — *Let R_1 be a ring. If M is a R_1-R-bimodule, then $M \otimes_R N$ is a left R_1-module.*
Let R_2 be a ring. If N is a right R_2-module then $M \otimes_R N$ is a right R_2-module.
If both conditions are satisfied, then $M \otimes_R N$ is a R_1-R_2-bimodule.

Proof. Let $r \in R_1$. There is a map

$$\begin{array}{rccc} \varphi_r : & M \times N & \to & M \otimes_R N \\ & (m,n) & \mapsto & rm \otimes n. \end{array}$$

This map is biadditive: $\varphi_r(mr_1, n) = \varphi_r(m, r_1 n)$. Thus it induces a map $\varphi_r : M \otimes_R N \to M \otimes_R N$.
We deduce the following map:

$$\begin{array}{rccc} \cdot : & R_1 \times M \otimes_R N & \to & M \otimes_R N \\ & (r,m) & \mapsto & \varphi_r(m) \end{array}.$$

All that is left to do is to show that $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$ which is to say that $\varphi_{r_1 r_2} = \varphi_{r_1} \circ \varphi_{r_2}$.

$$\begin{aligned} \varphi_{r_1 r_2}(m,n) &= r_1 r_2 m \otimes n \\ &= \varphi_{r_1}(r_2 m \otimes n) \\ &= \varphi_{r_1}(\varphi_{r_2}(m,n)) \end{aligned}$$

The proof is the same for the right R_2-module structure. If both conditions are verified then it is easy to see that for any $r_1, r_2 \in R_1 \times R_2$,

$$(r_1 \cdot m) \cdot m_2 = r_1 \cdot (m \cdot r_2).$$

□

PROPOSITION A.1.4. — *Let R_1 and R_2 be two rings, M be a right R_1-module, N a R_1-R_2-bimodule and N' a left R_2-module. Then*

$$(M \otimes_{R_1} N) \otimes_{R_2} N' \simeq M \otimes_{R_1} (N \otimes_{R_2} N')$$

Proof. The proof is tedious but not hard. One must construct two morphism $(M \otimes_{R_1} N) \otimes_{R_2} N' \to (M \otimes_{R_1} (N \otimes_{R_2} N')$ and $M \otimes_{R_1} (N \otimes_{R_2} N') \to (M \otimes_{R_1} N) \otimes_{R_2} N'$. By universal property it will follow that the composition of the two maps is the identity. □

A.2 Morita's theorem

Let R be a ring (not necessarily commutative). We denote $P := R^n$. P has a natural $M_n(R)$-R-bimodule structure. We denote by $P^* := \mathrm{Hom}_R(P, R)$. P^* has a natural R-$M_n(R)$-bimodule structure.

REMARK A.2.1. — P^* is the set of morphism of right R-module from P to R while $M_n(R)$ can be seen as the set of endomorphism of P as a right R-module.

LEMMA A.2.2. —

$$P \otimes_R P^* \simeq M_n(R)$$

and

$$P^* \otimes_{M_n(R)} P \simeq R$$

Proof. We write $\pi_i : P \to R$ the projection on the i-th vector of the canonical basis. The first isomorphism is induced by the following application:

$$\begin{array}{rccc} \Phi : & P \times P^* & \to & M_n(R) \\ & (u, \varphi) & \mapsto & (\pi_i(u)\varphi(e_j))_{i,j} \end{array}$$

The induced morphism on $P \otimes_R P^*$ is surjective since the elementary matrix $E_{ij} = \Phi(e_i, e_j^*)$. It is now easy for any biadditive map $P \otimes P^* \to G$ to construct a morphism $M_n(R) \to G$ verifying the universal property of $P \otimes_R P^*$.

The second isomorphism comes from the map

$$\begin{array}{rccc} \Psi : & P^* \times P & \to & R \\ & (\varphi, u) & \mapsto & \varphi(u) \end{array}$$

Let us show that R verifies the universal property of the tensor product. Let G be an abelian group and $f : P^* \times P \to G$ be a biadditive and R-associative map. We define

$$\begin{array}{rccc} \overline{f} : & R & \to & G \\ & r & \mapsto & f(e_1^*, e_1 \cdot r) \end{array} .$$

Then $\overline{f} \circ \psi = f$. Indeed

$$\overline{f} \circ \Psi(\varphi, u) = f(e_1^*, e_1 \cdot \varphi(u))$$

Let $M \in M_n(R)$ such that $Me_j = e_1 \cdot \varphi(e_j)$.

$$\begin{aligned} f(e_1^*, e_1 \cdot \varphi(u)) &= f(e_1^*, M \cdot u) \\ &= f(e_1^* M, u) \end{aligned}$$

But $e_1^* M = \varphi$ so

$$\overline{f} \circ \Psi = f.$$

□

THEOREM A.2.3. — *The functors*

$$\begin{array}{rccc} F : & \mathbf{Mod}_R^g & \to & \mathbf{Mod}_{M_n(R)}^g \\ & X & \mapsto & P \otimes_R X \end{array}$$

and

$$\begin{array}{rccc} G : & \mathbf{Mod}_{M_n(R)}^g & \to & \mathbf{Mod}_R^g \\ & X & \mapsto & P^* \otimes_{M_n(R)} X \end{array}$$

are quasi-inverse of one another.

Proof. This is obvious from what precedes and the associativity of the tensor product. □

COROLLARY A.2.4. — *Let $D \subset R$ be a division algebra. F denote the same functor as in the previous theorem.*

i) Let M be a left R-module. Then $\dim_D F(M) = n \dim_D M$.

ii) Two $M_n(D)$-modules are isomorphic if and only if they have the same dimension as right D-modules.

Proof. i) For any left R-module, $R \otimes_R M \simeq M$. Thus $F(M) \simeq \bigoplus_{i=1}^{n} M$.

ii) If two left $M_n(D)$-modules are isomorphic then in particular, there are isomorphic as D-modules so they have the same dimension.
Conversely if M and N are two left $M_n(D)$-modules of same dimension, we write $F(M) = X_1$ and $F(N) = X_2$. Then $\dim_D M = n \dim_D X_1$ and $\dim_D N = n \dim_D X_2$.
Thus $\dim_D X_1 = \dim_D X_2$. It follows that $X_1 \simeq X_2$ so $M \simeq N$.

□

REMARK A.2.5. — The same things are true for right modules and bimodules.

Appendix B

Reminder: Places, Zeros and Poles in algebraic function field

The goal of this appendix is to recall some theory on places over algebraic function fields. The formalism we use is the one of [Sti08]. We refer to it for the missing proofs. The notions developed here are used to conceive an irreducibility test for differential operators of the form $N(\partial^p) \in C[\partial^p]$ where N is irreducible over N, and to compute solution of the p-Riccati equation in K_N.

B.1 General Notions

Definition B.1.1. — Let K be any field and F be a field extension of K. We say that F/K is an algebraic function field if and only if F contains an element x, transcendental over K such that F is algebraic over $K(x)$.

Example B.1.2. —

- $\mathbb{Q}(x)/\mathbb{Q}$ is an algebraic function field.
- In the context of our work we will study the algebraic function field $K_N/\mathbb{F}_p$. K_N is a separable finite extension over $\mathbb{F}_p(x)$ so $K_N/\mathbb{F}_p$ fits our definition of algebraic function fields.

Remark B.1.3. — The choice of the transcendental element x is not fixed. As such one could also see $K(x)$ as an algebraic extension of $K(x^2)$.
However, notice that $K(x, y)/K$, where x and y are independent variables, is never an algebraic function field no matter the choice of the transcendental element. This is because by definition an algebraic function field F/K is of transcendental degree 1 over K. Since $K(x, y)/K$ has two algebraically independent element over K, x and y, it is of transcendental degree 2.

Definition B.1.4. — A valuation ring of the algebraic function field F/K is a ring $\mathcal{O} \subset F$ such that:

- $K \subsetneq \mathcal{O} \subsetneq F$.
- For every $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Example B.1.5. — What motivates this definition is the observation that in $K(x)/K$, the following rings are valuation rings.

i) Let $P \in K[x]$ be an irreducible polynomial.

$$\mathcal{O}_P := \left\{ \frac{f}{g} \middle| (f,g) \in K[x]^2, P \nmid g \right\}.$$

ii)

$$\mathcal{O}_\infty := \left\{ \frac{f}{g} \middle| (f,g) \in K[x]^2, \deg(f) \leqslant \deg(g) \right\}.$$

We will show later that those are in fact the only valuation rings of $K(x)$.

Proof. Let P be an irreducible polynomial and $(f,g) \in K[x]^2$ such that $\frac{f}{g} \notin \mathcal{O}_P$. We can suppose that $\gcd(f,g) = 1$. Since $\frac{f}{g} \notin \mathcal{O}_P$ this means that $P \nmid f$ and $\frac{f}{g} \in \mathcal{O}_P$. Furthermore, since P is irreducible, $K[x]\backslash PK[x]$ is a multiplicative set. This means that $\mathcal{O}_P$ is indeed a subring of $K(x)$.

The fact that for any $(f,g) \in K[x]^2$ we either have $\frac{f}{g} \in \mathcal{O}_\infty$ or $\frac{g}{f} \in \mathcal{O}_\infty$ is obvious and it is easy to check that $\mathcal{O}_\infty$ is stable by addition and multiplication. □

Example B.1.6. — Let K be a field and $N \in K[x,y]$ be an irreducible polynomial. $F_N := {}^{K(x)[y]}/_{N(x,y)}$ is an algebraic function field over K. For any $(x_\alpha, y_\alpha) \in \mathbb{P}^2(K)$ such that $N(x_\alpha, y_\alpha) = 0$

$$\mathcal{O}_{x_\alpha, y_\alpha} := \{ f(x,y) | f(x,y) \in F_N^\times, f^{-1}(x_\alpha, y_\alpha) \neq 0 \} \cup \{0\}$$

defines a valuation ring.
Another way to think about $\mathcal{O}_{x_\alpha,y_\alpha}$ is that its the ring of regular functions over the curve defined by $N(x,y) = 0$, well defined in (x_α, y_α). When K is algebraically closed, those are the only valuation rings of F_N/K. This justify the later denomination of "places", since we can think of those as the points of a curve.

Proposition B.1.7. — *Let $\mathcal{O}$ be a valuation ring of the function field F/K. Then:*

i) $\mathcal{O}$ has a unique maximal ideal $\mathfrak{P} = \mathcal{O}\backslash\mathcal{O}^\times$.

ii) The field $\tilde{K} := \{x \in F | x$ is algebraic over $K\}$ is imbedded in $\mathcal{O}^\times \cup \{0\}$.

iii) $\tilde{K} \cap \mathfrak{P} = \{0\}$.

Proof. i) If $\mathcal{O}$ has a unique maximal ideal then it has to be $\mathcal{O}\backslash\mathcal{O}^\times$ since we know that any non invertible element is included in a maximal ideal. We only have to prove that $\mathfrak{P} := \mathcal{O}\backslash\mathcal{O}^\times$ is an ideal. Let $x \in \mathfrak{P}$ and $z \in \mathcal{O}$. If x is not invertible then neither is xz (otherwise x would have an inverse). Let now $x, y \in \mathfrak{P}$. We want to show that $x + y \in \mathfrak{P}$. Since $\mathcal{O}$ is a valuation ring, either $\frac{x}{y}$ or $\frac{y}{x}$ belong to $\mathcal{O}$. We can suppose that $\frac{x}{y} \in \mathcal{O}$. Thus $1 + \frac{x}{y} \in \mathcal{O}$ as well and $y(1 + \frac{x}{y}) = x + y \in \mathfrak{P}$. $\mathfrak{P}$ is thus stable by addition and multiplication by element of $\mathcal{O}$ and is an ideal of $\mathcal{O}$.

ii) Let $x \in F$ be algebraic over K. Then $x^{-1} \in K[x]$ and conversely $x \in K[x^{-1}]$ since x^{-1} is also algebraic over K. It follows that $K[x] = K[x^{-1}]$. Since $\mathcal{O}$ is a valuation ring we either have $x \in \mathcal{O}$ and $x^{-1} \in \mathcal{O}$. In both case $K[x] = K[x^{-1}] \subset \mathcal{O}$ and $x \in \mathcal{O}^\times \cup \{0\}$.

iii) This is immediate from what precedes.

□

Proposition B.1.8. — *Let $\mathcal{O}$ be a valuation ring of F/K and let $\mathfrak{P}$ be its maximal ideal.*

i) $\mathfrak{P}$ is a principal ideal.

ii) Let $\mathfrak{P} = t\mathcal{O}$. For all $z \in F^\times$ there exists a unique $n \in \mathbb{Z}$ and a unique $u \in \mathcal{O}^\times$ such that $z = t^n u$.

iii) $\mathcal{O}$ is a principal ideal domain.

Proof. The proof rely on the following fact:

Lemma B.1.9. — *Let $(x_i)_{i\in[\![1;n]\!]} \in \mathfrak{P}^n$ be a family of elements of P. If for any $i \in [\![1; n-1]\!]$, $x_i \in x_{i+1}P$ then $(x_i)_{i\in[\![1;n]\!]}$ is a $K(x_1)$-free family.*

In particular such a family cannot be of higher cardinality than $[F : K(x_1)]$ which is finite since $x_1 \in P$ is transcendental over K and F is of transcendental degree 1 over K.

i) Let us assume that $\mathfrak{P}$ is not principal and let $y_1 \in \mathfrak{P}$. By our assumption there is $y_2 \in \mathfrak{P}\backslash y_1\mathcal{O}$. This means that $\frac{y_2}{y_1} \notin \mathcal{O}$. But since $\mathcal{O}$ is a valuation ring $\frac{y_1}{y_2} \in \mathcal{O}$ and is not invertible so $\frac{y_1}{y_2} \in \mathfrak{P}$ which means that $y_1 \in y_2\mathfrak{P}$.
By induction we construct a sequence $(y_n)_{n\in\mathbb{N}} \in \mathfrak{P}^{\mathbb{N}}$ such that $y_n \in y_{n+1}\mathfrak{P}$. But according to Lemma B.1.9 such a sequence has to be finite which is a contradiction. Thus $\mathfrak{P}$ is principal.

ii) Let $t^n u = t^m v$ with $n, m \in \mathbb{Z}$ and $u, v \in \mathcal{O}^\times$. With no loss of generality we can suppose that $n \geqslant m$. Then $t^{n-m}u = v$. It follows that t^{n-m} is invertible so $n - m = 0$ and $u = v$.
Let us show that such a pair (n, u) always exists.
Let $z \in F$. We can show the result for z or z^{-1}. Since $\mathcal{O}$ is a valuation ring we can restrict ourselves to the case $z \in \mathcal{O}$. If $z \in \mathcal{O}^\times$ $z = z$ fits so we can suppose that $z \in \mathfrak{P}$.
We claim that $\{k \in \mathbb{N} | z \in t^k\mathcal{O}\}$ is finite. Indeed let $d = [F : K(z)]$. Then $x_1 = z$, $x_2 = t^d, \ldots, x_{d+1} = t$ is a family of elements of $\mathfrak{P}$ verifying $x_i \in x_{i+1}\mathfrak{P}$ so it is a free $K(z)$-family of cardinality $d + 1$ which is in contradiction with the definition of d.
Let $n := \max\{k \in \mathbb{N} | z \in t^k\mathcal{O}.\}$. Then $z = t^n u$ for some $u \in \mathcal{O}$. Since n is maximal, $u \notin \mathfrak{P}$ so $u \in \mathcal{O}^\times$.

iii) Let I be a nonzero ideal of $\mathcal{O}$. Let $n := \min\{k \in \mathbb{N} | t^k \in \mathcal{I}\}$. This n exists necessarily since if a is a nonzero element of I it is of the form $t^k u$ with $u \in \mathcal{O}^\times$ and $t^k = au^{-1} \in I$. Then we claim that $I = t^n\mathcal{O}$. The fact that $t^n\mathcal{O} \subset I$ is obvious since I is an ideal. Now let $a \in I$. There exists $(k, u) \in \mathbb{N} \times \mathcal{O}^\times$ such that $a = t^k u$. Since $t^k = au^{-1} \in I$ it follows that $k \geqslant n$ and $a \in t^n\mathcal{O}$.

The only thing left is to demonstrate Lemma B.1.9. Let $(x_i)_{i\in[\![1;n]\!]} \in \mathfrak{P}^n$ be such that $x_i \in x_{i+1}\mathfrak{P}$ and assume that it is $K(x_1)$-linearly dependent. Then there exists $(\varphi_i(x_1))_{i\in[\![1;n]\!]} \in K(x_1)^n$ such that

$$\sum_{i=1}^{n} \varphi_i(x_1)x_i = 0.$$

With no loss of generality we can suppose that all $\varphi_i(x_1) \in K[x_1]$ and furthermore that x_1 does not divide them all (or that $\varphi_i(0)$ is not equal to 0 for all i). Then we can set $j \in [\![1;n]\!]$ such $\varphi_j(0) \neq 0$ but $\varphi_i(0) = 0$ for all $i > j$. Then

$$\varphi_j(x_1)x_j = \sum_{i<j} \varphi_i(x_1)x_i + \sum_{i>j} \varphi_i(x_1)x_i.$$

But for all $i < j$ we have $x_i \in x_j\mathfrak{P}$, and for all $i > j$, $\varphi(x_1) \in x_1\mathcal{O}$ thus $\varphi_(x_1)x_i \in x_1\mathfrak{P} \subset x_j\mathfrak{P}$. It follows that $\varphi_j(x_1)x_j \in x_j\mathfrak{P}$. Thus $\varphi_j(x_1) \in \mathfrak{P}$ and again $\varphi_j(0) \in K \cap \mathfrak{P}$. But since $K \cap \mathfrak{P} = \{0\}$ we have a contradiction as per the definition of j.
Thus $(x_i)_{i\in[\![1;n]\!]}$ is $K(x_1)$-linearly independent □

We can now easily define the places of a algebraic function field and the valuations in those places.

Definition B.1.10. — Let $\mathfrak{P}$ be the unique maximal ideal of a valuation ring of F/K. We say that $\mathfrak{P}$ is a place of F/K (or a place of F). We denote by $\mathbb{P}_F$ the set of places of F.
Let $t \in \mathfrak{P}$ be such that $\mathfrak{P} = t\mathcal{O}$. Such an element t is called a prime element of $\mathfrak{P}$. For any $x \in F^\times$ there exists a unique $n \in \mathbb{Z}$ and $u \in \mathcal{O}^\times$ such that $x = t^n u$. We call that n the valuation of x in $\mathfrak{P}$, which we denote by $\nu_\mathfrak{P}(x)$.
If $x = 0$ then by convention we set $\nu_\mathfrak{P}(x) = \infty$.

The valuation $\nu_\mathfrak{P}$ is a valuation in the usual term, which is to say that it verifies the following conditions:

Definition B.1.11. — Let $\nu : F \to \mathbb{Z} \cup \{0\}$. We say that ν is a valuation if and only if:

i) $\nu(x) = \infty \Leftrightarrow x = 0$

ii) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F$.

iii) $\nu(x + y) \geqslant \min(\nu(x), \nu(y))$ for all $x, y \in F$.

iv) There exists $z \in F$ such that $z = 1$.

v) $\nu(a) = 0$ for all $a \in K$.

The fact that $\nu_\mathfrak{P}$ verifies (i), (iv) and (v) have already been shown previously. As for (ii), if $x = t^{\nu_\mathfrak{P}(x)}u$ and $y = t^{\nu_\mathfrak{P}(y)}v$ then $xy = t^{\nu_\mathfrak{P}(x)+\nu_\mathfrak{P}(y)}uv$. Finally, if we suppose that $\nu_\mathfrak{P}(x) \leqslant \nu_\mathfrak{P}(y)$ then $x + y = t^{\nu_\mathfrak{P}(x)}(u + t^{\nu_\mathfrak{P}(y)-\nu_\mathfrak{P}(x)}v)$. Since $a := u + t^{\nu_\mathfrak{P}(y)-\nu_\mathfrak{P}(x)}v \in \mathcal{O}$, its valuation in $\mathfrak{P}$ is positive which yields *(iii)*. Furthermore, when $\nu_\mathfrak{P}(x) \neq \nu_\mathfrak{P}(y)$, a has to be invertible otherwise u would belong in $\mathfrak{P}$. This yields the strict triangle inequality:

Proposition B.1.12. — *Let $\mathfrak{P}$ be a place of F/K. For any $x, y \in F$, if $\nu_\mathfrak{P}(x) \neq \nu_\mathfrak{P}(y)$ then*

$$\nu_\mathfrak{P}(x + y) = \min(\nu_\mathfrak{P}(x), \nu_\mathfrak{P}(y)).$$

The notion of valuation as in Definition B.1.11 is another way of defining the places of an algebraic function field as, if ν is a valuation over F/K then $\mathcal{O}_\nu := \{x \in F | \nu(x) \geqslant 0\}$ is a valuation ring of unique maximal ideal $\mathfrak{P}_\nu := \{x \in F | \nu(x) > 0\}$.
Then let $z \in F$ be such that $\nu(z) = 1$. z is a generator of $\mathfrak{P}_\nu$ and $\nu = \nu_{\mathfrak{P}_\nu}$. There is thus a bijection between valuations and valuation rings over F/K. In particular, all valuations of F/K verify Proposition .

Lemma B.1.13. — *Any valuation ring of F/K is a maximal proper subring of F.*

Proof. Let $\mathcal{O}$ be a valuation ring of F/K and $\mathfrak{P}$ be its unique maximal ideal. Let now $z \in F \backslash \mathcal{O}$. We want to show that $F = \mathcal{O}[z]$. Let $y \in F$. Since $z \notin \mathcal{O}$ there exists $k \in \mathbb{N}$ sufficiently large so that $\nu_{\mathfrak{P}}(yz^{-k}) \geqslant 0$, thus $y \in z^k\mathcal{O} \subset \mathcal{O}[z]$. □

The maximality of valuation rings allows us to conclude Example B.1.5:

Corollary B.1.14. — *The valuation rings presented in Example B.1.5 are the only valuation rings of $K(x)/K$.*

Proof. Let $\mathcal{O}$ be a valuation ring of $K(x)/K$ and $\mathfrak{P}$ be its unique maximal ideal.

- **1st case**: $x \notin \mathcal{O}$. Then $\nu_{\mathfrak{P}}(x) < 0$ and for all $Q \in K[x]$, $\nu_{\mathfrak{P}}(g) = \nu_{\mathfrak{P}}(x)\deg(g)$. It follows that for any $f, g \in K[x]$, $\frac{f}{g} \in \mathcal{O}$ if and only if $\deg(g) \geqslant \deg(f)$. Thus $\mathcal{O} = \mathcal{O}_\infty$.
- **2nd case**: $x \in \mathcal{O}$. Then $K[x] \subset \mathcal{O}$. Let $I = \mathfrak{P} \cap K[x]$. I is an ideal of $K[x]$ so it is of the form $PK[x]$ for some $P \in K[x]$. Furthermore P is irreducible. Indeed if P isn't then at least one of its irreducible factors P_1 must have a valuation in $\mathfrak{P}$ strictly positive and so belongs in I. But then $P_1K[x] \subset PK[x] \subset P_1K[x]$ so P must be equal to P_1.
  Let $f, g \in K[x]$ be such that $P \nmid g$. Then $g \in \mathcal{O}^\times$ so $\frac{f}{g} \in \mathcal{O}$. It follows that $\mathcal{O}_P \subset \mathcal{O}$. Since we have shown that $\mathcal{O}_P$ is a valuation ring, it is a maximal proper subring so we must have $\mathcal{O} = \mathcal{O}_P$.

□

We can now define the zeros and poles of an algebraic function.

Definition B.1.15. — Let $f \in F$ and $\mathfrak{P}$ be a place of F/K. We say that

- $\mathfrak{P}$ is a zero of f if and only if $\nu_{\mathfrak{P}}(f) > 0$.
- $\mathfrak{P}$ is a pole of f if an only if $\nu_{\mathfrak{P}}(f) < 0$.

As is the case for rational functions in $K(x)/K$, "non constant" functions (that is to say, transcendental element of F over K) always have at least one zero and one pole. To show it we demonstrate a stronger result.

Proposition B.1.16. — *Let $K \subsetneq R \subsetneq F$ be a ring and $\{0\} \subsetneq I \subsetneq R$ be a proper ideal of R. There exists a valuation ring $\mathcal{O}$ of unique maximal ideal $\mathfrak{P}$ such that $R \subset \mathcal{O}$ and $I \subset \mathfrak{P}$.*

Proof. Let

$$\mathcal{F} := \{S | S \text{ is a subring of } F,\ R \subset S \text{ and } IS \neq S\}$$

.
$\mathcal{F}$ is not empty, as it contains R. Furthermore, we claim that it is inductively ordered by inclusion. Indeed, if $\mathcal{F}'$ is a totally ordered subset of $\mathcal{F}$ then

$$T = \bigcup_{S \in \mathcal{F}'} S$$

is a subring of F containing R. Furthermore $IT \neq T$. Indeed if such was the case then there would be $(i_1, \ldots, i_n) \in I^n$ and $(t_1, \ldots, t_n) \in T^n$ such that

$$1 = \sum_{k=1}^{n} i_k t_k.$$

But since $\mathcal{F}'$ is partially ordered, all the t_k would belong to some $S \in \mathcal{F}'$ and so we would have $IS = S$ which is impossible, thus $IT \neq T$ and $T \in \mathcal{F}$.
Since $\mathcal{F}$ is inductively ordered by inclusion it contains a maximal element $\mathcal{O} \subset F$. We want to show that $\mathcal{O}$ is a valuation ring.
Suppose that there is $z \in F \backslash \mathcal{O}$ such that $z^{-1} \notin \mathcal{O}$. Then but maximality of $\mathcal{O}$ in $\mathcal{F}$, $I\mathcal{O}[z] = \mathcal{O}[z]$ and $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Thus there exists n and $m \in \mathbb{N}$ (we can take them minimal) and $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ such that

$$1 = a_0 + a_1 z + \ldots + a_n z^n$$
$$1 = b_0 + b_1 z^{-1} + \ldots + b_m z^{-m}.$$

With no loss of generality, we can suppose that $m \leqslant n$. Thus

$$1 - b_0 = (1 - b_0)(a_0 + a_1 z + \ldots + a_n z^n) = (1 - b_0)a_0 + \ldots (1 - b_0)a_n z^n$$

and

$$a_n z^n = a_n z^n (b_0 + \ldots + b_m z^{-m})$$

which is to say that

$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \ldots b_m a_n z^{n-m}.$$

Since all the terms of those equalities are in $I\mathcal{O}$, summing the two equalities yields

$$1 = c_0 + c_1 z + \ldots + c_{n-1} z^{n-1}$$

with the $c_i \in I\mathcal{O}$, contradicting the minimality of n.

Thus $\mathcal{O}$ is a valuation ring. Since $I\mathcal{O} \neq \mathcal{O}$ it is included in its maximal ideal $\mathfrak{P}$ and $I \subset I\mathcal{O} \subset \mathfrak{P}$. □

Corollary B.1.17. — *Any transcendental element z of F has at least one zero or one pole.*

Proof. This is immediate by applying the previous proposition to $R = K(z)$ and $I = zK(z)$ to find a zero. A pole of z is a zero of z^{-1} which is also transcendental. □

Places are not all of equal "importance" so to say. For example let us consider the algebraic function field $K(x)/K$ and $P \in K[x]$. Any $x_\alpha \in K$ such that $P(x_\alpha) = 0$ defined a zero of P as $\nu_{x-x_\alpha}(P) > 0$. We know that if K is algebraically closed, then all the zeros of P are of this form. Thus to one zero of P corresponds one root of P in K.
However if K is not algebraically closed then P can be a multiple of an irreducible polynomial P_1 of higher degree and P_1 would thus be a zero of P which correspond this time to $\deg(P_1)$ roots (counted with multiplicity) of P in an algebraic closure $\tilde{K}$ of K.
This motivates the following notion of degree of a place.

Definition-Proposition B.1.18. — *Let $\mathfrak{P} \in \mathbb{P}_F$ and $\mathcal{O}$ be the associated valuation ring. $F_{\mathfrak{P}} := {}^{\mathcal{O}}/_{\mathfrak{P}}$ is a finite field extension of K called the residue class field of F in $\mathfrak{P}$.*
We define the degree of $\mathfrak{P}$ as

$$\deg(\mathfrak{P}) = [F_{\mathfrak{P}} : K].$$

For any $z \in \mathfrak{P}$, $\deg(\mathfrak{P}) \leqslant [F : K(z)]$. For any $f \in \mathcal{O}$ we write $f(\mathfrak{P})$ the image of $f \in F_{\mathfrak{P}}$.

Proof. Let $z \in \mathfrak{P}$. Let $(z_1, \cdots, z_n) \in \mathcal{O}^n$. We claim that if the family $(z_1, \ldots, z_n)$ is linearly dependent over $K(z)$ then $(z_1(\mathfrak{P}), \ldots, z_n(\mathfrak{P}))$ is linearly dependent over K. Indeed, if there is a family $(\varphi_i)_{i\in[\![1;n]\!]} \in K(z)^n$ not all equal to zero such that

$$\sum_{i=1}^{n} \varphi_i(z) z_i = 0$$

then with no loss of generality we can suppose that the φ_i are polynomial and that at least one of them as a nonzero constant coefficient. It follows that the $\varphi_i(z)(\mathfrak{P}) \in K$ are not all equal to zero and

$$\sum_{i=1}^{n} \varphi_i(z)(\mathfrak{P}) z_i(\mathfrak{P}) = 0.$$

In particular if $(\overline{z_1}, \ldots, \overline{z_n}) \in F_{\mathfrak{P}}^n$ is a family of cardinality strictly higher than $[F : K(z)]$ then it is K-linear dependent.
Thus $[F_{\mathfrak{P}} : K] \leqslant [F : K(z)]$. □

Remember that the goal of this section is to develop a method to solve the p-Riccati equation in K_N,

$$b^{(p-1)} + b^p = y_N$$

by comparing the poles of an hypothetical solution to those of y_N. The following result ensure that those are always finitely many poles to consider. This is consistent with what we already know of the zeros and poles of rational functions.
The proof depends heavily on a result called the Weak Approximation Theorem. While this result is important to the general theory of algebraic function field, we will not be using this result directly for our purpose. Thus we choose to refer to [Sti08, Corollary 1.3.4] for the proof of the following proposition.

Proposition B.1.19. — *Any element of F only has a finite number of poles and zeros.*

Notation B.1.20. From now on if $\mathfrak{P}$ is a place of some algebraic function F/K then $\mathcal{O}_{\mathfrak{P}}$ will designate its associated valuation field and $t_{\mathfrak{P}}$ will designate a prime element of $\mathfrak{P}$.

B.2 Places and algebraic field extension

As previously mentioned, the algebraic function fields that we will consider don't exist in a vacuum but are separable extension of $\mathbb{F}_p(x)$. In this part we explore how places behave through algebraic function field extensions. We also suppose that for any algebraic function field of the form F/K considered from now on, K is its own integral closure in F.

Let F/K and F'/K' be algebraic function fields such that F' and K' are algebraic (finite) field extensions of F and K respectively.

Definition B.2.1. — i) An algebraic function field F'/K' is called an algebraic extension of F/K if and only if F' is an algebraic extension of F' and $K \subset K'$.

ii) An algebraic extension F'/K' of F/K is called a constant field extension if and only if $F' = FK'$.

iii) An algebraic extension F'/K' of F/K is called finite if $[F' : F] < \infty$.

Remark B.2.2. — An algebraic function field extension F'/K' of F/K is actually finite if and only if $[K' : K] < \infty$. Indeed, if $[F' : F] < \infty$ then F'/K can be considered as an algebraic function field. Then K' is included in the field of elements of F that are algebraic over K. In particular it is a subfield of any $F'_{\mathfrak{P}}$ for any place $\mathfrak{P}$ of F'/K, which is finite dimensional over K.
Conversely, if $[K'/K] < \infty$ then any element x transcendental over K is also transcendental over K'. It follows that $[F' : K'(x)] < \infty$. But as $K'(x) = K(x) \otimes_K K'$ we also have $[K'(x) : K(x)] = [K' : K]$. Thus $[F' : F] \leqslant [F' : K(x)] = [F' : K'(x)][K'(x) : K] < \infty$.

In particular, any algebraic function field extension F'/K' of F/K can be decomposed as the combination of the constant field extension FK'/K' of F/K and the finite field extension F'/FK' of FK'/K'.

Definition B.2.3. — Let F'/K' be an algebraic extension of F/K. A place $\mathfrak{P}'$ of F' is said to lie over a place $\mathfrak{P}$ of F if and only if $\mathfrak{P} \subset \mathfrak{P}'$. We write $\mathfrak{P}'|\mathfrak{P}$.

Proposition B.2.4. — *Let F'/K' be an algebraic extension of F/K. Let $\mathfrak{P}' \in \mathbb{P}'_F$ and $\mathfrak{P} \in \mathbb{P}_F$ and $\mathcal{O}_{\mathfrak{P}'}$ and $\mathcal{O}_{\mathfrak{P}}$ be their respective associated valuation rings. The following assertions are equivalent:*

i) $\mathfrak{P}'|\mathfrak{P}$.

ii) $\mathcal{O}_{\mathfrak{P}} \subset \mathcal{O}_{\mathfrak{P}'}$

iii) There exists $e \in \mathbb{N}^*$ such that for all $f \in F$,

$$\nu_{\mathfrak{P}'}(f) = e \cdot \nu_{\mathfrak{P}}(f).$$

Proof. Let us suppose that $\mathfrak{P}'|\mathfrak{P}$ and suppose that there exists $u \in \mathcal{O}_{\mathfrak{P}} \backslash \mathcal{O}_{\mathfrak{P}'}$. Then $u \notin \mathfrak{P}$ otherwise u would belong in $\mathfrak{P} \subset \mathfrak{P}' \subset \mathcal{O}_{\mathfrak{P}'}$. Thus $\nu_{\mathfrak{P}}(u) = 0$. Let $e := \nu_{\mathfrak{P}'}(t_{\mathfrak{P}})$. Then

$$\nu_{\mathfrak{P}}(u^e t_{\mathfrak{P}}) = e \cdot \nu_{\mathfrak{P}}(u) + \nu'_{\mathfrak{P}}(t_{\mathfrak{P}}) = 1.$$

But

$$\nu_{\mathfrak{P}'}(u^e t_{\mathfrak{P}}) = e\nu_{\mathfrak{P}'}(u) + \nu_{\mathfrak{P}'}(t_{\mathfrak{P}}) \leqslant -e + e = 0.$$

Thus $u^e t_{\mathfrak{P}} \in \mathfrak{P} \backslash \mathfrak{P}' = \varnothing$ which is a contradiction.
Thus $\mathfrak{P} \subset \mathfrak{P}' \Rightarrow \mathcal{O}_{\mathfrak{P}} \subset \mathcal{O}_{\mathfrak{P}'}$.

Let us now suppose that $\mathcal{O}_{\mathfrak{P}} \subset \mathcal{O}_{\mathfrak{P}'}$. We claim that $t_{\mathfrak{P}} \in \mathfrak{P}'$. Indeed, $\mathcal{O}_{\mathfrak{P}}^{\times} \subset \mathcal{O}_{\mathfrak{P}'}^{\times}$ and if $t_{\mathfrak{P}}$ was not an element of $\mathfrak{P}'$ then so too would it be invertible in $\mathcal{O}_{\mathfrak{P}'}$. It would result that $F^{\times} \subset \mathcal{O}_{\mathfrak{P}'}^{\times}$

and F would be imbedded in $F'_{\mathfrak{P}'}$. However $F'_{\mathfrak{P}'}$ is algebraic over K which is a contradiction.

Let $e := \nu_{\mathfrak{P}'}(t_{\mathfrak{P}})$. Then for any $f \in F$ there exists $u \in \mathcal{O}_{\mathfrak{P}}^{\times} \subset \mathcal{O}_{\mathfrak{P}'}^{\times}$ such that $f = t_{\mathfrak{P}}^{\nu_{\mathfrak{P}}(f)}u$. But then

$$\nu_{\mathfrak{P}'}(f) = \nu_{\mathfrak{P}}(f)\nu_{\mathfrak{P}'}(t_{\mathfrak{P}}) + \nu_{\mathfrak{P}'}(u) = e\nu_{\mathfrak{P}}(f).$$

Finally let us suppose that there exists $e \in \mathbb{N}^*$ such that for any $f \in F$, $\nu'_{\mathfrak{P}}(f) = e\nu_{\mathfrak{P}}(f)$. Then if $f \in \mathfrak{P}$, $\nu_{\mathfrak{P}}(f) > 0$, thus $\nu_{\mathfrak{P}'}(f) = e\nu_{\mathfrak{P}}(f) > 0$ and $f \in \mathfrak{P}'$. It follows that $\mathfrak{P} \subset \mathfrak{P}'$. □

Proposition B.2.5. — *Let F'/K' be an algebraic extension of F/K.*

- *For each place $\mathfrak{P}' \in \mathbb{P}'_F$ there exists a unique place $\mathfrak{P} \in \mathbb{P}_F$ such that $\mathfrak{P}'|\mathfrak{P}$*
- *For each place $\mathfrak{P} \in \mathbb{P}_F$ there is at least one, and finitely many places $\mathfrak{P}' \in \mathbb{P}'_F$ such that $\mathfrak{P}'|\mathfrak{P}$.*

Proof.
- $\mathcal{O} := \mathcal{O}_{\mathfrak{P}'} \cap F$ is a valuation ring. It is obvious that for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. We have to show that $\mathcal{O} \subsetneq F$. But if we had $\mathcal{O} = F$ then for any valuation ring $\mathcal{O}_{\mathfrak{P}}$ of F we would have $\mathcal{O}_{\mathfrak{P}} \subset \mathcal{O}_{\mathfrak{P}'}^{\times}$. It follows that for any element f of F and any place $\mathfrak{P}$ of f, $\nu_{\mathfrak{P}}(f) = e^{-1}\nu_{\mathfrak{P}'}(f) = 0$ for some $e \in \mathbb{N}^*$ which is a contradiction since transcendental element of F have at least one pole and one zero.
- $t_{\mathfrak{P}}$ is a transcendental element over K' as such it has at least one and finitely many zeros.

□

Definition B.2.6. — Let F'/K' be an algebraic extension of F/K and let $\mathfrak{P}' \in \mathbb{P}'_F$ be lying over $\mathfrak{P} \in \mathbb{P}_F$. The integer $e \in \mathbb{N}^*$ such that for all $f \in F$, $\nu'_{\mathfrak{P}}(f) = e \cdot \nu_{\mathfrak{P}}(f)$ is called the ramification index of $\mathfrak{P}'$ over $\mathfrak{P}$ and is denoted by $e(\mathfrak{P}'|\mathfrak{P})$.
We say that $\mathfrak{P}'$ is ramified if and only if $e(\mathfrak{P}'|\mathfrak{P}) > 1$.

[Sti08, Corollary 3.5.5] states, among other things, the following result.

Proposition B.2.7. — *Any algebraic function field extension only has a finite number of ramified places.*

The finiteness of the set of ramified places of an algebraic function field extension is a very important property for our work. This is because the relations between valuations and derivation are harder to control in those places. A consequence is that all the solutions of the p-Riccati equation over K_N could have a pole in any ramified place of K_N. Fortunately, those are only finitely many places to check.

We can now explore the relations between derivation and valuations.

Proposition B.2.8. — *Let F'/K' be an separable extension of $\mathbb{F}_p(x)/\mathbb{F}_p$. Let $\mathfrak{P}$ be a place of F' and $f \in F'$. Let $t \in F'$ be a prime element of $\mathfrak{P}$.*

1. *$\nu_{\mathfrak{P}}(f') \geqslant \nu_{\mathfrak{P}}(f) + \nu_{\mathfrak{P}}(t') - 1$ with it being an equality if and only if $p \nmid \nu_{\mathfrak{P}}(f)$.*

2. *Let e be the ramification index of $\mathfrak{P}$.*

- *if* $\mathfrak{P} \nmid \mathfrak{P}_\infty$, $\nu_{\mathfrak{P}}(t') - 1 \leqslant -e$.
- *if* $\mathfrak{P}[\mathfrak{P}_\infty$, $\nu_{\mathfrak{P}}(t') - 1 \leqslant e$

Both are equalities if and only if $p \nmid e$. *Furthermore* p *never divides* $\nu_{\mathfrak{P}}(t') - 1$.

3. *If* $\mathfrak{P}$ *is not a ramified place and* $p \nmid \nu_{\mathfrak{P}}(f)$ *then:*

- *if* $\mathfrak{P} \nmid \mathfrak{P}_\infty$, $\nu_{\mathfrak{P}}(f') = \nu_{\mathfrak{P}}(f) - 1$
- *if* $\mathfrak{P}|\mathfrak{P}_\infty$, $\nu_{\mathfrak{P}}(f') = \nu_{\mathfrak{P}}(f) + 1$.

4. *If* $\mathfrak{P}$ *is not ramified and* $\mathfrak{P}$ *is not a pole of* f *then* $\mathfrak{P}$ *is not a pole of* f'.

Proof. 1. Assume for now that $\deg(\mathfrak{P}) = 1$. Then according to [Sti08, Theorem 4.2.6], F' is imbedded in $K'((t))$. Thus there exists $(a_i)_{i\in\mathbb{Z}} \in K^{\mathbb{Z}}$ such that

$$f = \sum_{i=\nu_{\mathfrak{P}}(f)}^{\infty} a_i t^i.$$

Thus

$$f' = t' \frac{\mathrm{d}}{\mathrm{d}t}\left(\sum_{i=\nu_{\mathfrak{P}}(f)}^{\infty} a_i t^i\right) = t' \sum_{i=\nu_{\mathfrak{P}}(f)}^{\infty} i a_i t^{i-1}.$$

$\nu_{\mathfrak{P}}(\sum_{i=\nu_{\mathfrak{P}}(f)}^{\infty} i a_i t^i) \geqslant \nu_{\mathfrak{P}}(f) - 1$ with it being an equality if and only if $p \nmid \nu_{\mathfrak{P}}(f)$. The result follows.

If $\deg(\mathfrak{P}) \neq 1$ then there exists an algebraic extension K'' of K' such that all places of $F'K''$ lying over $\mathfrak{P}$ are of degree 1. Let $\mathfrak{P}'|\mathfrak{P}$ in $F'K''$. Then ([Sti08, Theorem 3.6.3]) for all $g \in F'$ we have

$$\nu_{\mathfrak{P}'}(g) = \nu_{\mathfrak{P}}(g)$$

and we can apply the result for places of degree 1.

2. • Since F'/K' is an algebraic extension of $\mathbb{F}_p(x)/\mathbb{F}_p$ and $\mathfrak{P} \nmid \mathfrak{P}_\infty$, there exists $P \in \mathbb{F}_p[x]$ an irreducible polynomial such that $\mathfrak{P}|P$. Then

$$\nu_{\mathfrak{P}}(P) = e$$

and

$$\nu_{\mathfrak{P}}(P') = 0 = \nu_{\mathfrak{P}}(t') + \nu_{\mathfrak{P}}\left(\frac{\mathrm{d}P}{\mathrm{d}t}\right).$$

Furthermore $\nu_{\mathfrak{P}}\left(\frac{\mathrm{d}P}{\mathrm{d}t}\right) \geqslant e - 1$ so

$$0 = \nu_{\mathfrak{P}}(t') + \nu_{\mathfrak{P}}\left(\frac{\mathrm{d}P}{\mathrm{d}t}\right) \geqslant \nu_{\mathfrak{P}}(t') - 1 + e.$$

The result follows. Furthermore $\frac{\mathrm{d}P}{\mathrm{d}t} = e - 1$ if and only if $p \nmid e$.

We also see that

$$\nu_{\mathfrak{P}}(t') - 1 \equiv -1 - \nu_{\mathfrak{P}}\left(\frac{\mathrm{d}P}{\mathrm{d}t}\right) \mod p.$$

Thus for p to divide $\nu_{\mathfrak{P}}(t') - 1$ we would need $\nu_{\mathfrak{P}}\left(\frac{\mathrm{d}P}{\mathrm{d}t}\right) \equiv -1 \mod p$ which is impossible.

- If now $\mathfrak{P}|\mathfrak{P}_\infty$ then we have
$$\nu_{\mathfrak{P}}\left(\frac{1}{x}\right) = e$$
and
$$\nu_{\mathfrak{P}}(-1/x^2) = 2e = \nu_{\mathfrak{P}}(t') + \nu_{\mathfrak{P}}\left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{x}\right).$$
Furthermore $\nu_{\mathfrak{P}}\left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{x}\right) \geqslant e-1$ so
$$2e = \nu_{\mathfrak{P}}(t') + \nu_{\mathfrak{P}}\left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{x}\right) \geqslant \nu_{\mathfrak{P}}(t') + e - 1.$$
The result follows. Furthermore $\frac{\mathrm{d}P}{\mathrm{d}t} = e-1$ if and only if $p \nmid e$. In this case it is obvious that p doesn't divide $\nu_{\mathfrak{P}}(t') - 1 = e$.

  If $p|e$ however we have
$$\nu_{\mathfrak{P}}(t') - 1 \equiv -1 - \nu_{\mathfrak{P}}\left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{x}\right) \mod p$$
and the same argument as for $\mathfrak{P} \nmid \mathfrak{P}_\infty$ applies.

3. This is a direct consequence of the previous propositions in the case $e = 1$.

4. If $\mathfrak{P}$ is not a pole of f then $\nu_{\mathfrak{P}}(f) \geqslant 0$. If $\nu_{\mathfrak{P}}(f) \geqslant 1$ then $\nu_{\mathfrak{P}}(f') = \nu_{\mathfrak{P}}(f) - 1 \geqslant 0$. If $\nu_{\mathfrak{P}}(f) = 0$ then $p|\nu_{\mathfrak{P}}(f)$ and
$$\nu_{\mathfrak{P}}(f') \geqslant \nu_{\mathfrak{P}}(f) + \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) = \nu_{\mathfrak{P}}(f) = 0.$$

□

B.3 Divisors and Riemann-Roch spaces

Finally we need to introduce two very important results for solving the p-Riccati equation that is to say Riemann-Roch spaces and the Picard group, or divisor class group, of K_N. Both of those objects requires that we first introduce the formalism of divisors on K_N.

Definition B.3.1. — Let F/K be an algebraic function field. The group of divisor of F, $\mathrm{Div}(F)$, is the free group generated by $\mathbb{P}_F$. In other words a divisor is a formal sum
$$D = \sum_{\mathfrak{P}\in\mathbb{P}_F} n_{\mathfrak{P}}\mathfrak{P}$$
with $n_{\mathfrak{P}} \in \mathbb{Z}$ being almost all (but a finite number) equal to zero.

Definition B.3.2. — A divisor $D \in \mathrm{Div}(F)$ is called effective if and only if $D \geqslant 0$.

Example B.3.3. — Let F/K be an algebraic function field. We know that any $f \in F^\times$ has finitely many zero and poles. It follows that
$$(f) := \sum_{\mathfrak{P}\in\mathbb{P}_F} \nu_{\mathfrak{P}}(f)\cdot\mathfrak{P}$$

is a divisor of F which we call the principal divisor of f. We can also define the divisor of zeros and poles of f, respectively:

$$(f)_+ := \sum_{\mathfrak{P}\in \mathrm{Zeros}(f)} \nu_{\mathfrak{P}}(f)\cdot P$$

and

$$(f)_- := \sum_{\mathfrak{P}\in \mathrm{Poles}(f)} -\nu_{\mathfrak{P}}(f)\cdot P.$$

This example actually defines a interesting class of divisors of F called principal divisors which will play an important role in our work.

Definition B.3.4. — We say that a divisor D over F is principal if and only if there exists $f \in F$ such that $D = (f)$.

We denote $\mathrm{Princ}(F)$ the set of principal divisor of F. It is a subgroup of $\mathrm{Div}(F)$.

Notice that if $f \in F$, then its valuation in a place $\mathfrak{P}$ can be read on the corresponding coefficients of (f). This motivates the following generalisation:

Definition B.3.5. — Let F/K be an algebraic function field and $D = \sum_{\mathfrak{P}\in\mathbb{P}_F} n_{\mathfrak{P}}\mathfrak{P}$ be a divisor over F. For all $\mathfrak{P} \in \mathbb{P}_F$,

$$\nu_{\mathfrak{P}}(D) := n_{\mathfrak{P}}.$$

Furthermore we can now define the degree of a divisor.

Definition B.3.6. — Let F/K be an algebraic function field and $D \in \mathrm{Div}(F)$.

$$\deg(D) = \sum_{\mathfrak{P}\in\mathbb{P}_F} \nu_{\mathfrak{P}}(D)\cdot \deg(\mathfrak{P}).$$

An important property of principal divisor is that all principal divisors have the same degree as stated in the following proposition:

Proposition B.3.7. — *Let F/K be an algebraic function field. For all $f \in F^\times$,*

$$\deg\,(f)_+ = \deg\,(f)_- = [F : K(f)]$$

and

$$\deg\,(f) = 0.$$

Proof. This is a direct consequence of [Sti08, Theorem 1.4.11]. □

Notation B.3.8. We denote by $\mathrm{Div}^0(F)$ the subgroup of $\mathrm{Div}(F)$ formed by the divisors of degree 0.

Definition B.3.9. — Let F/K be an algebraic function field. We define the divisor class group of F as $\mathrm{Cl}(F) := {}^{\mathrm{Div}(F)}/_{\mathrm{Princ}(F)}$. We also define $\mathrm{Cl}^0(F) := {}^{\mathrm{Div}^0(F)}/_{\mathrm{Princ}(F)}$.
We will also refer to those groups as the Picard group and Picard 0 group of F respectively.

For two divisors $D, D' \in \mathrm{Div}(F)$ we say that

$$D \sim D'$$

if and only if their classes in $\mathrm{Cl}(F)$ are equal ie if there exists $f \in F$ such that

$$D = (f) + D'.$$

We will use $\mathrm{Cl}^0(K_N)$ to mesure how close or how far a given divisor is from being a principal element. An most important property of Cl^0 is the following:

Proposition B.3.10. — *Let $F/\mathbb{F}_q$ be an algebraic function field over some finite constant field. Then $\mathrm{Cl}^0(F)$ is a finite group and $\mathrm{Cl}(F) \simeq \mathbb{Z} \times \mathrm{Cl}^0(F)$*

Proof. The fact that $\mathrm{Cl}^0(F)$ is a finite group can be found in [Sti08, Proposition 5.1. 3]. Let now $\eta = \min\{\deg(D) | D \in \mathrm{Div}(F)\} \cap \mathbb{N}^*$ and $\mathfrak{O} \in \mathrm{Div}(F)$ such that $\deg \mathfrak{O} = \eta$. Then for any divisor $D \in \mathrm{Div}(F)$, $\eta | \deg D$. Indeed if that was not the case then there would exists $u, v \in \mathbb{Z}$ such that $0 < \deg(uD + v\mathfrak{O}) < \eta$ which is a contradiction.
We claim that

$$\begin{array}{rccc} \varphi : & \mathbb{Z} \times \mathrm{Cl}^0(F) & \to & \mathrm{Cl}(F) \\ & (n, D) & \mapsto & n\mathfrak{O} + D \end{array}$$

is an isomorphism. It is injective since $\varphi(n, D) = 0$ implies $\deg(n\mathfrak{O}+D) = 0$ and since $\deg(D) = 0$ it follows that $n = 0$ and thus $D = 0$. It is furthermore surjective since if $D \in \mathrm{Cl}(F)$ then $D = \varphi(\frac{\deg(D)}{\eta}, D - \deg D\eta\mathfrak{O})$. □

This proposition allows us to "bound", in a sense, how far any divisor can be from being principal.

We now introduce the second important tool of the resolution of the p-Riccati equation: Riemann-Roch spaces. For that purpose it is important to note that $\mathrm{Div}(F)$ is a partially ordered set.

Definition B.3.11. — Let F/K be an algebraic function field and $D, D' \in \mathrm{Div}(F)$. $D \leqslant D'$ if and only if

$$\nu_{\mathfrak{P}}(D) \leqslant \nu_{\mathfrak{P}}(D').$$

for all $\mathfrak{P} \in \mathbb{P}_F$.

Definition B.3.12. — Let F/K be an algebraic function field and $A \in \mathrm{Div}(F)$. We define the Riemann-Roch space associated to A by

$$\mathcal{L}(A) := \{x \in F | (x) \geqslant -A\} \cup \{0\}.$$

For all $A \in \mathrm{Div}(F)$, $\mathcal{L}(A)$ is a $\tilde{K}$-vector space, where $\tilde{K}$ is the field of all K-algebraic elements in F.

Theorem B.3.13 (Riemann-Roch). — *For all $A \in \mathrm{Div}(F)$:*

- *If $\deg(A) \geqslant 0$ then $\dim_{\tilde{K}}(\mathcal{L}(A)) \leqslant \deg(A) + 1$.*
- *If $\deg(A) < 0$ then $\mathcal{L}(A) = \{0\}$.*

Proof. For the second point, see [Sti08, Corollary 1.4.12].
According to [Sti08, Proposition 1.4.9], the first point holds if $A \geqslant 0$. If this is not the case then we can assume that $\mathcal{L}(A) \neq \{0\}$. Then there exists $g \in \mathcal{L}(A) \backslash \{0\}$ which means that $(g) \geqslant -A$ and $A+(g) \geqslant 0$. Then $\mathcal{L}(A+(g)) = g^{-1}\mathcal{L}(A)$ so $\dim \mathcal{L}(A) = \dim \mathcal{L}(A+(g)) \leqslant \deg(A+(g))+1 = \deg(A) + 1$. □

REMARK B.3.14. — It can in fact be shown ([Sti08, Theorem 1.5.17]) that if A is a divisor of degree higher than $2g-1$ (with g being the genus of F/K) then

$$\dim_{\tilde{K}}(\mathcal{L}(A)) = \deg(A) + 1 - g.$$

This will be useful later for complexity analysis.

We introduce one last notation to denote the set of places for which a divisor's valuation is not zero.

DEFINITION B.3.15. — For any $D \in \mathrm{Div}(F)$ we define the support of D as

$$\mathrm{supp}(D) := \{\mathfrak{P} \in \mathbb{P}_F | \nu_{\mathfrak{P}}(D) \neq 0\}.$$

B.4 Representations of places and algorithmic aspects

B.4.1 Places and prime ideals of integral closure

DEFINITION B.4.1. — An integral domain A is called a Dedekind ring if it is Noetherian and integrally closed and if every non-zero prime ideal of A is maximal.

EXAMPLE B.4.2. —

- Any principal domain is a Dedekind ring.
- In particular, if F is an algebraic function field and $\mathcal{O}$ is a valuation ring of F, then $\mathcal{O}$ is a Dedekind domain.
- [Sam70, Theoreme I Section 3.4] If A is a Dedekind ring, K is its fraction field and L is a finite separable extension of K, then the integral closure of A in L is a Dedekind ring.

DEFINITION B.4.3. —

- Let A be an integral domain and K be its fraction field. A A-module I of K is called a fractional ideal of A if and only if there exists $a \in A$ such that aI is an ideal of A.
- Let A be an integral domain and I, I' be two fractional ideal of A. Then

  $$II' = \Big\{ \sum_{\text{finite}} s_i s_i' \,|\, (s_i, s_i') \in I \times I' \Big\}$$

  is a fractional ideal of A. This operation provides the set of fractional ideal of A with a monoid structure.
- A fractional ideal I of A is said to be invertible if there exists I' a fractional ideal of A such that $II' = A$.

THEOREM B.4.4. — *[Sam70, Théorème 2 section 3.4] Let A be a Dedekind ring. Every maximal ideal of A is invertible.*

THEOREM B.4.5. — *[Sam70, Théorème 3 section 3.4] Let A be a Dedekind ring and let P be the set of non-zero prime ideals of A. Then*

- *Every non-zero fractional ideal $\mathfrak{b}$ of A can be uniquely written*

  $$\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$$

  where for any $\mathfrak{p} \in P$, $n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$ and is equal to zero for almost all $\mathfrak{p} \in P$.

- *The monoid of non-zero fractional ideals of A is a group.*

Definition B.4.6. — Let A be a commutative ring and $\mathfrak{p}$ be a prime ideal of A. We denote

$$A_{\mathfrak{p}} = (A\backslash\mathfrak{p})^{-1}A$$

the localised of A in $\mathfrak{p}$.

Corollary B.4.7. — *Let A be a Dedekind ring, K be its fraction field and $\mathfrak{p}$ be a non-zero prime ideal of A. Then $A_{\mathfrak{p}}$ is a valuation ring of K.*

Proof. –Let $l \in K\backslash A_{\mathfrak{p}}$. We want to show that $l^{-1} \in A_{\mathfrak{p}}$. Let

$$I = \{a \in A | al \in A\}.$$

I is an ideal of A and since $l \notin A_{\mathfrak{p}}$, we know that $I \subset \mathfrak{p}$. Let $n_I = \max\{n \in \mathbb{N} | I \subset \mathfrak{p}^n\}$. There exists an ideal I' not contained in $\mathfrak{p}$ such that $I = \mathfrak{p}^{n_I} I'$. By definition of I, lI is also an ideal of A. Let $n_l = \max\{n \in \mathbb{N} | lI \subset \mathfrak{p}^n\}$. There exists an ideal I'' not contained in $\mathfrak{p}$ such that $lI = \mathfrak{p}^{n_l} I''$.
But then, if $n_l \neq 0$ we see that that

$$\begin{aligned} l(I\mathfrak{p}^{-1}) &= (lI)\mathfrak{p}^{-1} \\ &= \mathfrak{p}^{n_l - 1} I'' \subset A \end{aligned}$$

It follows that $I\mathfrak{p}^{-1} \subset I$ by definition but this is absurd. Thus $n_l = 0$ and there exists $s \in lI\backslash\mathfrak{p}$. Let $a \in A$ be such that $al = s$. Then $l^{-1} = \frac{a}{s} \in A_{\mathfrak{p}}$. □

Corollary B.4.8. — *Let A be a Dedekind ring which is not a field, K be its fraction field and $A \subset \mathcal{O}$ be a valuation ring of K of maximal ideal $\mathfrak{p}$. Then $\mathcal{O} = A_{A \cap \mathfrak{p}}$.*

Proof. Since $A \subset \mathcal{O}$, $A \cap \mathfrak{p}$ is an ideal of A. Furthermore, since $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, $A \cap \mathfrak{p}$ is a prime ideal of A. Finally let π be a nonzero element of $\mathfrak{p}$. Since K is the fraction field of A, there exists $a \in A\backslash\{0\}$ such that $a\pi \in A$ and since $A \subset \mathcal{O}$, $a\pi \in \mathfrak{p}$.
Thus $A \cap \mathfrak{p} \neq \{0\}$. It follows that $A_{A\cap\mathfrak{p}}$ is a valuation ring of K. It is also the smallest ring containing A in which all the element $f \in A\backslash\mathfrak{p}$ are invertible. $\mathcal{O}$ is also a ring containing A in which all the elements of $A\backslash\mathfrak{p}$ are invertible. Thus $A_{A\cap\mathfrak{p}} \subset \mathcal{O}$. Since valuation rings are maximal, we have the result. □

Proposition B.4.9. — *Let A be a Dedekind ring, K its fraction field and L a finite separable extension of K. We denote A' the integral closure of A in L. The following map is a bijection:*

$$\begin{aligned} \mathbb{P}: \quad \mathrm{Spec}(A')\backslash\{0\} &\to \{\mathcal{O} \subset L | \mathcal{O} \text{ is a valuation ring of } L \text{ and } A \subset \mathcal{O}\} \\ \mathfrak{p} &\mapsto A_{\mathfrak{p}} \end{aligned}$$

Proof. We know from Corollary B.4.7 that $\mathbb{P}$ is well defined. It is also injective. Indeed if $\mathfrak{p}$ and $\mathfrak{p}'$ are two non zero prime ideals of A' such that $A_{\mathfrak{p}} = A_{\mathfrak{p}'}$ then $\mathfrak{p}$ is included in the set of non invertible elements of $A_{\mathfrak{p}'}$, so it is included in $\mathfrak{p}'$. By symmetry, we conclude that $\mathfrak{p} = \mathfrak{p}'$.

Let now $\mathcal{O}$ be a valuation ring of L containing A. We know that $L = \mathrm{Frac}(A')$. Since $\mathcal{O}$ is integrally closed it must contain A'. But then we know that $\mathcal{O} = A'_{A'\cap\mathfrak{p}}$ where p is the maximal ideal of $\mathcal{O}$. □

We now fix a perfect field k and a F finite separable extension of $k(x)$. F/k is an algebraic function field.
Let $\mathcal{O}'$ be the integral closure of $k[x]$ in F and $\mathcal{O}'_\infty$ be the integral closure of the ring

$$\mathcal{O}_\infty = \left\{ \frac{P}{Q} \in k(x) | P, Q \in k[x] \text{ and } \deg(P) \leqslant \deg(Q) \right\}.$$

Corollary B.4.10. — *There is a canonical bijection:*

$$\mathbb{P} : (\mathrm{Spec}(\mathcal{O}') \backslash \{0\}) \sqcup (\mathrm{Spec}(\mathcal{O}'_\infty) \backslash \{0\}) \to \mathbb{P}_F.$$

Furthermore if $\mathfrak{I}'$ denote the group of nonzero fraction ideal of $\mathcal{O}'$ and $\mathfrak{I}'_\infty$ the one of $\mathcal{O}'_\infty$ then we have a commutative group isomorphism

$$\mathrm{Div} : \mathfrak{I}' \times \mathfrak{I}'_\infty \to \mathrm{Div}(F).$$

Proof. This is a direct consequence of the previous proposition applied to $A = k[x]$ or $A = \mathcal{O}_\infty$ because we know that any places $\mathfrak{P}$ of F either lie over an irreducible polynomial of $k[x]$, in which case its valuation ring contains $k[x]$, or lie over the place at infinity, in which case its valuation ring contains $\mathcal{O}_\infty$. □

The representation of places as nonzero prime ideals of either $\mathcal{O}'$ or $\mathcal{O}'_\infty$ is for example the one used in the symbolic computation software *Sagemath*.

Computing the divisor (f) when f is an element of F is the same as factoring the fractional ideal generated by f (meaning, as a product of nonzero prime ideals or their inverses) in both $\mathcal{O}'$ and $\mathcal{O}'_\infty$.

For this representation to be effective, one needs in particular to be able to compute $\mathcal{O}'$ and $\mathcal{O}'_\infty$

Theorem B.4.11. — *[Abe20] If $F = {}^{k(x)[y]}/_{f(x,y)}$ where $f(x,y) \in k[x,y]$ verifies $\deg_x f = d_x$ and $\deg_y f = d_y$, then $\mathcal{O}'$ and $\mathcal{O}'_\infty$ can be computed in polynomial time in d_x and d_y.*

Remark B.4.12. — The results from [Abe20] are actually much more precise as the author does a full complexity analysis on three different algorithm. The complexity of the best algorithm is given in [Abe20, Theorem 3]. However, this algorithm still lacks a proper implementation.

B.4.2 The different

We keep the notations of the previous section.

Definition B.4.13. — [Ser04, Section III.3]

- Let A be a Dedekind ring, K be its fraction field and L be a finite separable extension of K. Let B be the integral closure of A in L. We call the *codifferent* of B over A the fractional ideal of B:
$$I = \{y \in L | \forall x \in B, \mathrm{Tr}_{L/K}(xy) \in A\}.$$
- The different of B over A, denoted $\mathfrak{D}_{B/A}$, is the inverse ideal of the codifferent of B over A. It is an ideal of B.

- We define the different divisor of F as

$$\mathrm{Diff}(F) = \mathrm{Div}(\mathfrak{D}_{\mathcal{O}'/k[x]}) + \mathrm{Div}(\mathfrak{D}_{\mathcal{O}'_\infty/\mathcal{O}_\infty}).$$

Theorem B.4.14. — *The different is computable in polynomial time.*

Proposition B.4.15. — *[Ser04, Section III.6 Corollary 2] Let A be a Dedekind ring, K be its fraction field and L be a finite separable extension of K. Let B be the integral closure of A in L and let $a \in B$, of minimal polynomial f with coefficients in A of degree $[L : K]$.*

Then $f'(a)B \subset \mathfrak{D}_{A/B}$ and we have an equality if and only if $B = A[a]$.

Corollary B.4.16. — *Let $F = k(x)[a]$ and suppose that a is integral over $k[x]$ of minimal polynomial $f(x, y) \in k[x, y]$. Then for any place $\mathfrak{P}$ which is not at infinity,*

$$\nu_{\mathfrak{P}}(\mathrm{Diff}(F)) \leqslant \nu_{\mathfrak{P}}(\partial_y f(x, a)).$$

Proposition B.4.17. — *Remember that F is a finite separable extension of $k(x)$. For any place $\mathfrak{P} \in \mathbb{P}_F$, let $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$.*

$$\mathrm{Diff}(F) = 2(x)_- - \sum_{\mathfrak{P}\in\mathbb{P}_F} \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})\mathfrak{P}.$$

Proof. The proof is inspired by that of [Ser04, Proposition 13]. We refer to it for the missing details.

Let $\mathfrak{P}' \in \mathbb{P}_F$ and $t_{\mathfrak{P}'}$ be a prime element of $\mathfrak{P}'$. We want to show that

$$\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) = -\nu_{\mathfrak{P}'}(\mathrm{Diff}(F))$$

if $\mathfrak{P}'$ is not a place at infinity, and

$$\nu_{\mathfrak{P}'}(t'_{\mathfrak{P}'}) = 2e(\mathfrak{P}') - \nu_{\mathfrak{P}'}(\mathrm{Diff}(F))$$

otherwise.

Let $\mathfrak{P} \in \mathbb{P}_{k(x)}$ be an irreducible polynomial such that $\mathfrak{P}|P$. Let $\mathcal{O}_{\mathfrak{P}'}$ and $\mathcal{O}_{\mathfrak{P}}$ be the valuation rings associated to $\mathfrak{P}$ et P respectively.

By localising and completing, we can suppose that $\mathcal{O}_{\mathfrak{P}'}$ and $\mathcal{O}_{\mathfrak{P}}$ are complete discrete valuation rings. Furthermore we can suppose that $\mathfrak{P}'|\mathfrak{P}$ is totally ramified [Ser04, Section III.5 Corollary 3]. Let $e = e(\mathfrak{P}'|\mathfrak{P})$. There exists an Eisenstein polynomial

$$f(x, y) = X^e + \sum_{i=0}^{e-1} a_i(x)y^i.$$

Such that $a_i \in \mathfrak{P}^2$ for $i \in [\![1; e-1]\!]$ and $a_0 \in \mathfrak{P}\backslash\mathfrak{P}^2$ [Ser04, Section I.6 Proposition 18].

Furthermore, since $\mathcal{O}_{\mathfrak{P}'} = \mathcal{O}_{\mathfrak{P}}[t_{\mathfrak{P}'}]$ we know that $\nu_{\mathfrak{P}'}(\mathrm{Diff}(F)) = \nu_{\mathfrak{P}'}(\partial_y f(x, t_{\mathfrak{P}'}))$.

However we know that

$$t'_{\mathfrak{P}'} = -\frac{\partial_x f(x, t_{\mathfrak{P}'})}{\partial_y f(x, t_{\mathfrak{P}'})}$$

Furthermore,

$$\partial_x f(x, t_{\mathfrak{P}'}) = \sum_{i=0}^{e-1} a_i'(x) t_{\mathfrak{P}'}^i.$$

Since $a_0 \in \mathfrak{P} \backslash \mathfrak{P}^2$ and all the other a_i are in $\mathfrak{P}^2$ it follows that $\nu_{Pfrak'}(a_0') < \nu_{\mathfrak{P}'}(a_i' t_{\mathfrak{P}'}^i)$ for $i > 0$ and

$$\nu_{\mathfrak{P}'}(\partial_x f(x, t_{\mathfrak{P}'}) = \nu_{\mathfrak{P}'}(a_0').$$

It follows that

$$\nu_{\mathfrak{P}'}(t_{\mathfrak{P}'}') = \nu_{\mathfrak{P}'}(a_0') - \nu_{\mathfrak{P}'}(\partial_y f(x, t_{\mathfrak{P}'})) = \nu_{\mathfrak{P}'}(a_0') - \nu_{\mathfrak{P}'}(\mathrm{Diff}(F)).$$

Now since $\nu_{\mathfrak{P}}(a_0) = 1$, if $\mathfrak{P}'$ is not a place at infinity then $\nu_{\mathfrak{P}'}(a_0) = 0$ and if $\mathfrak{P}$ is a place at infinity, $\nu_{\mathfrak{P}'}(a_0) = 2e$ which yields the result. □

Proposition B.4.18. — *[Sti08, Corollary 3.4.14] Let g denote the genus of F.*

$$\deg(\mathrm{Diff}(F) - 2(x)_-) = 2g - 2.$$

Bibliography

[ABCL22] Simon Abelard, Elena Berardini, Alain Couvreur, and Grégoire Lecerf. Computing Riemann-Roch spaces via Puiseux expansions. *Journal of Complexity*, April 2022.

[Abe20] Simon Abelard. On the complexity of computing integral bases of function fields. In *Computer algebra in scientific computing*, volume 12291 of *Lecture Notes in Comput. Sci.*, pages 42–62. Springer, Cham, [2020] ©2020.

[ACL22] Simon Abelard, Alain Couvreur, and Grégoire Lecerf. Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities. *Applicable Algebra in Engineering, Communication and Computing*, December 2022.

[AF92] Frank W. Anderson and Kent R. Fuller. *Rings and categories of modules*, volume 13 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1992.

[And89] Yves Andre. *G-Functions and Geometry: A Publication of the Max-Planck-Institut Fur Mathematik (Aspects of Mathematics. E, V. 13.)*. Ballen Booksellers Intl, 1989.

[AVW21] Josh Alman and Virginia Vassilevska Williams. A refined laser method and faster matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 522–539. [Society for Industrial and Applied Mathematics (SIAM)], Philadelphia, PA, 2021.

[BBvdH12] Alexandre Benoit, Alin Bostan, and Joris van der Hoeven. Quasi-optimal multiplication of linear differential operators. In *FOCS 2012 - IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 524–530, New Brunswick, United States, October 2012. IEEE.

[BCCD19] Alin Bostan, Xavier Caruso, Gilles Christol, and Philippe Dumas. Fast coefficient computation for algebraic power series in positive characteristic. *The Open Book Series*, 2(1):119–135, jan 2019.

[BCL22] Elena Berardini, Alain Couvreur, and Grégoire Lecerf. A proof of the brill-noether method from scratch, 2022.

[BCS14] Alin Bostan, Xavier Caruso, and 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.

[BCS15] Alin Bostan, Xavier Caruso, and Éric Schost. A fast algorithm for computing the p-curvature. In *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, pages 69–76. ACM, New York, 2015.

[BCS16] Alin Bostan, Xavier Caruso, and Éric Schost. Computation of the similarity class of the p-curvature. In *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 111–118. ACM, New York, 2016.

[BCSL12] Alin Bostan, Frédéric Chyzak, Bruno Salvy, and Ziming Li. Fast computation of common left multiples of linear ordinary differential operators. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC'12. ACM, July 2012.

[BCvH+17] Alin Bostan, Frédéric Chyzak, Mark van Hoeij, Manuel Kauers, and Lucien Pech. Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. *European J. Combin.*, 61:242–275, 2017.

[BE23] N. Bourbaki and R. Erné. *Algebra: Chapter 8*. Springer International Publishing, 2023.

[Bee09] Peter Beelen. A generalization of Baker's theorem. *Finite Fields Appl.*, 15(5):558–568, 2009.

[BK10] Alin Bostan and Manuel Kauers. The complete generating function for Gessel walks is algebraic. *Proc. Amer. Math. Soc.*, 138(9):3063–3078, 2010. With an appendix by Mark van Hoeij.

[BKV21] Alin Bostan, Manuel Kauers, and Thibaut Verron. The generating function of Kreweras walks with interacting boundaries is not algebraic. *Sém. Lothar. Combin.*, 85B:Art. 78, 12, 2021.

[BLS+04] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, page 42–49, New York, NY, USA, 2004. Association for Computing Machinery.

[BNS13] Jens-Dietrich BaNaSt12, Enric Nart, and Hayden D. Stainsby. Complexity of OM factorizations of polynomials over local fields. *LMS J. Comput. Math.*, 16:139–171, 2013.

[Bru13] Peter Bruin. Computing in Picard groups of projective curves over finite fields. *Math. Comp.*, 82(283):1711–1756, 2013.

[BS09] Alin Bostan and Éric Schost. Fast algorithms for differential equations in positive characteristic. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, ISSAC '09, page 47–54, New York, NY, USA, 2009. Association for Computing Machinery.

[Car18] Xavier Caruso. Polynômes de Ore en une variable. Working paper or preprint, January 2018.

[CC85] D. V. Chudnovsky and G. V. Chudnovsky. Applications of Padé approximations to Diophantine inequalities in values of G-functions. In *Number theory (New York, 1983–84)*, volume 1135 of *Lecture Notes in Math.*, pages 9–51. Springer, Berlin, 1985.

[CGH14] Edgar Costa, Robert Gerbicz, and David Harvey. A search for Wilson primes. *Math. Comp.*, 83(290):3071–3091, 2014.

[CGM22] Frédéric Chyzak, Alexandre Goyer, and Marc Mezzarobba. Symbolic-numeric factorization of differential operators. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, page 73–82, New York, NY, USA, 2022. Association for Computing Machinery.

[CK91] David G. Cantor and Erich Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28(7):693–701, 1991.

[CLB17] Xavier Caruso and Jérémy Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *Journal of Symbolic Computation*, 79(2):411–443, March 2017.

[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.

[CRV17] Xavier Caruso, David Roe, and Tristan Vaccon. Characteristic polynomials of p-adic matrices. In *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation*, pages 389–396. ACM, New York, 2017.

[EC11] Bas Edixhoven and Jean-Marc Couveignes, editors. *Computational aspects of modular forms and Galois representations*, volume 176 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2011. How one can compute in polynomial time the value of Ramanujan's tau at a prime.

[Eid21] Elie Eid. Fast computation of hyperelliptic curve isogenies in odd characteristic. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, page 131–138, New York, NY, USA, 2021. Association for Computing Machinery.

[GMN11] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *Journal de théorie des nombres de Bordeaux*, 23(3):667–696, 2011.

[Gri90] D.Yu. Grigor'ev. Complexity of factoring and calculating the gcd of linear ordinary differential operators. *Journal of Symbolic Computation*, 10(1):7–37, 1990.

[GS06] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[GTLN15] José Gómez-Torrecillas, F. J. Lobillo, and Gabriel Navarro. Factoring Ore polynomials over $\mathbb{F}_q(t)$ is difficult, 2015.

[GTLN19] José Gómez-Torrecillas, F. J. Lobillo, and Gabriel Navarro. Computing the bound of an Ore polynomial. Applications to factorization. *J. Symbolic Comput.*, 92:269–297, 2019.

[GZ03] Mark Giesbrecht and Yang Zhang. Factoring and decomposing Ore polynomials over $\mathbb{F}_q(t)$. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 127–134. ACM, New York, 2003.

[Har14] David Harvey. Counting points on hyperelliptic curves in average polynomial time. *Ann. of Math. (2)*, 179(2):783–803, 2014.

[HvdH21] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n \log n)$. *Ann. of Math. (2)*, 193(2):563–617, 2021.

[Kat82] Nicholas M. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2):203–239, 1982.

[KM07] Kamal Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.

[KV05] Erich Kaltofen and Gilles Villard. On the complexity of computing determinants. *Comput. Complex.*, 13(3–4):91–130, February 2005.

[Lam99] T. Y. Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[Lau04] Alan G. B. Lauder. Counting solutions to equations in many variables over finite fields. *Found. Comput. Math.*, 4(3):221–267, 2004.

[Lec06] Grégoire Lecerf. Sharp precision in hensel lifting for bivariate polynomial factorization. *Mathematics of Computation*, 75(254):921–933, 2006.

[Lec10] Grégoire Lecerf. New Recombination Algorithms for Bivariate Polynomial Factorization Based on Hensel Lifting. *Applicable Algebra in Engineering, Communication and Computing*, 21(2):151–176, 2010. Version préliminaire (2007) d'un travail publié de façon définitive (2010).

[LGS20] Aude Le Gluher and Pierre-Jean Spaenlehauer. A fast randomized geometric algorithm for computing riemann-roch spaces. *Mathematics of Computation*, 89(325):2399–2433, February 2020.

[LV16] Pierre Lairez and Tristan Vaccon. On p-adic differential equations with separation of variables. In *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 319–323. ACM, New York, 2016.

[Mum11] David Mumford. *Varieties Defined by Quadratic Equations*, pages 29–100. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[Nar11] Enric Nart. Okutsu-Montes representations of prime ideals of one-dimensional integral closures. *Publicacions Matemàtiques*, 55(2):261 – 294, 2011.

[Oku62] Kôtaro Okugawa. Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory. *Journal of Mathematics of Kyoto University*, 2(3):295 – 322, 1962.

[Pag21] Raphaël Pagès. Computing characteristic polynomials of p-curvatures in average polynomial time. In *ISSAC '21—Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation*, pages 329–336. ACM, New York, [2021] ©2021.

[PW22] Adrien Poteaux and Martin Weimann. Local polynomial factorisation: Improving the montes algorithm. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, page 149–157, New York, NY, USA, 2022. Association for Computing Machinery.

[PWed] Adrien Poteaux and Martin Weimann. Fast integral basis computation. To be published.

[Sam70] P. Samuel. *Algebraic Theory of Numbers*. Hermann, 1970.

[Ser03] J-P. Serre. Sur la topologie des variétés algébriques en caractéristique p. 2003.

[Ser04] J.P. Serre. *Corps locaux*. Actualités scientifiques et industrielles. Hermann, 2004.

[Sti08] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer Publishing Company, Incorporated, 2nd edition, 2008.

[Sto03] Arne Storjohann. High-order lifting and integrality certification. volume 36, pages 613–648. 2003. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017.

[Van97] Mark Van Hoeij. Factorization of differential operators with rational functions coefficients. *Journal of Symbolic Computation*, 24(5):537–561, 1997.

[van02] Mark van Hoeij. Factoring polynomials and the knapsack problem. *Journal of Number Theory*, 95(2):167–189, 2002.

[vdH07a] J. van der Hoeven. Around the numeric-symbolic computation of differential Galois groups. *JSC*, 42:236–264, 2007.

[vdH07b] Joris van der Hoeven. Efficient accelero-summation of holonomic functions. *JSC*, 42(4):389–428, 2007.

[vdP95] Marius van der Put. Differential equations in characteristic p. volume 97, pages 227–251. 1995. Special issue in honour of Frans Oort.

[vdP96] Marius van der Put. Reduction modulo p of differential equations. *Indag. Math. (N.S.)*, 7(3):367–387, 1996.

[vdP97] Marius van der Put. Modular methods for factoring differential operators. 1997. Unpublished manuscript (Preliminary Version).

[vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

[Wei15] Martin Weimann. Bivariate factorization using a critical fiber, 2015.

Abstract:

The study of linear differential operators is an important part of the algebraic study of differential equations. Rings of linear differential operators share many properties with rings of polynomials, but the noncommutative aspect of the multiplication makes the design of factorisation algorithms harder. This thesis focuses mainly on developing an algorithm computing an irreducible right factor of a given linear differential operator with coefficients in an algebraic function field of positive characteristic p. The situation differs greatly from the same problem in characteristic 0 because algebraic function fields of characteristic p are finite dimensional over their field of constants. This simple fact provides the ring of differential operators in characteristic p with an additional structure of Azumaya algebra, which gives additional tools to attack our problem.

A first step in this direction is the computation of the p-curvature, a classical invariant of primary importance attached to differential operations in characteristic p. The first important result of this thesis is an algorithm computing, for a given operator L in characteristic 0 and an integer N, all the characteristic polynomials of the p-curvatures of its reduction modulo p, for all primes $p \leqslant N$.

The second part of the thesis is dedicated to the factorisation itself. We use the Azumaya algebra structure to show that finding irreducible right irreducible factors reduces to solving the p-Riccati equation

$$f^{(p-1)} + f^p = a^p$$

in $K[a]$, where a is a suitable algebraic function over K. This observation leads to two important algorithms. The first one is an application of the global-local principle which eventually provides a polynomial time irreducibility test for differential operators. The second one is an actual resolution algorithm for the p-Riccati equation that uses tools of algebraic geometry for curves such as Riemann-Roch spaces and Picard group. We perform a complexity analysis of this algorithm, and show that the p-Riccati equation always admits a solution whose size is comparable to that of the parameter a. As a byproduct, this algorithm makes the factorisation of central operators possible (a situation which was often left aside) and lower the size of right factors of general operators by a factor p compared to previous works. We finally deduce a full factorisation algorithm for differential operators of positive characteristic.

Résumé :

L'étude des opérateurs différentiels linéaires est une partie importante de l'étude algébrique des équations différentielles. Les anneaux d'opérateurs différentiels linéaires partagent de nombreuses propriétés avec les anneaux de polynômes, mais le caractère non commutatif de la multiplication rend la conception d'algorithmes de factorisation plus compliquée. L'objet de cette thèse est le développement d'un algorithme calculant un facteur droit irréductible d'un opérateur différentiel linéaire donné dont les coefficients sont des éléments d'un corps de fonctions algébriques de caractéristique p. La situation diffère grandement du problème analogue en caractéristique 0 car les corps de fonctions algébriques de caractéristique positive sont de dimension finie sur leur corps des constantes. De ceci découle une structure additionnelle d'algèbre d'Azumaya qui fournit des outils supplémentaires pour attaquer le problème de la factorisation.

Une première étape est le calcul de la p-courbure, un invariant classique de première importance des opérateurs différentiels en caractéristique p. Le premier résultat significatif de cette thèse est un algorithme calculant, pour un opérateur différentiel L en caractéristique 0 et un entier $N \in \mathbb{N}^*$ donnés, tous les polynômes caractéristiques des p-courbures des réductions de L modulo p, pour tous les nombres premiers $p \leqslant N$.

La deuxième partie de la thèse est consacrée à la factorisation en elle-même. Nous utilisons la structure d'algèbre d'Azumaya pour montrer que la recherche de facteurs irréductibles à droite revient à la résolution de l'équation de p-Riccati

$$f^{(p-1)} + f^p = a^p$$

dans $K[a]$, où a est une certaine fonction algébrique sur K.

Cette observation nous permet de développer deux algorithmes importants. Le premier est une application du principe global-local conduisant à un test d'irréductibilité de complexité polynomiale pour les opérateurs différentiels. Le second est un algorithme de résolution de l'équation de p-Riccati utilisant plusieurs outils de la géométrie algébriques pour les courbes, dont les espaces de Riemann-Roch et les groupes de Picard. Nous effectuons une analyse de complexité approfondie de cet algorithme et montrons que l'équation de p-Riccati admet toujours une solution dont la taille est comparable à celle du paramètre a. Cet algorithme rend en particulier possible la factorisation des opérateurs centraux (un cas qui a souvent été laissée de côté par le passé) et diminue la taille des facteurs droits irréductibles d'opérateurs différentiels linéaires d'un facteur p en comparaison des travaux précédents.

On en déduit finalement un algorithme de factorisation complet pour les opérateurs différentiels linéaires de caractéristique positive.