UNIVERSITÉ CAEN-NORMANDIE

Laboratoire de Mathématiques Nicolas Oresme

Incursions en géométrie algébrique effective et calcul formel

Martin Weimann

Mémoire d'habilitation à diriger des recherches.

Mention : Mathématiques

Date de soutenance : 14 juin 2024

Devant un jury composé de :

Xavier Caruso	-	DR CNRS, Université de Bordeaux
Pierrette Cassou-Nogues	-	PR, Université de Bordeaux
Alain Couvreur (rapporteur)	-	DR INRIA, Saclay
Grégoire Lecerf (rapporteur)	-	DR CNRS, Ecole Polytechnique
Enric Nart	-	PR, Université Autonome de Barcelone
Denis Simon	-	PR, Université Caen-Normandie
Martin Sombra	-	DR ICREA, Université de Barcelone
Bernard Teissier (rapporteur)	-	DR CNRS, Université Paris-Sorbonne

´

Table des matières

Remerciements

Je remercie très chaleureusement Alain Couvreur, Grégoire Lecerf et Bernard Teissier d'avoir accepté la charge d'être les rapporteurs de cette habilitation. J'exprime aussi toute ma gratitude aux autres membres du jury, Xavier Caruso, Pierrette Cassou-Nogues, Enric Nart, Denis Simon et Martin Sombra. Réunir autant de mathématicien.ne.s dont les travaux de grande qualité ont influencé mes recherches est un grand honneur.

Lors de ma maîtrise à Bordeaux, j'ai découvert les distributions, qui permettaient de "dériver des fonctions non dérivables". Concept si séduisant que mon intention première de me spécialiser en théorie des nombres dériva en une thèse en géométrie analytique complexe sous la direction patiente et passionnante d'Alain Yger, à qui j'adresse ma plus profonde reconnaissance. Mes années de post-doctorat furent ensuite l'occasion de nouvelles rencontres qui m'ont indubitablement apporté scientifiquement et je me dois de mentionner ici quelques noms : André Galligo, Mohamed Elkadi et Laurent Busé à Nice, Mikaël Passare à Stockholm, Michel Brion et Jean-Pierre Demailly à Grenoble, Martin Sombra, Jose Burgos et Carlos D'Andrea à Barcelone, ou Joseph Schicho en Autriche, liste évidemment non exhaustive. Spéciale dédicace à Adrien Poteaux, avec qui nous avons maintenant partagé beaucoup d'aventures mathématiques. Merci à tous.

Depuis maintenant douze ans j'ai le plaisir d'être membre du LMNO, laboratoire mathématiques caennais. D'aucuns me rappelleront mesquinement que ces douze années furent entrecoupées d'une légère parenthèse de cinq ans sous les tropiques - et j'en profite pour saluer les collègues de Tahiti -, donc disons plus honnêtement sept années passées à Caen. C'est un grand plaisir d'y partager mon bureau avec Denis Simon, avec qui il est si agréable (mais trop rare, satané emploi du temps) de parler de maths, et qui au demeurant a accepté d'être le garant de cette habilitation. Le LMNO offre un cadre de travail chaleureux. Les groupes de travail, le séminaire de théorie des nombres, les rencontres arithmétiques de Caen, ou encore les rencontres de l'équipe TNGA où l'on maîtrise l'art d'éplucher les patates en écoutant les exposés, sont autant d'évènements propices à une cogestion sereine, aux échanges et à la créativité scientifique. Je remercie chaleureusement tous les collègues qui participent à ce bon fonctionnement du labo et du département, à cette dynamique et à cette bonne humeur, en particulier nos secrétaires Anita, Vanessa et Carole qui sont en première ligne des mutations "étamineuses" chronophages et contre-productives de notre métier.

Un petit clin d'oeil aux écoolien.ne.s avec qui je partage le plaisir de nos rencontres champêtres et scientifiques, et avec qui, munis de quelques craies et un tableau noir, nous causons de sciences dans d'inlassables discussions captivantes et formatrices. L'écoole a 20 ans cette année, vive l'écoole. Et merci aux retraites Barracuda - si écooliennes dans l'esprit - pour leur accueil. Vive Barracuda.

Merci les amis, du bocage ou des villes, de la Creuse ou des îles, bref d'ici et d'ailleurs. Merci pour tous ces moments de partages intimes, festifs, musicaux, sportifs, militants, ingrédients fondamentaux de mon équilibre, et sans lesquels j'aurais parfois bien du mal à déconnecter de mes recherches.

Une pensée particulière pour mes parents qui m'ont tant donné, pour mon frangin Théo avec qui j'ai tant partagé, et pour la famille élargie, cousins, neveux, taties, tontons et toute la smala.

Et bien sûr Elodie, Polin et Oreste, merci pour votre soutien indéfectible, votre amour, et pour tellement plus. Je vous dédie ce travail.

J'allais oublier : je ne remercie pas celles et ceux qui depuis leur tour d'ivoire œuvrent sans relâche à l'évolution désastreuse de l'université, à la précarisation du personnel, à la bureaucratisation, à la rentabilisation, à la marchandisation et au contrôle du savoir, à la privatisation, à la mise en compétition, à la paye à la prime, aux financements par projets, au pilotage de la recherche, aux ANRisations, aux labexisations, aux pôles d'excellentisation, à la shangaïtisation. Bref, je ne remercie pas celles et ceux qui cherchent à nous faire oublier que l'université devrait avant tout être un lieu de partage, de transmission, de critique, de création, d'émancipation et d'autogestion, au service du bien commun. Université comme universel.

Introduction

Rédiger un mémoire d'habilitation n'est certes pas écrire un livre, mais c'est l'occasion d'inscrire l'ensemble de ses contributions dans un contexte mathématique cohérent plus vaste. Exercice bien difficile en vérité, et je ne suis pas convaincu d'avoir réalisé avec brio cette ambition première d'échapper à une présentation linéaire des résumés de mes travaux. Le lecteur jugera. Quoi qu'il en soit, ce mémoire aura j'espère le mérite d'illustrer que la recherche est amenée à évoluer, souvent de manière imprévue, au gré des découvertes et des rencontres humaines, qui apportent chacune à leur manière leur lot de nouvelles réponses et de nouvelles questions.

La suite de cette introduction offre un survol de mes thèmes de recherche et de mes contributions principales, puis présente quelques projets de recherches à court ou moyen terme. Bonne lecture.

****

Ce mémoire se compose de 6 chapitres, répartis en trois parties. La première partie porte sur mes travaux dans la lignée de ma thèse [134], à l'interface de l'analyse complexe et la géométrie torique. La seconde partie à visée plus algorithmique concerne la factorisation des polynômes, bivariés puis univariés. La dernière partie décrit deux autres projets relativement transverses, l'un sur le lieu flex des hypersurfaces et l'autre sur la gonalité des courbes algébriques. Les intitulés des chapitres sont suivis de la liste de mes articles concernés.

Partie I : Incursions en géométrie torique complexe.

Cette partie concerne mes travaux sur les liens entre le calcul résiduel multivarié et certains problèmes d'extensions algébriques dans les variétés toriques complexes. Pour citer quelques mots clés, disons formes méromorphes, courants, résidus, résultants, polytopes de Newton, variétés toriques.

• Chapitre 1 : Autour du théorème d'Abel-inverse torique [134, 135, 139, 136].

Un objectif majeur de ma thèse, encadrée par Alain Yger à l'Université de Bordeaux, était de généraliser la transformée d'Abel-Radon et le théorème d'Abel-inverse projectif de Griffiths et Henkin-Passare [58, 66] au cadre des variétés toriques complexes. Moralement, on cherche à caractériser à l'aide de traces l'existence d'objets algébriques globaux (variétés, formes différentielles) dont certains germes analytiques locaux sont prescrits. Le cadre torique a l'avantage notable de permettre de contrôler les polytopes de Newton (enveloppes convexes des exposants) des éventuels polynômes interpolant, et certains résultats ont trouvé par la suite des applications à la factorisation des polynômes à deux variables (Chapitre 3). Le calcul résiduel multivarié joue un rôle prépondérant, en particulier les courants résiduels, le théorème des résidus et le théorème de dualité, outils connus pour la résolution des problèmes d'appartenance aux idéaux. J'ai délibérément choisi de relativement détailler

cette partie, espérant donner au lecteur un aperçu de l'utilisation d'outils d'analyse en géométrie algébrique complexe.

• Chapitre 2 : Le théorème d'osculation torique [138].

Motivé par des applications à la factorisation bivariée, j'ai établi un critère permettant de déterminer si un fibré en droites d'un diviseur de Cartier d'une variété rationnelle complexe compacte peut s'étendre à la variété. La preuve est basée sur la cohomologie $\bar{\partial}$ de Dolbeault et, encore une fois, sur des outils relevant du calcul résiduel. En corollaire, et c'était le but premier, j'ai obtenu une formule explicite permettant de caractériser l'existence d'une courbe algébrique dont les jets sont prescrits au bord d'une compactification torique du plan affine. Ces résultats ont été obtenus en partie lors de mon année d'ATER à l'Institut Fourier de Grenoble.

Partie II : Contributions à la factorisation des polynômes.

A la sortie de ma thèse, André Galligo a suggéré d'utiliser mon théorème d'interpolation torique [136] afin de tenir compte du polygone de Newton en factorisation bivariée. Ceci occasionna un post-doctorat à Nice, qui fût le point de départ de nouvelles recherches de nature plus algorithmiques, consacrées à la factorisation des polynômes bivariés puis, plus récemment, à la factorisation univariée sur les corps locaux. On parlera donc ici de calcul formel, de polynômes, de courbes algébriques, de singularités et de corps valués.

• Chapitre 3 : Factorisation des polynômes bivariés [43, 137, 138, 140, 141, 125].

Il existe depuis la fin des années 2000 des algorithmes de factorisation bivariée de très bonne complexité en le degré total, basés sur la recombinaison des facteurs dans $\mathbb{K}[[x]][y]$ *via* des méthodes d'algèbre linéaire (travaux de Lecerf et al. [85, 83]). J'ai cherché à développer de nouvelles méthodes dont la complexité se mesure en terme d'indicateurs plus fins que le degré dans le but d'accélérer la factorisation pour certaines familles de polynômes.

Approches toriques [43, 138, 137].

Le théorème d'Ostrovski assure que le polygone de Newton du produit de deux polynômes est la somme de Minkovski des polygones. Les sections 3.2 et 3.3 expliquent comment tenir compte de cette contrainte combinatoire en se basant sur des résultats des chapitres 1 et 2, conduisant *in fine* à un algorithme déterministe de factorisation dans $\mathbb{Q}[x, y]$ de complexité polynomiale en le volume du polygone et en le périmètre entier, résultat obtenu lors de mon post-doctorat à Barcelone. L'idée est de plonger la courbe dans une compactification torique adéquate, et de combiner le théorème d'osculation torique [138] avec le théorème des dérivées logarithmiques de Ruppert [111]. Pour certaines familles de polynômes, la complexité est meilleure que celle des algorithmes denses rapides (mais malheureusement pas dans tous les cas, cf ouverture 3.3.4).

Approches singulières [141, 140, 125].

Il existe des liens évidents entre la factorisation d'un polynôme et les singularités des courbes algébriques. Par exemple, le fait qu'une courbe projective plane lisse est nécessairement irréductible, ou encore le fait que les approches toriques s'interprètent finalement comme la

prise en compte d'invariants attachés aux singularités aux trois points $\mathbb{T}$-fixes de $\mathbb{P}^2$. Ce constat m'a encouragé à étudier plus en détail la factorisation sous l'angle des singularités. Un premier résultat [141] est une extension des algorithmes "remontées de Hensel et recombinaisons" au cas $f(0, y)$ non séparable, un avantage étant que la complexité baisse en présence de ramification. Le second résultat [140] est un algorithme basé sur la résolution totale des singularités, lié au théorème des résidus et au calcul d'une base des polynômes adjoints, et dont la complexité dépend cette fois du genre géométrique.

Polynômes minimaux [125].

La valuation du discriminant jouant un rôle majeur dans ces questions, nous avons étudié dans un travail annexe avec Denis Simon les polynômes bivariés dont le discriminant (par rapport à l'une des variables) est de degré minimal relativement au degré, au genre et au nombre de composantes. Nous avons également cherché les formes réduites de ces polynômes minimaux sous l'action de $GL_2(\mathbb{K}[x])$, action qui préserve les propriétés de minimalité.

• Chapitre 4 : Factorisation univariée sur un corps valué et applications [108, 110, 125, 107, 109, 10].

La pertinence des approches singulières en factorisation restait toutefois dépendante d'une hypothétique factorisation rapide dans $\mathbb{K}[[x]][y]$. Ces considérations m'ont conduit à travailler sur une version rapide de l'algorithme de Newton-Puiseux, en collaboration avec Adrien Poteaux. Nos résultats positifs nous ont encouragés à considérer par la suite la factorisation des polynômes univariés sur un anneau de valuation discrète complet, puis plus récemment sur un anneau hensélien muni d'une valuation non nécessairement discrète de rang un.

Séries formelles et séries de Puiseux [108, 110, 107, 125].

Un résultat majeur de cette série de papiers est une variante rapide de l'algorithme de Newton-Puiseux, d'où découle un algorithme rapide de factorisation dans $\mathbb{K}[[x]][y]$ en caractéristique zéro ou suffisamment grande [107]. La preuve repose entre autres sur une méthode diviser pour régner sur la précision des calculs et sur un lemme de Hensel "critique" de convergence quadratique. Au-delà de donner du crédit à la factorisation singulière des polynômes bivariés (ce qui était ma motivation initiale), c'est un résultat important de calcul formel du fait du rôle central des séries de Puiseux dans l'algorithmique des courbes. Combiné à la formule de Riemann-Hurwitz, notre résultat permet par exemple de calculer le genre d'une courbe algébrique plane avec une complexité quasi-cubique en le degré, donc quasi-équivalente au calcul du discriminant. Notre algorithme a trouvé d'autres applications notables au calcul rapide d'une base intégrale d'un corps de fonctions [1], ou encore des espaces de Riemann-Roch [3], ces derniers étant des éléments clés de la construction des codes correcteurs géométriques. Par la suite, l'utilisation des racines approchées d'Abhyankhar nous a permis d'obtenir un test d'irréductibilité et d'équisingularité d'un polynôme de Weierstrass de complexité quasi-linéaire en la taille de l'entrée [108, 110], qui calcule en bonus le type topologique des germes de courbes sous-jacents.

Généralisation aux anneaux locaux [109].

L'algorithme de Newton-Puiseux n'est plus valable en petite caractéristique, un cadre pourtant fondamental du fait des nombreuses applications des courbes sur les corps finis, par exemple en théorie des codes correcteurs ou en cryptographie. Motivés par ce problème,

nous avons développé avec Adrien une variante rapide de l'algorithme OM de Montes de factorisation des polynômes sur les corps locaux, en nous inspirant de nos travaux sur les séries de Puiseux. Les conséquences sont importantes en théorie algorithmique des nombres, la factorisation dans $\mathbb{Q}_p[x]$ y jouant un rôle fondamental : calcul des extensions de la valuation p-adique à un corps de nombre et des données arithmétiques afférentes (ramification, inertie, uniformisante, base d'Okustsu), factorisation des idéaux dans un anneau de Dedekind, valuation p-adique du discriminant, bases intégrales, etc.

Généralisation aux anneaux henséliens [10].

Dans un travail commun avec Enric Nart et ses collaborateurs de Barcelone, nous avons démontré récemment l'existence d'un algorithme de factorisation des polynômes univariés sur des anneaux henséliens munis d'une valuation non nécessairement discrète de rang un. Notre preuve repose sur le formalisme moderne des valuations augmentées de Mac Lane - Vaquié (arbre valuatif, algèbres graduées, etc), combiné aux racines approchées de Abhyankhar - Moh et au lemme de Hensel valué multifacteurs [109], en supposant la caractéristique résiduelle nulle ou assez grande si la valuation n'est pas discrète. Ce travail apporte aussi un nouvel éclairage à la construction originelle technique de Montes des polygones et des opérateurs résiduels d'ordre supérieur dans le cas discret de rang un. Enfin, on classifie précisément les différents types obstructions à la terminaison de notre algorithme dans le cas d'un anneau hensélien général, liées au rang de la valuation ou à la caractéristique résiduelle positive. Ces résultats ouvrent la voie à de nouvelles applications arithmético-géométriques, de nature théorique ou algorithmique. Notons à ce propos les liens étroits entre le problème des extensions des valuations de rang un non discrètes et le problème ouvert de l'uniformisation locale en caractéristique positive [93].

Partie III : Autres contributions.

Cette dernière partie est consacrée à deux autres collaborations sur des thématiques relativement annexes à mes travaux principaux, toujours à l'interface de la géométrie algébrique effective et de l'algorithmique des courbes.

• Chapitre 5 : Sur le lieu flex des hypersurfaces [21].

Le lieu flex d'une hypersurface $V \subset \mathbb{P}^n$ est le lieu des points de V par lesquels passe une droite avec un ordre de contact anormalement élevé. Dans le cas d'une courbe de $\mathbb{P}^2$, le lieu flex est déterminé par le lieu des zéros du Hessien. Dans le cas d'une surface de degré $d \geq 3$ définie sur un corps de caractéristique zéro et sans composantes réglées, un théorème de Salmon [114] assure que le lieu flex est une courbe sur la surface de degré au plus $11d^2 - 24d$, un résultat qui a trouvé récemment des applications notables en géométrie d'incidence [73]. En collaboration avec Laurent Busé, Carlos D'Andrea et Martin Sombra, nous avons utilisé la théorie des résultants multivariés afin de généraliser le théorème de Salmon en toute dimension. On montre en particulier que pour une hypersurface générale, le lieu flex est une intersection complète réduite de codimension 1 de V et on calcule explicitement son degré et une équation homogène. On montre de plus que par un point flex général passe une unique droite flex, et que celle-ci a exactement l'ordre de contact attendu.

• **Chapitre 6 : Calcul de la gonalité d'une courbe algébrique [117].**

La gonalité d'une courbe algébrique C est le degré minimal d'un morphisme dominant $C \to \mathbb{P}^1$ (éventuellement défini sur une extension finie du corps de base). Au même titre que le genre, cet invariant birationnel mesure le défaut de rationalité de C, mais le calcul de la gonalité est beaucoup plus délicat, problème intimement lié aux systèmes linéaires spéciaux. Dans un travail en collaboration avec Joseph Schicho et Franck-Olaf Schreyer lors de mon post-doctorat à Ricam (Linz, Autriche), nous avons développé un algorithme qui calcule la gonalité et un morphisme gonal d'une courbe irréductible quelconque. Ce problème était ouvert pour la gonalité ≥ 4. Notre approche repose sur l'étude des syzygies des courbes canoniques. Etant donnée la résolution projective minimale de l'idéal d'un modèle canonique $C \subset \mathbb{P}^{g-1}$ (qui peut se calculer *via* les bases de Gröbner), on montre qu'il est possible de détecter le sous-complexe d'une variété scrollaire rationnelle normale X de dimension minimale contenant C, et de calculer ensuite le morphisme naturel $X \to \mathbb{P}^1$. Par construction, la restriction de ce morphisme à C fournit un morphisme gonal. Fait notable, on obtient en corollaire un algorithme de paramétrisation par radicaux des courbes de gonalité ≤ 4.

****

Quelques travaux en cours et perspectives.

Décrivons pour finir quelques travaux en cours et quelques projets à plus long terme. Le lecteur trouvera plus de détails dans les chapitres de ce mémoire qui sont régulièrement ponctués de sous-sections "ouvertures".

Sur le degré du lieu hyperflex d'une hypersurface (ouverture 5.3).

Dans un travail en cours avec Cristina Bertone (Université de Turin), nous cherchons à déterminer le degré du lieu k-flex d'une hypersurface $V \subset \mathbb{P}^n$ (points d'ordres de contact $\geq k$ avec une droite projective). La théorie des résultants utilisée dans [21] ne répond plus à ce problème général. Inspirés par le livre de Eisenbud et Harris [42], l'idée est de ramener ce problème au calcul de la classe de Chern maximale d'un fibré vectoriel des "parties principales relatives" au-dessus de la variété d'incidence de la Grassmannienne $\mathbb{G}(1, n)$, puis de calculer ladite classe en s'aidant du calcul de Schubert dans les Grassamaniennes.

Séries de Puiseux rationnelles multivariées (ouverture 4.2.4).

Dans un travail en collaboration avec Jose Cano, Sebastian Falkensteiner et Adrien Poteaux, on cherche à calculer efficacement les séries de Puiseux multivariées d'un polynôme $f \in \mathbb{K}[t_1, \ldots, t_n][x]$, introduites par Mac Donald [89] (en caractéristique nulle). L'enjeu est de calculer des paramétrisations de Puiseux "rationnelles" en s'inspirant du cas bivarié [39, 108], afin de maintenir les calculs dans des extensions résiduelles minimales. Ce problème est intimement lié à nos travaux [10] sur la factorisation des polynômes sur les anneaux henséliens, l'idée sous-jacente étant de compléter $\mathbb{K}(t_1, \ldots, t_n)$ pour une valuation non discrète de rang un et de rang rationnel n.

Espaces de Riemann-Roch (ouvertures 3.5.1 et 4.3.1).

Il y a eu récemment de nouvelles avancées pour le calcul efficace des espaces de Riemann-Roch sur une courbe plane, basées sur les séries de Puiseux et la théorie de Brill-Noether [3]. Les nouveaux algorithmes rapides de factorisation sur les corps locaux [109] offrent des perspectives sérieuses de généraliser ces résultats en petite caractéristique et d'en améliorer la complexité par des méthodes arithmétiques locales-globales, dans l'esprit des travaux de Okutsu sur le calcul des bases intégrales [96, 64] pour la partie affine et dans l'esprit des travaux de Hess [69] pour tenir compte des places à l'infini.

Factorisation univariée sur des anneaux henséliens de caractéristique résiduelle positive (ouverture 4.4.1).

Ce problème ouvert reste un challenge majeur, la difficulté étant que l'on n'a plus accès aux racines approchées pour calculer les polynômes clés "limites" en petite caractéristique résiduelle. Le cas discret se traite avec un nombre fini d'étapes de raffinements des polynômes clés, mais quid des valuations non discrètes ? Traiter le cas des extensions algébriques infinies des corps locaux (donc de groupe des valeurs un sous-groupe ordonné de $\mathbb{Q}$) serait une première étape importante à franchir. L'autre étape est de traiter les extensions transcendantes, dans le cadre desquelles on peut trouver par exemple les groupes de valeurs non discrets de rang un et de rang rationnel > 1 du type $\mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ qui interviennent dans la théorie des séries de Puiseux multivariées (ouverture 4.2.4).

Factorisation bivariée, le retour (ouvertures 3.3.4 et 3.5.1).

Au regard de la récente factorisation rapide dans $\mathbb{K}[[t]][x]$ [109], il semble opportun de se repencher sur la factorisation bivariée singulière développée dans [140]. Existe-t-il un algorithme de factorisation dans $\mathbb{K}[t, x]$ basé sur la résolution des singularités, de complexité polynomiale en le genre et le degré, et qui soit compétitif en toute généralité avec les approches Hensel et recombinaisons ?

Dans le même esprit, existe-t-il une variante de l'algorithme torique [138] qui tienne compte du volume et du périmètre entier du polygone de Newton et qui soit inconditionnellement compétitive avec les approches denses classiques ?

Plus spéculativement, est-il possible de borner la complexité binaire de la factorisation dans $\mathbb{Q}[t, x]$ en fonction d'indicateurs arithmético-géométriques *via* l'utilisation de valuations de rang deux mixant les aspects p-adiques et t-adiques ?

****

Première partie

Incursions en géométrie torique complexe

Chapitre 1

Trace, résidus et problèmes d'Abel-inverse toriques

Contents

1.1 Motivations

Ce chapitre est en grande partie consacré aux travaux issus de ma thèse. Son but est de donner au lecteur un aperçu de l'utilisation du calcul résiduel multivarié pour la résolution de certains problèmes d'algébricité dans les variétés toriques complexes.

Soit X une variété algébrique complexe compacte lisse et considérons une collection finie $V = V_1 \cup \ldots \cup V_N$ de germes d'hypersurfaces analytiques en des points distincts de X. On cherche à répondre aux questions suivantes :

- Soit $\alpha \in \mathrm{Pic}(X)$ une classe de Picard donnée. A quelles conditions existe-t-il une hypersurface algébrique $\tilde{V} \subset X$ contenant V et de classe α ?
- Si on se donne de plus une forme holomorphe Φ sur V, à quelles conditions existe-t-il une forme rationnelle $\tilde{\Phi}$ sur $\tilde{V}$ telle que $\tilde{\Phi}_{|V} = \Phi$? A quelle condition $\tilde{\Phi}$ est-elle holomorphe ?

La trace. Un concept important est la notion de trace. L'idée est d'intersecter les germes V_i avec une famille de courbes algébriques C_a convenable et de considérer la forme trace

$$Tr_V \Phi(a) := \sum_{p \in V \cap C_a} \Phi(p),$$

vue comme germe de forme différentielle holomorphe dans l'espace des paramètres. On se ramène ainsi à des problèmes dits de type Abel-inverse : l'enjeu est de démontrer que les problèmes d'algébricité ci-dessus sont équivalents à des problèmes de rationalité ou d'annulation de traces. Ce point de vue est dans la lignée des travaux fondateurs de Griffiths [58] et Henkin-Passare [66] qui traitent le cas de germes alignés de l'espace projectif $X = \mathbb{P}^n$ intersectés par des droites.

Résidus. La théorie des résidus multivariés joue un rôle particulièrement important. En effet, on montre que les formes traces admettent des représentations résiduelles qui offrent une souplesse de calcul et qui permettent de profiter de théorèmes puissants comme le théorème de dualité ou le théorème des résidus, connus pour incarner l'obstruction à l'extension algébrique d'objets analytiques. Ces outils réapparaîtront régulièrement dans mes travaux [134, 135, 139, 136, 137, 140].

Variétés toriques. J'ai abordé ces problèmes d'algébricité dans le cadre des variétés toriques. Contrairement au cas de la trace relative à des droites de l'espace projectif traité dans [58, 66], le cadre torique permet d'un côté de ne plus supposer les germes V_i alignés, et d'un autre côté de contrôler le polytope de Newton du polynôme interpolant. Mes résultats ont trouvé par la suite des applications inattendues en calcul formel, dans le domaine de la factorisation des polynômes creux multivariés qui sera abordée au chapitre suivant.

Articles concernés. Les résultats présentés dans cette section concernent ma thèse [134] et les publications afférentes [135, 139, 136].

1.2 Le cadre projectif

On considère dans cette section la trace d'une forme méromorphe sur un sous-ensemble analytique relativement à une famille de sous-espaces linéaires de l'espace projectif, comme abordé dans [58, 66, 135].

La trace et le théorème d'Abel. Soit $U \subset \mathbb{P}^n$ un ouvert connexe non vide de l'espace projectif complexe de dimension n muni de sa topologie de variété différentielle. Soit $V \subset U$ une sous-variété analytique de codimension pure k et soit Φ une q-forme méromorphe sur V, i.e. localement restriction à V d'une q-forme méromorphe dont le lieu polaire coupe V proprement. On se pose la question de l'algébricité du couple (V, Φ).

On supposera ici que U est linéairement k-concave, c'est à dire union de k-plans projectifs, et on notera $U^* \subset \mathbb{G}(k, n)$ l'ouvert de la grassmannienne paramétrant les k-plans de U. D'après le théorème de Sard-Bertini, il existe un sous-espace analytique fermé $W^* \subset U^*$ tel que pour tout paramètre $a \in U^* \setminus W^*$, le k-plan correspondant $C_a \subset U$ coupe V transversalement en d points distincts $p_1(a), \ldots, p_d(a)$ n'appartenant pas au lieu polaire de Φ.

Les applications $a \mapsto p_j(a)$ sont localement holomorphes par le théorème des fonctions implicites et on peut alors définir localement *la trace de* Φ *sur* V :

$$Tr_V(\Phi)(a) := \sum_{j=1}^{d} \Phi(p_j(a)),$$

où il est entendu que $\Phi(p_j(a)) = p_j^*(\Phi)(a)$. La trace est une q-forme *a priori* définie et holomorphe sur $U^* \setminus W^*$. Il est montré dans [66] qu'elle s'étend en fait en une forme méromorphe sur U^* :

Théorème 1 *Si* Φ *est méromorphe (resp. holomorphe*[1]*) sur* V*, alors* $Tr_V\Phi$ *s'étend en une forme méromorphe (resp. holomorphe) sur* U^**.*

On verra en Section 1.4.4 une preuve de ce résultat basée sur le formalisme des courants.

Lien avec les travaux d'Abel. Historiquement, ce théorème trouve sa source d'inspiration dans les travaux d'Abel [1], dont un des buts était de contourner le caractère transcendant des intégrales abéliennes. Le théorème originel d'Abel assure que si $C \subset \mathbb{P}^2$ est une courbe algébrique de degré d et $p_0 \in C$ est un point donné, alors la somme d'intégrales abéliennes

$$S(a) = \sum_{i=1}^{d} \int_{p_0}^{p_i(a)} r(x,y)dx$$

d'une 1-forme rationnelle $\Phi = r(x,y)dx$ sur C est une fonction de a (définie modulo les périodes de C) de la forme $S = A + \log(B)$ où A et B sont rationnelles : bien que chaque intégrale prise individuellement soit en général hautement transcendante, leur somme s'exprime à partir des fonctions usuelles. Ce résultat est une conséquence du théorème 1 du fait de l'égalité

$$dS(a) = Tr_C(\Phi)(a)$$

et du fait qu'une forme méromorphe sur $\mathbb{G}(1,2)$ est rationnelle par le principe GAGA. Si l'on suppose de plus que Φ est holomorphe sur C (section globale du faisceau dualisant ω_C), alors sa trace est nulle car il n'y a pas de 1-forme holomorphe non nulle sur $\mathbb{G}(1,2) \simeq \mathbb{P}^2$. La réciproque est vraie d'après le théorème 2 (Abel-inverse) ci-après :

$$\Phi \in H^0(C, \omega_C) \Longleftrightarrow Tr_C\,\Phi \equiv 0. \tag{1.1}$$

Les travaux d'Abel, suivis de Jacobi et d'autres sont à la base d'une intense activité autour des courbes algébriques et des résidus. L'équivalence (1.1), avatar du théorème des résidus et du théorème de dualité, est par exemple un point clé dans la preuve que la jacobienne d'une courbe projective lisse de genre g (paramétrant les diviseurs de degrés 0 modulo équivalence rationnelle) est un groupe algébrique de dimension g. On renvoie le lecteur à [58] pour plus de détails historiques.

Le théorème d'Abel-inverse. Le théorème 1 donne des conditions nécessaires à l'extension algébrique du couple (V, Φ) : la trace doit s'étendre en une forme rationnelle sur la grassmanienne $\mathbb{G}(k,n)$. Le théorème suivant, dit "d'Abel-inverse" assure que cette condition est également suffisante :

1. L'holomorphie sur un espace analytique singulier doit être ici comprise au sens d'un courant $\bar{\partial}$-fermé, cf Section 1.4.3

Théorème 2 *[58, 66] Si Φ n'est identiquement nulle sur aucune composante de V, alors il existe $\tilde{V} \subset \mathbb{P}^n$ algébrique de degré d contenant V et $\tilde{\Phi}$ une forme rationnelle sur $\tilde{V}$ telle que $\tilde{\Phi}_{|V} = \Phi$ si et seulement si $Tr_V \Phi$ est rationnelle. De plus, $\tilde{\Phi}$ est holomorphe sur $\tilde{V}$ si et seulement si $Tr_V \Phi \equiv 0$.*

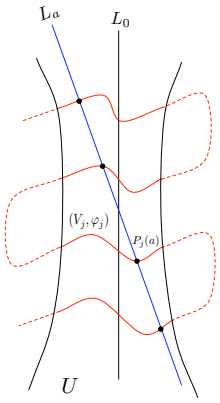

FIGURE 1.1 – Le théorème d'Abel-inverse dans le cadre projectif

On renvoie le lecteur à [58] pour le cas de la trace nulle et à [66] où les auteurs prouvent une version locale plus générale donnant des critères d'extension du couple (V, ϕ) à un ouvert linéairement concave U' contenant U.

Le théorème de Wood. Ce théorème donne un critère simple d'algébricité d'une hypersurface analytique dans le contexte projectif (sans considérations de formes différentielles) exprimé cette fois en termes de la trace d'une fonction coordonnée. Je l'énonce dans le cas des courbes pour alléger : $C = C_1 \cup \cdots \cup C_d$ est une collection de germes de courbes analytiques de $\mathbb{C}^2$ transverses à la droite "verticale" $x = 0$ et les droites voisines ont pour équation $x = ay + b$. On peut donc considérer la trace $Tr_C\, y$, germe de fonction holomorphe en (a, b) au voisinage de $(0, 0)$.

Théorème 3 *[144] Il existe une courbe algébrique $\tilde{C} \subset \mathbb{P}^2$ de degré d contenant V si et seulement si $Tr_C\, y$ est polynomiale de degré 1 en b.*

Il est aisé de voir que cette condition est nécessaire par un calcul direct ou bien comme conséquence de la formule d'Abel-Jacobi [135]. Pour une droite L fixée, cette condition se traduit par la relation de Reiss [55] :

$$\sum_{p \in C \cap L} \frac{f_{xx} f_y^2 - 2 f_{xy} f_x f_y + f_{yy} f_x^2}{f_y^3}(p) = 0, \tag{1.2}$$

où les notations $f_x, f_{xy}, \ldots$ désignent les dérivées partielles du polynôme f définissant la courbe algébrique C.

Quelques contributions au cadre projectif. Mes premiers travaux dans [135] ont consisté à revisiter la preuve de Henkin-Passare afin de mettre en lumière les liens entre les théorèmes d'inversions et le calcul résiduel multivarié, en particulier le théorème de dualité et le théorème des résidus. Une des conséquences est une forme légèrement plus forte du théorème 2 d'Abel-inverse :

Théorème 4 *[135, Thm.3] Il suffit que la trace $Tr_V\Phi$ soit rationnelle en les coefficients constants des équations du k-plan (donc en la variable b avec les notations précédentes) pour que la paire (V,Φ) s'étende algébriquement à $\mathbb{P}^n$.*

Au-delà de ce résultat, j'établis dans [135] le lien entre le théorème d'Abel-inverse et le théorème de Wood et j'obtiens une nouvelle preuve de la dimension

$$\dim\, H^0(V,\omega_V^{n-1}) = \binom{d-1}{n}$$

de l'espace des $(n-1)$-formes holomorphes (encore une fois au sens des sections globales du faisceau dualisant) sur une hypersurface algébrique $V \subset \mathbb{P}^n$ de degré d. Ces résultats s'appuient sur une représentation résiduelle des formes traces sur laquelle nous reviendrons plus en détails en Section 1.5.2.

1.3 Généralisations au cadre torique

Les théorèmes d'algébricité ci-dessus requièrent de considérer des germes analytiques de $\mathbb{C}^n$ qui sont alignés, ce qui est bien entendu une contrainte forte. Pour des germes en position quelconque, on est amené à considérer des traces relatives à des sous-variétés de plus grands degrés. D'un autre côté, il est naturel de considérer les problèmes d'algébricité dans des variétés plus générales que l'espace projectif $\mathbb{P}^n$.

Ces considérations m'ont poussé à m'intéresser à la trace dans les variétés toriques. D'un point de vue effectif, le cadre torique permet de contrôler le polytope de Newton du polynôme interpolant recherché, défini comme l'enveloppe convexe des exposants du développement monomial : si $f = \sum_{m=(m_1,\dots,m_n)} a_m x_1^{m_1}\cdots x_n^{m_n}$, son polytope de Newton est

$$P_f := \mathrm{Conv}(m \in \mathbb{N}^n,\, a_m \neq 0) \subset \mathbb{R}^n.$$

Cet objet est au coeur de la géométrie torique, offrant une passerelle entre théorie de l'intersection torique et combinatoire. Un exemple classique est donné par le *théorème de Bernstein-Kushnirenko* [18, 79] : si $f_1,\dots,f_n \in \mathbb{C}[x_1^{\pm 1},\dots,x_n^{\pm 1}]$ sont n polynômes de Laurent définissant une intersection complète dans le tore, le nombre de zéros communs (avec multiplicités) est majoré par le volume mixte de leurs polytopes. Afin d'avoir égalité, il faut tenir compte des zéros à l'infini dans une certaine compactification torique du tore dépendante des polytopes en jeu (généralisation torique du théorème de Bézout).

Je décris ici mes contributions principales autour de la trace dans les variétés toriques. Les publications afférentes sont [139, 136].

1.3.1 Rudiments de géométrie torique.

Pour une introduction plus détaillée aux variétés toriques, on renvoie le lecteur aux nombreux ouvrages sur le sujet. Quelques livres classiques sont [47, 36, 94]. Je me permets de citer aussi le Chapitre 2 de ma thèse [134] pour une introduction adaptée aux problèmes évoqués dans ce mémoire.

Une variété torique lisse sur $\mathbb{C}$ est construite à partir d'un éventail régulier Σ de $\mathbb{R}^n$, réunion de cônes rationnels polyédraux réguliers stable par face et par intersection. La variété torique $X = X_\Sigma$ est obtenue en recollant les cartes affines

$$U_\sigma := \mathrm{Spec}\,\mathbb{C}\,[\check{\sigma} \cap \mathbb{Z}^n] \simeq \mathbb{C}^n$$

où $\sigma \in \Sigma(n)$ parcourt les cônes de l'éventail de dimension maximale n, et où $\check{\sigma}$ désigne le cône dual. Les changements de cartes entre deux cartes affines U_σ et $U_{\sigma'}$ sont donnés par les applications monomiales induites par le changement de base de $\check{\sigma} \cap \mathbb{Z}^n$ à $\check{\sigma'} \cap \mathbb{Z}^n$. La variété X est compacte si et seulement si Σ est complet (*i.e.* recouvre $\mathbb{R}^n$), ce que l'on supposera désormais. Des exemples typiques sont les espaces projectifs, les espaces projectifs à poids, ou les produits de tels espaces.

L'action du tore algébrique

$$\mathbb{T} := (\mathbb{C}^*)^n = \operatorname{Spec} \mathbb{C}\,[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$$

sur lui-même s'étend en une action sur chaque carte affine qui est compatible avec les changements de cartes, donc le tore agit sur X. La variété X peut ainsi être vue comme une compactification du tore

$$X = \mathbb{T} \cup \bigcup_{\rho \in \Sigma(1)} D_\rho,$$

où les diviseurs D_ρ sont les diviseurs de Cartier irréductibles $\mathbb{T}$-invariants de X (clôtures de Zariski des orbites de codimension 1), en bijection avec les cônes ρ de dimension 1 de Σ.

Les fibrés en droites associés aux diviseurs D_ρ engendrent le groupe de Picard $\operatorname{Pic}(X)$ de X. Tout $\mathbb{T}$-diviseur (i.e. $\mathbb{T}$-invariant) $D \in \operatorname{Div}(X)$ s'écrit

$$D = \sum_{\rho \in \Sigma(1)} k_\rho D_\rho, \quad k_\rho \in \mathbb{Z}.$$

Tout monôme de Laurent $x^m = x_1^{m_1} \cdots x_n^{m_n}$ définit une fonction rationnelle sur X dont le diviseur est $\mathbb{T}$-invariant :

$$\operatorname{Div}(x^m) = \sum_{\rho \in \Sigma(1)} \langle m, \eta_\rho \rangle D_\rho,$$

où $\eta_\rho \in \mathbb{Z}^n$ est le générateur du semi-groupe $\rho \cap \mathbb{Z}^n$ et où $\langle \cdot, \cdot \rangle$ désigne le produit scalaire canonique sur $\mathbb{R}^n$. Notons L_D le fibré en droite associé au diviseur D, que l'on identifiera avec le faisceau $\mathcal{O}_X(D)$ des fonctions méromorphes de diviseur polaire borné par D. On a alors

$$\Gamma(X, L_D) \simeq \bigoplus_{m \in P_D \cap \mathbb{Z}^n} \mathbb{C} \cdot x^m, \tag{1.3}$$

où P_D est le polytope

$$P_D = \{m \in \mathbb{R}^n, \langle m, \eta_\rho \rangle + k_\rho \geq 0 \quad \forall \rho \in \sigma(1)\}.$$

Le fibré L_D est globalement engendré (i.e. le système linéaire associé est sans point base) si et seulement si

$$k_\rho = - \min_{m \in P_D \cap \mathbb{Z}^n} \langle m, \eta_\rho \rangle \qquad \forall\, \rho \in \Sigma(1).$$

Ceci équivaut au fait qu'une hypersurface générale $H \in |L_D|$ ne passe pas par les points $\mathbb{T}$-invariants de X. Dit autrement : dans chaque carte affine U_σ, son équation polynomiale a un terme constant non nul. Ces termes constants joueront un rôle important dans ce qui suit.

1.3.2 Concavité torique et théorème d'Abel.

Soit X une variété complexe compacte lisse de dimension n et soit $L_1, \dots, L_k$ une collection de $k < n$ fibrés en droite sur X. En supposant les systèmes linéaires $|L_i|$ de dimensions positives, on peut considérer l'espace de paramètres

$$X^* := \mathbb{P}(\Gamma(X, L_1)) \times \cdots \times \mathbb{P}(\Gamma(X, L_k)).$$

Tout élément $a = (a_1, \dots, a_k) \in X^*$ définit une sous-variété (non nécessairement réduite)

$$C_a = H_{a_1} \cap \cdots \cap H_{a_k} \subset X$$

où $H_{a_i} \in |L_i|$ est le diviseur effectif associé à a_i. Il est naturel de chercher à généraliser la trace relativement à la famille de sous-variétés $(C_a)_{a \in X^*}$. Encore faut-il s'assurer que celles-ci soient génériquement des intersections complètes. Le cadre torique offre des critères combinatoires explicites permettant de s'en assurer.

On suppose désormais X torique et on se fixe une carte affine torique $X_0 \simeq \mathbb{C}^n$ de X. Quitte à effectuer un changement de coordonnées du tore, on supposera sans pertes de généralité que

$$X_0 \subset X, \qquad X_0 = \operatorname{Spec} \mathbb{C}[x_1, \dots, x_n]$$

et (1.3) permet d'identifier les sections globales de L_i à des polynômes en x supportés par un polytope explicite $P_i \subset (\mathbb{R}^+)^n$ d'intersection non vide avec les hyperplans de coordonnées. La proposition suivante donne des conditions combinatoires pour pouvoir définir raisonnablement la trace relativement aux fibrés $L_1, \dots, L_k$.

Proposition 1 *[134, Thm 2.2] La sous-variété $C_a \subset X$ est génériquement une intersection complète lisse si et seulement si les fibrés L_i sont globalement engendrés et la famille $(P_1, \dots, P_k)$ est essentielle, i.e. si pour tout sous-ensemble $I \subset \{1, \dots, k\}$, la dimension de la somme de Minkovski $\sum_{i \in I} P_i$ est au moins le cardinal de I.*

Si les fibrés ne sont pas globalement engendrés, l'intersection n'est plus génériquement complète : il existe des composantes immergées de dimensions variées sur les différentes $\mathbb{T}$-orbites de X (et on peut expliciter combinatoirement cette décomposition, voir [134, Thm 2.1]). Si les fibrés sont globalement engendrés mais la famille n'est pas essentielle, l'intersection C_a est génériquement vide, situation pathologique que l'on exclut.

Remarque 1 *Les conditions de la Proposition 1 n'assurent pas que C_a soit génériquement irréductible, ni que C_a intersecte toutes les orbites de dimension complémentaires k (penser au fibré $L = \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(2, 0)$, essentiel et globalement engendré, mais pour lequel un diviseur générique $C \in |L|$ est union de deux "droites verticales" dans $\mathbb{P}^1 \times \mathbb{P}^1$ qui ni ne s'intersectent entre elles, ni n'intersectent le $\mathbb{T}$-diviseur $\{0\} \times \mathbb{P}^1$).*

On dira qu'un ouvert $U \subset X$ est *concave* (relativement aux fibrés $L_1, \dots, L_k$) si par tout point de U passe une sous-variété C_a incluse dans U. On pose alors

$$U^* = \{a \in X^*, C_a \subset U\}$$

que l'on appelle le "dual" de U. On note $\operatorname{Reg}(U^*) \subset U^*$ le sous-ensemble des a pour lesquels C_a est une intersection complète lisse. On note

$$I_U := \{(x, a) \in U \times U^*, \ x \in C_a\}$$

la variété d'incidence associée.

Proposition 2 *[139, Proposition 2.9] Soit $U \subset X$ un ouvert concave relativement à une famille essentielle de fibrés en droites $L_1, \dots, L_k$ globalement engendrés.*

- *U^* est un ouvert de X^*, connexe si U l'est.*
- *$\mathrm{Reg}(U^*)$ est un ouvert de Zariski non vide de U^*.*
- *La projection $I_U \to U$ est une submersion holomorphe et la projection $I_U \to U^*$ est surjective, holomorphe, propre, et définit une submersion sur $\mathrm{Reg}(U^*)$.*
- *Si $W \subset U$ est un fermé de codimension $> k$, le sous-ensemble $W^* \subset U^*$ pour lequel l'intersection $C_a \cap W$ n'est pas vide est un fermé de codimension > 0.*

Pour plus de détails concernant les problèmes de concavité torique, en particulier la notion de dégénérescence, de traces de cycles, et du lien avec la théorie des résultants, j'encourage le lecteur à consulter [134, Chapitre 2].

Le théorème d'Abel torique. Soit $U \subset X$ un ouvert concave connexe de X associé à une famille de fibrés $L_1, \dots, L_k$ globalement engendrée et essentielle. Soit $V \subset U$ une sous-variété analytique fermée de codimension pure $k > 0$. Supposons que V ne soit pas dégénérée, *i.e.* qu'il existe $\alpha \in \mathrm{Reg}(U^*)$ tel que l'intersection $V \cap C_\alpha$ soit transverse (donc de dimension zéro, donc finie par un argument de compacité). Si Φ est une q-forme méromorphe sur V et holomorphe au voisinage de $V \cap C_\alpha$, on peut à nouveau définir un germe de trace

$$Tr_V \Phi(a) = \sum_{p \in C_a \cap V} \Phi(p),$$

définie et holomorphe dans au voisinage de α (fonctions implicites). Le théorème 1 se généralise naturellement :

Théorème 5 *Sous les hypothèses ci-dessus, le germe de trace $Tr_V \Phi$ holomorphe en α s'étend en une q-forme méromorphe sur U^*.*

Comme pour le cas projectif, ce théorème découle de l'interprétation de la trace comme un courant méromorphe (Section 1.4.4), la Proposition 2 assurant que ce courant n'est pas trivial. Le cadre torique est ici anecdotique, ce théorème s'étend à toute variété compacte X dès lors que $\mathrm{Reg}(U^*)$ est un ouvert de Zariski non vide de U^*.

1.3.3 Le théorème d'Abel-inverse torique.

On se restreint au cas hypersurface, *i.e.* on considère $k = n - 1$. D'après (1.3), la sous-variété C_a a pour équations polynomiales

$$C_a \cap X_0 = \{q_1(a_1, x) = \cdots = q_{n-1}(a_{n-1}, x) = 0\} \tag{1.4}$$

dans la carte affine $X_0 \simeq \mathbb{C}^n$, où $q_i(a_i, x) = \sum_{m \in P_i \cap \mathbb{Z}^n} a_{im} x^m$.

Si les fibrés L_i sont globalement engendrés, on a en particulier $0 \in P_i$. Autrement dit, chaque polynôme q_i a un coefficient constant a_{i0} génériquement non nul. Ces coefficients jouent un rôle particulier dans les problèmes d'inversion.

La condition que C_a soit génériquement une intersection complète ne suffit malheureusement pas à généraliser le théorème d'Abel-inverse ou le théorème de Wood au cadre torique, comme l'illustre l'exemple élémentaire suivant :

Exemple. *Considérons l'union de deux germes analytiques $V = \{y - e^x = 0\} \cup \{y + e^x\}$ de $\mathbb{C}^2$ aux points $(0, 1)$ et $(0, -1)$, transverses à la droite $x = 0$, et pensons le problème*

d'algébricité dans la variété torique $\mathbb{P}^1 \times \mathbb{P}^1$. Si l'on considère la trace relativement au fibré $L = \mathcal{O}_{\mathbb{P}^1\times\mathbb{P}^1}(1,0)$ (essentiel et globalement engendré), alors $\mathrm{Tr}_V\, y \equiv 0$ bien que l'hypersurface V ne s'étende pas algébriquement, en contradiction avec la généralisation souhaitée du théorème de Wood.

Cet exemple illustre le fait que les courbes C_a doivent être suffisamment "mobiles", ce que nous assurerons ici *en supposant les fibrés $L_1, \dots, L_{n-1}$ très amples* (en particulier X projective[2]). En particulier, ils sont globalement engendrés et $\dim P_i = n$ donc la famille est essentielle [134, Lemme 2.4].

Considérons alors $V \subset U$ une hypersurface analytique d'un ouvert concave relativement à la famille $L_1, \dots, L_{n-1}$. Les L_i étant très amples, V est transverse à C_a pour $a \in U^*$ générique [134, Lemme 2.14]. Nous supposerons que V n'a aucune composante incluse à l'infini $X \setminus X_0$, ce qui n'impacte pas les problèmes d'algébricité. Soit Φ une $(n-1)$-forme méromorphe sur V, non identiquement nulle sur chacune des composantes de V.

Théorème 6 *[139, Thm.4.1] Sous les hypothèses ci-dessus, il existe une hypersurface algébrique $\tilde{V} \subset X$ telle que $\tilde{V} \cap U = V$ et une forme rationnelle $\tilde{\Phi}$ sur $\tilde{V}$ telle que $\tilde{\Phi}_{|V} = \Phi$ si et seulement si la trace $Tr_V\Phi \in M^q(U^*)$ est rationnelle en les coefficients constants $(a_{10}, \dots, a_{n-1,0})$.*

Il n'échappera pas au lecteur que ce résultat est une généralisation du Théorème 4, version forte du théorème d'Abel-inverse.

1.3.4 Le théorème de Wood torique.

Soit $L_1, \dots, L_{n-1}$ une famille de fibrés en droites très amples sur une variété torique projective lisse. Soit $\alpha \in \mathrm{Reg}(X^*)$ et soit $V = V_1 \cup \cdots \cup V_N$ une collection de germes d'hypersurfaces analytiques transverses à la courbe C_α, que nous supposerons inclus dans la carte X_0. On veut cette fois caractériser la classe de Picard de l'éventuelle hypersurface interpolante, toujours en fonction des intersections locales $V \cap C_a$ pour a voisin de α.

D'après [134, Lemme 2.8], il existe $E_1, \dots, E_s$ des $\mathbb{T}$-diviseurs effectifs très amples supportés par $X \setminus X_0$ formant une base de $\mathrm{Pic}(X) \otimes \mathbb{Q}$. Toute section $f \in \Gamma(X, L_{E_j})$ - vue comme fonction rationnelle sur X de diviseur polaire borné par E_j - est holomorphe au voisinage de $V \cap C_\alpha$ et on peut considérer sa "norme" sur V,

$$N_V(f)(a) := \prod_{p \in V \cap C_a} f(p),$$

fonction définie et holomorphe au voisinage de $\alpha \in U^*$.

Théorème 7 *[136, Thm 1 et 2] Soit V comme ci-dessus. Supposons pour simplifier qu'aucun des germes V_i ne soit de la forme $x_n = $ constante.*

1. *Il existe $\tilde{V} \subset X$ algébrique contenant les V_i et telle que $\tilde{V} \cap C_\alpha = V \cap C_\alpha$ si et seulement si $Tr_V(x_n)$ est affine en $(a_{10}, \dots, a_{n-1,0})$.*
2. *Le polytope $P \subset (\mathbb{R}^+)^n$ associé au fibré en droite défini par $\tilde{V}$ vérifie*

$$MV(P_1, \dots, P_{n-1}, P) = N$$

où $MV(\,)$ désigne le volume mixte.

2. Il suffit en fait que les fibrés soient globalement engendrés et que les polytopes P_i contiennent le simplexe élémentaire, cf [139]. Une telle famille existe, quand bien même X n'est pas projective. Il est très probable que cette condition puisse elle aussi être affaiblie, piste à creuser d'un point de vue effectivité.

3. Le polytope P est uniquement caractérisé par les égalités

$$deg_{a_{10}}\ N_V(f_j) = MV(P_{E_j}, P_2, \ldots, P_{n-2}, P)$$

pour $f_j \in \Gamma(X, L_{E_j})$ générique et $j = 1, \ldots, s$.

Le point 3 caractérise la classe de Picard de $\tilde{V}$ dans $\mathrm{Pic}(X)$ (donc sa classe modulo équivalence rationnelle ici), donc caractérise "presque" le polytope de Newton du polynôme interpolant f. Plus précisément, on a $P_f \subset P$, avec au moins un point sur chaque facette. Il y a égalité $P_f = P$ si et seulement si $\tilde{V}$ ne passe pas par les points $\mathbb{T}$-fixes de X, ce qui est le cas générique.

Exemple. Dans le cas de la trace relativement à des droites de $\mathbb{P}^n$, le point 1 implique que $\tilde{V}$ est de degré N, caractérisant ici sa classe dans $\mathrm{Pic}(\mathbb{P}^n) \simeq \mathbb{Z}$. Soit Δ le simplexe élémentaire. On a $P_i = \Delta$ et $P = N\Delta$, d'où

$$MV(\Delta, \ldots, \Delta, N\Delta) = Nn!\mathrm{Vol}(\Delta) = N$$

en accord avec le point 2. Le point 3 traduit ici le fait que la norme sur $\tilde{V}$ d'un polynôme de degré 1 est de degré $\leq N$ en a_{10}, ce qui est ici automatiquement vérifié.

1.4 Trace et courants : la transformée d'Abel-Radon

La notion de trace est intimement liée à la théorie des *courants* introduite par Laurent Schwartz dans les années 1950. On esquisse ici brièvement quelques points essentiels pour notre propos, conduisant à une preuve élégante du théorème d'Abel, et préparant le terrain aux relations entre traces et résidus, éléments clés des théorèmes d'inversion.

1.4.1 Courants.

Rappelons qu'il existe une bigraduation des formes différentielles suivant le z-degré et le $\bar{z}$-degré, où $z = (z_1, \ldots, z_n)$ et $\bar{z} = (\bar{z}_1, \ldots, \bar{z}_n)$ sont les coordonnées holomorphes et anti-holomorphes de $\mathbb{C}^n$ (ou dans un ouvert de $\mathbb{C}^n$ si on travaille dans une carte d'une variété analytique lisse X de dimension n). La différentiation extérieure d est la somme $d = \partial + \bar{\partial}$ des différentielles partielles par rapport à z et $\bar{z}$, chacune augmentant d'une unité le z-degré (resp. le $\bar{z}$-degré), i.e. $\partial f = \sum \frac{\partial f}{\partial z_i} dz_i$ et $\bar{\partial} f = \sum \frac{\partial f}{\partial \bar{z}_i} d\bar{z}_i$. On a

$$\partial \circ \partial = \bar{\partial} \circ \bar{\partial} = 0 \quad \text{et} \quad \bar{\partial} \circ \partial = \partial \circ \bar{\partial}.$$

Les formes holomorphes sont les $(q, 0)$-formes $\bar{\partial}$-fermées. Les formes méromorphes sont des quotients de formes holomorphes par une fonction holomorphe non nulle. Les formes tests sont des formes de bidegrés (p, q) arbitraires, indéfiniment différentiables et à support compact. On notera $\mathcal{D}^{p,q}(X)$ l'espaces des formes tests de bidegrés (p, q) sur X. Un (p, q)-courant est une forme linéaire continue sur l'espace $\mathcal{D}^{n-p,n-q}(X)$ que l'on munit de la topologie faible. Une (p, q)-forme localement intégrable ψ définit un (p, q)-courant

$$T_\psi(\theta) = \int_U \psi \wedge \theta.$$

La différentiation sur un (p, q)-courant est définie par :

$$\langle \partial T, \theta \rangle = (-1)^{p+q+1} \langle T, \partial\theta \rangle \quad \text{et} \quad \langle \bar{\partial} T, \theta \rangle = (-1)^{p+q+1} \langle T, \bar{\partial}\theta \rangle.$$

Une $(p, 0)$-forme localement intégrable est holomorphe si le courant associé est $\bar{\partial}$-fermé. Nous aurons besoin également d'une caractérisation des formes méromorphes et holomorphes sur des espaces singuliers.

1.4.2 Méromorphie sur un sous-ensemble analytique singulier.

Soit $V \subset U$ un sous-ensemble analytique (possiblement singulier) de dimension pure d'un ouvert U de $\mathbb{C}^n$. On dit qu'une $(q,0)$-forme Φ est méromorphe sur V si elle est localement restriction à V d'une forme méromorphe dans l'espace ambiant, dont le lieu polaire coupe proprement V. On note M_V^q le faisceau sur V correspondant.

Soit $W \subset V$ une sous-variété contenant le lieu singulier de V et telle que $\dim W < \dim V$. Soit Φ une $(q,0)$-forme holomorphe sur la variété lisse $V \setminus W$. Alors Φ s'étend en une forme méromorphe sur V si et seulement si le courant

$$\theta \mapsto \int_{V\setminus W} \Phi \wedge \theta$$

défini sur les formes test de $U \setminus W$ s'étend en un courant sur U. Cette condition est aussi équivalente au fait que si g est une fonction holomorphe au voisinage V s'annulant sur W mais non identiquement nulle sur chacune des composantes de V, alors l'application

$$T : \theta \mapsto \lim_{\varepsilon\to 0} \int_{V\cap\{|g|>\varepsilon\}} \Phi \wedge \theta$$

définit un courant sur U, indépendant du choix de g. Ce courant, noté

$$T = [V] \wedge \Phi$$

est le produit du courant d'intégration $[V]$ avec le courant valeur principal associé à Φ [66, Thm1]. Il est supporté par V et $\bar\partial$-fermé sur $U \setminus W$.

1.4.3 Holomorphie sur un sous-ensemble analytique singulier.

Soit $\Phi \in M_V^q$. On dit que la forme Φ est holomorphe sur V (au sens de [66, def 2]) si le courant $\Phi \wedge [V]$ est $\bar\partial$-fermé sur U, i.e.

$$\bar\partial(\Phi \wedge [V]) \equiv 0. \tag{1.5}$$

On note ω_V^q le faisceau correspondant. On parle aussi du faisceau des formes abéliennes, ou du faisceau de Barlet. Si V est lisse, on retrouve le faisceau usuel $\omega_V^q = \Omega_V^q$. Si V est possiblement singulière et $q = \dim V$, alors ω_V^q coïncide avec le faisceau dualisant de Serre-Gröthendieck [66].

La restriction à V d'une forme holomorphe dans l'espace ambient est holomorphe. Si V est lisse, la réciproque est vraie. Si V est singulière, ce n'est plus le cas comme le montre l'exemple simple suivant, extrait de [66].

Exemple : Considérons la forme méromorphe $\Phi = dx/y$ sur le germe de courbe $(C,0)$ défini par $y^2 - x^3 = 0$. Considérons la paramétrisation $t \mapsto (t^2, t^3)$ de C. Pour une fonction test θ, on a :

$$\begin{aligned}\langle\bar\partial([C]\wedge\Phi),\theta\rangle &:= \lim_{\varepsilon\to0}\int_{C\cap|x|>\varepsilon}\frac{\bar\partial\theta\wedge dx}{y} = \lim_{\varepsilon\to0}\int_{C\cap|x|=\varepsilon}\frac{\theta dx}{y}\\ &= \lim_{\varepsilon\to0}\int_{|t|=\varepsilon}\frac{\theta(t^2,t^3)2dt}{t^2} = 4i\pi\frac{d}{dt}\theta(t^2,t^3)_{|t=0} = 0,\end{aligned}$$

la seconde égalité par le théorème de Stokes et la dernière égalité par le théorème de Cauchy généralisé aux fonctions semi-méromorphes, i.e. quotients de fonctions $\mathcal{C}^\infty$ par une fonction holomorphe. Ainsi, $\Phi \in \omega_{C,0}$. Pour autant, Φ n'est pas restriction à C d'un germe de

forme holomorphe en $(\mathbb{C}^2, 0)$. En effet, sinon Φ serait en particulier holomorphe sur toute normalisée de C, contredisant le fait que $\Phi(t^2, t^3) = \frac{2dt}{t^2}$ n'est pas holomorphe en 0.

Il existe plus généralement d'autres notions d'holomorphies sur un espace analytique singulier qui ne coïncident pas nécessairement entre elles (voir [66]).

1.4.4 La trace comme transformée d'Abel-Radon.

Plaçons nous dans le cadre de la section 1.3, i.e. d'une variété torique compacte lisse X et d'un ouvert concave U associé à une famille essentielle de fibrés en droites globalement engendrés $(L_1, \dots, L_k)$. Soit $V \subset U$ de codimension pure k et $\Phi \in M^q(V)$. Supposons qu'il existe $a \in U^*$ tel que l'intersection $V \cap C_a$ soit transverse. D'après la Proposition 2, le sous-ensemble $W^* \subset U^*$ des a pour lesquels l'intersection $V \cap C_a$ n'est pas transverse ou rencontre le lieu polaire de Φ est un sous-ensemble analytique fermé de codimension ≥ 1 et la forme $Tr_V(\Phi)$ est ainsi définie et holomorphe sur l'ouvert dense $U^* \setminus W^*$.

Considérons la variété d'incidence $I_U := \{(x, a) \in U \times U^* \ ; \ x \in C_a\}$, munie des projections $p_U : I_U \to U$ et $q_U : I_U \to U^*$. L'application p_U est une submersion et l'application q_U est propre du fait de la compacité de l'espace projectif. On peut ainsi définir pour tout sous-ensemble analytique fermé V de U et toute q-forme méromorphe Φ sur V le courant sur U^*

$$\mathcal{A}(\Phi \wedge [V]) := q_{U*}(p_U^* \Phi \wedge [p_U^{-1}(V)]),$$

que l'on appelle la *transformée d'Abel-Radon* de $\Phi \wedge [V]$. Le lien entre trace et courants est fourni par le résultat suivant :

Proposition 3 *On a l'égalité $\mathcal{A}(\Phi \wedge [V]) = Tr_V(\Phi)$ vue comme une égalité de courants sur l'ouvert $U^* \setminus W^*$.*

Preuve des théorèmes 1 et 5.

Puisque le courant $\mathcal{A}(\Phi \wedge [V])$ est par construction défini sur U^*, il suit de la Proposition 3 et de la Section 1.4.2 que $Tr_V(\Phi)$ s'étend en une forme méromorphe sur U^*, ce qui démontre la version méromorphe du théorème 5. Si de plus Φ est holomorphe (au sens des courants (1.5)), l'holomorphie des applications q_U et p_U implique l'égalité

$$\bar{\partial} Tr_V \Phi = \bar{\partial} \mathcal{A}(\Phi \wedge [V]) = \mathcal{A}(\bar{\partial}(\Phi \wedge [V])) = 0.$$

Autrement dit, $Tr_V \Phi$ est holomorphe sur U^*. □

Outre le fait que la définition (1.5) des formes holomorphes sur un espace singulier coïncide avec le faisceau dualisant dans le cas $q = \dim V$, cette dernière égalité montre que la définition (1.5) est aussi naturelle du point de vue de la transformée d'Abel-Radon.

1.5 Trace et résidus

Les preuves des théorèmes d'inversion sont basées sur une représentation "résiduelle" des formes trace dans le cadre torique. Puisque les résidus reviendront régulièrement dans ce mémoire, y compris les courants résiduels, prenons le temps d'une brève introduction au calcul résiduel.

1.5.1 Rudiments de calcul résiduel

La théorie des résidus multivariés est un vaste sujet à l'interface de l'analyse complexe et de la géométrie algébrique. Au-delà du sujet qui nous préoccupe ici, les résidus multivariés interviennent par exemple dans des problèmes effectifs d'appartenance aux idéaux polynomiaux (Nullstellensatz, relations de Bézout multivariées, clôture intégrale, etc.) ou encore pour la réalisation explicite des théorèmes de dualité pour la cohomologie des faisceaux cohérents (nous y reviendrons dans le chapitre suivant).

Je présente ici modestement quelques aspects significatifs pour notre propos. Le lecteur curieux pourra consulter par exemple l'ouvrage récent très complet de Yger et Vidras [133] contenant de nombreuses références.

1.5.1.1 Courants résiduels.

Soit U un ouvert de $\mathbb{C}^n$ et soit $f : U \to \mathbb{C}$ une fonction holomorphe. En s'appuyant sur le théorème de désingularisation d'Hironaka, Herrera et Liebermann ont montré en 1971 [67] que l'on peut associer à f un courant *valeur principale* $[\frac{1}{f}]$ agissant sur $\theta \in \mathcal{D}^{n,n}(U)$ par

$$< [\frac{1}{f}], \theta >:= \lim_{\varepsilon \to 0} \int_{|f|>\varepsilon} \frac{\theta}{f}.$$

On appelle *courant résiduel* associé à f le courant $\bar\partial[\frac{1}{f}]$. Par le théorème de Stokes, ce courant de degré $(0,1)$ agit sur $\theta \in \mathcal{D}^{n,n-1}(U)$ par

$$< \bar\partial[\frac{1}{f}], \theta >= \lim_{\varepsilon \to 0} \int_{|f|=\varepsilon} \frac{\theta}{f}.$$

Plus généralement, si $f_1, ..., f_k \in \mathcal{O}(U)$ définissent une intersection complète $V \subset U$ de codimension k, Coleff et Herrera ont montré que l'on pouvait définir un courant résiduel de degré $(0,k)$ agissant sur $\mathcal{D}^{n,n-k}(U)$ par

$$\langle \bar\partial[\frac{1}{f_1}] \wedge \cdots \wedge \bar\partial[\frac{1}{f_k}], \theta \rangle := \lim_{\underline{\varepsilon} \to 0} \int_{|f_1|=\varepsilon_1,\ldots,|f_k|=\varepsilon_k} \frac{\theta}{f_1 \cdots f_k}, \tag{1.6}$$

où la limite doit être précautionneusement considérée selon un chemin admissible (voir par exemple [35, 99]). Ce courant est $\bar\partial$-fermé, supporté par V et nul sur les formes-test à coefficients anti-holomorphes. Il est lié au courant d'intégration $[V] : \theta \mapsto \int_V \theta$ par la formule de Lelong-Poincaré

$$[V] = \frac{1}{(2i\pi)^k} \bar\partial[\frac{1}{f_1}] \wedge \cdots \wedge \bar\partial[\frac{1}{f_k}] \wedge df_1 \wedge \cdots \wedge df_k, \tag{1.7}$$

que l'on peut considérer comme la généralisation multivariée de la célèbre formule de Cauchy

$$f(a) = \frac{1}{2i\pi} \int_{|z-a|=\varepsilon} \frac{f(z)dz}{z-a}.$$

Un outil majeur du calcul résiduel est *le théorème de dualité* caractérisant l'appartenance aux idéaux : si U est un domaine d'holomorphie et $h \in \mathcal{O}(U)$, alors

$$h \in (f_1, \ldots, f_k) \iff h\bar\partial[\frac{1}{f_1}] \wedge \cdots \wedge \bar\partial[\frac{1}{f_k}] \equiv 0. \tag{1.8}$$

Le théorème de dualité et les courants résiduels sont des outils puissants pour les problèmes effectifs d'appartenance aux idéaux polynomiaux comme le Nullstellensatz d'Hilbert ou les relations de Bézout [17, 11, 16, 126].

Remarque 2 *Dans [100], Passare, Tsikh et Yger donnent une autre construction du courant de Coleff-Herrera dans laquelle le noyau de Cauchy est remplacé par un noyau de Bochner-Martinelli. L'avantage de leur approche est double : elle évite l'inconvénient des chemins admissibles dans la limite (1.6) et elle permet d'étendre le théorème de dualité aux intersections non complètes.*

1.5.1.2 Résidus de Grothendieck.

Lorsque $k = n$, le courant résiduel est intimement lié aux résidus de Grothendieck, généralisation multivariée du résidu de Cauchy. Soit U un ouvert de $\mathbb{C}^n$ et soit $f_1, \dots, f_n \in \mathcal{O}(U)$ définissant une intersection complète (i.e. ayant un nombre fini de zéros communs dans ce cas) et soit $p \in U$ un zéro isolé de $f = (f_1, \dots, f_n)$. Considérons une n-forme méromorphe de la forme $\Phi = \frac{\omega}{f_1 \cdots f_n}$ où $\omega \in \Omega^n(U)$. On appelle résidu ponctuel de Grothendieck de Φ en p le nombre complexe

$$\operatorname{res}_p \left(\frac{\omega}{f_1 \cdots f_n} \right) := \frac{1}{(2i\pi)^n} \int_{\gamma_\varepsilon \cap B} \frac{\omega}{f_1 \cdots f_n},$$

où $\gamma_\varepsilon = \{|f_1| = \varepsilon_1, \dots, |f_n| = \varepsilon_n\}$ est un n-cycle réel d'intégration convenablement orienté (cf [57, Chapitre 6]) et où B est une boule centrée en p suffisamment petite pour ne contenir aucun autre zéro commun aux f_i. Cette définition ne dépend pas de $(\varepsilon_1, \dots, \varepsilon_n)$ pour les ε_j suffisamment petits par le théorème de Stokes.

On appelle *résidu global* de la forme méromorphe Φ sur U la somme de ses résidus ponctuels en les zéros communs $p_1, \dots, p_r \in U$ des f_i. Il découle de la formule de Stokes que cette somme de résidus locaux peut se voir comme l'action globale d'un courant résiduel multiplié par une forme holomorphe : si θ est une fonction test valant 1 au voisinage des p_i, on a

$$\sum_{i=1}^{r} \operatorname{res}_{p_i} \left(\frac{\omega}{f_1 \cdots f_n} \right) = \frac{1}{(2i\pi)^n} \langle \bar\partial \big[\frac{1}{f_1}\big] \wedge \cdots \wedge \bar\partial \big[\frac{1}{f_n}\big], \theta \cdot \omega \rangle. \tag{1.9}$$

Cette formule est une généralisation multivariée du théorème des résidus (et de la formule de Cauchy). Il est commun de noter ce résidu global sous la forme (en omettant abusivement la dépendance en U) :

$$\operatorname{Res} \left[\begin{matrix} \omega \\ f_1, f_2, \dots, f_n \end{matrix} \right] := \sum_{i=1}^{r} \operatorname{res}_{p_i} \left(\frac{\omega}{f_1 \cdots f_n} \right).$$

1.5.1.3 Théorème des résidus sur une variété compacte.

Soit X une variété analytique lisse de dimension n, et soit $\Phi \in M^n(X)$ une forme méromorphe dont le diviseur polaire D vérifie

$$D = D_1 + \cdots + D_n \qquad \text{et} \qquad |D_1 \cap \cdots \cap D_n| = \{p_1, \dots, p_r\}.$$

On peut alors considérer les résidus ponctuels de Φ en chaque point $p_i \in X$. Le cas des variétés compactes (par exemple les variétés projectives) conduit au résultat fondamental suivant.

Théorème des résidus. *Si X est compacte, on a $\sum_{i=1}^{r} \operatorname{res}_{p_i} \Phi = 0$.*

En effet, on peut définir globalement sur X un courant résiduel R^f localement de la forme (1.6), en remplaçant $(f_1, \dots, f_k)$ par une section f d'un fibré vectoriel Hermitien de rang k.

Les égalités (1.7), (1.8) et (1.9) s'étendent à ce cadre global [3] voir par exemple [145]. Ceci permet d'associer à Φ un courant $T = R^f \wedge \Phi$ sur X de bidegré (n,n) (i.e. une distribution). Le point clé est que le courant T est $\bar\partial$-exact, i.e. il existe un courant T' de degré $(n,n-1)$ sur X tel que $T = \bar\partial T'$. En agissant sur la fonction test $\theta = 1$ (à support compact du fait de la compacité de X), la formule (1.9) conduit alors à l'égalité voulue

$$\sum_{i=1}^{r} \mathrm{res}_{p_i}\Phi = \langle T, 1\rangle = \langle \bar\partial T', 1\rangle = \pm\langle T', \bar\partial 1\rangle = 0.$$

Une autre preuve du théorème des résidus est esquissée dans [57, Chapitre 6] via la cohomologie $\bar\partial$ de Dolbeault (le théorème de Stokes étant toujours caché derrière).

1.5.1.4 Formule de Jacobi torique.

Le théorème des résidus dans le cadre torique implique le résultat suivant, connu sous le nom de formule de Jacobi torique, dûe à Khovanskii [74]. Soient $f_1,\dots,f_n$ des polynômes de Laurent en $t = (t_1,\dots,t_n)$ de polytopes de Newton respectifs $P_1,\dots,P_n$, que l'on suppose non dégénérés, i.e. tels que les polynômes de facettes n'aient pas de zéros communs non triviaux. Notons $\mathrm{Int}(P)$ l'intérieur relatif de la somme de Minkovski $P = P_1 + \cdots + P_n$. Alors pour tout polynôme de Laurent $h \in \mathbb{C}[t_1^{\pm 1},\dots,t_n^{\pm 1}]$, on a

$$P_h \subset \mathrm{Int}(P) \quad \Longrightarrow \quad \mathrm{Res}\begin{bmatrix} h\frac{dt_1\wedge\cdots\wedge dt_n}{t_1\cdots t_n} \\ f_1,\dots,f_n \end{bmatrix} = 0. \tag{1.10}$$

En effet, considérons X une variété torique compacte dont l'éventail est un raffinement de l'éventail normal à P. Soit $D_i \subset X$ la clôture de l'hypersurface $f_i = 0$. L'hypothèse de non dégénérescence assure que $D_1 \cap \cdots \cap D_n \subset \mathbb{T}$ et la condition $P_h \subset \mathrm{Int}(P)$ implique précisément que la fonction rationnelle

$$\Phi = \frac{dt_1\wedge\cdots\wedge dt_n}{t_1\cdots t_n}\frac{h}{f_1\cdots f_n}$$

a pour lieu polaire $D_1 + \cdots + D_n$ dans X (il n'y a pas de pôles supplémentaires qui apparaissent sur le bord $X \setminus \mathbb{T}$). Le théorème des résidus permet de conclure.

1.5.2 Représentation résiduelle de la trace

Etablissons maintenant le lien entre trace et résidus. Considérons pour simplifier le cas hypersurface. On garde les notations de la section 1.4.4. Soit $(L_1,\dots,L_{n-1})$ une famille essentielle de fibrés en droites globalement engendrés sur une variété torique compacte lisse X et soit $U \subset X$ un ouvert connexe et concave relativement aux fibrés L_i. Soit $V \subset U$ une hypersurface analytique fermée et Φ une q-forme méromorphe sur V.

Considérons $\alpha \in \mathrm{Reg}(U^*)$ tel que l'intersection $V \cap C_\alpha$ soit transverse, incluse dans la carte affine $X_0 \simeq \mathbb{C}^n$ munie de coordonnées $x = (x_1,\dots,x_n)$. On note $f(x) = 0$ l'équation analytique de l'hypersurface V au voisinage de $V \cap C_\alpha$, et $q_1,\dots,q_{n-1}$ les équations affines (1.4) de C_a.

3. Afin de définir un courant résiduel global, on utilise plutôt les représentations intégrales basées sur le noyau de Bochner-Martinelli [100]. Une autre motivation de mes travaux, peu explorée finalement, était d'ailleurs de s'inscrire dans l'intense activité autour des résidus et des résultants dans les variétés toriques, comme l'illustre le livre de Gelfan'd, Kapranov et Zelevinski [51]. Cette dynamique a poussé les analystes complexes à généraliser différentes transformées intégrales (Cauchy, Abel, Abel-Radon, Fantappié-Martineau, Bochner-Martinelli) au cadre torique, afin de développer des représentations intégrales dont les noyaux sont intrinsèquement associés à la variété torique (indépendant d'un plongement projectif), cf [80, 123].

Proposition 4 *Soit P_i le polytope associé au fibré L_i par (1.3). Pour a voisin de α, on a*

$$Tr_V\Phi = \sum_{|I|=q} \sum_{M\in\prod_{i\in I} P_i} \mathrm{Res}\begin{bmatrix} x^{|M|}\Phi\wedge df\wedge \bigwedge_{j\notin I} dq_j \\ f(x), q_1(a_1,x),\dots,q_{n-1}(a_{n-1},x)\end{bmatrix} da_M, \tag{1.11}$$

où $M=(m_{i_1},\dots,m_{i_q})$, $|M|=m_{i_1}+\cdots+m_{i_q}$ et $da_M=\wedge_{i\in I} da_{im_i}$.

Preuve. Pour toute forme-test φ sur U^* de bidegré convenable, on a

$$\begin{aligned}\langle \mathrm{Tr}_V(\Phi),\varphi\rangle &= \int_{U^*} \mathrm{Tr}_V(\Phi)\wedge\varphi \\ &= \int_{\mathrm{I}_U} [p_U^{-1}(V)]\wedge p_U^*[\Phi]\wedge {q_U}^*(\varphi) \\ &= \int_{U\times U^*} [V]\wedge[I_U]\wedge\Phi\wedge\varphi,\end{aligned}$$

la seconde égalité d'après la Proposition 3. Le courant $T:=[V]\wedge[I_U]\wedge\Phi$ est donc un courant de bidegré $(q+n,n)$ sur $U\times U^*$ d'image directe $q_{U*}T=\mathrm{Tr}_V\Phi$. Le résultat découle alors de la formule de Lelong-Poincaré (1.7) et de la formule des résidus à plusieurs variables (1.9). □

Ainsi, la forme trace $\mathrm{Tr}_V\Phi$ est une $(q,0)$-forme méromorphe sur U^* dont les coefficients sont des résidus globaux dans U dépendant méromorphiquement de a. Regardons de plus près les cas extrémaux $q=0$ et $q=n-1$ qui nous intéressent :

- Si $\Phi=h$ est une fonction méromorphe, la formule devient

$$\mathrm{Tr}_V h = \mathrm{Res}\begin{bmatrix} h\,J(f,q)dx_1\wedge\cdots dx_n \\ f,q_1,\dots,q_{n-1}\end{bmatrix} \tag{1.12}$$

où $J(f,q)$ désigne le jacobien en x de l'application $(f,q_1,\dots,q_{n-1}):\mathbb{C}^n\to\mathbb{C}^n$.

- Si Φ est une forme méromorphe de degré maximal $n-1$ sur V, la formule devient

$$\mathrm{Tr}_V\Phi = \sum_{M\in P_1\times\cdots\times P_{n-1}} \mathrm{Res}\begin{bmatrix} x^{|M|}\Phi\wedge df \\ f,q_1,\dots,q_{n-1}\end{bmatrix} da_M. \tag{1.13}$$

Ces calculs se généralisent naturellement en toute codimension dès lors que l'on suppose que V est une intersection complète (le cas intersection non complète requiert des courants résiduels plus sophistiqués, cf [100]).

Dans le cas algébrique $U=X$, la Proposition 4 assure que les coefficients de la trace coïncident avec des *résidus toriques globaux* à la Cox, définis comme la trace (au sens de la dualité de Poincaré) d'un certain cocyle $\omega\in H^n(X,\Omega_X^n)$ construit à partir des coordonnées homogènes toriques (anneau de Cox) et de la forme d'Euler associée à l'éventail Σ de X, cf [28]. Ces résidus dépendent ici de paramètres : la théorie des résultants mixtes [51] permet alors de calculer explicitement le diviseur polaire des formes traces [29], tandis que la formule de Jacobi torique permet d'obtenir des majorations variées des degrés de la trace en certains coefficients a_{im} (e.g. Proposition 5 ci-après). Le lecteur curieux pourra consulter les Sections 1.4, 1.5, 3.2.2 et 3.3 de ma thèse [134] (en particulier les Propositions 3.4 et 3.5) et les références qui y sont mentionnées.

1.6 Eléments de preuve des théorèmes d'inversions

Terminons par donner quelques éléments de preuve du théorème 6 et du théorème 7.

1.6.1 Preuve du théorème d'Abel-inverse torique

Penchons-nous sur le théorème 6. On garde les notations et hypothèses de la section 1.3.3. Outre la représentation résiduelle des formes traces, un élément clé de la preuve est donné par le *lemme de propagation* [139, Lemme 4.3] ci-dessous.

Lemme 1 *Soit Φ une forme méromorphe de degré maximal sur l'hypersurface analytique $V \subset U$. Si la trace $Tr_V \Phi$ est rationnelle en a_{i0}, alors la trace $Tr_V h\Phi$ l'est aussi pour tout polynôme $h \in \mathbb{C}[x_1, \ldots, x_n]$ supporté par le polyèdre $\mathbb{R}^+ P_i$.*

Preuve. Pour $m \in \mathbb{N}^n$, notons $v_m := \mathrm{Res}\begin{bmatrix} x^m \Phi \wedge df \\ f, q_1, \ldots, q_{n-1} \end{bmatrix}$. D'après (1.13), on a :

$$Tr_V\, x^m \phi = \sum_{M \in P_1 \times \cdots \times P_{n-1}} v_{|M|+m}\, da_M.$$

On a $|M| \in P := P_1 + \cdots + P_{n-1}$, et on veut montrer que $v_{m'}$ (méromorphe sur U^*) est rationnelle en a_{i0} pour tout $m' \in P + kP_i$ et tout $k \in \mathbb{N}$. On le montre par récurrence sur k. Pour $k = 0$, c'est notre hypothèse. Supposons $v_{m'}$ rationnelle en a_{i0} pour $m' \in P + kP_i$ et montrons que $v_{m+m'}$ est rationnelle en a_{i0} pour tout $m \in P_i$.

La représentation intégrale de Cauchy des résidus de Grothendieck combinée à la formule de Stokes assure que pour tout $m \in P_i$ et tout $m' \in \mathbb{N}^n$, on a

$$\begin{aligned} \partial_{a_{im}} v_{m'} &= -\mathrm{Res}\begin{bmatrix} x^{m'} \partial_{a_{im}} q_i \Phi \wedge df \\ f, q_1, \ldots, q_i^2, \ldots, q_{n-1} \end{bmatrix} \\ &= -\mathrm{Res}\begin{bmatrix} x^{m+m'} \Phi \wedge df \\ f, q_1, \ldots, q_i^2, \ldots, q_{n-1} \end{bmatrix} = \partial_{a_{i0}} v_{m+m'}. \end{aligned}$$

Il s'ensuit que si $m' \in P + kP_i$, on a par hypothèse de récurrence $\partial_{a_{i0}} v_{m+m'}$ rationnelle en a_{i0}. Si $\partial_{a_{i0}} v_{m+m'} = 0$, alors $v_{m+m'}$ est évidemment rationnelle en a_{i0} comme voulu. Sinon, il existe $c \in \mathbb{C}^*$ tel que $v_{m'}$ et $v_{m'} + c\, v_{m+m'}$ sont $\mathbb{C}$-linéairement indépendantes. On a :

$$\partial_{a_{i0}}[v_{m'} + c v_{m+m'}] = \partial_{a_{i0}}[v_{m'}] + c\, \partial_{a_{im}}[v_{m'}] = \partial_{a_{i0} + c a_{im}}[v_{m'}]$$

donc $\partial_{a_{i0}}[v_{m'} + c v_{m+m'}]$ (rationnelle en a_{i0}) admet deux primitives linéairement indépendantes dans deux directions indépendantes a_{i0} and $a_{i0} + c\, a_{im}$. Elle n'a ainsi pas de pôles simples dans sa décomposition en éléments simples en a_{i0}. Donc sa primitive $v_{m'} + c v_{m+m'}$ est rationnelle en a_{i0}. Puisque $v_{m'}$ l'est aussi par hypothèse, la fonction $v_{m+m'}$ l'est. Ce dernier argument des primitives indépendantes est inspiré du cas projectif, dû à Henkin et Passare [66]. □

La fin de la preuve du thèorème 6 s'articule alors comme suit :

• En supposant les fibrés très amples, on a $\mathbb{R}^+ P_i = (\mathbb{R}^+)^n$. Ainsi, le lemme de propagation ci-dessus assure que $Tr_V(h\Phi)$ est rationnelle en $a_0 = (a_{10}, \ldots, a_{n-1,0})$ pour tout polynôme $h \in \mathbb{C}[x_1, \ldots, x_n]$.

• D'après la Proposition 2, la restriction I_V de la variété d'incidence I_U à $p_U^{-1}(V)$ définit une extension de corps $\mathbb{C}(I_V)$ sur $\mathbb{C}(U^*)$ de degré fini $N = \mathrm{Card}\,(V \cap C_\alpha)$. Le théorème de

dualité (1.8) combiné au Lemme 1 permet de montrer que le polynôme minimal F_y d'un élément primitif $y \in \mathbb{C}(I_V)$ sur $\mathbb{C}(U^*)$ a ses coefficients rationnels en a_0.

• Travaillant sur la variété d'incidence, on peut remplacer dans F_y chaque coefficient a_{i0} par le polynôme $a_{i0} - q_i(a_i, x)$. On fabrique ainsi une fonction rationnelle $Q_{y,a}(x)$ dont le lieu des zéros est une hypersurface algébrique $\tilde{V}_{y,a}$ qui contient V. En faisant varier a et y, on s'assure que l'intersection $\tilde{V}$ des $\tilde{V}_{y,a}$ est une hypersurface algébrique vérifiant $\tilde{V} \cap U = V \cap U$, comme requis.

• On étend de même la forme Φ en une forme rationnelle $\tilde{\Phi}$ en utilisant à nouveau le théorème de dualité (1.8) et le lemme de propagation, combinés cette fois à la formule d'interpolation de Lagrange.

On renvoie le lecteur à [139, Section 4] pour les détails.

1.6.2 Preuve du théorème de Wood torique

On esquisse ici la preuve du théorème 7. On garde les notations et hypothèses de la section 1.3.4.

Sens direct. Montrons que les traces des fonctions coordonnées sur une hypersurface algébrique $\tilde{V} \subset X$ sont affines en les coefficients constants a_{i0}. Montrons en fait un résultat plus fort, illustrant à nouveau l'intérêt du calcul résiduel. On identifie encore $\Gamma(X, L_i)$ avec un espace de Riemann-Roch des fonctions rationnelles sur X de diviseur polaire borné par un certain $\mathbb{T}$-diviseur supporté à l'infini $X \setminus X_0$.

Proposition 5 *Pour tout $i = 1, \ldots, n-1$ et tout $k \in \mathbb{N}$, on a l'implication*

$$h \in \Gamma(X, L_i^{\otimes k}) \implies \deg_{a_{i0}} Tr_{\tilde{V}}(h) \leq k$$

avec égalité si $\mathrm{div}_0(h)$ *intersecte proprement le bord $X \setminus X_0$. En particulier,*

$$\deg_{a_{i0}} Tr_{\tilde{V}}(x_j) \leq 1,$$

avec égalité si et seulement si $e_j = (0, \ldots, 1, \ldots, 0)$ est un sommet de P_i.

Preuve (esquisse). Soit $m \in \mathbb{N}^n$. D'après (1.13), on obtient cette fois

$$\frac{\partial^k}{\partial a_{i0}} \mathrm{Tr}_V x^m = \pm k! \,\mathrm{Res} \begin{bmatrix} x^m \, J(f,q) dx_1 \wedge \cdots dx_n \\ f, q_1, \ldots, q_i^{k+1}, \ldots, q_{n-1} \end{bmatrix} \tag{1.14}$$

On a $h \in \Gamma(X, L_i^{\otimes k})$ si et seulement si $P_h \subset kP_i$. Le résultat découle alors de la formule de Jacobi torique (1.10) (cf [134, Corollaire 3.6] pour les détails). □

Sens indirect. La preuve que $\deg_{a_{i0}} \mathrm{Tr}_V(x_n) \leq 1$ implique V algébrique est dans le même esprit que le théorème d'Abel-inverse. Discutons plutôt brièvement de la caractérisation de la classe de Picard de l'hypersurface interpolante $\tilde{V}$.

La formule du produit [103] assure que la norme $N_V(f_j)$ est un quotient de résultants mixtes associés aux divers fibrés en droite en jeu. Le résultant au dénominateur est liés aux intersections à l'infini et ne dépend pas des coefficients constants a_{i0} tandis que le degré en a_{10} du résultant au numérateur est majoré par le nombre d'intersection

$$N_j := E_j \cdot D_2 \cdots D_{n-1} \cdot \tilde{V},$$

avec égalité pour f_j générique. Du fait que les E_j sont très amples et forment une base de $Pic(X) \otimes \mathbb{Q}$, le théorème de Lefschetz fort assure que les entiers $N_1, \ldots, N_s$ caractérisent la classe de $\tilde{V}$, donc le polytope P associé au fibré en droites au correspondant. D'un autre côté, le théorème de Bernstein-Kushnirenko [18, 79] assure que ces nombres s'interprètent effectivement comme les volumes mixtes

$$N_j = MV(P(E_j), P_2, \ldots, P_{n-1}, P)$$

de l'énoncé du théorème 7. Voir [136] pour plus de détails. □

Chapitre 2

Problèmes d'osculation

Plutôt que d'interpoler des germes analytiques par une hypersurface algébrique, on requiert seulement des ordres de contact prescrits. On parle d'osculation. On va considérer ce problème non plus dans une carte affine, mais au contraire sur le bord d'une compactification de $\mathbb{C}^n$. On se restreindra au cas $n = 2$. Le problème considéré ici est traité dans [137], avec des applications à la factorisation des polynômes bivariés dans [137, 138].

2.1 Enoncé du problème

Soit $X = X_0 \sqcup \partial X$ une compactification du plan affine $X_0 \simeq \mathbb{C}^2$, dont le bord est un diviseur à croisements normaux simples [1]

$$\partial X = D_1 + \cdots + D_r.$$

Soit $D = (k_1 + 1)D_1 + \cdots + (k_r + 1)D_r$ un diviseur de Cartier effectif de support $|\partial X|$ et soit $\gamma \in \mathrm{Div}(D)$ un diviseur de Cartier sur le schéma $(|D|, \mathcal{O}_D)$ (noté D pour alléger).

Problème d'osculation. A quelles conditions γ se prolonge-t-il à X ? Plus formellement, à quelles conditions existe-t-il un diviseur de Cartier $E \in \mathrm{Div}(X)$ tel que $i^*(E) = \gamma$ où $i : D \hookrightarrow X$ est le morphisme d'inclusion.

Expliquons en quoi ce problème est effectivement un problème "d'osculation". On peut écrire

$$\gamma = \sum_{p \in |\Gamma|} \gamma_p,$$

où $\Gamma = \gamma \cdot \partial X$ et où γ_p est supporté par p. Chaque diviseur γ_p est localement la restriction à D d'un germe de 1-cycle analytique sur X

$$\tilde{\gamma}_p = \mathrm{div}(f_p) \tag{2.1}$$

défini par un germe de fonction méromorphe $f_p \in \mathcal{M}_{X,p}$, et dont le support intersecte ∂X proprement. Dans le cas particulier où les $\tilde{\gamma}_p$ sont des germes de courbes analytiques transverses au bord ∂X, une courbe $C \subset X$ est solution du problème d'osculation (i.e. $i^*C = \gamma$) si et seulement si pour chaque $p \in |D_i|$, la courbe C a un ordre de contact au moins $k_i + 1$ avec le germe $\tilde{\gamma}_p$.

1. *i.e.* ∂X est localement lisse ou intersection transverse de deux courbes lisses.

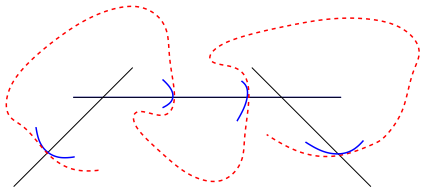

FIGURE 2.1 – Le problème d'osculation. On cherche une courbe algébrique (en pointillé rouge) ayant un ordre de contact prescrit avec des germes de courbes (en bleu) transverses au bord (en noir) d'une compactification à croisements normaux de $\mathbb{C}^2$.

2.2 Le théorème d'osculation

Le lecteur ne sera pas surpris que les résidus vont jouer un rôle clé. Soit Ω^2_X le faisceau canonique de X et soit $\Omega^2_X(D)$ le faisceau inversible des 2-formes méromorphes dont le lieu polaire est borné par D. Soit $\Psi \in H^0(X, \Omega^2_X(D))$. Puisque $X \setminus |D| = X_0 \simeq \mathbb{C}^2$ est simplement connexe, Ψ est exacte : il existe une 1-forme rationnelle ψ sur X, holomorphe sur X_0, telle que $\Psi = d\psi$. Notons ψ_p le germe de ψ en $p \in |\Gamma|$ et notons f_p l'équation locale d'un relevé $\tilde{\gamma}_p$ comme en (2.1). Le théorème de Stokes et le théorème de dualité assurent que le résidu de Grothendieck $\mathrm{res}_p\left[\frac{df_p}{f_p} \wedge \psi_p\right]$ ne dépend que de Ψ et du diviseur $\gamma_p \in \mathrm{Div}(D)$. On peut ainsi définir une application

$$\begin{array}{ccc} \mathrm{Div}(D) \times H^0(X, \Omega^2_X(D)) & \longrightarrow & \mathbb{C} \\ (\gamma, \Psi) & \longmapsto & \langle \gamma, \Psi \rangle_p := \mathrm{res}_p\left[\frac{df_p}{f_p} \wedge \psi_p\right], \end{array} \tag{2.2}$$

qui est $\mathbb{Z}$-linéaire en γ et $\mathbb{C}$-linéaire en Ψ. Notre résultat principal est le suivant :

Théorème 8 *Soit X une compactification du plan affine à bord ∂X à croisements normaux. Soit (D, γ) définissant un problème d'osculation sur le bord ∂X.*

1) Le diviseur $\gamma \in \mathrm{Div}(D)$ s'étend en un diviseur $E \in \mathrm{Div}(X)$ si et seulement si

$$\sum_{p \in |\Gamma|} \langle \gamma, \Psi \rangle_p = 0 \ \textit{pour tout} \ \Psi \in H^0(X, \Omega^2_X(D)). \tag{2.3}$$

Le diviseur E est unique à équivalence rationnelle près.

2) Si de plus γ est effectif et $H^1(X, \mathcal{O}_X(E-D)) = 0$, alors γ s'étend de manière unique en un diviseur effectif de X.

Exemple (Relation de Reiss). Considérons une collection de d germes analytiques lisses $\tilde{\gamma}_p$ transverses à une droite $L \subset \mathbb{P}^2$. A quelle condition existe-t-il une courbe algébrique $C \subset \mathbb{P}^2$ de degré d ayant un ordre de contact ≥ 3 avec chacun des germes ? Ceci est un problème d'osculation attaché au couple (D, γ), où $D = 3L$ et γ est la restriction à D de $\sum_p \tilde{\gamma}_p$. Munissons $\mathbb{P}^2$ de coordonnées homogènes $[T_0 : T_1 : T_2]$ de sorte que $L = \{T_0 = 0\}$ et supposons que γ soit supporté dans la carte affine $T_2 \neq 0$, munie des coordonnées affines $x = T_0/T_2$ et $y = T_1/T_2$. Chaque germe $\tilde{\gamma}_p$ est donné par une équation de Weierstrass

$$\tilde{\gamma}_p = \{y - \phi_p(x) = 0\}$$

où $\phi_p \in \mathbb{C}\{x\}$. Il y a un isomorphisme

$$H^0(\mathbb{P}^2, \Omega^2_{\mathbb{P}^2}(3L)) \simeq H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) \simeq \mathbb{C}$$

et ce $\mathbb{C}$-espace vectoriel est engendré par la forme $\Psi = \frac{dx\wedge dy}{x^3}$, dont une primitive est $\psi = -\frac{ydx}{x^3}$. La formule de Cauchy conduit à l'égalité :

$$\mathrm{res}_p\big[\frac{ydx\wedge d(y-\phi_p)}{x^3(y-\phi_p)}\big] = \mathrm{res}_0\big[\phi_p(x)\frac{dx}{x^3}\big] = \frac{1}{2}\phi_p''(0),$$

où res_0 est le résidu univarié en 0. Ainsi, (2.3) est dans ce cadre équivalent à

$$\sum_{p\in|\Gamma|}\phi_p''(0) = 0. \tag{2.4}$$

On a ici $H^1(\mathcal{O}_{\mathbb{P}^2}(d-3)) = 0$, et le point 2 du théorème 8 assure que (2.4) est finalement équivalent à l'existence d'une *courbe* $C\subset\mathbb{P}^2$ de degré d osculant les germes $\tilde{\gamma}_p$ à l'ordre 3. Noter que la nécessité de (2.4) est une conséquence immédiate du théorème de Wood, ou encore de la relation de Reiss (1.2). □

Ce cas particulier est obtenu par Griffiths et Harris [57, Chapitre 6], et généralisé par Wood dans [143] dans le cas d'ordre de contacts plus élevés. Une difficulté supplémentaire dans le Théorème 8 est que l'on ne suppose pas les germes γ_p inclus dans une carte affine.

Esquisse de preuve. La nécessité des conditions (2.3) découle du théorème des résidus (cf Section 1.5.1.3). La partie délicate concerne la suffisance de ces conditions. Donnons les grandes lignes de la preuve.

La donné d'un diviseur de Cartier $\gamma\in\mathrm{Div}(D)$ équivaut à la donnée d'un fibré en droite $\mathcal{L}\in\mathrm{Pic}(D)$ et d'une section $f\in\Gamma(D,\mathcal{L})$. Etendre γ revient à étendre dans un premier temps $\mathcal{L}$ en $\tilde{\mathcal{L}}\in\mathrm{Pic}(X)$, puis étendre ensuite f en une section méromorphe $\tilde{f}$ de $\tilde{\mathcal{L}}$. Le deuxième point découle automatiquement du théorème d'annulation de Serre, et la difficulté principale réside donc dans la caractérisation du conoyau du morphisme de restriction

$$\mathrm{Pic}(X)\to\mathrm{Pic}(D).$$

Un premier résultat clé permet d'identifier cohomologiquement cette obstruction :

Lemme 2 *Il y a une décomposition en somme directe*

$$\mathrm{Pic}(D)\simeq\mathrm{Pic}(X)\oplus H^1(D,\mathcal{O}_D) \tag{2.5}$$

Preuve (esquisse). Les isomorphismes $\mathrm{Pic}(X)\simeq H^1(X,\mathcal{O}_X^*)$ et $\mathrm{Pic}(D)\simeq H^1(D,\mathcal{O}_D^*)$ suggèrent de regarder les suites exactes courtes exponentielles de D et X

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_X & \longrightarrow & \mathcal{O}_X & \overset{\exp(2i\pi\cdot)}{\longrightarrow} & \mathcal{O}_X^* & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}_D & \longrightarrow & \mathcal{O}_D & \longrightarrow & \mathcal{O}_D^* & \longrightarrow & 0. \end{array} \tag{2.6}$$

Ici, $\mathbb{Z}_D\subset\mathcal{O}_D$ est le sous-faisceau des fonctions à valeurs dans $\mathbb{Z}$, et les flèches verticales de restriction sont surjectives. Puisque la variété X est rationnelle, on a $H^i(X,\mathcal{O}_X) = 0$ pour $i>0$. La cohomologie à support compact de la variété affine $X_0 = X\setminus|D|$ s'annule en degré >0. Ainsi la suite cohomologique longue induite par la suite exacte courte

$$0\to j_!(\mathbb{Z}_{X_0})\to\mathbb{Z}_X\to\mathbb{Z}_{|D|}\to 0 \tag{2.7}$$

sous-jacente au morphisme d'inclusion $j : X_0\hookrightarrow X$ conduit aux isomorphismes $H^1(D,\mathbb{Z}_D)\simeq H^1(X,\mathbb{Z}_X) = 0$ et $H^2(D,\mathbb{Z}_D)\simeq H^2(X,\mathbb{Z}_X)$. Ces considérations combinées aux suites cohomologiques exactes longues dérivées de (2.6) permettent de conclure. □

La suite exacte courte $0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$ combinée aux annulations $H^1(X,\mathcal{O}_X) = H^2(X,\mathcal{O}_X) = 0$ induit un isomorphisme

$$H^1(D,\mathcal{O}_D) \simeq H^2(X,\mathcal{O}_X(-D)).$$

Avec (2.5), on en déduit l'existence d'un 2-cocyle de Cech $\beta = \beta(\mathcal{L}) \in H^2(X,\mathcal{O}_X(-D))$ qui s'annule si et seulement si $\mathcal{L}$ s'étend à X, cocycle que l'on peut expliciter. Pour caractériser l'annulation $\beta = 0$, on s'appuie sur le théorème de dualité de Serre : il y a une application bilinéaire non dégénérée

$$H^2(X,\mathcal{O}_X(-D)) \otimes H^0(X,\Omega^2_X(D)) \longrightarrow H^2(X,\Omega^2_X) \overset{\mathrm{Tr}}{\simeq} \mathbb{C},$$

composée du cup-produit pour les cocycles avec un morphisme trace Tr [12]. Notons β_Ψ le cup-produit de β et $\Psi \in H^0(X,\Omega^2_X)$. Donc $\mathcal{L} \in \mathrm{Pic}(D)$ s'étend à X si et seulement si $\mathrm{Tr}(\beta_\Psi) = 0$ pour tout Ψ.

Afin d'expliciter l'application trace dans notre cadre, on utilise la cohomologie de Dolbeault. Notons $\mathcal{D}^{p,q}_X$ le faisceau des courants de degrés (p,q) sur X. La résolution $\bar\partial$ de Dolbeault du faisceau Ω^2_X est donnée par la suite exacte longue de faisceaux

$$0 \longrightarrow \Omega^2_X \xrightarrow{[\cdot]} \mathcal{D}^{(2,0)}_X \xrightarrow{\bar\partial} \mathcal{D}^{(2,1)}_X \xrightarrow{\bar\partial} \mathcal{D}^{(2,2)}_X \longrightarrow 0$$

où $[\omega] : \theta \mapsto \int_X \omega \wedge \theta$. Il en découle l'isomorphisme de Dolbeault

$$H^2(X,\Omega^2_X) \simeq H^0(X,\mathcal{D}^{2,2}_X)/\bar\partial H^0(X,\mathcal{D}^{2,1}_X).$$

La partie délicate consiste alors à expliciter un $(2,2)$-courant global $T_\Psi \in H^0(X,\mathcal{D}^{2,2}_X)$ tel que

$$\mathrm{Tr}(\beta_\Psi) = \langle T_\Psi, 1\rangle.$$

L'opérateur $\bar\partial$ joue un rôle clé et la construction du courant T_Ψ s'appuie sur les courants résiduels (1.6) et la formule de Lelong-Poincaré (1.7), voir [137, Section 2.4] pour les détails. On obtient au final la formule désirée

$$\langle T_\Psi, 1\rangle = \sum_{p\in|\Gamma|} \mathrm{res}_p\big[\frac{df_p}{f_p} \wedge \psi_p\big].$$

Si elle existe, l'extension $E \in \mathrm{Div}(X)$ du diviseur $\gamma \in \mathrm{Div}(D)$ est unique à équivalence rationnelle près du fait que $\mathrm{Pic}(X)$ est un facteur direct de $\mathrm{Pic}(D)$ d'après (2.5). Voilà pour un aperçu de la preuve du point 1. Le point 2 découle de la suite cohomologique associée à la suite exacte courte $0 \to \mathcal{O}_X(E-D) \to \mathcal{O}_X(E) \to \mathcal{O}_D(E) \to 0$. □

2.2.1 Ouvertures.

1. Osculation pour d'autres couples (D,X). Il serait intéressant de généraliser le théorème d'osculation en considérant $D \subset X$ un diviseur effectif d'une variété projective lisse quelconque X, a minima lorsque X est rationnelle. La décomposition clé (2.5) n'est plus valable : d'autres obstructions topologiques ou cohomologiques apparaissent. Peut-on les expliciter ? Quel rôle jouent les résidus ?

2. Caractéristique positive. Un autre point serait bien sûr de généraliser le théorème d'osculation sur un corps quelconque, en particulier sur un corps fini. La théorie des résidus et le théorème de dualité s'étendent à ce cadre, mais nous n'avons plus accès à la cohomologie de Dolbeault inhérente à l'analyse complexe.

2.3 Formules explicites dans le cadre torique

Supposons que $X = X_\Sigma$ soit une compactification torique lisse de $X_0 \simeq \mathbb{C}^2$. On peut écrire d'un point de vue ensembliste

$$X = \mathbb{T} \sqcup (D_0 \cup \cdots \cup D_{r+1}) = X_0 \sqcup (D_1 \cup \cdots \cup D_r),$$

où les D_i sont les diviseurs $\mathbb{T}$-invariants. Soit $\rho_i \in \Sigma(1)$ le rayon définissant D_i et ordonnons les diviseurs $D_0, \ldots, D_{r+1}$ de sorte que les cônes $\sigma_i = \rho_i\mathbb{R}^+ \oplus \rho_{i+1}\mathbb{R}^+$ soient les cônes maximaux de Σ (avec la convention $\rho_{r+2} = \rho_0$). La carte affine associée au cône σ_i s'écrit

$$U_i = \operatorname{Spec} \mathbb{C}[\check{\sigma}_i \cap \mathbb{Z}^2] = \operatorname{Spec} \mathbb{C}[x_i, y_i] \simeq \mathbb{C}^2,$$

où les coordonnées affines (x_i, y_i) sont liées aux coordonnées $t = (t_1, t_2)$ du tore $\mathbb{T}$ par les relations

$$t^m = x_i^{\langle m, \eta_i \rangle} y_i^{\langle m, \eta_{i+1} \rangle}.$$

Les diviseurs D_i et D_{i+1} ont alors pour équations affines respectives $x_i = 0$ et $y_i = 0$.

• Soit $D = \sum_{i=1}^r (k_i + 1)D_i$. Le diviseur $K_X = -D_0 - \cdots - D_{r+1}$ est un diviseur canonique de X et on a un isomorphisme naturel

$$H^0(X, \Omega_X^2(D)) \simeq \bigoplus_{m \in P_{D+K_X} \cap \mathbb{Z}^2} \mathbb{C} \cdot t^m \frac{dt_1 \wedge dt_2}{t_1 t_2},$$

où P_{D+K_X} est le polytope associé au $\mathbb{T}$-diviseur $D + K_X$ par (1.3).

• Soit $\gamma \in \operatorname{Div}(D)$ que l'on suppose transverse au bord ∂X et notons $\Gamma_i = |\gamma \cdot D_i|$. Pour chaque $p \in \Gamma_i$, le diviseur $\gamma_p \in \operatorname{Div}(D)$ est donné par une équation de Weierstrass

$$y_i - \phi_p(x_i) = 0$$

dans la carte affine U_i, où $\phi_p \in \mathbb{C}\{x_i\}$ est une fonction analytique définie modulo $(x_i^{k_i+1})$ et ne s'annulant pas en 0.

La proposition suivante rend explicite les critères d'osculation (2.3) dans le cadre torique.

Proposition 6 *Le diviseur $\gamma \in \operatorname{Div}(D)$ est la restriction à D d'un diviseur $E \in \operatorname{Div}(X)$ si et seulement si*

$$\sum_{i=1}^r \sum_{p \in |\Gamma_i|} \frac{1}{(-\langle m, \eta_i \rangle)!} \frac{\partial^{-\langle m, \eta_i \rangle}}{\partial x_i^{-\langle m, \eta_i \rangle}} \Big(\frac{\phi_p^{\langle m, \eta_{i+1} \rangle}}{\langle m, \eta_{i+1} \rangle} \Big)(0) = 0 \qquad \forall\, m \in P_{D+K_X} \cap \mathbb{Z}^2,$$

avec les conventions $\phi_p^k/k = \log(\phi_p)$ si $k = 0$ et $\frac{\partial^a}{\partial x^a}(\phi_p^k/k) = 0$ si $a < 0$.

Les termes de cette double somme sont simplement des coefficients de Taylor, faciles à calculer. On notera aussi que l'on a $-\langle m, \eta_i \rangle \leq k_i$ pour tout $m \in P_{D+K_X}$ de sorte que cette expression ne dépend que des ϕ_p tronqués à précision $x_i^{k_i+1}$ pour $p \in |\Gamma_i|$, donc seulement de γ, comme requis. La preuve est calculatoire, la formule de Cauchy et la combinatoire des variétés torique permettant d'expliciter les calculs de résidus (2.2).

Des applications à la factorisation bivariée sont décrites dans la section 3.3.

Deuxième partie

Contributions à la factorisation des polynômes

Chapitre 3

Factorisation des polynômes bivariés

Contents

3.1 Introduction

On s'intéresse ici à la factorisation d'un polynôme à deux variables $f \in \mathbb{K}[x, y]$ à coefficients dans un corps $\mathbb{K}$, en supposant résolu le problème de la factorisation univariée sur $\mathbb{K}$. Ce problème central du calcul formel a reçu beaucoup d'attention depuis les années 70. Le lecteur trouvera des historiques détaillés et de nombreuses références dans [50, Notes du Chapitre III] ou dans les articles [32, 34, 83, 85].

Nous nous concentrerons ici essentiellement sur des méthodes basées sur le lemme de Hensel, popularisées par Zassenhaus [147] à la fin des années 60 : l'idée centrale est de recombiner les facteurs analytiques de f dans $\mathbb{K}[[x]][y]$ en facteurs rationnels. On peut distinguer deux stratégies :

• Une stratégie probabiliste à "petite précision" : On effectue un changement affine générique de coordonnées, puis on détecte les facteurs de f à partir de sa factorisation modulo (x^3) en testant des sommes nulles inhérentes à la relation de Reiss (2.4), voir par exemple [30, 33, 48, 112]. L'algorithme sous-jacent est probabiliste, généralement utilisé dans le cadre de la factorisation absolue, *i.e.* sur $\bar{\mathbb{K}}[x, y]$: les calculs sont conduits numériquement, et des stratégies basées sur l'algorithme LLL de réduction des réseaux permettent de retrouver les coefficients exacts [30]. On parle d'algorithmes semi-numériques. Bien que ces algorithmes soient de complexité exponentielle dû à la recherche exhaustive des sommes nulles, ils sont en pratique très efficaces sur une grande classe de polynômes, pouvant traiter des degrés relativement grands > 200 [30]. Ils peuvent de plus s'adapter pour calculer la décomposition

absolue d'ensemble algébriques plus généraux que les courbes planes [127]. Cependant, il existe des polynômes pour lesquels cet algorithme est peu efficace en pratique.

• Une stratégie déterministe à "grande précision" : en supposant F séparable modulo x, on factorise cette fois f dans $\mathbb{K}[[x]][y]$ jusqu'à une précision suffisamment grande afin de détecter avec certitude quelles combinaisons des facteurs analytiques produisent des facteurs rationnels. On parle d'algorithmes "remontées et recombinaisons". Inspirés de l'algorithme de recombinaison de Sasaki et al. [116, 115] et de la méthode des dérivées logarithmiques de Ruppert-Gao [111, 49], les travaux importants de Bostan et al. [20], Lecerf [85, 83] et Chèze-Lecerf [34] ont montré que les recombinaisons pouvaient se réduire à la résolution d'un système linéaire dépendant d'une précision en x linéaire en $d = \deg(f)$. Il en découle un algorithme déterministe de complexité polynomiale en d, sous-quadratique en la taille de l'entrée, qui reste la meilleure complexité théorique connue à ce jour pour les polynômes denses (i.e. représentés par la liste des coefficients de tous les monômes de degré $\leq d$).

Contributions. La complexité arithmétique (nombres d'opérations élémentaires dans $\mathbb{K}$) des algorithmes usuels s'exprime en terme du degré total (voire du bidegré). Je me suis intéressé dans mes travaux à tenir compte d'indicateurs de complexité plus fins :

Approches toriques [31, 43, 137, 138]. On cherche à tenir compte du polytope de Newton P_f, dans la lignée de [9]. Rappelons tout de suite que ce dernier se comporte bien avec la multiplication : si $g, h \in \mathbb{K}[x, y]$, le théorème d'Ostrovski assure que

$$P_{gh} = P_g + P_h,$$

où la somme désigne la somme de Minkovski. Cette égalité impose de fortes contraintes combinatoires à la factorisation, que l'on cherche à exploiter au maximum.

Approches singulières [141, 140]. La courbe projective d'un polynôme réductible est nécessairement singulière et il est légitime de se demander si l'on peut tirer avantage de la combinatoire de la résolution de (certaines) singularités pour la factorisation. L'approche torique permet de tirer profit des éventuelles singularités aux trois points $\mathbb{T}$-fixes de $\mathbb{P}^2$, en les supposant non dégénérées (i.e. résolues par un seul éclatement monomial au voisinage du point considéré). Peut-on tirer d'avantage profit des singularités en factorisation ?

Organisation. Les sections 3.2 et 3.3 sont dédiées aux approches toriques, en lien étroit avec les sections 1.3.1, 1.3.4 et la section 2. Les sections 3.4 et 3.5 sont dédiées aux approches singulières. La valuation du discriminant joue un rôle important, et la dernière section 3.6 légèrement annexe s'intéresse à la description des polynômes dont le discriminant par rapport à y est de degré minimal en x, travaux en collaboration avec Denis Simon (Université de Caen).

Un regain d'intérêt. D'un point de vue complexité, mes travaux autour des relations entre factorisation et singularités étaient spéculatifs dans les années 2012 du fait que les algorithmes de factorisation analytique dans $\mathbb{K}[[x]][y]$ et de désingularisation des courbes planes n'étaient pas compétitifs pour intervenir en factorisation bivariée. Ce n'est plus le cas depuis nos travaux récents avec Adrien Poteaux [110, 107, 108] autour des séries de Puiseux (sur lesquels je reviendrai dans le chapitre suivant), encourageant *a posteriori* la pertinence des singularités en factorisation, et qui de mon point de vue offrent aujourd'hui un indéniable regain d'intérêt pour les travaux décrits dans ce chapitre.

3.2 Un algorithme torique probabiliste

J'ai découvert après ma thèse le problème de la factorisation et les enjeux du calcul formel par l'intermédiaire d'André Galligo, qui a repéré que le théorème 7 d'interpolation dans les variétés toriques pourrait conduire à un algorithme probabiliste de factorisation bivariée tenant compte du polytope de Newton. Cette section est dédiée à nos travaux sur ce thème en collaboration avec André Galligo et Mohammed Elkadi, publiés dans [31, 43].

Soit $f \in \mathbb{Q}[x,y]$ un polynôme bivarié de degré total d. On cherche à déterminer la factorisation absolue de f, i.e. sa décomposition en facteurs irréductibles sur $\bar{\mathbb{Q}}[x,y]$.

L'approche classique. Soit $\mathcal{C} \subset \mathbb{C}^2$ la courbe complexe définie par f. Soient $p_1, \ldots, p_d$ les points d'intersection de $\mathcal{C}$ avec une droite L générique. Soit $I \subset \{1, \ldots, d\}$ de cardinal k. Si la collection de points $\{p_i, i \in I\}$ appartient à une composante $\mathcal{C}_I$ de $\mathcal{C}$ de degré k, alors la formule de Reiss (1.2) assure que

$$\sum_{i \in I} \frac{f_{xx} f_y^2 - 2 f_{xy} f_x f_y + f_{yy} f_x^2}{f_y^3}(p_i) = 0.$$

De plus, le théorème de Wood projectif assure que cette condition est également suffisante pour une droite L générique (la preuve de ce dernier point est plutôt basée sur des arguments de monodromie dans les travaux originaux [112, 48]). On est ainsi ramené à tester des sommes nulles minimales parmi toutes les collections possibles de points pour identifier les facteurs absolument irréductibles de f. Une fois une telle collection identifiée, on peut calculer le facteur de f correspondant et son cofacteur à l'aide du lemme de Hensel. Il y a au plus 2^d choix de I possibles et les algorithmes sous-jacents sont de complexité exponentielle en le degré.

L'approche torique. Soit $X = X_P$ la surface torique projective associée au polytope de Newton $P = P_f$, polytope que nous supposerons contenir l'origine pour simplifier (cette hypothèse n'est pas restrictive).

Notons $C \subset X$ la clôture de Zariski de la courbe affine $\mathcal{C} \subset \mathbb{C}^2$ définie par f. Soit $Q \subset (\mathbb{R}^+)^2$ un polytope contenant l'origine, et dont toutes les arêtes sont parallèles à celles de P. Cela revient à choisir un fibré en droite très ample sur X. Ce polytope est en pratique choisi "le plus petit possible". Soit $q \in \mathbb{Q}[x,y]$ un polynôme générique de polytope de Newton Q. Pour tout $t \in \mathbb{C}$, considérons la clôture de Zariski

$$C_t = \overline{\{q(x,y) = t\}} \subset X.$$

De la généricité de q découle le fait que l'intersection

$$C_t \cap C = \{p_1(t), \ldots, p_N(t)\}$$

est transverse, incluse dans le plan affine $\mathbb{C}^2$, et de cardinal le volume mixte $N = MV(P,Q)$ (théorème de Bernstein-Kushnirenko).

La surface X n'est pas nécessairement lisse, mais elle est simpliciale. On peut montrer que le théorème 7 et la proposition 5 restent valables dans ce cadre [43, Thm 2, Thm 3]. Nous supposerons (toujours pour simplifier) que le point $(0,1)$ appartient au bord de Q, mais n'est pas un sommet. La proposition 5 assure alors que la trace de y sur une courbe algébrique $\tilde{C}$ relativement à la famille C_t ne dépend pas de t :

$$\frac{\partial \operatorname{Tr}_{\tilde{C}} y}{\partial t} \equiv 0.$$

Soit $I \subset \{1,\dots,N\}$ de cardinal k. Si la collection de points $\{p_i, i \in I\}$ appartient à une composante C_I de C telle que $C_I \cdot C = \sum_{i\in I} p_i$, alors il suit de ce qui précède et de l'égalité (1.12) que l'on a

$$\sum_{i\in I} \frac{y}{J(f,q)}(p_i(t)) \equiv 0, \tag{3.1}$$

où $J(f,q)$ désigne le jacobien de l'application $(f,q) : \mathbb{C}^2 \to \mathbb{C}^2$. On a en fait mieux : du fait du choix générique de q, le théorème 7 assure que la condition (3.1) est aussi suffisante pour qu'il existe une composante $C_I \subset C$ comme ci-dessus. Notons que la courbe C_I est alors nécessairement supportée par un polytope P_I tel que $MV(P, P_I) = k$.

Il semble à première vue que l'on perde en complexité par rapport à l'approche classique du fait que $N > d$. Un point important est que la collection de points $p_1,\dots,p_N$ n'est pas distribuée aléatoirement. En effet, lorsque $|t| \to \infty$, la courbe C_t "dégénère" en un diviseur $D = \sum_{j=1}^{r} k_j D_j$ supporté au bord $\partial X = X \setminus \mathbb{C}^2$, dont les composantes D_j sont en bijection avec les arêtes extérieures de Q, et dont les multiplicités k_j se calculent explicitement à partir du polytope Q. Le zéro-cycle $C \cdot C_t$ (réduit) dégénère donc en un zéro-cycle (non réduit) supporté à l'infini :

$$\lim_{|t|\to\infty} C \cdot C_t = C \cdot D = \sum_j k_j (C \cdot D_j).$$

Ainsi, il existe une unique partition

$$\{1,\dots,N\} = J_1 \cup \cdots \cup J_r \qquad \text{telle que} \qquad \lim_{|t|\to\infty} \sum_{i\in J_j} p_i(t) = k_j (C \cdot D_j), \quad \forall\, j = 1,\dots,r. \tag{3.2}$$

Pour $|t|$ suffisamment grand, cette partition se calcule explicitement en repérant quelles coordonnées tendent vers 0 dans des cartes affines adaptées.

D'autre part, le théorème d'Ostrovski impose au polytope de Newton Q d'un facteur g de f d'être un facteur de Minkovski du polytope P de f. Se donner un tel polytope Q fixe les degrés d'intersection $C' \cdot D_j$ de la courbe $C' \subset X$ de g avec chaque composante D_j, cf Théorème 9 ci-après. On obtient ainsi des contraintes combinatoires très fortes pour les choix des sous-ensembles $I \subset \{1,\dots,N\}$ candidats aux sommes nulles (3.1). On peut montrer que le nombre total de choix possibles est toujours inférieur à la borne 2^d inhérente à l'approche classique, et drastiquement inférieur dès lors que le polytope a peu de points entiers sur ses arêtes extérieures. C'est tout l'intérêt de l'approche torique. Un exemple simple illustratif est détaillé dans [43].

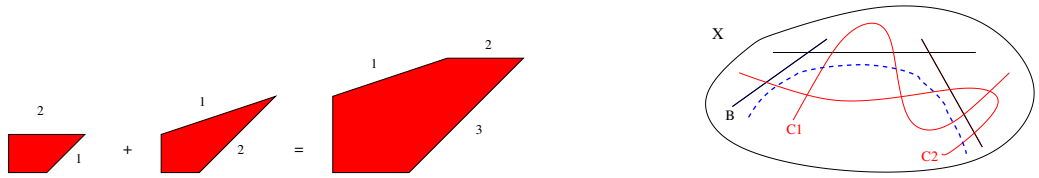

FIGURE 3.1 – Représentation schématique de la compactification torique associée au polytope de Newton. La courbe C_t (en bleu) intersecte la courbe $C = C_1 \cup C_2$ en 6 points (en pratique en 6 "îlots" de points) dont on peut lire la répartition asymptotique quand $t \to +\infty$. Il n'y a alors que 3 sommes nulles à tester en accord avec la décomposition de Minkovski donnée. La courbe C étant de degré projectif 7, l'approche classique coûterait potentiellement 2^7 sommes nulles à tester.

3.3 Algorithmes toriques déterministes

Soit $f \in \mathbb{K}[x,y]$ un polynôme bivarié défini sur un corps de nombres $\mathbb{K}$. Soit X une variété torique lisse dont l'éventail Σ raffine l'éventail normal au polytope de f. On note $C \subset X$ la clôture de Zariski de la courbe affine $f = 0$. Les résultats de cette section sont basés sur la remarque suivante :

Si la somme des multiplicités d'intersection de C avec une courbe irréductible $C' \subset X$ de polytope donné dépasse la borne de Bernstein-Kushnirenko, alors C' est nécessairement une composante de C.

Cette observation, combinée avec les critères d'osculation explicites donnés par le Théorème 8 et la Proposition 6 m'ont conduit à développer deux algorithmes de factorisation toriques déterministes du type "remontées et recombinaisons".

3.3.1 Préambule

Les algorithmes toriques qui suivent sont valables sous une hypothèse de non dégénérescence à la Kushnirenko que nous expliquons brièvement.

Nous supposerons pour simplifier que $f(0,0) \neq 0$ (cette hypothèse n'est pas restrictive, voir [138, Remarque 3.1]). Quitte à raffiner l'éventail de X, on peut alors supposer que X est une compactification lisse de $X_0 = \operatorname{Spec} \mathbb{C}[x,y] \simeq \mathbb{C}^2$, dont le bord

$$\partial X = X \setminus X_0 = D_1 + \cdots + D_r$$

est un $\mathbb{T}$-diviseur réduit à croisements normaux. On dira que f est *non dégénéré* si l'intersection $C \cap \partial X$ est transverse.

Pour un polytope Q, on note $Q^{(i)}$ la face de Q qui minimise le produit scalaire $\langle m, \eta_i \rangle$, où η_i est le générateur primitif du cône de dimension 1 associé au $\mathbb{T}$-diviseur D_i. Cette face est soit une arête extérieure (i.e. ne contenant pas l'origine), soit un sommet de Q.

Soit $P = P_f$ le polytope de Newton de $f = \sum c_m x^{m_1} y^{m_2}$. Les polynômes de facette de f sont les polynômes

$$f^{(i)} = \sum_{m \in P^{(i)} \cap \mathbb{Z}^2} c_m x^{m_1} y^{m_2},$$

polynômes quasi-homogènes qui deviennent univariés après un changement monomial de coordonnées, et dont les zéros non triviaux déterminent l'intersection $C \cap D_i$. En particulier, on a

$$\deg(C \cdot D_i) = \operatorname{Card}(P^{(i)} \cap \mathbb{Z}^2) - 1$$

et f est non dégénéré si et seulement si tous ses polynômes de facettes extérieures sont sans facteurs carrés dans $\mathbb{C}[x^{\pm 1}, y^{\pm 1}]$. Cette hypothèse est l'analogue torique de l'hypothèse $f(0,y)$ séparable inhérente aux approches classiques [83, 85].

3.3.2 Un algorithme de complexité exponentielle.

Cet algorithme est présenté dans [138, Section 3]. Le polynôme f définit une fonction rationnelle sur X, holomorphe sur X_0. Ainsi, le diviseur

$$D = \operatorname{div}_\infty(f) + \partial X$$

est un diviseur de Cartier effectif (non réduit) de support $|\partial X|$. Soit $i : D \hookrightarrow X$ le morphisme d'inclusion. On note $\gamma = i^*(C) \in \operatorname{Div}(D)$ la restriction à D de la courbe $C \subset X$ de f.

Théorème 9 *[138, Thm 3.3] Supposons f non dégénéré. Soit Q un facteur de Minkowski non trivial du polytope P de f et soit $\mathbb{L}$ une extension finie de $\mathbb{K}$. Alors f admet un facteur $q \in \mathbb{L}[x,y]$ de polytope Q si et seulement s'il existe un diviseur $0 < \gamma' < \gamma$ de D défini sur $\mathbb{L}$ tel que*

$$\deg(\gamma' \cdot D_i) = \mathrm{Card}(Q^{(i)} \cap \mathbb{Z}^2) - 1, \ i = 1, \ldots, r \tag{3.3}$$

et tel que la paire (D, γ') obéisse aux critères d'osculation de la Proposition 6. On peut alors calculer le polynôme q à partir de γ'.

Un point clé de la preuve est que si un fibré en droite L sur la variété torique X est globalement engendré, alors $H^1(X, L) = 0$, permettant d'appliquer le point 2 du Théorème 8. Il découle de ce théorème un algorithme de factorisation torique dont voici les grandes lignes :

- Calcul de γ : on factorise (sur le corps $\mathbb{L}$ considéré) les polynômes de facettes (factorisations univariées) que l'on lifte après un changement monomial de coordonnées adéquat à la précision donnée par les multiplicités des D_i dans D. Les facteurs modulaires ainsi obtenus représentent le diviseur $\gamma = i^*(C)$.
- Recombinaisons : pour chaque choix possible de γ', contraint par (3.3), on teste les annulations de sommes de résidus déterminées par la Proposition 6.
- Calcul des facteurs : si γ' est effectivement la restriction à D d'une composante C' de C, on calcule le facteur $q \in \mathbb{L}[x,y]$ de f correspondant comme unique solution d'un certain système linéaire ([138, Prop 3.5]).

Le nombre de sommes nulles à tester en tenant compte des contraintes du théorème d'Ostrowski et de l'équation (3.3) est le même que pour la méthode présentée en Section 3.2. Deux avantages majeurs ici : l'algorithme sous-jacent est cette fois déterministe et le calcul de la décomposition du 0-cycle réduit $C \cap C_t$ (résolution d'un système polynômial) et de sa répartition asymptotique est maintenant remplacé par le calcul moins coûteux de la décomposition du 0-cycle non réduit $C \cap D$ associé au diviseur $i^*(C)$ (factorisations univariées et lemme de Hensel multifacteur).

Exemple. Un exemple caricatural est donné par un polynôme f de polytope

$$P = \mathrm{Conv}((0,0), (2N, 0), (0, 2N-2)).$$

Dans ce cas, il y a une seule arête extérieure, qui est de longueur entière 2 : il y a seulement 2 recombinaisons à tester, alors que l'approche classique demanderait potentiellement 2^N recombinaisons à tester. On renvoie à [138, Section 3.5] pour plus de précisions sur la comparaison entre les approches classiques et toriques, en particulier sur le nombre de recombinaisons.

3.3.3 Un algorithme de complexité polynomiale.

J'obtiens dans [137] un algorithme torique de complexité polynomiale en le volume du polytope. L'idée centrale est de réduire le problème des recombinaisons à de l'algèbre linéaire. L'algorithme présenté ici peut être considéré comme une généralisation au cadre torique de l'algorithme de Lecerf [85, 83]. Cette méthode hybride mélange le point de vue "remontées de Hensel et recombinaisons" esquissé ci-dessus avec la méthode des "dérivées logarithmiques" introduite par Ruppert [111] et développée par Gao [49].

3.3.3.1 Recombinaisons *via* l'algèbre linéaire.

On cherchera ici à factoriser f sur $\mathbb{K}[x,y]$ (on parle de factorisation rationnelle). En supposant f non dégénéré, la décomposition irréductible sur $\mathbb{K}$ du diviseur $\gamma = i^*(C) \in \mathrm{Div}(D)$ s'écrit

$$\gamma = \sum_{p\in\mathcal{P}} \gamma_p$$

où l'indexation porte sur l'ensemble $\mathcal{P}$ des facteurs irréductibles des polynômes de facettes extérieurs de f. Les composantes γ_p engendrent un $\mathbb{K}$-espace vectoriel

$$V = \left\{ \sum_{p\in\mathcal{P}} \mu_p\gamma_p,\ \mu_p \in \mathbb{K} \right\} \subset \mathrm{Div}(D)\otimes\mathbb{K}$$

que l'on considérera comme espace ambiant.

Déterminer la factorisation irréductible de f sur $\mathbb{K}$ équivaut à déterminer la décomposition irréductible

$$C = C_1 \cup \cdots \cup C_s$$

de C sur $\mathbb{K}$. Le polynôme f étant supposé non dégénéré, les restrictions $\gamma_j := i^*(C_j) \in V$ s'expriment dans la base $(\gamma_p)_{p\in\mathcal{P}}$ comme des $(0,1)$-combinaisons orthogonales deux à deux. Résoudre le problème des recombinaisons dans le cadre torique revient à déterminer les vecteurs γ_j.

Afin d'obtenir des équations explicites, on veut à nouveau utiliser le théorème 8 d'osculation. Il est donc naturel d'introduire le sous-espace vectoriel $V(D) \subset V$ engendré par les combinaisons des γ_p qui s'étendent à X. On a par construction les inclusions

$$\langle \gamma_1, \ldots, \gamma_s \rangle \subset V(D) \subset V,$$

et ce pour tout choix de D supporté par $|\partial X|$. Le résultat central est le suivant :

Théorème 10 *[137, Thm 2] Supposons f non dégénéré. Si D est supporté au bord de X et satisfait l'inégalité*

$$D \geq 2\mathrm{div}_\infty(f)$$

alors $(\gamma_1, \ldots, \gamma_s)$ coïncide à une permutation près avec la base échelonnée réduite de $V(D)$.

La preuve de ce théorème repose en partie sur la méthode des dérivées logarithmiques introduite par Ruppert [111]. Celle-ci est basée sur le fait que le premier groupe de cohomologie de de Rham du complémentaire de la courbe affine $\mathcal{C} = \{f = 0\} \subset \bar{\mathbb{K}}^2$ admet pour base les dérivées logarithmiques des facteurs absolument irréductibles $\bar{f}_1, \ldots, \bar{f}_r$ de f :

$$H^1(\bar{\mathbb{K}}^2 \setminus \mathcal{C}, \bar{\mathbb{K}}) = \left\langle \frac{d\bar{f}_1}{\bar{f}_1}, \ldots, \frac{\bar{f}_r}{\bar{f}_r} \right\rangle_{\bar{\mathbb{K}}}.$$

Toute l'idée est alors d'associer à $\gamma \in V(D)$ une (classe de) 1-forme rationnelle fermée $\omega \in H^1(\bar{\mathbb{K}}^2 \setminus \mathcal{C}, \bar{\mathbb{K}})$. L'égalité ci-dessus combinée à un argument galoisien assure alors que ω est combinaison linéaire des dérivées logarithmiques des facteurs *rationnels* de f, impliquant que γ est combinaison $\mathbb{K}$-linéaire des γ_j.

Le Théorème 8 d'osculation et la Proposition 6 donnent des équations explicites du sous-espace $V(D) \subset V$ des diviseurs qui s'étendent à X. Combiné au théorème ci-dessus et à l'égalité (1.3), cela conduit au corollaire suivant :

Corollaire 1 *[137, Thm 3] Les vecteurs* $(\gamma_1, \ldots, \gamma_s)$ *forment la base échelonnée réduite du noyau* $\mathrm{Ker}(A) \subset V$ *d'une matrice* explicite $A = (a_{p,m})_{p\in\mathcal{P}, m\in M}$*, où* M *est l'ensemble des points entiers intérieurs au polytope* $2P_f$*.*

Notons que la résolution des recombinaisons par l'algèbre linéaire requiert des précisions un peu plus élevées que la méthode des $\{0,1\}$-combinaisons (Théorème 9) du fait de l'inégalité

$$2\mathrm{div}_\infty(f) \geq \mathrm{div}_\infty(f) + \partial X.$$

Il existe cependant des situations où la précision $D = \mathrm{div}_\infty(f) + \partial X$ est suffisante pour une réduction des recombinaisons à l'algèbre linéaire [137, Section 4.2]. Notons aussi que dans le cas projectif, on retrouve les précisions $2\deg(f)$ et $\deg(f)+1$ qui apparaissent dans les travaux [20, 85, 83, 34].

3.3.3.2 Complexité.

Une fois les recombinaisons résolues, on peut calculer les facteurs f_j à partir de la restriction de sa courbe $\gamma_j = C_j \cap D$ *via* l'algèbre linéaire [137, Prop.3]. Finalement, on obtient une complexité polynomiale en le volume Δ du polytope de Newton de f. On note $2 \leq \omega < 2,5$ l'exposant de multiplication des matrices (la dernière référence étant [142]).

Théorème 11 *[137, Thm.1] Il existe un algorithme déterministe qui, étant donné* $f \in \mathbb{K}[x,y]$ *non dégénéré et dont le polytope contient le simplexe élémentaire, factorise* f *sur* $\mathbb{K}$ *avec* $\mathcal{O}(\Delta^\omega)$ *opérations dans* $\mathbb{K}$ *modulo la factorisation univariée des polynômes de facettes extérieures.*

La figure 3.2 donne un exemple pour lequel on gagne un facteur $d = \deg(f)$ comparé aux approches classiques. Le lecteur trouvera un autre exemple détaillé dans [137, Section 3.5], incluant des figures explicatives.

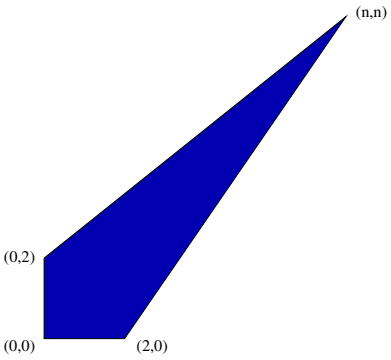

FIGURE 3.2 – Pour un tel polytope, les meilleurs algorithmes classiques [85] utilisent un changement générique de coordonnées puis 1 factorisation univariée de degré $2n$ et $\mathcal{O}(n^{\omega+1})$ opérations dans $\mathbb{K}$. L'approche torique maintient l'aspect creux et réduit la complexité à 2 factorisations univariées de degré 2 et $\mathcal{O}(n^\omega)$ opérations.

Remarque 3 *Il est sous-entendu ici que nous utilisons le modèle de complexité RAM, chargeant un coût constant pour chaque opération arithmétique dans* $\mathbb{K}$*. Dans la suite, nous utiliserons aussi au besoin la notation habituelle* $\tilde{\mathcal{O}}(n) = \mathcal{O}(n\log(n)^{\mathcal{O}(1)})$ *pour exprimer plus simplement nos résultats "à un facteur logarithmique près".*

D'autres algorithmes toriques. Mentionnons [9] où les auteurs vérifient si une factorisation d'un polynôme de facette peut se relever en une factorisation rationnelle en tenant compte de la géométrie du polygone de Newton. Mentionnons également [19] où les auteurs calculent (vite) un automorphisme de $\mathbb{Z}^2$ qui rend le polytope de Newton de f "presque" rectangulaire. Il n'y a alors plus qu'à appliquer les algorithmes "remontées et recombinaisons" classiques, conduisant à un algorithme en $\tilde{\mathcal{O}}(\Delta d^{\omega-1})$ où $d = \deg(f)$. Cependant, les factorisations des polynômes de facettes ne sont pas prises en compte, et le nombre de facteurs à recombiner reste supérieur à l'approche torique ci-dessus.

3.3.4 Ouverture : une meilleure complexité torique.

Si l'on spécialise notre algorithme au cas d'un polynôme dense, on retrouve essentiellement l'algorithme de Lecerf [85]. Or ce dernier a une complexité de $\mathcal{O}(d^{\omega+1})$ tandis que notre complexité se spécialise tristement en $\mathcal{O}(d^{2\omega})$.

La différence avec l'approche classique réside dans le coût de la construction de la matrice A sous-jacente aux recombinaisons (coût $\tilde{\mathcal{O}}(\Delta^2)$, cf [137, Cor.1]) et dans le coût du calcul des facteurs à partir de leurs développements de Taylor à l'infini torique, basé sur la résolution "brute-force" d'un système linéaire [137, Prop.3] de complexité $\mathcal{O}(\Delta^\omega)$ [137, Cor.2]. Concernant ce dernier point, le cas projectif classique requiert simplement un produit multi-facteurs dans $\mathbb{K}[[x]][y]$ à une précision donnée, de complexité quasi-linéaire. Généraliser cette approche au cadre torique requiert de gérer en plus les recollements entre les différentes cartes affines. Réussir à traiter ces tâches en temps quasi-linéaire $\tilde{\mathcal{O}}(\Delta)$ conduirait à une factorisation torique de complexité

$$\tilde{\mathcal{O}}(\Delta r^{\omega-1}) \subset \mathcal{O}(d^{\omega+1})$$

où r est la somme des longueurs entières des arêtes extérieures du polytope $N(f)$. On a toujours $r \leq d$, et bien souvent $r << d$, comme par exemple la figure 3.2. Notons que les enjeux sous-jacents d'interpolation bivariée rapide sont importants dans d'autres domaines du calcul formel, en particulier en lien avec les calculs d'espaces de Riemann-Roch [3].

3.4 Factorisation *via* une fibre critique

Les algorithmes de factorisation basés sur la recombinaison rationnelle des facteurs analytiques dans $\mathbb{K}[[x]][y]$ supposent au préalable que $f(0, y)$ est séparable, quitte à effectuer un changement de variable $x \mapsto x + a$ adéquat (en supposant $\mathbb{K}$ de cardinal suffisamment grand). Dans [141], je me suis intéressé à ne plus effectuer ce changement de variable et à travailler le long de la fibre $x = 0$ quand bien même $f(0, y)$ n'est pas séparable. L'idée sous-jacente est double :

- Ne plus perdre de temps à déterminer et effectuer un "bon" changement affine de coordonnées $f(x + a, y)$.
- Profiter précisément de la présence de ramification afin de faire baisser le nombre de facteurs analytiques à recombiner, dans le même esprit que les approches toriques.

Recombinaisons. Nous pouvons supposer sereinement que f est séparable et primitif dans $\mathbb{K}[x][y]$ (voir par exemple [84]). Considérons alors les factorisations irréductibles rationnelles et analytiques,

$$f = F_1 \cdots F_r \in \mathbb{K}[x, y] \qquad \text{et} \qquad f = \mathcal{F}_1 \cdots \mathcal{F}_s \in \mathbb{K}[[x]][y]. \tag{3.4}$$

Le problème des recombinaisons consiste à calculer les vecteurs $\mu_i \in (0,1)^s$ tels que $F_i = \prod_{j=1}^{s} \mathcal{F}_j^{\mu_{ij}}$. En passant par la dérivée logarithmique par rapport à y, on obtient

$$\hat{F}_i \partial_y F_i = \sum_{j=1}^{s} \mu_{ij} \hat{\mathcal{F}}_j \partial_y \mathcal{F}_j$$

où $\hat{F}_i = f/F_i$ et $\hat{\mathcal{F}}_j = f/\mathcal{F}_j$. On se ramène alors à un problème d'algèbre linéaire en cherchant des combinaisons linéaires des $\hat{\mathcal{F}}_j \partial_y \mathcal{F}_j$ qui sont polynomiales en x de degré $\leq d_x$ [20, 83], ou *via* des techniques à base de "résidus constants" [85]. Dans [141], on généralise ces méthodes au cas d'une fibre critique.

Factorisation rationnelle. Considérons l'entier $N = N(F)$ défini par

$$N := \left\lfloor \max\left(\frac{\mathrm{val}_x \operatorname{Res}_y(\mathcal{F}_i, \hat{\mathcal{F}}_i \partial_y \mathcal{F}_i)}{\deg(\mathcal{F}_i)},\ i = 1, \ldots, s \right) \right\rfloor,$$

où val_x est la valuation x-adique. L'entier N est en quelque sorte une borne supérieure sur la précision nécessaire pour "séparer" toutes les branches analytiques de f le long de la droite $x = 0$.

Il suit de nos travaux (ultérieurs) avec Adrien Poteaux [108, 109] que l'on peut calculer les facteurs analytiques $\mathcal{F}_i$ à précision N en temps quasi-linéaire, *i.e.* avec $\tilde{\mathcal{O}}(N d_y)$ opérations dans $\mathbb{K}$. Combiné avec [141, Thm.1], on peut énoncer aujourd'hui :

Théorème 12 *Notons $p = char(\mathbb{K})$ la caractéristique de $\mathbb{K}$. Soit s le nombre de facteurs analytiques de f et soit N comme ci-dessus. On peut factoriser f sur $\mathbb{K}$ avec :*

- $\mathcal{O}(\max(N, d_x) d_y s^{\omega-1})$ *opérations dans $\mathbb{K}$ si $p = 0$ ou $p > d_x(2d_y - 1)$;*
- $\mathcal{O}(k \max(N, d_x) d_y s^{\omega-1})$ *opérations dans $\mathbb{F}_p$ si $\mathbb{K} = \mathbb{F}_{p^k}$.*

Si $f(0, y)$ est séparable de degré d_y, on a $N = 0$. Notre algorithme se spécialise en celui développé dans [85], de complexité $\mathcal{O}(d_x d_y s^{\omega-1})$. En général, on a les inégalités

$$0 \leq N \leq \frac{\mathrm{val}_x \mathrm{Disc}_y(F)}{d_{\min}} \leq \frac{d_x(2d_y - 1)}{d_{\min}},$$

où $d_{\min} := \min\{\deg \mathcal{F}_i\,,\ i = 1, \ldots, s\}$. En particulier, $N \in \mathcal{O}(d_x d_y)$. Cette borne est malheureusement atteinte dans certains cas. Par exemple, pour

$$f(x, y) := (y - x^m)^2 + y^n \in \mathbb{Q}[x, y],$$

avec $n \geq 3$ impair, on a $N = \lfloor d_x d_y / 4 \rfloor$. Dans ce cas, on perd un facteur d_y par rapport à la complexité de [85]. Cependant, ces situations "extrémales" sont très particulières [1], et il est plus fréquent en pratique de constater que $N = \mathcal{O}(d_x)$, auquel cas on retrouve une complexité sous-quadratique comparable à [85], mais avec des recombinaisons plus rapides du fait que le nombre de facteurs à recombiner diminue en présence de ramification.

Une large classe de polynômes pour laquelle c'est le cas est celle des polynômes "non dégénérés" le long de la fibre $x = 0$, i.e. pour lesquels pour tout $a \in \bar{\mathbb{K}} \cup \infty$, le polynôme $f(x + a, y)$ est non dégénéré en $(0, 0)$ (au sens de Kushnirenko), voir [141, Section 8].

1. Ce problème nous a poussé avec Denis Simon à étudier dans [125] les polynômes dont le discriminant ont une valuation maximale au-dessus d'un point, nous y reviendrons plus tard.

Une autre classe importante est celle des polynômes localement irréductibles, *i.e.* pour lesquels $\mathrm{val}_x \operatorname{Res}_y(\mathcal{F}_j, \hat{\mathcal{F}}_j) = 0$ pour tout j : bien que la borne N puisse encore être de l'ordre de $d_x d_y$, on peut montrer que les recombinaisons nécessitent une précision $\mathcal{O}(d_x)$.

Le résultat suivant résume la situation pour ces cas spécifiques :

Théorème 13 *[141, Thm.2, Thm.3, Prop. 8.7] Soit s le nombre de facteurs irréductibles dans $\mathbb{K}[[x]][y]$. Supposons $\mathrm{char}(\mathbb{K}) = 0$ ou $\mathrm{char}(\mathbb{K}) > d_x(2d_y - 1)$ pour simplifier.*

- *On peut tester l'irréductibilité de f sur $\mathbb{K}$ avec $\mathcal{O}(d_x d_y s^{\omega-1})$ opérations dans $\mathbb{K}$.*
- *Si f est non dégénéré le long de la fibre $x = 0$, on peut factoriser f sur $\mathbb{K}$ avec $\mathcal{O}(d_x d_y s^{\omega-1})$ opérations dans $\mathbb{K}$.*
- *Si f est localement irréductible le long de la fibre $x = 0$, on peut factoriser f sur $\mathbb{K}$ avec $\tilde{\mathcal{O}}(d_x d_y^2) + \mathcal{O}(d_x d_y s^{\omega-1})$ opérations dans $\mathbb{K}$.*

Dans chacun de ces cas, la complexité est inférieure ou égale à celle des approches classiques [85], avec un gain dès lors que le nombre s de facteurs à recombiner est plus petit que dans le cas séparable (ce qu'il est légitime d'espérer, en particulier en petite caractéristique). Notons aussi que dans le cas critique, la factorisation de $f(0, y)$ est remplacée par des factorisations de facette univariées dont la somme des degrés est au plus d_y.

Factorisation absolue. On peut montrer que l'on peut calculer le nombre de facteurs absolument irréductibles (en particulier tester l'irréductibilité absolue) avec une précision $\mathcal{O}(d_x)$ en toutes circonstances, quand bien même la fibre est critique.

Théorème 14 *[141, Thm. 5] Soit $\bar{s}$ le nombre de facteurs irréductibles dans $\mathbb{K}[[x]][y]$. Supposons $\mathrm{char}(\mathbb{K}) = 0$ ou $\mathrm{char}(\mathbb{K}) > d_x(2d_y - 1)$ pour simplifier. On peut calculer le nombre de facteurs absolument irréductibles de f (en particulier tester l'irréductibilité absolue) avec $\mathcal{O}(d_x d_y \bar{s}^{\omega-1})$ opérations dans $\mathbb{K}$.*

Ce résultat est à comparer à $\mathcal{O}(d^{\omega+1})$ dans [34, Prop. 12], où les auteurs se ramènent au cas $f(0, y)$ séparable de degré $d = \deg(f)$ par un changement affine de coordonnées. Il y a alors exactement $d \geq d_y$ facteurs analytiques absolus à recombiner. Travailler le long d'une fibre "critique" permet de réduire ce nombre à

$$\bar{s} = \sum_{i=1}^{r} f_i \;\leq\; d_y = \sum_{i=1}^{r} e_i f_i \;\leq\; d$$

avec les notations usuelles pour les degrés résiduels et la ramification. Des gains similaires sont obtenus pour la factorisation absolue [141, Thm. 4]. L'approche "critique" dans le cas absolu est avantageuse par rapport à l'approche "régulière" en théorie, et ce d'autant plus que la ramification est élevée.

Exemple. Soient a, b deux entiers positifs et soit $\mathbb{K}$ de caractéristique zéro ou supérieure à $2a + b$. Soit

$$f(x, y) = (y^a + x^b + y^a x^b)(x^a y^b + 1)((y-1)^a + x^b + x^b(y-1)^a) \in \mathbb{K}[x, y].$$

La courbe $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ définie par f intersecte la droite $x = 0$ aux trois points $(0, 0), (0, 1), (0, \infty)$. Il est facile de montrer que f est non dégénéré et localement irréductible en chacun de ces points. On a alors $s = \bar{s} = 3$, indépendamment du degré de f. Les algorithmes sous-jacents aux deux théorèmes précédents requièrent seulement $\tilde{\mathcal{O}}(d_x d_y)$ opérations sur $\mathbb{K}$, à comparer aux complexités $\tilde{\mathcal{O}}(d_x d_y^{\omega+1})$ de [85] (cas rationnel) ou $\tilde{\mathcal{O}}(d^{\omega+1})$ de [34] (cas absolu) inhérentes au choix d'une fibre régulière [34].

Méthodes $\mathbb{Z}$-modules. Nous explorons aussi dans [141, Section 4] des méthodes à base d'élimination sur $\mathbb{Z}$ lorsque $\mathrm{char}(\mathbb{K}) = 0$. On montre que calculer des formes normales d'Hermite permet de résoudre les recombinaisons avec une précision $\mathcal{O}(d_x)$ pour des familles plus larges de polynômes.

3.5 Factorisation *vs* désingularisation

Une courbe projective plane réductible est nécessairement singulière d'après le théorème de Bezout. Cette observation évidente m'a poussé à étudier dans [140] les relations entre les factorisation d'un polynôme $f \in \mathbb{K}[x,y]$ et la désingularisation de sa courbe projective $\mathcal{C} \subset \mathbb{P}^2$. Je propose un nouvel algorithme de factorisation, méthode hybride entre [40] (calcul des fonctions rationnelles localement constantes) et [83, 85, 34] (remontées et recombinaisons).

Recombinaisons. On supposera cette fois pour simplifier que $f(0,y)$ est séparable de degré $d = \deg(f)$. Considérons alors les factorisations irréductibles sur $\mathbb{K}$

$$\begin{cases} f(x,y) = F_1(x,y)\cdots F_r(x,y) \\ f(0,y) = f_1(y)\cdots f_s(y) \end{cases}$$

Les facteurs analytiques de f étant ici en bijection avec les facteurs de $f(0,y)$ (lemme de Hensel), le problème des recombinaisons introduit dans la Section 3.4 consiste à déterminer les vecteurs $\mu_j \in (0,1)^s$ tels que $F_i(0,y) = \prod_{j=1}^s f_j^{\mu_{ij}}$.

L'idée cette fois est de calculer les μ_j non plus à partir des facteurs analytiques de f, mais à partir de la désingularisation de la courbe $\mathcal{C}$ de f. Cette étape franchie, le calcul des facteurs rationnels se fait alors par remontée de Hensel, de complexité quasi-linéaire.

Géométrie. Soit $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{K}}$ la clôture de Zariski de la courbe affine $f = 0$ et soit

$$\pi : X \to \mathbb{P}^2$$

une résolution faible plongée de $\mathcal{C}$ (la surface X étant obtenue par éclatement de $\mathbb{P}^2$). Une telle résolution existe sur tout corps $\mathbb{K}$ (même non parfait), voir par exemple [77, Thm 1.43 et Chapitre 1.8]. Soit $C \subset X$ la transformée stricte de $\mathcal{C}$ par π. Notons que du fait que C est lisse, ses composantes irréductibles ne s'intersectent pas. Il en découle que

$$\dim_{\mathbb{K}} H^0(\mathcal{O}_C) = \bar{r} \tag{3.5}$$

où $\bar{r}$ est le nombre de facteurs absolument irréductibles de f [140, Lem. 6].

Considérons l'intersection schématique $Z = C \cap L$ (réduite par hypothèse) avec la transformée stricte $L \subset X$ de la droite projective d'équation affine $x = 0$. L'application π induit par hypothèse un isomorphisme

$$H^0(\mathcal{O}_Z) \simeq \frac{\mathbb{K}[x,y]}{(x,f)} \simeq \frac{\mathbb{K}[y]}{(f_1)} \oplus \cdots \oplus \frac{\mathbb{K}[y]}{(f_s)}. \tag{3.6}$$

Combiné avec l'inclusion $\mathbb{K} \subset \mathbb{K}[y]/(f_j)$, on obtient une inclusion naturelle

$$\mathbb{K}^s \subset H^0(\mathcal{O}_Z).$$

D'un autre côté, l'inclusion $Z \subset C$ induit un morphisme de restriction

$$\alpha : H^0(\mathcal{O}_C) \hookrightarrow H^0(\mathcal{O}_Z).$$

Le résultat suivant réduit les recombinaisons au calcul du conoyau de α :

Lemme 3 *[140, Lem.5] Les vecteurs $(\mu_1, \ldots, \mu_r)$ forment la base échelonnée réduite (à permutation près) du sous-espace vectoriel $W := \mathbb{K}^s \cap Im(\alpha) \subset \mathbb{K}^s$.*

Résidus et dualité. Soit ω_C le faisceau des 1-formes régulières sur C (faisceau dualisant ou faisceau canonique) et soit $\omega_C(Z)$ le faisceau des 1-formes rationnelles de diviseur polaire borné par Z. Soit $p \in C$ une place de C, soit $\mathbb{K}_p$ son corps résiduel et soit $\psi \in \omega_{C,p}(Z)$. Etant donnée une uniformisante t de C en p, il existe une unique série formelle $h \in \mathbb{K}_p[[t]]$ telle que $\psi = h(t)dt/t$. On définit alors le *résidu de ψ en p* par la formule

$$\mathrm{res}_p\, \psi := \mathrm{Tr}_p\,(h(0))\,,$$

où $\mathrm{Tr}_p : \mathbb{K}_p \to \mathbb{K}$ est l'application trace. Cette définition ne dépend pas du choix de l'uniformisante [121], et généralise le résidu de Grothendieck sur $\mathbb{C}$ introduit en Section 1.5.1.2. Le théorème de dualité locale [2] induit la suite exacte courte

$$0 \to \omega_C \to \omega_C(Z) \stackrel{\mathrm{Res}}{\to} \omega_Z \to 0$$

où $\mathrm{Res}_{|U}(\psi)$ est défini localement comme la somme des résidus de ψ sur U, réalisation de la formule d'adjonction [86, Thm 9.1.39]. La suite cohomologique duale sous-jacente combinée à la dualité de Serre induit le résultat clé suivant, établissant le lien entre factorisation et désingularisation :

Proposition 7 *On a une suite exacte de $\mathbb{K}$-espaces vectoriels*

$$0 \longrightarrow H^0(\mathcal{O}_C) \stackrel{\alpha}{\longrightarrow} H^0(\mathcal{O}_Z) \stackrel{R}{\longrightarrow} H^0(\omega_C(Z))^\vee \stackrel{\beta}{\longrightarrow} H^0(\omega_C)^\vee \longrightarrow 0$$

où $^\vee$ désigne l'espace dual et où l'application R associe à ν la forme linéaire

$$R_\nu : \ \psi \longmapsto \sum_{p \in C} \mathrm{res}_p(\nu\psi).$$

En particulier, $\dim H^0(\omega_C(Z)) = g + d - \bar{r}$ où g est le genre géométrique de $\mathcal{C}$ (somme des genres des composantes absolument irréductibles).

On notera que l'inclusion $\mathrm{Im}(\alpha) \subset \ker(R)$ découle du théorème des résidus [3] qui assure que

$$\sum_{p \in C_j} \mathrm{res}_p \psi = 0$$

pour tout composante C_j de C, cf [129, Thm 3]. L'égalité $\dim H^0(\omega_C(Z)) = g + d - \bar{r}$ est un avatar du théorème de Riemann-Roch pour les courbes réductibles sur un corps $\mathbb{K}$ quelconque [86, Thm 7.3.26].

Espaces de Riemann-Roch et polynômes adjoints. Une courbe $\mathcal{H} \subset \mathbb{P}^2_{\mathbb{K}}$ est dite *adjointe* à $\mathcal{C}$ si elle s'annule avec multiplicité $m-1$ en chaque singularité de $\mathcal{C}$ de multiplicité m (incluant les singularités infiniment proches, cf [140, Def. 11]). Notons $\mathrm{Adj}(n) \subset \mathbb{K}[x,y]$ le $\mathbb{K}$-espace vectoriel des polynômes adjoints de f de degrés $\leq n$, i.e. définissant les équations affines des courbes adjointes à $\mathcal{C}$ de degré n. On a pour tout $k \in \mathbb{Z}$ un isomorphisme [140, Prop. 12]

$$\begin{array}{ccc} \mathrm{Adj}(d-3+k) & \stackrel{\simeq}{\longrightarrow} & H^0(\omega_C(kZ)) \\ h & \longmapsto & \pi^*\left(\frac{h dx}{x^n \partial_y h}\right)_{|C}. \end{array} \tag{3.7}$$

2. Analogue à (1.8), mais sur une courbe définie sur un corps quelconque
3. Généralisation du théorème des résidus sur $\mathbb{C}$, cf Section 1.5.1.3

Résolution des recombinaisons. Notons alors $A \subset \mathbb{K}[y]$ le sous-espace vectoriel des polynômes adjoints de degrés $d-2$ évalués en $x=0$:

$$A := \{h(0,y),\ h \in \mathrm{Adj}(d-2)\} \subset \mathbb{K}[y],$$

On a $\dim A = d - \bar{r}$ d'après [140, Cor.14]. Considérons alors l'application linéaire $T : k^s \to A^\vee$ qui à $\nu = (\nu_1, \ldots, \nu_s) \in \mathbb{K}^s$ associe la forme linéaire $T(\nu) : A \to \mathbb{K}$ définie par

$$T(\nu) : h \longmapsto \sum_{i=1}^{s} \nu_i \,\mathrm{Tr}_i \left(\frac{h(0,y)}{\partial_y f(0,y)} \right),$$

où $\mathrm{Tr}_i : \mathbb{K}[y]/(f_i) \to \mathbb{K}$ est l'application trace. Les isomorphismes (3.7) combinés avec la Proposition 7 et le Lemme 3 conduisent au résultat suivant :

Théorème 15 *[140, Cor.16] La famille $(\mu_1, \ldots, \mu_r)$ est à permutation près la base échelonnée réduite de $\ker(T)$.*

Une fois une base de A calculée, la matrice sous-jacente de l'application T est de taille $(d-\bar{r}) \times s$ et de rang $d-r$ d'après (3.5), (3.7) et la Proposition 7. La matrice est donc de taille quasi-optimale (*i.e.* linéaire en d) pour résoudre les recombinaisons. Une fois les vecteurs μ_j calculés, on calcule les facteurs F_j de f associés par remontée de Hensel multi-facteurs. Il en découle un algorithme de factorisation, que le lecteur trouvera détaillé sur deux exemples dans [140, Section 7] :

Corollaire 2 *[140, Thm.1] Etant donnée une base du sous-espace $A \subset \mathbb{K}[y]$ et étant donnée la factorisation de $f(0,y)$, on peut factoriser f sur $\mathbb{K}$ avec $\mathcal{O}(d^\omega)$ opérations dans $\mathbb{K}$.*

Factorisation absolue. Une variante de l'application linéaire T inspirée de [34, Prop.4] permet également de résoudre les recombinaisons dans le cas de la factorisation absolue (cf [140, Cor.18 et Lem.21]), la matrice sous-jacente étant dans ce cas une matrice de taille optimale $(d-\bar{r}) \times d$. En particulier, f est absolument irréductible si et seulement si $\dim A = d-1$. Il en découle un algorithme de factorisation absolue, voir [140, Thm.2 et Thm.3] ainsi que [140, Section 7] pour des exemples détaillés.

Le cas $f(0,y)$ non séparable. La même stratégie s'applique quand la fibre $x=0$ est critique. Les inconnues sont cette fois en bijection avec les places $p_1, \ldots, p_s \in C$ (rationnelles ou absolues, en fonction de la factorisation recherchée) supportées sur $|C \cap L|$. La forme linéaire $T(\nu)$ se calcule selon la formule [140, Prop.25]

$$h \longmapsto \sum_{i=1}^{r} \nu_i \, res_{p_i} \left(\pi^* \left(\frac{h(0,y)dy}{f(0,y)} \right) \right),$$

formule qui devient explicite dès lors que l'on connaît des uniformisantes de C en les places considérées (par exemple *via* les paramétrisations de Puiseux). Notons que le cas où f est localement irréductible le long de la droite $x=0$ se traite directement sans passer par la désingularisation, voir [140, Section 8] pour un exemple illustratif. Il découle de nos travaux ultérieurs [108] sur les séries de Puiseux que l'algorithme sous-jacent est de complexité $\mathcal{O}(d^\omega) + \tilde{\mathcal{O}}(d\delta)$ modulo le calcul d'une base de A, où δ est la valuation en x du discriminant de f. Une fois de plus, l'avantage comparé au cas d'une fibre régulière est d'avoir moins de facteurs analytiques à recombiner en présence de ramification.

3.5.1 Ouverture : calcul des adjoints modulo (x).

L'approche "désingularisation" requiert de calculer une base de A en temps raisonnable. La complexité de cette tâche dépend du degré du *diviseur adjoint* $\mathcal{A} \in \mathrm{Div}(\mathcal{C})$ (cf [3, Section 3.2] pour une définition concrète basée sur les séries de Puiseux). Ce degré, que nous noterons σ, vérifie

$$\sigma = \sum_{p \in \mathrm{Sing}(\mathcal{C})} m_p(m_p - 1)$$

où la somme porte sur les points singuliers (incluant les points infinitésimaux) de $\mathcal{C}$, et où m_p désigne la multiplicité de $\mathcal{C}$ en p. Il est lié aux invariants globaux de $\mathcal{C}$ par *la formule du genre*

$$\sigma = \frac{(d-1)(d-2)}{2} - g + (\bar{r} - 1).$$

On a donc $0 \leq \sigma \leq (d-1)(d-2)/2$ et σ est d'autant plus petit que la courbe est peu singulière. Expliquons brièvement comment calculer une base de A en s'appuyant sur les travaux récents [4, 5, 3] concernant le calcul des espaces de Riemann-Roch via la théorie des $\mathbb{K}[x]$-modules. On suppose ici que $\mathbb{K}$ est de caractéristique zéro ou $> d$.

- Une représentation adéquate du diviseur adjoint $\mathcal{A}$ se calcule en $\tilde{\mathcal{O}}(d^3)$ opérations grâce au calcul rapide des séries de Puiseux [108] [4].
- En supposant la courbe $\mathcal{C}$ en position "générale" [5], une base de Popov du $\mathbb{K}[x]$-module des polynômes adjoints de y-degrés $< d$ se déduit de $\mathcal{A}$ en temps $\tilde{\mathcal{O}}(d^\omega + d^{\omega-1}\sigma) \subset \tilde{\mathcal{O}}(d^{\omega+1})$ si les singularités sont ordinaires [5, Lem.7.4] et en temps $\tilde{\mathcal{O}}(\sigma^\omega \lceil d/\sigma \rceil) \subset \tilde{\mathcal{O}}(d^{2\omega})$ dans le cas de singularités quelconques [3, Thm. 6.4].
- Un dernier point clé, que la rédaction de ce mémoire m'a permis de remarquer, est qu'étant donnée une base de Popov comme ci-dessus, on peut calculer une base de A en temps $\mathcal{O}(d^\omega)$ (découle de [3, Prop 6.3] ou [69, Thm. 1.5]).

Il semble ainsi se dessiner dans le cas de singularités ordinaires un algorithme de factorisation de complexité totale

$$\tilde{\mathcal{O}}(d^3 + d^{\omega-1}\sigma) \subset \tilde{\mathcal{O}}(d^{\omega+1}) \tag{3.8}$$

sous-quadratique en la taille de l'entrée. Cette complexité améliore celle des algorithmes classiques remontées et recombinaisons, et ce d'autant plus que le genre de $\mathcal{C}$ est élevé, ou de manière équivalente, d'autant plus que la courbe $\mathcal{C}$ est peu singulière (le cas extrême d'une courbe lisse se traitant en $\tilde{\mathcal{O}}(d^3)$). Notons de plus que l'on peut réduire σ en négligeant les singularités en lesquelles $\mathcal{C}$ est localement irréductible [140, Section 9]. Il serait intéressant de coder un tel algorithme afin de faire des tests expérimentaux comparatifs.

Dans le cas de singularités quelconques, cela reste un challenge d'atteindre la complexité (3.8), voir [3, Section 7.7] pour une ouverture à ce propos. Quand bien même la complexité théorique serait compétitive, la difficile mise en oeuvre de [108] (séries de Puiseux) et [3] (Riemann-Roch) laisse douter d'un avantage pratique à passer par ces sous-algorithmes pour factoriser. Tout n'est pas perdu pour autant ! Il existe d'autres approches locales-globales prometteuses (d'un point de vue théorique et expérimental), basées sur la version rapide de l'algorithme de Montes [109] et les bases intégrales [69, 64], cf ouverture 4.3.1.

Bien entendu, l'enjeu d'un calcul rapide des polynômes adjoints concerne plus généralement le calcul des espaces de Riemann-Roch et dépasse très largement le cadre de la factorisation.

4. L'algorithme est Las-Vegas probabiliste dû à des calculs d'éléments primitifs, mais il découle de [109] un algorithme déterministe de complexité $\mathcal{O}(d^{3+o(1)})$ basé sur l'évaluation dynamique [70].

5. Une position générale s'atteint avec un algorithme probabiliste de complexité $\tilde{\mathcal{O}}(d^3)$ dès lors que $\mathbb{K}$ est de cardinal suffisamment élevé, cf [3].

3.6 Polynômes de petits discriminants

En arrivant au LMNO, l'ordinateur de mon collègue et cobureau Denis Simon turbinait pour chercher des polynômes dans $\mathbb{Z}[y]$ de petit discriminant [124]. De mon côté, j'étudiais des méthodes de factorisation $\mathbb{K}[x][y]$ dont la complexité dépendait des valuations du discriminant en les différentes places de $\mathbb{K}[x]$, comme nous l'avons vu en Section 3.4, et comme nous le verrons dans le chapitre suivant.

Ces considérations nous ont encouragés à déterminer une borne inférieure pour le degré en x du discriminant d'un polynôme $f \in \mathbb{K}[x][y]$ et à caractériser les polynômes dont le discriminant atteint cette borne. Dans une certaine mesure, nos résultats valident sur $\mathbb{K}[x]$ l'analogue d'une conjecture de Denis sur $\mathbb{Z}$. On s'est penché également sur la réduction de ces polynômes de discriminants "minimaux" sous l'action de $\mathrm{Aut}(\mathbb{A}^2)$ et $GL_2(\mathbb{K}[x])$. Nos résultats sont publiés dans [125].

Bornes inférieures. Dans ce qui suit $\mathbb{K}$ est supposé algébriquement clos de caractéristique nulle. Le discriminant par rapport à y d'un polynôme $f \in \mathbb{K}[x,y]$ est défini par

$$\mathrm{Disc}_y(f) := \frac{(-1)^{d_y(d_y-1)/2}}{\mathrm{lc}_y(f)}\mathrm{Res}_y(f, \partial_y f) \in \mathbb{K}[x].$$

Nous dirons que f est *primitif* s'il n'a pas de facteurs dans $\mathbb{K}[x]$, et *unitaire* si son coefficient dominant $\mathrm{lc}_y(f)$ relativement à y est constant. Le résultat suivant résume les principales bornes obtenues :

Théorème 16 *Soit $f \in \mathbb{K}[x,y]$ primitif et sans facteurs carrés.*

1. *[125, Thm.1.7] On a une borne inférieure uniforme*

$$\deg_x \mathrm{Disc}_y(f) \geq \lceil \frac{d_y - 1}{2} \rceil,$$

   et il y a une classification complète des polynômes pour lesquels il y a égalité.

2. *[125, Thm.1.2] Soit r le nombre de facteurs irréductibles de f. On a*

$$\deg_x \mathrm{Disc}_y(f) \geq d_y - r.$$

   Si f est unitaire, il y a égalité si et seulement s'il existe un automorphisme polynomial $\sigma \in \mathrm{Aut}(\mathbb{A}^2)$ tel que $f \circ \sigma \in \mathbb{K}[y]$, avec $f \circ \sigma$ séparable de degré r.

3. *[125, Thm.1.3] Supposons f irréductible et soit g le genre de la courbe $f = 0$. On a*

$$\deg_x \mathrm{Disc}_y(f) \geq 2g + d_y - 1,$$

   avec égalité si et seulement si la courbe $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ de f a une unique place au-dessus de $x = \infty$ et est lisse en dehors de cette place.

Réduction des polynômes minimaux. On dira qu'un polynôme f est *minimal* s'il est irréductible et s'il atteint la borne inférieure

$$\deg_x \mathrm{Disc}_y(f) = d_y - 1$$

prévue par les points 2 ou 3.

• Si f est *unitaire*, il découle du point 2 que f est minimal si et seulement s'il existe un automorphisme $\sigma \in \mathrm{Aut}(\mathbb{A}^2)$ tel que $f \circ \sigma = y$. Ceci équivaut au fait que f est un

polynôme coordonnée, *i.e* qu'il existe un polynôme g tel que $\mathbb{K}[x,y] = \mathbb{K}[g,f]$. De plus, on peut calculer récursivement σ *via* le polytope de Newton de f. La preuve découle du point 3 combiné au fameux "embedding line theorem" de Abhyankar et Moh [8] qui assure que la courbe affine $f = 0$ est rationnelle lisse avec une seule place à l'infini si et seulement si f est un polynôme coordonnée, un résultat profond, lié à la célèbre conjecture du jacobien. Une conséquence surprenante est que dans le cas unitaire, la minimalité par rapport à y équivaut à la minimalité par rapport à x (voir [125, Appendice A] pour des résultats analogues partiels dans le cas non unitaires).

• Dans le cas non unitaire, l'action de $\mathrm{Aut}(\mathbb{A}^2)$ ne préserve plus la minimalité et la classification des polynômes minimaux est plus délicate (au-delà de la caractérisation géométrique donnée par le point 3). Une approche naturelle pour réduire ces polynômes est de considérer l'action du groupe $G = \mathrm{GL}_2(\mathbb{K}[x])$ sur $\mathbb{K}[x,y]$ définie par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(f) = (c+dy)^{d_y} f\big(x, \frac{a+by}{c+dy}\big), \tag{3.9}$$

qui a la propriété de préserver la minimalité (cf [125, Section 2.4] pour les détails). Il est alors légitime de se demander si tout polynôme minimal non unitaire est G-équivalent à un polynôme minimal unitaire (donc à un polynôme coordonnée), complétant ainsi la classification des polynômes minimaux. Un résultat dans cette direction est [125, Thm 4.3] qui offre une caractérisation combinatoire des polynômes G-réduits *via* le polygone de Newton. Il en découle le résultat partiel suivant :

Théorème 17 *[125, Thm.1.6] Tout polynôme minimal dont le degré d_y est premier est G-équivalent à un polynôme coordonnée.*

La preuve est élégante : on plonge la courbe de f dans une surface torique projective adaptée, et la théorie de l'intersection torique impose des contraintes de divisibilité qui assurent par récurrence que f est G-équivalent à un polynôme unitaire minimal, cf [125, Thm 4.14].

Mais en s'appuyant sur [125, Thm 4.3] et sur des longs calculs sur ordinateur, le verdict tombe : il existe des polynômes minimaux non G-équivalents à des polynômes coordonnées.

Théorème 18 *[125, Thm.1.5] Pour tout $\lambda \in \mathbb{K}^\times$, le polynôme*

$$f(x,y) = x(x-y^2)^2 - 2\lambda y(x-y^2) + \lambda^2$$

est minimal mais n'est pas G-équivalent à un polynôme coordonnée.

La recherche exhaustive de contre-exemples par ordinateur est fastidieuse (voir [125, Appendice B] pour une discussion sur ce point), et nous n'avons pas réussi à en exhiber d'autres que ceux donnés par les G-orbites des polynômes f ci-dessus.

3.6.1 Ouverture.

Les groupes $\mathrm{GL}_2(\mathbb{K}[x])$ et $\mathrm{Aut}(\mathbb{A}^2)$ sont des sous-groupes du groupe de Cremona $\mathrm{Bir}(\mathbb{A}^2)$ des transformations birationnelles du plan. Quand bien même l'action de ce groupe ne préserve pas la minimalité, il préserve certaines propriétés géométriques des polynômes minimaux (la rationalité par exemple), et il est alors légitime de se demander :

Question : *Tout polynôme minimal est-il Cremona-équivalent à un polynôme coordonnée ?*

Ce problème est dans l'esprit de la Conjecture de Coolidge-Nagata pour les courbes unicuspidales de $\mathbb{P}^1 \times \mathbb{P}^1$, prouvée récemment par Koras et Palka [78]. On répond par l'affirmative pour la famille de contre-exemples ci-dessus [125, Prop.4.11], mais la question reste ouverte dans le cas général.

Chapitre 4

Factorisation univariée sur un anneau valué et applications

Contents

4.1 Introduction

La factorisation des polynômes à coefficients dans un anneau complet de valuation discrète est un problème fondamental du calcul formel. C'est en particulier une brique élémentaire essentielle pour résoudre diverses tâches plus élaborées dans les corps de nombres et les corps de fonctions (calcul des places et de leurs uniformisantes, factorisation des idéaux, bases intégrales, groupes de Galois, calcul du genre, espaces de Riemann-Roch, arithmétique dans les jacobiennes ou dans les groupes de classes d'idéaux, etc.).

Ce chapitre présente mes contributions les plus significatives sur ce sujet. La section 4.2 aborde le calcul rapide des séries de Puiseux et ses applications. La section 4.3 aborde la factorisation rapide sur un corps local et enfin la section 4.4 aborde la factorisation sur un anneau hensélien muni d'une valuation non nécessairement discrète de rang un.

Calcul du coût. Nous utiliserons à nouveau le modèle de complexité RAM, chargeant un coût constant pour chaque opération arithmétique élémentaire dans le corps spécifié (qui sera essentiellement le corps résiduel). On utilise la notation $\tilde{\mathcal{O}}(n) = \mathcal{O}(n \log(n)^{\mathcal{O}(1)})$ pour ne pas tenir compte des facteurs logarithmiques.

4.2 Le cas des séries formelles.

La factorisation d'un polynôme à coefficients dans un anneau de série formelle est étroitement lié au calcul des séries de Puiseux. Ces dernières interviennent dans des problèmes variés d'algorithmique des courbes planes. En particulier, elles permettent de calculer les

paramétrisations rationnelles locales d'une courbe plane (définition 1), offrant une représentation très pratique des places d'un corps de fonctions. En collaboration avec Adrien Poteaux, et à la suite de ses travaux avec Marc Rybowic (cf [106] et références), nous avons résolu le problème du calcul déterministe de la partie singulière des séries de Puiseux en temps quasi-optimal en la taille de la sortie [108], et par là même résolu le problème de la factorisation sur $\mathbb{K}[[t]][x]$ en temps quasi-linéaire. Une conséquence remarquable est le calcul du genre d'une courbe plane de degré d en temps $\tilde{\mathcal{O}}(d^3)$.

4.2.1 Séries de Puiseux

Soit $\mathbb{K}$ un corps de caractéristique nulle. Le célèbre théorème de Newton-Puiseux assure que le corps des séries de Puiseux

$$\overline{\mathbb{K}}\{\{t\}\} := \bigcup_{e\in\mathbb{N}} \overline{\mathbb{K}}((t^{1/e}))$$

est un corps algébriquement clos. En particulier, tout polynôme $f \in \mathbb{K}((t))[x]$ séparable de degré d en x admet d racines distinctes dans $\overline{\mathbb{K}}\{\{t\}\}$. Ce dernier point reste valable en caractéristique positive dès lors que l'on suppose $\mathrm{char}(\mathbb{K}) > d$.

Séries de Puiseux et factorisation. Les séries de Puiseux sont ainsi intimement liées à la factorisation dans $\mathbb{K}((t))[x]$. Elles peuvent être regroupées en fonction de l'extension de corps qu'elles engendrent. Plus précisément, on peut distinguer trois niveaux de factorisations :

$$\begin{aligned} f &= \prod_{i=1}^{\rho} F_i \text{ avec } F_i \text{ irréductible dans } \mathbb{K}((t))[x] \\ F_i &= \prod_{j=1}^{f_i} F_{ij} \text{ avec } F_{ij} \text{ irréductible dans } \overline{\mathbb{K}}((t))[x] \\ F_{ij} &= \prod_{k=0}^{e_i-1} \left(x - S_{ij}(t^{1/e_i}\zeta_{e_i}^k)\right) \text{ avec } S_{ij} \in \overline{\mathbb{K}}((t)) \end{aligned}$$

où $\zeta_{e_i} \in \overline{\mathbb{K}}$ est une racine primitive e_i-ème de l'unité. Les racines de f sont alors les séries de Puiseux

$$S_{ijk}(x) = S_{ij}(t^{1/e_i}\zeta_{e_i}^k) \in \overline{\mathbb{K}}((t^{1/e_i})).$$

Soit $S = S_{ijk}$ une telle série de Puiseux de f.

- L'entier e_i est *l'indice de ramification* de la série S.
- L'entier f_i est le *degré résiduel* de la série S, égal au degré de l'extension résiduelle $\mathbb{K}_i$ de $\mathbb{K}$ engendrée par les coefficients des facteurs F_{ij}.
- L'*indice de régularité* de la série S est le plus petit entier r_i tel que toutes les séries de f tronquées avec précisions r_i/e_i soient deux à deux distinctes.

Les entiers e_i et f_i ne dépendent que du facteur analytique F_i et vérifient l'égalité $\sum_{i=1}^{\rho} e_i f_i = d$. L'entier r_i dépend de F_i et de ses multiplicités d'intersections avec les cofacteurs F_j.

Paramétrisations rationnelles. A bien des égards, en particulier d'un point de vue calculatoire, il est préférable de déterminer plutôt les paramétrisations sous-jacentes aux séries de Puiseux, que l'on cherche à coefficients dans une extension minimale de $\mathbb{K}$. Ces considérations conduisent à la définition suivante, introduite par Duval [40] :

Définition 1 *Un système de* paramétrisations rationnelles locales *de f au-dessus de 0 est la donnée d'une famille $\{R_i\}_{i=1,\ldots,\rho}$ telle que*

$$R_i(t) = (\gamma_i t^{e_i}, S_i(t)) \in \mathbb{K}_i((t))^2$$

et vérifiant $F_i(\gamma_i t^{e_i}, S_i(t)) \equiv 0$. La partie singulière *de la paramétrisation R_i est sa troncation à précision r_i.*

Les paramétrisations *rationnelles* sont donc définies sur $\mathbb{K}_i$, et il est facile de montrer que c'est la plus petite extension de $\mathbb{K}$ possible. Un tel système de paramétrisations existe toujours [40] et on peut alors en déduire aisément les séries de Puiseux de f. La difficulté du calcul concerne la partie singulière, le reste des coefficients pouvant alors s'obtenir par itération de Newton quadratique.

Représentations résiduelles. Afin de s'affranchir des factorisations univariées potentiellement coûteuses, on peut considérer plus généralement des paramétrisations définies sur des produits de corps (anneaux non intègres), en s'appuyant sur le principe de l'évaluation dynamique (voir [108, Def.18]) afin de tenir compte des potentiels diviseurs de zéros. Les paramétrisations rationnelles sur un corps s'en déduisent par restes chinois. Afin d'énoncer des résultats déterministes, on supposera dans ce qui suit que $\mathbb{K}_i$ est une $\mathbb{K}$-algèbre définie par un idéal triangulaire zéro-dimensionnel multivarié, en contraste de [108] où nous calculons des représentations primitives *via* une procédure probabiliste Las-Vegas. Le faible prix à payer est de remplacer les complexités probabilistes $\tilde{\mathcal{O}}(n)$ de [108] par les complexité déterministes $\mathcal{O}(n^{1+o(1)})$ inhérentes à l'évaluation dynamique rapide dans les algèbres triangulaires [70].

Résultat principal. Nous assumerons que $\mathbb{K}$ est un corps effectif, *i.e.* qu'il supporte le test d'égalité et les opérations arithmétiques élémentaires. Soit $f \in \mathbb{K}[[t]][x]$ séparable, primitif de degré d. On notera δ la valuation en t du discriminant de f (plus 1 pour être rigoureux).

Théorème 19 *[108, Thm.1] Si $\mathrm{char}(\mathbb{K}) = 0$ ou $\mathrm{char}(\mathbb{K}) > d$, on peut calculer la partie singulière d'un système de paramétrisations rationnelles locales de f au-dessus de 0 avec au plus $\mathcal{O}(\delta\, d^{1+o(1)})$ opérations sur $\mathbb{K}$.*

L'algorithme est une variante de l'algorithme de Duval [40], qui est lui même une variante rationnelle de l'algorithme originel de Newton-Puiseux : on applique récursivement à f des transformations monomiales et des shifts sur x déterminés respectivement par les pentes du polytope de Newton et les racines des polynômes de facettes. L'algorithme de Duval a été amélioré dans une importante série de papiers par Poteaux et Rybowic, culminant dans [106] avec une complexité $\tilde{\mathcal{O}}(\delta d^2)$. Notre résultat améliore encore d'un facteur d ce résultat, conduisant à une complexité quasi-linéaire en la taille de la sortie dès lors que l'on travaille à précision δ. Outre l'évaluation dynamique, un ingrédient clé est de montrer qu'une petite précision $\mathcal{O}(\delta/d)$ permet de calculer "la moitié" des séries de Puiseux. Combiné à un lemme de Hensel généralisé, on met ainsi en place une stratégie diviser pour régner.

4.2.2 Applications.

Les séries de Puiseux sont des ingrédients fondamentaux pour de nombreuses tâches concernant l'algorithmique des courbes planes. Mentionnons tout de suite quelques unes des applications immédiates du théorème 19.

Factorisation analytique. Une première application est la résolution de notre problème initial, *i.e* un algorithme de factorisation dans $\mathbb{K}[[t]][x]$ à précision $N \geq \delta$ de complexité quasi-optimale.

Théorème 20 *[108, Thm.3] Soit $f \in \mathbb{K}[[t]][x]$ séparable de degré d tel que $char(\mathbb{K}) = 0$ ou $char(\mathbb{K}) > d$. On peut calculer les facteurs irréductibles de f à une précision donnée $N \in \mathbb{N}$ avec au plus*

$$\mathcal{O}(dN + \delta d^{1+o(1)})$$

opérations dans $\mathbb{K}$, plus des factorisations univariées dont la somme des degrés est $\leq d$.

Nous avons vu en Section 3.4 une conséquence immédiate du théorème 20 sur la factorisation bivariée *via* l'utilisation d'une fibre critique (voir aussi [141]).

Désingularisation. On peut appliquer nos résultats pour calculer les séries de Puiseux d'un polynôme $f \in \mathbb{K}[t, x]$ au-dessus de tout point critique t_0 (i.e. au-dessus de toute racine du discriminant). On obtient le résultat important suivant :

Théorème 21 *[108, Thm.2] Soit $f \in \mathbb{K}[t, x]$ de bidegré (n, d), sans facteurs carrés et tel que $char(\mathbb{K}) = 0$ ou $char(\mathbb{K}) > d$. On peut calculer les paramétrisations rationnelles locales de f au-dessus de tous les points critiques avec $\mathcal{O}(nd^{2+o(1)})$ opérations dans $\mathbb{K}$.*

On renvoie à [108, Section 6] pour le détail des représentations des paramétrisations en évaluation dynamique.

Calcul du genre. Il découle du théorème 21 et de la formule de Riemann-Hurwitz le résultat suivant :

Corollaire 3 *[108, Cor.1.1] Il existe un algorithme déterministe qui calcule le genre géométrique d'une courbe algébrique plane de degré d définie sur un corps $\mathbb{K}$ de caractéristique nulle ou $> d$ avec $\mathcal{O}(d^{3+o(1)})$ opérations dans $\mathbb{K}$.*

Ce résultat améliore drastiquement [13, Thm.3.6 et Rem.3.8]. Cette complexité est optimale dans l'état actuel des connaissances, dans le sens où améliorer cette borne demanderait d'améliorer la complexité d'opérations arithmétiques fondamentales, comme le calcul du résultant de deux polynômes bivariés de degré d, de complexité $\tilde{\mathcal{O}}(d^3)$. Combiné à des procédés de bonnes réductions modulo des idéaux premiers, il découle du corollaire 3 de très bonnes complexités binaires probabilistes pour le calcul du genre d'une courbe plane définie sur un corps de nombre [108, Cor.1.2 et Cor.1.3].

Bases intégrales. Les séries de Puiseux interviennent dans le calcul des bases intégrales d'un corps de fonction [130, 22, 2] et le théorème 19 a permis d'améliorer récemment la complexité algorithmique de cette tâche : en combinant nos résultats avec l'algorithme de Böhm et. al [22], Abelard montre dans [2] que le calcul d'une base intégrale du corps de fonction d'une courbe plane de degré d peut s'effectuer en temps $\mathcal{O}(d^{4+o(1)})$. C'est à notre connaissance la meilleure complexité à ce jour (cependant, des résultats récents laissent espérer pouvoir faire mieux, cf ouverture 4.3.1).

Espaces de Riemann-Roch. Les espaces de Riemann-Roch interviennent dans des domaines variés du calcul formel tels que la factorisation bivariée (section 3.5), les calculs dans les jacobiennes [71, 75], la paramétrisation des courbes rationnelles [131] ou encore les codes correcteurs de Goppa [52] pour ne citer que quelques exemples. Dans [3], les auteurs calculent les espaces de Riemann-Roch en se basant sur le calcul rapide des paramétrisations rationnelles locales afin de représenter les places d'un corps de fonction et de manipuler efficacement les diviseurs d'une courbe algébrique plane : le théorème 19 assure que le coût du calcul de ces places est maintenant négligeable dans le calcul des espaces de Riemann-Roch.

4.2.3 Irréductibilité et type d'équisingularité.

Il suit de [108, Prop.3.18] qu'il suffit de travailler à précision $\mathcal{O}(\delta/d)$ pour détecter l'irréductibilité d'un polynôme séparable $f \in \mathbb{K}[[t]][x]$, ce qui laisse espérer un test d'irréductibilité de complexité $\mathcal{O}(\delta^{1+o(1)})$ (donc quasi-linéaire en la taille de l'entrée en supposant $f \in \mathbb{K}[t][x]$). Malheureusement, notre algorithme à la Puiseux induit une complexité $\mathcal{O}(\delta d^{1+o(1)})$ [108, Thm.4] et on peut montrer que cette borne est potentiellement atteinte du fait de la taille des polynômes intermédiaires utilisés lors des diverses transformations de Newton-Puiseux [108, Exemple 9].

Racines approchées. Dans [110], on introduit une nouvelle approche inspirée du test d'irréductibilité de Abhyankhar [7, 6] pour les germes de courbes planes sur $\mathbb{C}$. Ce concept est basé sur la notion fondamentale de *racine approchée*.

Définition 2 *Soit $\mathbb{A}$ un anneau et soit $f \in \mathbb{A}[x]$ unitaire de degré d. Pour tout entier N divisant d et inversible dans $\mathbb{A}$, il existe un unique polynôme unitaire $\psi \in \mathbb{A}[x]$ de degré d/N tel que $\deg\left(F - \psi^N\right) < d - \frac{d}{N}$. Le polynôme ψ est la racine approchée N-ème de f, notée $\psi = \sqrt[N]{f}$.*

Une définition équivalente plus parlante est que le développement ψ-adique de f n'ait pas de termes de degré $N-1$, *i.e* qu'il s'écrive

$$f = \psi^N + a_{N-2}\psi^{N-2} + \cdots + a_1\psi + a_0.$$

Abhyankhar a mis en valeur les racines approchées dans l'étude des germes complexes, en montrant qu'elles constituent des polynômes clés à la MacLane [7]. En particulier, le semi-groupe des multiplicités d'intersection d'un germe complexe irréductible $f \in \mathbb{C}[[x,y]]$ est minimalement engendré par les multiplicités d'intersections avec des racines approchées $\psi_0, \ldots, \psi_g$ de degrés convenables, caractérisant ainsi le type topologique. On renvoie le lecteur au survey [105] pour plus de détails dans le cas complexe.

Un test d'irréductibilité quasi-optimal. L'utilisation des racines approchées permet de démontrer le résultat suivant :

Théorème 22 *[110, Thm.1.2] On peut tester l'irréductibilité d'un polynôme de Weierstrass $f \in \mathbb{K}[[t]][x]$ de degré premier à char$(\mathbb{K})$ avec $\mathcal{O}(\delta^{1+o(1)})$ opérations dans $\mathbb{K}$.*

L'algorithme se déroule ainsi. On calcule récursivement une séquence de racines approchées $\psi_0, \ldots, \psi_k$ de f de degré strictement croissants $N_0 = 1 < N_1 < \cdots < N_k$. On calcule alors le développement $(\psi_0, \ldots, \psi_k)$-adique de f, à partir duquel on construit un polygone de Newton généralisé de f. On montre que ce polygone coïncide (à une translation près) avec le polygone d'une certaine transformée de Newton-Puiseux de f. Si le polygone a plusieurs arêtes alors f est réductible. Sinon, on calcule un polynôme résiduel associé à l'unique

arête (*via* une formule récursive). Si ce polynôme a plusieurs facteurs irréductibles, alors f est réductible. Sinon, on déduit le degré N_{k+1} de la prochaine racine approchée ψ_{k+1} à calculer et on procède récursivement. Le polynôme f est irréductible si et seulement si on atteint $N_g = 1$ après un certain nombre g d'étapes.

Outre sa complexité, l'algorithme est plus simple à mettre en oeuvre que les algorithmes type Newton-Puiseux, en ce sens que l'essentiel des opérations élémentaires consiste en des divisions euclidiennes ne faisant pas intervenir d'extension algébrique de $\mathbb{K}$.

Si f est irréductible, la suite $\psi_0, \psi_1, \ldots, \psi_g$ permet de retrouver la plupart des quantités numériques attachées à la singularité locale $(C, 0) \subset (\mathbb{A}^2_{\mathbb{K}}, 0)$ définie par $f = 0$ (degré résiduel, indice de ramification, valuation du discriminant, générateurs minimaux du semi-groupe, nombre de Milnor, type topologique).

Type d'équisingularité. Le type d'équisingularité d'un germe $(C, 0) \subset (\mathbb{A}^2_{\mathbb{K}}, 0)$ est caractérisé par les exposants caractéristiques de Puiseux de chaque branche et par les multiplicités d'intersection entre les branches. Cette notion, introduite par Zariski [146] (généralisée en caractéristique positive dans [23]) est fondamentale en théorie des singularités et en théorie des déformations [56, 24], en particulier du fait du théorème de Zariski qui assure que deux germes complexes sont topologiquement équivalents si et seulement s'ils ont même type d'équisingularité.

Il découle des résultats ci-dessus que le type d'équisingularité d'un germe de courbe se calcule en temps $\mathcal{O}(d\delta^{1+o(1)})$ dans le cas réductible (théorème 19) et $\mathcal{O}(\delta^{1+o(1)})$ dans le cas irréductible (théorème 22). En apportant de légères modifications à l'algorithme sous-jacent, et en utilisant l'évaluation dynamique, on montre dans [107] que l'on peut étendre la complexité $\mathcal{O}(\delta^{1+o(1)})$ aux germes *pseudo-irréductibles*, définis comme les germes de courbes dont les branches sont équisingulières et ont mêmes ensembles d'intersection [107, Def.1]. On donne de plus une caractérisation algorithmique (explicite) précise des germes pseudo-irréductibles [107, Thm.2], qui assure en particulier un test de pseudo-irréductibilité de complexité quasi-optimale basé sur les racines approchées. La preuve repose sur une analyse détaillée des monômes caractéristiques des paramétrisations rationnelles locales.

4.2.4 Ouvertures

1. Calcul des coefficients des séries de Puiseux. L'algorithme du théorème 22 permet seulement de déterminer les termes *caractéristiques* de la paramétrisation locale, termes pour lesquels on découvre un facteur non trivial du degré résiduel ou de l'indice de ramification (voir [107]). Mais peut-on calculer *tous les coefficients* de la partie singulière d'une paramétrisation rationnelle locale d'un polynôme irréductible de $\mathbb{K}[[t]][x]$ avec la même complexité quasi-optimale $\mathcal{O}(\delta^{1+o(1)})$?

2. Séries de Puiseux multivariées. Soit $f \in \mathbb{K}(t_1, \ldots, t_n)[x]$. Si $\mathbb{K}$ est de caractéristique zéro, les racines de f peuvent à nouveau se calculer comme des séries de Puiseux multivariées dont les exposants peuvent être choisis dans un cône rationnel polyhédral convexe de $\mathbb{R}^n$ (travaux de MacDonald [89]). En s'inspirant du cas univarié, on cherche à définir puis calculer des représentations rationnelles de ces séries de Puiseux, le but étant de maintenir les calculs dans des extensions minimales de $\mathbb{K}$ afin d'obtenir des bonnes bornes de complexités et d'extraire des données arithmétiques significatives. Ce problème est étroitement lié à nos travaux récents [10] sur la factorisation sur les anneaux de valuations non discrètes (ouvertue 4.4.1), l'idée étant de considérer le complété de $\mathbb{K}(t_1, \ldots, t_n)$ pour une valuation non discrète de rang un du type $v(t_1^{i_1} \cdots t_n^{i_n}) = \sum_{k=1}^n i_k \lambda_k$ où $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$

sont $\mathbb{Q}$-linéairement indépendants. Calculer les coefficients des séries de Puiseux multivariées rationnelles dépasse toutefois le problème de la factorisation sur ce complété. Ceci est un travail en cours, en collaboration avec Jose Cano, Sebastian Falkensteiner et Adrien Poteaux,

4.3 Anneaux de valuation discrète complets

Toujours en collaboration avec Adrien Poteaux, nous avons cherché à généraliser dans un travail récent [109] le théorème 20 de factorisation locale rapide au cas d'un polynôme $f \in \mathbb{A}[x]$ à coefficients dans un anneau de valuation discrète complet quelconque $(\mathbb{A}, v)$. Les exemples typiques sont bien sûr :

- L'anneau $\mathbb{A} = \mathbb{Z}_p$ des entiers p-adiques (muni de la valuation p-adique, de corps résiduel $\mathbb{F}_p$) ;
- L'anneau $\mathbb{A} = \mathbb{K}[[t]]$ des séries formelles (muni de la valuation t-adique, de corps résiduel $\mathbb{K}$), comme considéré dans la section précédente mais sans hypothèses sur la caractéristique résiduelle.

Un cas important est lorsque $\mathbb{A} = \hat{A}_P$ est le complété du localisé d'un anneau de Dedekind A en un idéal premier P et $f \in A[x]$ est unitaire irréductible. Le théorème de Hensel assure alors qu'il y a une bijection entre les facteurs irréductibles locaux de f dans $\mathbb{A}[x]$ et les idéaux premiers divisant P dans l'extension du corps des fractions $\mathrm{Frac}(A)$ définie par f. A ce titre, la factorisation locale est un problème fondamental du calcul formel, pierre angulaire de l'algorithmique des corps de nombres et des corps de fonctions.

Bref historique. Les premiers algorithmes de factorisation sur $\mathbb{Z}_p[x]$ sont basés sur l'algorithme probabiliste "round 4" de Zassenhaus (voir par exemple [25, 101, 46, 102]), mais ce dernier souffre de la perte de précision lors du calcul des polynômes caractéristiques. Dans une autre direction impulsée par les travaux fondateurs de Dedekind, Hensel et Bauer, Ore [97, 98] a montré dans les années 1920 que l'on pouvait détecter des factorisations partielles à partir de la décomposition du polytope de Newton p-adique (version arithmétique du polytope de Newton-Puiseux) et de la factorisation de certains polynômes résiduels associés. Malheureusement, la factorisation issue de cette double dissection n'est pas complète lorsque le polynôme est "dégénéré". Mac Lane résout ce problème quelques années plus tard dans le langage des valuations [87, 88], mais sa méthode n'est pas constructive. Il faut attendre les travaux de Okutsu à la fin des années 80 puis de Montes [104] à la fin des années 90 pour qu'une généralisation implémentable de la "double dissection" de Ore voit le jour (repris et expliqué en détail dans [60]). Au-delà d'utiliser des polytopes d'ordres supérieurs (déjà introduits par Mac Lane en termes de valuations augmentées), Montes réussit à construire explicitement des polynômes résiduels d'ordres supérieurs, dernière pierre manquante à l'édifice. L'algorithme qui en découle permet ainsi de calculer, représenter et manipuler efficacement les idéaux premiers d'un corps de nombre vivant au-dessus d'un idéal premier de $\mathbb{Z}$ (cf par exemple [61]), outil crucial en théorie algorithmique des nombres. On parle de *OM-algorithmes*, des noms de Ore, Mac Lane, Okutsu et Montes. Du point de vue de la factorisation locale, il restait alors à introduire un lifting à la Newton-Hensel afin de poursuivre le calcul des facteurs à une précision arbitraire, étape franchie plus tard grâce à l'algorithme *Single-Factor Lifting* de [62]. Ces algorithmes sont implémentés dans Magma, très efficaces en pratique. Nous montrons cependant dans [109] que l'on peut être encore plus efficace et atteindre une complexité quasi-optimale.

Résultats. Nous noterons $\mathbb{F}$ le corps résiduel de $\mathbb{A}$ et nous supposerons que $\mathbb{F}$ est un corps effectif, *i.e.* qu'il supporte le test d'égalité et les opérations arithmétiques élémentaires. Pour simplifier, on exprimera dans ce qui suit la complexité en termes du nombre d'opérations dans $\mathbb{F}$, en chargeant le cas échéant une opération arithmétique dans $\mathbb{F}$ pour une opération arithmétique entre deux éléments d'un système fixé $A \subset \mathbb{A}$ de représentants de $\mathbb{F}$.

On notera d le degré du polynôme d'entrée $f \in \mathbb{A}[x]$ et δ la valuation de son discriminant, supposé non nul (*i.e* f séparable). On note pour simplifier $\mathcal{O}_\varepsilon(n) = \mathcal{O}(n^{1+o(1)})$.

Il est montré dans [15, Thm.5.18] que l'OM-algorithme combiné au Single-factor lifting permet de factoriser f dans $\mathbb{A}[x]$ à précision n avec $\mathcal{O}_\varepsilon(d\delta^2 + d^2 n)$ opérations dans $\mathbb{F}$, plus le coût des factorisations résiduelles univariées. Nous améliorons significativement cette complexité :

Théorème 23 *[109, Thm.4] Soit $f \in \mathbb{A}[x]$ un polynôme unitaire séparable et soit $p = \mathrm{Char}(\mathbb{F})$ la caractéristique résiduelle. On peut calculer les facteurs irréductibles de f à précision n avec*

- *$\mathcal{O}_\varepsilon(d\delta + dn)$ opérations sur $\mathbb{F}$ si $p = 0$ ou $p > d$*
- *$\mathcal{O}_\varepsilon(d\delta + dn + \delta^2)$ opérations sur $\mathbb{F}$ sinon,*

modulo le coût des factorisations résiduelles univariées, coût qui rentre dans l'estimation ci-dessus dès lors que le cardinal de $\mathbb{F}$ est polynomial en d, δ.

L'algorithme est déterministe, de complexité quasi-optimale si $p = 0$ ou $p > d$ et si $n \geq \delta$. Dans le cas des séries formelles, on retrouve la même complexité que l'approche à la Newton-Puiseux (Théorème 20), mais l'algorithme est ici beaucoup plus facile à mettre en oeuvre (essentiellement des divisions euclidiennes) et il est légitime d'espérer que la complexité expérimentale coïncide asymptotiquement avec la complexité théorique (une implémentation est en cours).

Notons que l'utilisation de l'évaluation dynamique [38] permet de s'affranchir de la factorisation résiduelle univariée, si l'on ne cherche que certaines informations arithmétiques (*e.g.* valuation du discriminant ou du résultant, ramification, nombre de Milnor, etc.). Notons enfin qu'il suffit de considérer une précision $n = \delta + 1$ pour récupérer toute l'information locale nécessaire pour résoudre les problèmes d'arithmétique usuels dans les corps globaux, en particulier le calcul des bases intégrales.

Irréductibilité. L'algorithme de Montes conduit à un test d'irréductibilité dans $\mathbb{A}[x]$ de complexité $\mathcal{O}_\varepsilon(\delta^2)$. Nous améliorons à nouveau ce résultat dès lors que la ramification n'est pas sauvage. On supposera pour simplifier que f est Weierstrass, *i.e.* $f = x^d + \sum_{i<d} a_i x^i$ avec $v(a_i) > 0$.

Théorème 24 *[109, Thm.2 et Prop.5] Soit $f \in \mathbb{A}[x]$ un polynôme de Weierstrass séparable et soit $p = \mathrm{Char}(\mathbb{F})$. On peut tester l'irréductibilité de f avec*

- *$\mathcal{O}_\varepsilon(\delta)$ opérations sur $\mathbb{F}$ si p ne divise pas d,*
- *$\mathcal{O}_\varepsilon(\delta^2)$ opérations sur $\mathbb{F}$ sinon,*

modulo le coût des tests d'irréductibilité univariés sur les corps résiduels, coût qui rentre dans l'estimation ci-dessus dès lors que le cardinal de $\mathbb{F}$ est polynomial en d, δ.

Comme dans le cas des séries formelles, cet algorithme retourne en bonus une séquence de polynômes clés $\psi_0, \ldots, \psi_g$ associés à f (on peut prendre des racines approchées si p ne divise pas d). Il est montré dans [59] que cette séquence constitue une base d'Okutsu, de laquelle on peut extraire les quantités numériques les plus significatives attachées à l'extension locale $\mathbb{A}[x]/(f)$ de $\mathbb{A}$.

Ingrédients. Les preuves des théorèmes 23 et 24 sont basées sur les améliorations suivantes de [61] :

- On met en place une stratégie diviser pour régner basée sur la gestion de la précision, stratégie similaire à celle développée dans le cadre des séries de Puiseux [108].
- On prouve un lemme de Hensel valué et multifacteur [109, Cor.2], généralisation de [26], qui permet de remonter une factorisation résiduelle généralisée en une factorisation dans $\mathbb{A}[x]$ à précision souhaitée en temps quasi-linéaire (dans [62] les facteurs sont plutôt liftés un par un, selon une méthode à la Newton).
- Si p ne divise pas d, on montre que les racines approchées (Définition 2) sont des représentants des "types" de Montes [109, Prop.2]. Ces dernières se calculent en temps quasi-linéaire via une itération de Newton quadratique, plus efficace que les étapes de raffinement inhérentes à l'algorithme de Montes.
- On apporte enfin quelques améliorations techniques élémentaires basées sur l'arithmétique rapide des polynômes (cf en particulier [109, Prop.6]), et sur l'utilisation de l'évaluation dynamique.

4.3.1 Ouvertures

1. Bases intégrales et Riemann-Roch. Les théorèmes 23 et 24 ont des conséquences notables pour une arithmétique efficace dans les corps de nombres et les corps de fonctions (voir [61]), en particulier concernant le calcul rapide des bases intégrales. Dans le cas local (les p-bases), la complexité actuelle [14] se trouve immédiatement améliorée par nos résultats (voir [109, Section 6]). Dans le cas global, on montre dans un travail en cours de rédaction que l'on peut calculer la base intégrale d'un corps de fonctions présenté comme une extension finie de $\mathbb{K}(t)$ de degré d avec une complexité $\mathcal{O}_\varepsilon(d^{\omega+1})$ (resp. $\mathcal{O}_\varepsilon(d^4)$ en petite caractéristique), améliorant la complexité $\mathcal{O}_\varepsilon(d^4)$ de [2] (resp. $\mathcal{O}_\varepsilon(d^5)$ de [64] en petite caractéristique). La preuve repose sur le théorème 23 combiné à [64] et à l'arithmétique rapide des matrices polynomiales [81].

De ce fait, nos résultats offrent aussi des perspectives sérieuses pour calculer efficacement les polynômes adjoints (avec des conséquences en factorisation bivariée, cf ouverture 3.5.1) ou encore calculer les espaces de Riemann-Roch par des méthodes arithmétiques (voir par exemple [69]). A plus long terme, on peut espérer que ces avancées participent significativement au développement d'une arithmétique rapide et efficace dans les jacobiennes (corps de fonctions) ou dans les groupes de classes d'idéaux (corps de nombres).

2. La petite caractéristique. En petite caractéristique résiduelle, soit les racines approchées ne sont plus définies (caractéristique non mixte), soit elles ne sont plus des polynômes clés (caractéristique mixte). On utilise dans ce cas des étapes de raffinement à la Montes, dont la convergence linéaire ralentit significativement les calculs (dans le cas des séries de Puiseux, cela correspond moralement à calculer les coefficients un par un, tandis que les racines approchées permettent de progresser par blocs). Ceci explique la non optimalité des théorèmes 23 et 24 en petite caractéristique. Peut-on malgré tout atteindre une complexité quasi-linéaire en toute caractéristique ? Ceci semble être un problème ardu important, qui m'a déjà occasionné bien des désillusions. Mentionnons a minima [92] qui permet de calculer en toute caractéristique les facteurs locaux de degré 1 en temps quasi-linéaire dans le cas des séries formelles.

4.4 Anneaux henséliens

Nous nous sommes penchés sur la factorisation des polynômes univariés sur un anneau (ou un corps) hensélien dans un travail en collaboration avec Alberich-Carramiñana, Guàrdia, Nart, Poteaux et Roé [10]. La section précédente couvre le cas des valuations discrètes de rang 1 et nous cherchons à généraliser ces résultats au cas d'une valuation à valeur dans un groupe ordonné abélien de rang quelconque et non nécessairement discret. Une des motivations est d'aider à résoudre efficacement des tâches arithmético-géométriques dans un corps de fonctions d'une variété algébrique de dimension arbitraire et en toute caractéristique.

Nos travaux donnent suite à une importante série de papiers sur le sujet, menés indépendamment par Nart et Spivakovski et leurs collaborateurs (voir [90, 68] et autres références afférentes dans [10]). Le lecteur trouvera une bonne introduction aux corps valués dans le livre de Engler et Prestel [44].

Corps hensélien. Soit (K, v) un corps valué d'anneau de valuation $\mathcal{O}$ et de corps résiduel k. Le corps (K, v) est hensélien si le lemme de Hensel est valide, *i.e* si pour tout polynôme $f \in \mathcal{O}[x]$, toute racine simple du polynôme résiduel $\overline{f} \in k[x]$ se relève de manière unique en une racine de f dans $\mathcal{O}$. Un résultat important de la théorie des corps valués assure que cette condition équivaut au fait que pour toute extension algébrique L de K, la valuation v s'étend de manière unique à L [44, Thm.4.1.3]. Si la valuation v est de rang 1 (discrète ou non), le complété de K pour la topologie v-adique est hensélien, mais ce n'est plus le cas pour des valuations de rangs supérieurs.

Clôture hensélienne. Soit (K, v) un corps valué. Etant donnée une clôture algébrique $\overline{K}$ de K et une extension $\overline{v}$ de v à $\overline{K}$, il existe un unique plus petit corps valué hensélien (K^h, v^h) contenant K vérifiant les inclusions

$$(K, v) \subset (K^h, v^h) \subset (\overline{K}, \overline{v}).$$

On appelle ce corps valué la clôture hensélienne de K dans $\overline{K}$. C'est une extension immédiate de K (*i.e.* les valuations v et v^h ont même groupe de valeurs et même corps résiduel), incluse dans la clôture séparable de K dans $\overline{K}$. Si v est de rang 1, le corps K est dense dans K^h, mais ce n'est plus le cas en rang supérieur, ce qui conduit à de nouvelles difficultés évidentes pour approcher les facteurs dans $K^h[x]$ d'un polynôme de $K[x]$.

Facteurs henséliens *vs* extensions de valuation. Soit (K^h, v^h) la clôture hensélienne de K dans une clôture algébrique valuée $(\overline{K}, \overline{v})$ fixée. Soit $f \in K[x]$ un polynôme irréductible et soit $F \in K^h[x]$ un facteur irréductible de f. Notons $\theta \in \overline{K}$ une racine de F. L'application

$$q \in K^h[x] \longmapsto v_F(q) := \overline{v}(q(\theta))$$

définit une pseudo-valuation sur l'anneau $K^h[x]$ de noyau l'idéal premier $FK^h[x]$. Cette définition ne dépend pas du choix de la racine de F par hensélianité du corps K^h. L'idéal principal $FK^h[x] \cap K[x]$ a pour générateur f et la valuation v_F induit par restriction à $K[x]$ une pseudo-valuation w_F sur $K[x]$ de noyau $fK[x]$. Cette dernière induit donc une valuation $\overline{w}_F$ sur le corps $K[x]/(f)$, dont la restriction à K est v. De manière analogue au cas discret de rang 1, la correspondance

$$F \longmapsto \overline{w}_F$$

induit une bijection entre les facteurs irréductibles de f dans $K^h[x]$ et les extensions de v au corps $K[x]/(f)$ [10, Thm.1.3]. La valuation $\overline{w}_F$ est uniquement caractérisée par les pseudo-valuations v_F ou w_F.

Résultats principaux. Soit (K, v) un corps valué de caractéristique résiduelle p et soit $f \in K[x]$ un polynôme séparable de degré d. Nous supposerons que l'on a accès aux opérations élémentaires dans K et dans le corps résiduel k, à la factorisation univariée sur k et au calcul de la valuation v d'un élément de K.

Théorème 25 *Supposons v de rang 1 et supposons $p = 0$ ou $p > d$. Il existe un algorithme déterministe qui renvoie*

(i) Les facteurs irréductibles $F_1, \ldots, F_s$ de f dans $K^h[x]$ à une précision arbitraire.

(ii) Les extensions correspondantes $\overline{w}_{F_1}, \ldots, \overline{w}_{F_s}$ de v au corps $K[x]/(f)$, ainsi que leurs indices de ramification et leurs degrés résiduels.

Ce théorème est important entre autres au regard d'un résultat de Novacoski-Spivakovsky qui assure que l'uniformisation locale en rang 1 (non discret) implique l'uniformisation locale en toute généralité [93].

Si la valuation est de rang quelconque, on obtient a minima un test d'irréductibilité.

Théorème 26 *Supposons v de rang quelconque et supposons que p ne divise pas d. Il existe un algorithme déterministe qui teste l'irréductibilité de f dans $K^h[x]$, et renvoie le cas échéant la valuation w_f, son indice de ramification et son degré résiduel.*

Les preuves de ces deux théorèmes sont basées sur deux nouveaux résultats clés.

Premier résultat clé : un algorithme exécutable inconditionnel. On montre le résultat plus général suivant :

Théorème 27 *Il existe un algorithme déterministe qui, s'il termine, résout simultanément les problèmes (i) et (ii) du théorème 25.*

Cet algorithme est une généralisation de l'algorithme OM. Il construit pour chaque facteur irréductible $F \in K^h[x]$ de f une chaîne de *pseudo-valuations augmentées* sur $K[x]$

$$\mu_0 = v < \mu_1 < \cdots < \mu_n < \cdots < w_F \tag{4.1}$$

qui approchent w_F arbitrairement bien. On augmente chaque valuation μ_n en lui associant un *polynôme clé* $\phi_{n+1} \in K[x]$ (dépendant de f), polynôme irréductible jouissant de propriétés de primalité et de minimalité dans l'algèbre graduée associée à la valuation μ_n [10, Section 2]. La définition et l'existence de ces polynômes clés est dûe à MacLane dans le cas discret de rang 1, et indépendamment à Vaquié [132] et Spivakovski et al. [68] dans le cas général. Pour n suffisamment grand, le polynôme $\phi_n \in K[x]$ approche arbitrairement bien le facteur irréductible $F \in K^h[x]$.

La construction effective des chaînes (4.1) est basée sur les *doubles dissections* successives de f qui se déduisent des pentes de ses polygones ϕ-adiques généralisés [10, Définition 4.4] et de la factorisation des polynômes résiduels attachés à chacune de ces pentes [10, Définition 2.15]. La construction des opérateurs résiduels découle de [91], qui généralise de manière éclairante la construction originelle plus technique de Montes [104] dans le cas discret de rang 1.

Contrairement aux cas des valuations de rang 1 ou au cas $K = K^h$ traités dans [68, 90], une nouvelle difficulté dans le cas général réside dans le fait que le polynôme clé $\phi \in K[x]$

associé à la valuation courante μ n'est plus nécessairement irréductible dans $K^h[x]$. De ce fait, il est plus délicat de déterminer les liens entre la factorisation de f dans $K^h[x]$ et les pentes de son polygone ϕ-adique : un apport majeur de notre papier est la résolution de ce problème en toute généralité [10, Thm.4.4], conduisant à la preuve du théorème 27.

Second résultat clé : lemme de Hensel valué et racines approchées. L'obstruction à la terminaison de l'algorithme sous-jacent au théorème 27 provient de l'existence possible *de valuations augmentées limites* $\mu_i < \cdots < \mu_{i+1}$ dans la chaîne (4.1), qui nécessitent une infinité d'étapes de raffinements, situation exclue dans le cas discret de rang 1. On montre qu'il existe trois types d'augmentations infinies et on exhibe des exemples concrets pour chacune d'entre elles [10, Section 5.3]. Le rang de v n'est pas la seule obstruction, la caractéristique résiduelle pose elle aussi des difficultés (cf ouverture 2 ci-dessous). Un second apport majeur est de montrer que les racines approchées (définition 2), déjà utilisées dans [109], permettent de calculer malgré tout des *polynômes clés limites* (dont se déduisent les valuations augmentées limites) quel que soit le rang de v dès lors que la ramification est modérée.

Cependant, calculer ces racines approchées requiert d'être "en position de Weierstrass", ce qui nécessite de factoriser f à une précision suffisante dès qu'une factorisation est détectée. Nous développons pour cela un algorithme de Hensel valué multifacteur [10, Prop.6.5 et 6.3], valide indépendamment de la caractéristique résiduelle et du rang de v. Cependant, bien que la précision des facteurs soit doublée à chaque étape, cela n'assure pas nécessairement la convergence vers les facteurs de f dans le cas des valuations de rang > 1 du fait de la non densité de K dans K^h. Ce souci représente la seule obstruction pour la généralisation du théorème 25 au rang quelconque.

4.4.1 Ouvertures

1. Complexité. Les algorithmes sous-jacents aux théorèmes 25 et 26 sont déterministes et de complexité polynomiale (en comptant cette fois le nombre d'opérations élémentaires dans K ou k) dès lors que calculer la valuation ou calculer le résidu d'un élément de K et la factorisation dans $k[x]$ le sont aussi. Il serait souhaitable d'estimer plus précisément cette complexité en terme d'opérations dans le corps résiduel k (ou dans un système de représentants dans K), dans l'esprit de [109].

2. Résoudre le cas général. Peut-on résoudre algorithmiquement les problèmes i) et ii) en toute généralité ? Un point crucial est de construire des polynômes clés limites sans passer par les racines approchées. Traiter le cas particulier des extensions algébriques (infinies) des corps locaux serait une première étape importante dans cette direction. Illustrons nos espoirs par un exemple.

Exemple. Considérons dans ce cadre le corps des séries de Puiseux en caractéristique positive

$$K = \bigcup_{n\geq 0} \overline{\mathbb{F}}_p((t^{1/n})).$$

Ce corps muni de la valuation t-adique est hensélien, de groupe de valeurs non discret $\mathbb{Q}$. Si l'on cherche à appliquer l'algorithme OM sur le polynôme d'Artin-Schreier

$$g(x) = x^p - x - t^{-1} \in K[x]$$

pour en tester l'irréductibilité sur K, on constate qu'à chaque étape, le polygône de Newton généralisé a une seule pente et que le polynôme résiduel associé (cf [10]) vaut constamment

$$R(g) = (y-1)^p \in \overline{\mathbb{F}}_p[y].$$

L'algorithme OM ne termine pas dans ce cas, et ne permet donc pas a priori de tester l'irréductibilité de g sur K (voir [10, Exemple 5.9]). Ceci est lié au fait que les racines de g sont les $\alpha + c$ où

$$\alpha = t^{-1/p} + t^{-1/p^2} + t^{-1/p^3} + \cdots$$

et c parcourt $\mathbb{F}_p$. A chaque étape de l'algorithme, on découvre un nouveau terme de cette série, sans pour autant pouvoir décider *a priori* si la série tronquée courante provient ou non d'une racine de g dans K, i.e. si les dénominateurs des exposants de α seront bornés *in fine* (ce qui n'est évidemment pas le cas ici, α étant une série de Hahn mais pas une série de Puiseux).

Ceci étant dit, Xavier Caruso m'a fait remarquer récemment que l'on peut malgré tout tester l'irréductibilité d'un polynôme dans le cas particulier du corps K des séries de Puiseux. Expliquons.

Solution Soit $g \in K[x]$. Il existe n tel que $g \in \overline{\mathbb{F}}_p((t^{1/n}))[x]$ et quitte à remplacer $t^{1/n}$ par une nouvelle indéterminée, on peut supposer $n = 1$. De plus, on peut supposer g séparable (par exemple [84]). On a alors :

Proposition 8 *Soit $g \in \overline{\mathbb{F}}_p((t))[x]$ séparable. Alors g est irréductible sur le corps K des séries de Puiseux si et seulement si g est irréductible sur $\overline{\mathbb{F}}_p((t))$ et si $\deg(g)$ est une puissance de p.*

Preuve (esquisse). Notons $K_0 = \overline{\mathbb{F}}_p((t))$. Si g se factorise sur K_0, il se factorise sur K, c'est fini. Supposons g irréductible sur K_0 et notons $L = K_0(\alpha)$ le corps engendré par une racine de g dans une clôture algébrique de $K \supset K_0$ fixée. Alors g est irréductible sur K si et seulement si les corps K et L sont K_0-linéairement disjoints. Puisque K/K_0 est galoisienne, ceci équivaut à $K \cap L = K_0$. Notons $e = e(L/K_0)$ l'indice de ramification (on a ici $e = [L : K_0] = deg(g)$). S'il existe n premier à p divisant e, alors nécessairement $\overline{\mathbb{F}}_p((t^{1/n})) \subset K \cap L$ et g est réductible sur K. Si e est une puissance de p, on a nécessairement $K \cap L = \overline{\mathbb{F}}_p((t^{1/p^k}))$ pour un $k \geq 0$ et la séparabilité de g assure que $k = 0$, *i.e.* K et L sont K_0-linéairement disjoints et g est irréductible sur K. □

Cette proposition s'applique par exemple dans le cas du polynôme d'Artin-Schreier ci-dessus. Il est séparable (de dérivée -1) et irréductible sur K_0 en tant que polynôme de type Eisenstein. Comme $\deg(g) = p$, nécessairement g est irréductible sur K.

On peut obtenir des résultats similaires pour d'autres extensions algébriques particulières. Par exemple, sur l'extension infinie $\mathbb{Q}_p(\mu_{p^\infty})$ de $\mathbb{Q}_p$ engendrée par les racines p^n-èmes de l'unité, $n \in \mathbb{N}^\times$.

Proposition 9 *Soit $g \in \mathbb{Q}_p[x]$. Alors g est irréductible sur $\mathbb{Q}_p(\mu_{p^\infty})$ si et seulement si g est irréductible sur $\mathbb{Q}_p(\mu_{p^2})$.*

La preuve est dans le même esprit, mais exploite cette fois le fait que l'extension $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p$ est abélienne de groupe de Galois $\mathbb{Z}_p^\times$, compositum de $\mathbb{Q}_p(\mu_p)$ (modérément ramifiée, d'indice $p-1$) avec la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}_p$ (sauvagement ramifiée) dont tous les sous-corps sont emboîtés.

On se ramène ainsi à tester l'irréductibilité de g sur une extension finie K_1/K_0, donc un corps local sur lequel on dispose de l'algorithme OM. Notons que l'on a besoin au préalable d'une uniformisante de K_1 pour conduire les calculs, qui peut se calculer elle aussi avec l'algorithme OM dès lors que l'on connaît un polynôme irréductible $h \in K_0[x]$ qui engendre

K_1. Quoique relativement simples, ces exemples sont encourageants et on peut espérer que ce genre de méthodes conduise à des résultats plus généraux significatifs.

On peut aussi considérer des corps henséliens de rang un qui ne sont pas extensions algébriques d'un corps local. Un exemple pertinent en est donné par l'hensélianisé du corps $k(s,t)$ muni de la valuation de rang 1 définie par $v(t^i s^j) = i + \sqrt{2}j$, de groupe des valeurs $\mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \subset \mathbb{R}$ de rang un mais de rang rationnel 2. Cette valuation intervient par exemple dans le calcul des séries de Puiseux multivariées à la Mac Donald [89] (ouverture de la Section 4.2.1).

Enfin, dans le cas du rang supérieur à 1, se pose le problème supplémentaire que K n'est pas dense dans son hensélianisé en général. Mentionnons dans ce cadre le cas intéressant de $K = \mathbb{Q}(t)$ muni de la valuation de rang deux

$$v(c(t)) = (\mathrm{ord}_t(c), \mathrm{ord}_p(\mathrm{in}_t(c)).$$

Notons que cette valuation de rang deux pourrait - spéculativement - être appliquée à la factorisation dans $\mathbb{Q}[t,x]$ *via* des techniques "factorisation locale et recombinaisons" en rang 2, à des fins d'estimations de la complexité binaire de la factorisation bivariée sur $\mathbb{Q}$ en termes d'invariants arithmético-géométriques.

Troisième partie

Autres contributions

Chapitre 5

Sur le lieu flex des hypersurfaces

Contents

Soit $V \subset \mathbb{P}^n$ une sous-variété projective définie sur un corps $\mathbb{K}$ algébriquement clos de caractéristique nulle. Un point $p \in V$ est un "point flex" s'il existe une droite ayant un ordre de contact anormalement élevé avec V au point p. Ce concept généralise la notion classique de point d'inflexion d'une courbe algébrique. L'étude du lieu flex des courbes et des surfaces est un sujet classique de géométrie algébrique du 19ème siècle, étudié entre autres par Monge, Salmon et Cayley. On assiste à un regain d'intérêt pour cette thématique, dû à ses applications en géométrie d'incidence [42, 63, 73, 76, 122, 128].

Le but de ce chapitre est de déterminer la dimension, le degré et un système d'équations explicites du lieu flex d'une hypersurface projective, en s'appuyant sur la théorie des résultants multidimensionnels. Ce travail a été effectué en collaboration avec Laurent Busé, Carlos D'Andréa et Martin Sombra, publié dans [21].

5.1 Résultants et résultats

Soit V une sous-variété de $\mathbb{P}^n$. L'ordre de contact entre V et une droite L en un point $p \in V$ est défini par

$$\mathrm{ord}_p(V, L) = \dim_{\mathbb{K}}(\mathcal{O}_{L,p}/\iota^*\mathcal{I}_V),$$

où $\mathcal{O}_{L,p}$ est l'anneau local de L à p, $\mathcal{I}_V$ est le faisceau d'idéaux de V, et $\iota\colon L \hookrightarrow \mathbb{P}^n$ est le morphisme d'inclusion. On a en particulier :

— $\mathrm{ord}_p(V, L) = 0$ si et seulement si $p \notin V \cap L$
— $\mathrm{ord}_p(V, L) = 1$ si et seulement si l'intersection $V \cap L$ est transverse en p
— $\mathrm{ord}_p(V, L) = +\infty$ si et seulement si L est incluse dans V.

Soit $V \subset \mathbb{P}^n$ une *hypersurface* projective de degré $d \geq 1$. On peut montrer que par tout point $p \in V$ passe une droite avec ordre de contact au moins n [21, Prop. 3.6]. On dira qu'un point $p \in V$ est un *point flex* s'il existe une droite ayant un ordre de contact au moins $n+1$ avec V au point p. Une telle droite est une *droite flex*. Le *lieu flex* de V est l'ensemble de ses points flex.

• Un premier résultat important de Monge-Salmon-Cayley [128, 76] assure qu'une surface de $\mathbb{P}^3$ est réglée (i.e. union de droites) si et seulement si chacun de ses points est un point flex, résultat généralisé en toute dimension par Landsberg [82, Thm 3]. Une hypersurface de $\mathbb{P}^n$ de degré $< n$ étant nécessairement réglée [21, Prop. 3.6], on se restreindra donc aux hypersurfaces de $\mathbb{P}^n$ de degré $\geq n$.

• Si $C \subset \mathbb{P}^2$ est une courbe plane, il est bien connu que le lieu flex coïncide avec le lieu d'annulation du déterminant de la matrice hessienne de C. Il est donc défini par une équation de degré $3d-6$. Si la courbe ne contient aucune droite, le lieu flex est donc fini, de cardinal au plus $3d^2-6d$ par le théorème de Bézout.

• Si $S \subset \mathbb{P}^3$ est une surface de degré ≥ 3, un théorème de Salmon assure que le lieu flex est défini par l'intersection de S avec une hypersurface de degré $11d-24$, voir [114, Article 588, p. 277–278] ou [42, §11.2.1]. Ce résultat combiné au théorème de Monge-Salmon-Cayley et au théorème de Bézout assure que le lieu flex d'une surface S sans composantes réglées est une courbe sur S, de degré au plus $11d^2-24d$.

Soit $f \in \mathbb{K}[\mathbf{x}] = \mathbb{K}[x_0,\dots,x_n]$ un polynôme homogène sans facteurs carrés de degré d définissant une hypersurface $V \subset \mathbb{P}^n$. Soient t et $\mathbf{y} = (y_0,\dots,y_n)$ d'autres variables. Notons $f_k \in \mathbb{K}[\mathbf{x},\mathbf{y}]$ les polynômes définis par

$$f(\mathbf{x}+t\mathbf{y}) = \sum_{k=0}^{d} f_k(\mathbf{x},\mathbf{y})\frac{t^k}{k!}. \tag{5.1}$$

Le résultat suivant généralise le théorème de Salmon en toute dimension :

Théorème 28 *[21, Thm 1.1] Le lieu flex d'une hypersurface $V = \{f=0\} \subset \mathbb{P}^n$ de degré $d \geq n$ est défini par un polynôme g de degré*

$$\deg(g) = d\sum_{k=1}^{n}\frac{n!}{k} - (n+1)!.$$

Ce polynôme est uniquement déterminé modulo f par la condition

$$\mathrm{Res}^{\mathbf{y}}(f_1(\mathbf{x},\mathbf{y}),\dots,f_n(\mathbf{x},\mathbf{y}),\ell(\mathbf{y})) \equiv \ell^{n!}g \mod f,$$

où $\ell \in \mathbb{K}[\mathbf{x}]$ est une forme linéaire quelconque, et $\mathrm{Res}^{\mathbf{y}}$ désigne le résultant de $n+1$ polynômes homogènes relativement à la variable $\mathbf{y}$.

Le théorème 28 permet de définir une structure de sous-schéma au lieu flex. On appellera le *schéma flex* de V le sous-schéma

$$\mathrm{Flex}(V) := \{f = g = 0\} \subset \mathbb{P}^n$$

induit par les polynômes f et g ci-dessus. Ce schéma ne dépend pas du choix de g (unique modulo f).

Le résultat suivant assure que le schéma flex est génériquement réduit, i.e. que la borne sur le degré du lieu flex induite par le théorème 28 est optimale. Il montre plus généralement que la situation générique est celle à laquelle on s'attend. A noter que ces aspects ne sont pas considérés dans les travaux originaux de Salmon dans le cas des surfaces.

Théorème 29 *[21, Thm 1.4] Soit V une hypersurface* générique *de $\mathbb{P}^n$ de degré $d \geq n$.*

1. $\mathrm{Flex}(V)$ *est un sous-schéma réduit (i.e. une sous-variété) de V de dimension $n-2$ et degré*
$$\deg(\mathrm{Flex}(V)) = d^2\sum_{k=1}^{n}\frac{n!}{k} - d(n+1)!.$$
2. *Par un point* générique *$p \in \mathrm{Flex}(V)$ passe une unique droite flex. Si $d=n$, cette droite est incluse dans V, et si $d>n$, son ordre de contact avec V au point p est exactement $n+1$.*

Le cas $d = n$ découle du fait que si une droite L a un ordre de contact $\geq n+1$ avec une hypersurface V de degré n, alors L est incluse dans V d'après le théorème de Bézout. On en déduit en particulier le corollaire suivant sur l'ensemble des droites incluses dans une hypersurfaces.

Corollaire 4 *Soit V une hypersurface* générique *de $\mathbb{P}^n$ de degré n. La réunion $\mathcal{L}_V$ des droites incluses dans V est une sous-variété réglée de V, intersection complète de dimension $n-2$ et de degré*

$$\deg(\mathcal{L}_V) = n^3\,(n-1)!\sum_{k=2}^{n-1}\frac{1}{k}.$$

On notera que pour $n = 3$, on retrouve en particulier le résultat bien connu qu'une cubique générale dans $\mathbb{P}^3$ contient exactement 27 droites.

Le théorème de Salmon pour les surfaces a été revisité plusieurs fois. Dans leur livre [42], Eisenbud et Harris offrent une preuve *via* l'utilisation de l'anneau de Chow dans la grassmannienne des droites de $\mathbb{P}^3$. Notre approche, basée sur (5.1), identifie plutôt une droite de $\mathbb{P}^n$ avec les points $(\mathbf{x}, \mathbf{y}) \in \mathbb{P}^n \times \mathbb{P}^n$ en dehors de la diagonale, dans l'esprit de l'approche originelle de Salmon. Quoique moins naturelle du point de vue de la théorie de l'intersection, notre approche a le double avantage d'offrir des équations explicites via la théorie des résultants et d'offrir une généralisation naturelle du théorème de Salmon en toute dimension.

5.2 Eléments de preuves

Résultants. Le lecteur pourra consulter [37, 51, 72] pour des références complètes concernant les résultants multivariés. Nous nous contenterons ici d'une brève définition, suffisante pour illustrer notre propos.

A tout multi-degré $\mathbf{d} = (d_0, \ldots, d_n) \in \mathbb{N}^{n+1}$, on peut associer un polynôme universel, le résultant

$$\mathrm{Res}_{\mathbf{d}} \in \mathbb{Z}[c_0, \ldots, c_n].$$

Chaque multi-variable $c_i = (c_{i,\mathbf{a}})$ représente les $\binom{d_i+n}{n}$ coefficients d'un polynôme homogène général $F_i = \sum_{|\mathbf{a}|=d_i} c_{i,\mathbf{a}}\mathbf{y}^{\mathbf{a}}$, de degré d_i en $n+1$ variables $\mathbf{y} = (y_0, \ldots, y_n)$.

Le résultant est essentiellement défini (à une normalisation près) comme polynôme de plus petit degré[1] vérifiant la propriété fondamentale suivante :

Soient $f_0, \ldots, f_n \in \mathbb{K}[\mathbf{y}]$ des polynômes homogènes de degrés respectifs $d_0, \ldots, d_n$. Les f_i ont un zéro commun dans $\mathbb{P}^n$ si et seulement si $\mathrm{Res}_{\mathbf{d}}(f_0, \ldots, f_n) = 0$.

Notez que l'évaluation $\mathrm{Res}_{\mathbf{d}}(f_0, \ldots, f_n) \in \mathbb{K}$ est un élément de l'anneau des coefficients des f_i. On omettra par la suite la dépendance en $\mathbf{d}$ s'il n'y a pas d'ambiguïté.

Le cône Z_p^k. Soit $p \in \mathbb{P}^n$. Pour tout $k \in \mathbb{N}$, considérons la sous-variété de $\mathbb{P}^n$ définie par

$$Z_p^k = \{q \in \mathbb{P}^n \mid f_1(p,q) = \cdots = f_n(p,q) = 0\},$$

avec les f_i définis par (5.1). On peut montrer [21, Lem. 3.4, Cor. 3.5] que $Z_p^k \subset \mathbb{P}^n$ est un cône centré en p, union des droites avec ordre de contact $> k$ avec l'hypersurface V au

1. Voir [21, Section 2] pour une définition plus rigoureuse du résultant, vu comme générateur d'un idéal principal.

point p. L'ordre de contact maximal de V avec une droite en p, appelé ordre d'osculation de V en p, est le plus petit entier k tel que $Z_p^k = \{p\}$. En particulier, p est un point flex si et seulement si $Z_p^n \neq \{p\}$, ou de manière équivalente, si et seulement si $\dim Z_p^n \geq 1$. Ce constat, combiné avec la propriété fondamentale du résultant conduit au résultat suivant :

Lemme 4 *Soit $\ell \in \mathbb{K}[\mathbf{y}]$ un polynôme homogène. Le résultant*

$$R_{f,\ell} := \mathrm{Res}(\ell, f_1, \ldots, f_n) \in \mathbb{K}[\mathbf{x}]$$

par rapport à la variable $\mathbf{y}$ est un polynôme homogène qui définit le lieu flex de l'hypersurface $V = \{f = 0\}$ dans l'ouvert $\mathbb{P}^n \setminus \{\ell = 0\}$.

Preuve. En effet, $R_{f,\ell}(p) = 0$ si et seulement si les ensembles $\{\ell = 0\}$ et Z_p^n s'intersectent par définition de Z_p^n et par la propriété du résultant. Si $\ell(p) \neq 0$ ceci est équivalent à $\dim Z_p^n \geq 1$ d'après ce qui vient d'être dit, donc à ce que p soit un point flex. □

Cependant, le polynôme $R_{f,\ell}$ contient trop d'information pour notre propos : il peut s'annuler en des points de $\{\ell = f = 0\}$ qui ne sont pas des points flex. La clé est de montrer que $R_{f,\ell}$ admet un facteur g modulo f indépendant de ℓ. Plus précisément, il existe $g \in \mathbb{K}[\mathbf{x}]$ tel que

$$R_{f,\ell} \equiv \ell^{n!} g \mod f$$

pour tout polynôme homogène $\ell \in \mathbb{K}[\mathbf{x}]$. La preuve est basée sur la formule de Poisson [21, Prop. 2.2] (appelée parfois formule du produit). On montre alors que g détermine le lieu flex dans l'espace $\mathbb{P}^n$ en entier, conduisant à la preuve du Théorème 28.

Pour prouver le Théorème 29, on introduit une multi-variable $c = (c_{\mathbf{a}})$ représentant le polynôme général homogène $F = \sum c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$ de degré d en $n+1$ variables, et on montre l'existence d'un polynôme universel $\Phi_d \in \mathbb{K}[c, \mathbf{x}]$ qui satisfait la congruence

$$R_{F,\ell} \equiv \ell^{n!} \Phi_d \mod F$$

dans $\mathbb{K}[c, \mathbf{x}]$, pour tout $\ell \in \mathbb{K}(\mathbf{x}]$ homogène. On montre alors qu'il existe une spécialisation $f \in \mathbb{K}[\mathbf{x}]$ de F pour laquelle la variété $\{f(\mathbf{x}) = \Phi_d(f, \mathbf{x}) = 0\}$ est réduite, impliquant par un argument d'irréductibilité à la Bertini que c'est le cas pour f générique. La preuve du point 1 du Théorème 29 en découle.

Concernant le point 2, plus délicat, on exhibe plutôt une spécialisation (f, p) pour laquelle on est assuré que le point 2 est valide. Toujours par un argument d'irréductibilité, utilisant cette fois la formule d'inversion du résultant [21, Prop. 2.3], on en déduit que le point 2 est valide pour (f, p) générique (esquisse de preuve grossière, cf [21, Section 5] pour les détails). □

5.3 Ouverture : le lieu hyperflex

Dans un travail en cours avec Cristina Bertone (Université de Turin), nous étudions la géométrie du lieu k-flex d'une hypersurface $V \subset \mathbb{P}^n$ (points d'ordres de contact $\geq k$ avec au moins une droite L) pour tout entier k. On parle de points "hyperflex" dès lors que $k \geq n+2$. Notons ce lieu V_k. Si V est de degré d, on a une stratification

$$V = V_0 = \cdots = V_n \subset V_{n+1} \subset \cdots \subset V_d \subset V_{d+1} = \cdots = V_\infty$$

où V_∞ est la sous-variété réglée de V maximale pour l'inclusion ($V_{d+1} = V_\infty$ d'après le théorème de Bezout). Quelle est la dimension de chaque strate V_k pour une hypersurface générale ? Quel est son degré ?

On est cette fois conduit à caractériser l'annulation simultanée de k polynômes homogènes à $n+1$ variables. La théorie des résultants (dédiée au cas $k = n+1$) ne répond plus à ce problème général. L'idée est d'utiliser l'anneau de Chow de la grassmanienne, dans l'esprit de [42, Chapitre 11]. Plus précisément, partant du fibré tautologique

$$\Phi = \{(L, p) \in \mathbb{G}(1, n) \times \mathbb{P}^n\,,\ p \in L\},$$

les auteurs construisent un certain fibré vectoriel $\mathcal{E} = \mathcal{E}(k, d) \to \Phi$ appelé fibré des *parties principales relatives*, dont les fibres vérifient

$$\mathcal{E}_{(L,p)} \simeq H^0(\mathcal{O}_L(d)/\mathfrak{m}_p^k)$$

où $\mathfrak{m}_p \subset \mathcal{O}_L$ est l'idéal maximal de p. Autrement dit, les fibres représentent les développements de Taylor au point p à l'ordre $k-1$ des restrictions à la droite L des polynômes homogènes de degrés d. La construction est telle qu'à chaque hypersurface $V = \{f = 0\} \subset \mathbb{P}^n$ de degré d, on peut associer une section

$$\sigma_f \in \Gamma(\Phi, \mathcal{E})$$

dont la valeur au point (L, p) est la restriction de f à $H^0(\mathcal{O}_L(d)/\mathfrak{m}_p^k)$. En particulier, on a

$$\mathrm{ord}_p(V, L) \geq k \iff \sigma_f(p, L) = 0. \tag{5.2}$$

Nous avons établi avec Cristina que pour une hypersurface générale, la dimension du lieu k-flex est celle attendue, que par un point k-flex *général* passe une seule droite k-flex, et que cette dernière a un ordre de contact exactement k. Combiné à (5.2), on en déduit que pour f général, le cycle $[\sigma_f = 0] \subset \mathcal{E}$ est réduit de codimension le rang de $\mathcal{E}$, et que sa classe dans l'anneau de Chow détermine le degré de V_k. Pour une hypersurface $V \subset \mathbb{P}^n$ générale, le degré recherché coïncide donc finalement avec la classe de Chern maximale $c_k(\mathcal{E})$ du fibré vectoriel $\mathcal{E}$:

$$\deg(V_k) = c_k(\mathcal{E}) \in A^k(\Phi) \simeq \mathbb{Z}.$$

Le calcul de cette classe de Chern pour des valeurs quelconques de n, k, d est un travail en cours, qui demande quelques contorsions dans l'anneau de Chow de la Grassmanienne (calcul de Schubert).

Chapitre 6

Sur la gonalité des courbes algébriques

Contents

Ce chapitre concerne mes travaux sur le calcul de la gonalité des courbes algébriques, en collaboration avec Joseph Schicho et Franck-Olaf Schreyer [117] lors de mon post-doctorat à RICAM (Linz, Autriche). Les outils de géométrie algébrique sous-jacents basés sur les syzygies des courbes canoniques sortent singulièrement du cadre général de mes travaux.

6.1 Définitions et résultats

Définition 3 *La gonalité d'une courbe projective C est le plus petit entier $d \in \mathbb{N}$ tel qu'il existe une application rationnelle de degré d de C sur $\mathbb{P}^1$ (éventuellement définie sur une extension finie du corps de base). On note cet entier* $\mathrm{gon}(C)$. *Une application gonale est une telle application rationnelle de degré minimal.*

Comme le genre géométrique, la gonalité est un invariant birationnel qui donne une mesure de la non rationalité d'une courbe algébrique. En particulier, $\mathrm{gon}(C) = 1$ si et seulement si C est rationnelle et $\mathrm{gon}(C) = 2$ si et seulement si C est hyperelliptique. En général, genre et gonalité sont liés par l'inégalité

$$\mathrm{gon}(C) \leq \lfloor \frac{g+3}{2} \rfloor,$$

et il y a égalité pour une courbe générale de genre g. La gonalité coïncide avec le plus petit degré d'un système linéaire de dimension projective 1 (un pinceau) sur C et l'existence de tels systèmes linéaires "spéciaux" est elle-même intimement liée à la résolution minimale de l'anneau de coordonnées canonique d'un modèle lisse de C.

Outre son intérêt théorique, calculer explicitement une application gonale offre l'avantage pratique de représenter le corps de fonctions de C comme une extension algébrique de petit degré de $\mathbb{K}(t)$. Pour des petites gonalités, une telle présentation permet en particulier de calculer une paramétrisation par radicaux de C (*i.e.* en s'autorisant les symboles $\sqrt[k]{}$),

utilisée par exemple en modélisation géométrique dans les tracés de courbes ou les calculs de variétés enveloppantes et de conchoïdes (cf [120] et références afférentes).

Lorsque nous nous sommes penchés sur le problème du calcul d'une application gonale, il n'était résolu en toute généralité que pour les courbes de gonalité ≤ 3 [118, 120] ou les courbes de genre ≤ 6 [65]. Impulsé par J. Schicho, notre première intention était d'attaquer le cas des courbes de gonalité 4. Après des discussions intenses avec F.O. Schreyer autour de son remarquable article [119] sur les syzygies des courbes canoniques et autour des travaux de H.-C Graf von Bothmer sur les syzygies scrollaires [54, 53], il est apparu que nous pouvions en fait traiter ce problème en toute généralité.

Résultats. On suppose que le corps de base $\mathbb{K}$ est effectif, *i.e.* qu'il supporte les opérations arithmétiques élémentaires et la factorisation univariée. Le résultat principal est le suivant.

Théorème 1 *[117, Thm.1.1] Il existe un algorithme déterministe qui, étant donnée une courbe projective C absolument irréductible, calcule la gonalité de C et une application gonale $C \to \mathbb{P}^1$.*

Le lecteur trouvera des exemples implémentés et documentés sur les pages web des auteurs ou *via* les liens MAGMA ou Macaulay2. La preuve du théorème 1 repose sur les liens étroits entre les systèmes linéaires spéciaux et les syzygies des courbes canoniques, dans la lignée des travaux de Schreyer [119].

Lorsque la gonalité est inférieure ou égale à 4, la formule de Cardano permet d'inverser l'application gonale et de paramétrer la courbe C en combinant fonctions rationnelles et radicaux $\sqrt[k]{}$. La paramétrisation des courbes trigonales est traité dans [118, 120, 65]. Le théorème 1 ci-dessus offre la généralisation suivante :

Théorème 2 *[117, Thm.1.3] Il existe un algorithme déterministe qui, étant donnée une courbe projective C absolument irréductible, teste si* $\mathrm{gon}(C) \leq 4$. *Dans ce cas l'algorithme calcule une paramétrisation par radicaux de C dès lors que* $\mathit{char}(\mathbb{K}) \neq 2, 3$.

Bien que dans le même esprit que le théorème 1, l'algorithme sous-jacent au théorème 2 est beaucoup plus efficace et permet de traiter des courbes dont le genre est relativement élevé. Pour ce faire, on s'appuie sur une classification complète des courbes de gonalité ≤ 4 et de leurs tables de Betti [117, Thm.5.1] et on profite des situations géométriques spécifiques sous-jacentes pour accélérer les calculs de syzygies, voir [117, Algo.5.5].

6.2 Modèle canonique, syzygies et gonalité

Soit C une courbe géométriquement irréductible de genre $g \geq 2$. L'espace $H^0(C, \omega_C)$ des sections globales du fibré canonique ω_C définit un *morphisme canonique*

$$C \longrightarrow \mathbb{P}^{g-1} := \mathbb{P}(H^0(C, \omega_C)).$$

Ce morphisme est un plongement si et seulement si C n'est pas hyperelliptique, ce que l'on supposera désormais (le cas hyperelliptique est connu, cf [118]). Notons alors

$$I_C \subset S := \mathbb{K}[x_0, \ldots, x_{g-1}]$$

l'idéal homogène du modèle canonique de C. Il existe des algorithmes efficaces pour calculer cet idéal [1]. L'anneau de coordonnées homogènes $S_C = S/I_C$ de C est projectivement normal,

1. D'autres travaux décrits dans la seconde partie de ce mémoire se trouvent être fortement liés ou impliqué dans le calcul efficace d'une base de $H^0(C, \omega_C)$, cf en particulier la Section 3.5

i.e isomorphe à l'anneau canonique de C

$$S_C \simeq \bigoplus_{n\in\mathbb{N}} H^0(C, \mathcal{O}_C(n)),$$

et c'est un S-module de Cohen Macaulay. Le théorème des syzygies de Hilbert assure que la résolution minimale de S_C est un complexe exact de longueur $g-2$

$$(F_\bullet): \quad 0 \leftarrow S_C \leftarrow F_0 \leftarrow \cdots \leftarrow F_i \xleftarrow{f_i} F_{i+1} \leftarrow \cdots \leftarrow F_{g-2} \leftarrow 0 \tag{6.1}$$

de S-modules libres gradués (les modules de syzygies)

$$F_i = \bigoplus_{j\in\mathbb{N}} S(-i-j)^{\beta_{i,i+j}},$$

où $S(-i)$ désigne le module engendré par les polynômes homogènes de degrés i. Les exposants $\beta_{i,i+j}$ s'appellent les *nombres de Betti gradués*, que l'on collecte dans un tableau appelé la table de Betti de C.

Les tables de Betti des courbes canoniques sont très particulières. Elles sont toutes de la forme

$$\begin{array}{ccccccc} 1 & - & - & & - & - & - \\ - & \beta_{12} & \beta_{23} & \cdots & \beta_{g-4,g-3} & \beta_{g-3,g-2} & - \\ - & \beta_{13} & \beta_{24} & \cdots & \beta_{g-4,g-2} & \beta_{g-3,g-1} & - \\ - & - & - & & - & - & 1 \end{array}$$

et vérifient de plus une propriété fondamentale de symétrie $\beta_{i,i+1} = \beta_{g-i-2,g-i}$. liée à une propriété d'auto-dualité du complexe $(F_\bullet)$, cf [117, Section 2]. En particulier, l'idéal I_C est minimalement engendré par β_{12} quadriques et β_{13} cubiques et admet seulement des syzygies linéaires et quadratiques.

Les tables de Betti sont connues pour encoder des propriétés géométriques intrinsèques de C, en particulier l'existence de systèmes linéaires spéciaux sur C (voir [119]), comme les pinceaux de degrés minimaux qui nous intéressent ici. Par exemple, le théorème de Petri assure que I_C est engendré seulement par des quadriques (*i.e.* $\beta_{1,3} = 0$) sauf si C est hyperelliptique, trigonale ou provient d'une quintique lisse de $\mathbb{P}^2$.

Définition 4 *La colongueur linéaire $\ell(C)$ est le plus petit indice i tel que le nombre de Betti $\beta_{i,i+2}$ est non nul.*

Cet invariant est fondamental du fait de la célèbre conjecture de Green qui prédit que $\ell(C)$ coïncide avec l'indice de Clifford en caractéristique nulle. L'indice de Clifford est le plus petit entier c tel que la courbe C admette un système linéaire complet de dimension projective n et degré $2n+c$ pour un certain entier positif n, définition motivée par le théorème de Riemann-Roch pour les diviseurs spéciaux, voir [117, Section 2.3] pour les détails. Cette conjecture est résolue dans de nombreux cas, en particulier pour les courbes générales d'après un résultat de C. Voisin (voir [117, Thm.2.5] pour une liste plus exhaustive des cas résolus). L'indice de Clifford, la colongueur linéaire et la gonalité sont intimement liés. On a en particulier le résultat suivant :

Théorème 3 *[117, Section 2.3] On a* $\mathrm{gon}(C) \geq \ell(C)+2$, *avec égalité pour les courbes générales de genre $g \geq 2$. Si la conjecture de Green est vraie, on a aussi* $\mathrm{gon}(C) \leq \ell(C)+3$, *avec égalité dans quelques cas exceptionnels bien établis.*

6.3 Syzygies scrollaires

Afin de calculer explicitement une application gonale, on utilise une variété intermédiaire $C \subset X \subset \mathbb{P}^{g-1}$ plus facile à appréhender. Notons d la gonalité de C et considérons

$$f : C \xrightarrow{d:1} \mathbb{P}^1$$

une application gonale. On définit (ensemblistement)

$$X := \bigcup_{\lambda \in \mathbb{P}^1} \overline{D_\lambda}$$

où $D_\lambda := f^{-1}(\lambda)$ et $\overline{D_\lambda}$ est le plus petit sous-espace linéaire projectif contenant D_λ. Le théorème de Riemann-Roch géométrique assure que la variété $X \subset \mathbb{P}^{g-1}$ est une fibration au-dessus de $\mathbb{P}^1$ en sous-espaces projectifs $\mathbb{P}^{d-2}$, donc une variété rationnelle normale de dimension $d-1$ et degré minimal $g-d$ [117, Lem.3.1]. De telles variétés sont appelées scrolls. On a un diagramme commutatif

$$\begin{array}{ccc} C & \subset & X \\ {\scriptstyle d:1}\searrow & & \swarrow \\ & \mathbb{P}^1 & \end{array} \tag{6.2}$$

et calculer une application gonale se réduit à calculer l'idéal d'une scroll X de plus petite dimension contenant C, puis à calculer la restriction à C de la projection $X \to \mathbb{P}^1$. On s'appuie pour cela sur les travaux de G. von Bothmer [53, 54] autour des syzygies scrollaires, dont on esquisse maintenant les grandes lignes.

Sous-complexes linéaires. La résolution minimale de l'anneau de coordonnées $S_X = S/I_X$ d'une scroll est bien connue, c'est un complexe de Eagon-Northscott [41], que nous noterons $E_\bullet$. Ce complexe est linéaire (sauf pour les générateurs de degrés 2) de longueur $g-d$. Du fait de l'inclusion $C \subset X$, c'est donc nécessairement un sous-complexe du complexe (non exact) linéaire $L_\bullet \subset F_\bullet$ de C, défini par la partie haute de la table de Betti

$$(L_\bullet) : \qquad S \leftarrow S(-2)^{\beta_{1,2}} \leftarrow S(-3)^{\beta_{2,3}} \leftarrow S(-4)^{\beta_{3,4}} \leftarrow \cdots .$$

Notons que l'inclusion $E_\bullet \subset L_\bullet$ induit l'inégalité $\mathrm{len}(L_\bullet) \geq \mathrm{len}(E_\bullet) = g-d$ de laquelle découle l'inégalité $d \geq \ell(C)+2$ du théorème 3.

On est ainsi réduit à détecter et construire un sous-complexe $E_\bullet \subset L_\bullet$ définissant une scroll rationnelle normale X de dimension minimale.

Syzygies scrollaires. Soit $p \geq 2$ et soit $s \in L_p$ une syzygie linéaire de C. On note $V = V(s)$ le plus petit $\mathbb{K}$-espace vectoriel tel que l'on ait un diagramme commutatif

$$\begin{array}{ccc} L_{p-1} & \leftarrow & L_p \\ \cup & & \cup \\ V \otimes S(-p) & \leftarrow & S(-p-1) \cong \langle s \rangle \end{array}$$

Ce diagramme s'étend en un morphisme de complexes entre le complexe de Koszul de V et le complexe linéaire de C

$$\begin{array}{ccccccccc} S & \leftarrow & L_1 & \leftarrow \cdots \leftarrow & L_{p-1} & \leftarrow & L_p \\ \uparrow \varphi_2 & & \uparrow & & \uparrow & & \uparrow \\ \wedge^p V \otimes S(-1) & \xleftarrow{\phi} & \wedge^{p-1} V \otimes S(-2) & \leftarrow \cdots \leftarrow & V \otimes S(-p) & \leftarrow & S(-p-1) \end{array}$$

Proposition 10 *[54] On a* $\dim(V) \geq p+1$. *Si l'égalité a lieu, l'idéal quadratique* $I_s \subset S$ *défini par*

$$I_s := \mathrm{Im}(\varphi_2 \circ \phi : \wedge^{p-1} V \otimes S(-2) \to S)$$

définit une scroll rationnelle normale de codimension p *qui contient* C. *On dit alors que* s *est une* syzygy scrollaire.

Preuve (esquisse). Si $\dim V = p+1$, on obtient un diagramme

$$\begin{array}{ccccc} & & S & \longleftarrow & S(-2)^{b_1} \\ & & \uparrow \varphi_2 & & \uparrow \\ \wedge^{p+1} V \otimes S \cong S & \xleftarrow{\varphi_1} & \wedge^p V \otimes S(-1) & \xleftarrow{\phi} & \wedge^{p-1} V \otimes S(-2) \end{array}$$

où $\varphi_1 = (l_0, \ldots, l_p)$ et $\varphi_2 = (m_0, \ldots, m_p)$ sont des vecteurs de formes linéaires. La composition $\varphi_2 \circ \phi$ a pour entrée les mineurs de

$$\varphi := \begin{pmatrix} l_0 & l_1 & \cdots & l_p \\ m_0 & m_1 & \cdots & m_p \end{pmatrix}$$

qui engendrent par définition l'idéal I_s. Comme C est irréductible, on en déduit que la matrice φ est 1-générique et il suit de [41, Cor.3.12] que I_s est l'idéal d'une scroll X de codimension $p+1$. On a par construction $I_s \subset I_C$ donc $C \subset X$. □

Il découle des résultats précédents que $\mathrm{gon}(C) = g - p$, où $p \leq g - \ell - 2$ est le plus petit entier tel qu'il existe une p-ème syzygy scrollaire s. Dans ce cas, la scroll X d'idéal I_s vérifie (6.2). De plus, le quotient des deux entrées de n'importe quelle colonne de φ détermine une fonction rationnelle f sur $\mathbb{P}^{g-1}$ dont la restriction à C définit le morphisme gonal sous-jacent au diagramme (6.2). La dernière étape consiste à caractériser algébriquement les syzygies scrollaires.

Espace des syzygies scrollaires. Soit $p \geq 2$ et soit $\psi_p : L_p \to L_{p-1}$ la matrice des syzygies, à coefficients des formes linéaires en les indéterminées $x = (x_0, \ldots, x_{g-1})$. Soit $y = (y_0, \ldots, y_{\beta-1})$ de nouvelles indéterminées qui représentent $s \in L_p$ dans une base donnée. On a

$$\psi_p(x) \begin{pmatrix} y_0 \\ \vdots \\ y_{\beta-1} \end{pmatrix} = \Psi_p(y) \begin{pmatrix} x_0 \\ \vdots \\ x_{g-1} \end{pmatrix}$$

pour une matrice $\Psi_p(y)$ à coefficients des formes linéaires en y. On a alors l'égalité $\dim V(s) = \mathrm{rang}(\Psi_p(y))$, d'où il découle que l'espace des p-èmes syzygies scrollaires est le sous-schéma

$$Y_p \subset \mathbb{P}(\mathrm{Tor}_p^S(S_C, \mathbb{K})_{p+1}) \cong \mathbb{P}^{\beta-1}$$

d'idéal engendré par les $(p+2) \times (p+2)$ mineurs de $\Psi_p(y)$.

6.4 Algorithme et exemple.

On déduit de ce qui précède l'algorithme suivant, qui considère en entrée une courbe canonique lisse $C \subset \mathbb{P}^{g-1}$ de genre $g \geq 2$ définie sur un corps $\mathbb{K}$, et qui renvoie la gonalité de C et un morphisme gonal (possiblement défini sur une extension de $\mathbb{K}$).

1. Calculer le sous-complexe linéaire $L_\bullet$ de C.
2. Soit $p := g - \ell - 2$. Tant que Y_p est vide faire $p := p - 1$.

3. On a $gon(C) = g - p$. Déterminer un point $s \in Y_p$ (extension de corps probable).
4. Calculer les morphismes φ_1 et φ_2 induits par s.
5. Retourner la restriction à C du quotient des premières entrées de φ_1 et φ_2.

Exemple. Considérons pour exemple basique la sextique plane à 4 noeuds ($g = 6$). Le modèle canonique a pour table de Betti

$$\begin{array}{ccccc} 1 & - & - & - & - \\ - & 6 & 5 & - & - \\ - & - & 5 & 6 & - \\ - & - & - & - & 1 \end{array}$$

et pour sous-complexe linéaire

$$(L_\bullet): \qquad S \leftarrow S(-2)^6 \leftarrow S(-3)^5 \leftarrow 0.$$

L'espace $Y_2 \subset \mathbb{P}^4$ des syzygies scrollaires de degré 2 est donné ici par les 4-mineurs d'une matrice 6×5 de formes linéaires. On vérifie que Y_2 est union de 5 droites. Ainsi $\text{gon}(C) = g - 2 = 4$, avec 5 morphismes gonaux. De fait, 4 morphismes gonaux correspondent aux projections centrées en chacun des 4 noeuds et le dernier morphisme gonal correspond au pinceau des coniques passant par ces 4 noeuds. Les morphismes gonaux sont ici définis sur une extension de degré au plus 5 de $\mathbb{K}$.

Corps de définition d'un morphisme gonal. Si $\mathbb{K}$ est un corps fini, un morphisme gonal est souvent défini sur $\mathbb{K}$ (ou une petite extension de $\mathbb{K}$) du simple fait que les polynômes univariés sur les corps finis ont fréquemment des facteurs de petits degrés. Dans l'exemple ci-dessus, au moins l'un des 5 morphismes gonaux est défini sur $\mathbb{K}$ dans environ 63% des cas.

Complexité. L'algorithme se résume *in fine* à calculer l'idéal du modèle canonique C (si la courbe d'entrée est une courbe projective quelconque), à calculer les syzygies linéaires, puis à chercher les syzygies scrollaires *via* la résolution de systèmes polynomiaux déterminantaux. Tout ceci peut se faire de manière effective *via* l'utilisation des bases de Gröbner. Cependant, la complexité dépend exponentiellement du nombre de variables, qui peut potentiellement lui-même être doublement exponentiel en le genre !

Ainsi l'algorithme ci-dessus a en pratique un coût prohibitif dès que le genre est trop élevé. Par exemple, nous n'avons pas pu résoudre le système sous-jacent au calcul des syzygies scrollaires pour une courbe générale de genre $g \geq 7$ sur un corps fini.

6.5 Variantes.

6.5.1 Courbes gonériques.

Si C vérifie une condition dite de "gonéricité" [117, Def.4.1] portant sur *la valeur* du premier nombre de Betti $\beta_{\ell,\ell+2}$ non nul, alors elle admet un unique morphisme gonal, et les espaces Y_p des syzygies scrollaires se calculent plus efficacement. En particulier, le premier espace non vide Y_p est une courbe rationnelle normale de $\mathbb{P}^{p-1}$ sur laquelle il est relativement facile de déterminer un point. On a pu ainsi traiter des courbes de genre $g = 9$, voir [117, Ex.4.8].

Si de plus $\ell(C) << g$ (impliquant une gonalité petite relativement au genre), on peut remplacer la partie coûteuse du calcul du complexe linéaire $L_\bullet$ de C par un calcul rapide des premiers termes de la résolution totale $F_\bullet$ desquels on déduit aisément l'idéal I_X [117, Prop.4.11]. Dans ce cas, on n'a plus accès à la matrice ϕ pour calculer la projection $X \to \mathbb{P}^1$, mais on peut utiliser une méthode basée sur les algèbres de Lie. On a pu ainsi traiter des courbes de gonalité 4 et de genre $g = 12$, voir [117, Ex.4.13]. Cette méthode est particulièrement bien adaptée pour la paramétrisation par radicaux qui ne concerne *a priori* que les courbes de gonalité ≤ 4.

Quelles courbes sont gonériques ? Une courbe générale de genre g n'est malheureusement pas gonérique. Dans notre papier, nous énonçons cependant une conjecture qui assure en particulier qu'une courbe générale de gonalité non maximale (le genre g étant fixé) est gonérique [117, Conj.4.9]. Ce dernier point est maintenant un théorème, dû à G. Farkas et M. Kemeny [45, Thm.0.4], duquel découle de nouvelles familles de courbes pour lesquelles cette variante plus rapide de notre algorithme s'applique.

6.5.2 Courbes planes.

Si $C \subset \mathbb{P}^2$ est une courbe plane de degré d avec une singularité p de multiplicité maximale ν, alors la projection $C \dashrightarrow \mathbb{P}^1$ centrée en p définit une application rationnelle de degré $d-\nu$, conduisant à une inégalité évidente

$$\mathrm{gon}(C) \leq d - \nu.$$

Dans [95, 113] (et références afférentes), les auteurs établissent des critères numériques en fonction de d, g et ν (et plus généralement de l'ensemble des multiplicités des singularités de C) qui assurent que l'égalité $\mathrm{gon}(C) = d-\nu$ est atteinte (voir [117, Prop.4.14] pour un bref résumé). Ils montrent en particulier que lorsque C admet un modèle planaire nodal avec au plus $(d/2-1)^2$ noeuds, alors la gonalité est $d-2$. Dans ces cas particuliers, une application gonale se calcule aisément comme la projection centrée en une singularité de multiplicité maximale. Notez que cela n'exclut pas qu'il existe d'autres types d'applications gonales, comme le pinceau de coniques dans l'exemple de la sextique plane à 4 noeuds ci-dessus.

Dans le même esprit, on peut dans certains cas déduire la gonalité à partir du polygone de Newton lorsque celui-ci est suffisamment plat et que la courbe est générale relativement à son polygone [27].

Dans tous ces cas spécifiques, passer par un modèle plan est bien entendu préférable au calcul coûteux des syzygies d'un modèle canonique.

Bibliographie

[1] N. H. Abel. *Mémoire sur une propriété générale d'une classe très étendue de fonctions transcendantes*, volume 1 of *Cambridge Library Collection - Mathematics*, page 145–211. Cambridge University Press, 2012. (Cité en pages 5 et 13.)

[2] S. Abelard. On the complexity of computing integral bases of function fields. In *Computer Algebra in Scientific Computing*, pages 42–62. Springer International Publishing, 2020. (Cité en pages 60 et 65.)

[3] S. Abelard, E. Berardini, A. Couvreur, and G. Lecerf. Computing Riemann-Roch spaces via Puiseux expansions. *Journal of Complexity*, 73 :1–45, 2022. (Cité en pages 5, 8, 47, 53 et 61.)

[4] S. Abelard, A. Couvreur, and G. Lecerf. Sub-quadratic time for Riemann-Roch spaces. The case of smooth divisors over nodal plane projective curves. In *ISSAC 2020 - 45th International Symposium on Symbolic and Algebraic Computation*, pages 14–21, Kalamata, Greece, 2020. (Cité en page 53.)

[5] S. Abelard, A. Couvreur, and G. Lecerf. Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities. *Applicable Algebra in Engineering, Communication and Computing*, 2022. (Cité en page 53.)

[6] S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*, volume 35 of *Mathematical surveys and monographs*. Amer. Math. Soc., 1990. (Cité en page 61.)

[7] S. S. Abhyankar. Irreducibility criterion for germs of analytic functions of two complex variables. *Advances in Mathematics*, 74(2) :190 – 257, 1989. (Cité en page 61.)

[8] S. S. Abhyankar and T. T. Moh. Embeddings of the line in the plane. *J. Reine Angew. Math.*, 276 :148–166, 1975. (Cité en page 55.)

[9] F. Abu Salem, S. Gao, and A. G. B. Lauder. Factoring polynomials via polytopes. ISSAC '04, pages 4–11, New York, NY, USA, 2004. Association for Computing Machinery. (Cité en pages 40 et 47.)

[10] M. Alberich-Carramiñana, J. Guàrdia, E. Nart, A. Poteaux, J. Roé, and M. Weimann. Polynomial factorization over henselian fields, 2022. (Cité en pages 5, 6, 7, 62, 66, 67, 68 et 69.)

[11] M. Andersson and E. Wulcan. *Variants of the Effective Nullstellensatz and Residue Calculus*, pages 17–31. Springer Basel, Basel, 2011. (Cité en page 23.)

[12] W. P. Barth, K. Hulek, C. A. M. Peters, and A. Van de Ven. *Compact complex surfaces*, volume 4. Springer-Verlag, Berlin, second edition, 2004. (Cité en page 34.)

[13] J.-D. Bauch. Genus computation of global function fields. *Journal of Symbolic Computation*, 66 :8–20, 2015. (Cité en page 60.)

[14] J.-D. Bauch. Computation of integral bases. *Journal of Number Theory*, 165 :382–407, 2016. (Cité en page 65.)

[15] J.-D. Bauch, E. Nart, and H. Stainsby. Complexity of the OM factorizations of polynomials over local fields. *LMS Journal of Computation and Mathematics*, 16 :139–171, 2013. (Cité en page 64.)

[16] C. Berenstein, R. Gay, A. Vidras, and A. Yger. *Residue Currents and Bezout Identities*. Progress in Mathematics. Birkhäuser Basel, 1993. (Cité en page 23.)

[17] C. A. Berenstein and A. Yger. Residue calculus and effective nullstellensatz. *American Journal of Mathematics*, 121(4) :723–796, 1999. (Cité en page 23.)

[18] D. N. Bernstein. The number of roots of a system of equations. *Funkcional. Anal. i Prilozen.*, 9 :1–4, 1975. English translation : Functional Anal. Appl. **9** (1975), 183–185. (Cité en pages 15 et 29.)

[19] J. Berthomieu and G. Lecerf. Reduction of bivariate polynomials from convex-dense to dense, with application to factorizations. *Mathematics of Computation*, 81(279) :1799–1821, 2012. (Cité en page 47.)

[20] A. Bostan, G. Lecerf, B. Salvy, E. Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, pages 42–49, New York, NY, USA, 2004. Association for Computing Machinery. (Cité en pages 40, 46 et 48.)

[21] L. Busé, C. d'Andrea, M. Sombra, and M. Weimann. The geometry of the flex locus of a hypersurface. *Pacific Journal of Mathematics*, 304(2) :419–437, 2020. (Cité en pages 6, 7, 73, 74, 75 et 76.)

[22] J. Böhm, W. Decker, S. Laplagne, and G. Pfister. Computing integral bases via localization and hensel lifting. *Journal of Symbolic Computation*, 109 :283–324, 2022. (Cité en page 60.)

[23] A. Campillo. *Algebroid Curves in Positive Characteristic*, volume 378 of *LNCS*. Springer-Verlag, 1980. (Cité en page 62.)

[24] A. Campillo, G.-M. Greuel, and C. Lossen. Equisingular calculations for plane curve singularities. *J. of Symb. Comp.*, 42(1-2) :89–114, 2007. (Cité en page 62.)

[25] D. G. Cantor and D. Gordon. Factoring polynomials over p-adic fields. In *ANTS-IV*, volume 1838 of *LNCS*. Springer Verlag, 2000. (Cité en page 63.)

[26] X. Caruso, D. Roe, and T. Vaccon. Division and slope factorization of p-adic polynomials. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 159–166, New York, NY, USA, 2016. ACM. (Cité en page 65.)

[27] W. Castryck and F. Cools. Newton polygons and curve gonalities. *Journal of Algebraic Combinatorics*, 35(7) :345–366, 2012. (Cité en page 85.)

[28] E. Cattani, D. Cox, and A. Dickenstein. Residues in toric varieties. *Compositio Mathematica*, 108(1) :35–76, 1997. (Cité en page 26.)

[29] E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5 :119–148, 1998. (Cité en page 26.)

[30] G. Chèze. Absolute polynomial factorization in two variables and the knapsack problem. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, page 87–94, New York, NY, USA, 2004. Association for Computing Machinery. (Cité en page 39.)

[31] G. Chèze, M. Elkadi, A. Galligo, and M. Weimann. Absolute factoring of bidegree bivariate polynomials. *ACM SIGSAM Bulletin*, 42(3) :151, Feb. 2009. (Cité en pages 40 et 41.)

[32] G. Chèze and A. Galligo. *Four lectures on polynomial absolute factorization*, pages 339–392. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005. (Cité en page 39.)

[33] G. Chèze and A. Galligo. From an approximate to an exact absolute polynomial factorization. *Journal of Symbolic Computation*, 41(6) :682–696, 2006. (Cité en page 39.)

[34] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *Journal of Complexity*, 23(3) :380–420, 2007. (Cité en pages 39, 40, 46, 49, 50 et 52.)

[35] N. R. Coleff and M. E. Herrera. *Les courants residuels associes à une forme méromorphe*, volume 633 of *Lect. Notes Math.* Springer, Cham, 1978. (Cité en page 23.)

[36] D. A. Cox. Toric residues. *Arkiv för Matematik*, 34(1) :73 – 96, 1996. (Cité en page 15.)

[37] D. A. Cox, J. B. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Grad. Texts in Math.* Springer, second edition, 2005. (Cité en page 75.)

[38] X. Dahan, E. Schost, M. M. Maza, W. Wu, and Y. Xie. On the complexity of the D5 principle. *SIGSAM Bull.*, 39(3) :97–98, 2005. (Cité en page 64.)

[39] D. Duval. Rational Puiseux expansions. *Compositio Math.*, 70(2) :119–154, 1989. (Cité en page 7.)

[40] D. Duval. Absolute factorization of polynomials : A geometric approach. *SIAM Journal on Computing*, 20(1) :1–21, 1991. (Cité en pages 50 et 59.)

[41] D. Eisenbud. *Geometry of Syzygies.* Graduate Texts in Mathematics. Springer, 2005. (Cité en pages 82 et 83.)

[42] D. Eisenbud and J. Harris. *3264 and all that—a second course in algebraic geometry.* Cambridge Univ. Press, 2016. (Cité en pages 7, 73, 74, 75 et 77.)

[43] M. Elkadi, A. Galligo, and M. Weimann. Towards toric absolute factorization. *Journal of Symbolic Computation*, 44(9) :1194–1211, 2009. Effective Methods in Algebraic Geometry. (Cité en pages 4, 40, 41 et 42.)

[44] A. J. Engler and A. Prestel. *Valued Fields.* Springer Monographs in Mathematics. Springer Berlin, Heidelberg, 2005. (Cité en page 66.)

[45] G. Farkas and M. Kemeny. Linear syzygies of curves with prescribed gonality. *Advances in Mathematics*, 356 :106810, 2019. (Cité en page 85.)

[46] D. Ford, S. Pauli, and X.-F. Roblot. A fast algorithm for polynomial factorization over $\mathbb{Q}_p$. *Journal de Théorie des Nombres de Bordeaux*, 14 :151–169, 2002. (Cité en page 63.)

[47] W. Fulton. *Introduction to Toric Varieties. (AM-131).* Princeton University Press, 1993. (Cité en page 15.)

[48] A. Galligo and D. Rupprecht. Irreducible decomposition of curves. *Journal of Symbolic Computation*, 33(5) :661–677, 2002. (Cité en pages 39 et 41.)

[49] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comput.*, 72(242) :801–822, 2003. (Cité en pages 40 et 44.)

[50] J. v. z. Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, New York, NY, USA, 3rd edition, 2013. (Cité en page 39.)

[51] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants.* Math. Theory Appl. Birkhäuser, 1994. (Cité en pages 25, 26 et 75.)

[52] V. D. Goppa. Codes and information. *Russ. Math. Surv.*, 391 :87–141, 1984. (Cité en page 61.)

[53] H.-C. Graf von Bothmer. Generic syzygy schemes. *Journal of Pure and Applied Algebra*, 208(3) :867–876, 2007. (Cité en pages 80 et 82.)

[54] H.-C. Graf von Bothmer. Scrollar syzygies of general canonical curves with genus $\leq$ 8. *Transactions of the American Mathematical Society*, 359(2) :465–488, 2007. (Cité en pages 80, 82 et 83.)

[55] M. L. Green. Secant functions, the reiss relation and its converse. *Transactions of the American Mathematical Society*, 280(2) :499–507, 1983. (Cité en page 14.)

[56] G.-M. Greuel, C. Lossen, and E. Shustin. *Introduction to singularities and deformation*. Monographs in Mathematics. Springer, 2007. (Cité en page 62.)

[57] P. Griffiths and J. Harris. *Principles of Algebraic Geometry*. Wiley-Intersciences, 1978. (Cité en pages 24, 25 et 33.)

[58] P. A. Griffiths. Variations on a theorem of Abel. *Inventiones mathematicae*, 35 :321–390, 1976. (Cité en pages 3, 12, 13 et 14.)

[59] J. Guàrdia, J. Montes, and E. Nart. Okutsu invariants and Newton polygons. *Acta Arithmetica*, 145 :83–108, 2010. (Cité en page 64.)

[60] J. Guàrdia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Transsactions of the American Mathematical Society*, 364 :361–416, 2012. (Cité en page 63.)

[61] J. Guàrdia, J. Montes, and E. Nart. A new computational approach to ideal theory in number fields. *Foundations of Computational Mathematics*, 13(5) :729–762, 2013. (Cité en pages 63 et 65.)

[62] J. Guàrdia, E. Nart, and S. Pauli. Single-factor lifting and factorization of polynomials over local fields. *Journal of Symbolic Computation*, 47(11) :1318 – 1346, 2012. (Cité en pages 63 et 65.)

[63] L. Guth and N. H. Katz. On the Erdös distinct distances problem in the plane. *Ann. of Math. (2)*, 181 :155–190, 2015. (Cité en page 73.)

[64] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons and integral bases. *Journal of Number Theory*, 147 :549–589, 2015. (Cité en pages 8, 53 et 65.)

[65] M. Harrison. Explicit solution by radicals, gonal maps and plane models of algebraic curves of genus 5 or 6. *Journal of Symbolic Computation*, 51 :3–21, 2013. Effective Methods in Algebraic Geometry. (Cité en page 80.)

[66] G. Henkin and M. Passare. Abelian differentials on singular varieties and variations on a theorem of Lie-Griffiths. *Inventiones mathematicae*, 135(2) :297–328, 1999. (Cité en pages 3, 12, 13, 14, 21, 22 et 27.)

[67] M. Herrera and D. Lieberman. Residues and principal values on complex spaces. *Mathematische Annalen*, 194 :259–294, 1971. (Cité en page 23.)

[68] F. J. Herrera Govantes, W. Mahboub, M. A. Olalla Acosta, and M. Spivakovsky. Key polynomials for simple extensions of valued fields. *Journal of Singularities*, 25 :197–267, 2022. (Cité en pages 66 et 67.)

[69] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, 33(4) :425–445, 2002. (Cité en pages 8, 53 et 65.)

[70] J. v. d. Hoeven and G. Lecerf. Univariate polynomial factorization over finite fields with large extension degree. *Applicable Algebra in Engineering, Communication and Computing*, Jan 2022. (Cité en pages 53 et 59.)

[71] M.-D. Huang and D. Ierardi. Efficient algorithms for the riemann-roch problem and for addition in the jacobian of a curve. *Journal of Symbolic Computation*, 18(6) :519–539, 1994. (Cité en page 61.)

[72] J.-P. Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90 :117–263, 1991. (Cité en page 75.)

[73] N. Katz. The flecnode polynomial : a central object in incidence geometry. In *Proc. ICM 2014*, volume III, pages 303–314, 2014. (Cité en pages 6 et 73.)

[74] A. G. Khovanskii. Newton polyhedra and the euler-jacobi formula. *Russian Mathematical Surveys*, 33(6) :237, dec 1978. (Cité en page 25.)

[75] K. Khuri-Makdisi. Asymptotically fast group operations on jacobians of general curves. *Mathematics of Computation*, 76(260) :2213–2239, 2007. (Cité en page 61.)

[76] J. Kollár. Szemerédi-Trotter-type theorems in dimension 3. *Adv. Math.*, 271 :30–61, 2015. (Cité en page 73.)

[77] J. Kollár. *Lectures on Resolution of Singularities (AM-166)*. Princeton University Press, 2007. (Cité en page 50.)

[78] M. Koras and K. Palka. The Coolidge–Nagata conjecture. *Duke Mathematical Journal*, 166(16) :3085 – 3145, 2017. (Cité en page 55.)

[79] A. G. Kouchnirenko. Polyèdres de Newton et nombres de Milnor. *Inventiones Mathematicae*, 32(1) :1–31, 1976. (Cité en pages 15 et 29.)

[80] A. A. Kytmanov and A. Y. Semusheva. Averaging of the cauchy kernels and integral realization of the local residue. *Mathematische Zeitschrift*, 264 :87–98, 2010. (Cité en page 25.)

[81] G. Labahn, V. Neiger, and W. Zhou. Fast, deterministic computation of the hermite normal form and determinant of a polynomial matrix. *Journal of Complexity*, 42 :44–71, 2017. (Cité en page 65.)

[82] J. M. Landsberg. Is a linear space contained in a submanifold ? On the number of derivatives needed to tell. *J. Reine Angew. Math.*, 508 :53–60, 1999. (Cité en page 73.)

[83] G. Lecerf. Sharp precision in hensel lifting for bivariate polynomial factorization. *Mathematics of Computation*, 75(254) :921–933, 2006. (Cité en pages 4, 39, 40, 43, 44, 46, 48 et 50.)

[84] G. Lecerf. Fast separable factorization and applications. *Applicable Algebra in Engineering, Communication and Computing*, 19(2) :135–160, 2008. (Cité en pages 47 et 69.)

[85] G. Lecerf. New recombination algorithms for bivariate polynomial factorization based on Hensel lifting. *Applicable Algebra in Engineering, Communication and Computing*, 21(2) :151–176, 2010. (Cité en pages 4, 39, 40, 43, 44, 46, 47, 48, 49 et 50.)

[86] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. (Cité en page 51.)

[87] S. Mac Lane. A construction for prime ideals as absolute values of an algebraic field. *Duke Math. J.*, 2(3) :492–510, 1936. (Cité en page 63.)

[88] S. MacLane. A construction for absolute values in polynomial rings. *Trans. Amer. Math. Soc.*, 40(3) :363–395, 1936. (Cité en page 63.)

[89] J. McDonald. Fiber polytopes and fractional power series. *Journal of Pure and Applied Algebra*, 104(2) :213–233, 1995. (Cité en pages 7, 62 et 70.)

[90] N. Moraes de Oliveira and E. Nart. Defectless polynomials over henselian fields and inductive valuations. *Journal of Algebra*, 541 :270–307, 2020. (Cité en pages 66 et 67.)

[91] E. Nart. Key polynomials over valued fields. *Publicacions Matemàtiques*, 64(1) :195 – 232, 2020. (Cité en page 67.)

[92] V. Neiger, J. Rosenkilde, and E. Schost. Fast computation of the roots of polynomials over the ring of power series. In *ISSAC'17*, pages 349–356. ACM, 2017. (Cité en page 65.)

[93] J. Novacoski and M. Spivakovsky. Reduction of local uniformization to the rank one case. In *Valuation theory in interaction*, EMS Ser. Congr. Rep., pages 404–431. Eur. Math. Soc., Zürich, 2014. (Cité en pages 6 et 67.)

[94] T. Oda. *Convex bodies and algebraic geometry*. Springer, 1988. (Cité en page 15.)

[95] M. Ohkouchi and F. Sakai. The gonality of singular plane curves. *Tokyo Journal of Mathematics*, 27(1) :1–11, 2004. (Cité en page 85.)

[96] K. Okutsu. Construction of integral basis, i. *Proc. Japan Acad. Ser. A Math. Sci.*, 58(1) :47–49, 1982. (Cité en page 8.)

[97] Ö. Ore. Zur Theorie der Algebraischen Körper. *Acta Mathematica*, 44(none) :219 – 314, 1923. (Cité en page 63.)

[98] Ö. Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. *Mathematische Annalen*, 99 :84–117, 1928. (Cité en page 63.)

[99] M. Passare. Residues, currents, and their relation to ideals of holomorphic functions. *Mathematica Scandinavica*, 62(1) :75–152, 1988. (Cité en page 23.)

[100] M. Passare, A. Tsikh, and A. Yger. Residue currents of the bochner-martinelli type. *Publicacions Matemàtiques*, 44(1) :85–117, 2000. (Cité en pages 24, 25 et 26.)

[101] S. Pauli. Factoring polynomials over local fields. *J. Symb. Comp.*, 32 :533–547, 2001. (Cité en page 63.)

[102] S. Pauli. Factoring polynomials over local fields, ii. In *ANTS-IX*, LNCS. Springer Verlag, 2010. (Cité en page 63.)

[103] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Z.*, 214 :377–396, 1993. (Cité en page 28.)

[104] J. M. Peral. *Polígonos de Newton de orden superior y aplicaciones aritméticas*. PhD thesis, Universitat de Barcelona, 1999. (Cité en pages 63 et 67.)

[105] P. Popescu-Pampu. Approximate roots. *Fields Institute Communiations*, 33 :1–37, 2002. (Cité en page 61.)

[106] A. Poteaux and M. Rybowicz. Improving complexity bounds for the computation of Puiseux series over finite fields. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '15, pages 299–306, New York, NY, USA, 2015. ACM. (Cité en pages 58 et 59.)

[107] A. Poteaux and M. Weimann. Computing the equisingularity type of a pseudo-irreducible polynomial. *Applicable Algebra in Engineering, Communication and Computing*, 31 :435 – 460, 2020. (Cité en pages 5, 40 et 62.)

[108] A. Poteaux and M. Weimann. Computing Puiseux series : a fast divide and conquer algorithm. *Annales Henri Lebesgue*, 4 :1061–1102, 2021. (Cité en pages 5, 7, 40, 48, 52, 53, 58, 59, 60, 61 et 65.)

[109] A. Poteaux and M. Weimann. Local polynomial factorisation : Improving the montes algorithm. ISSAC '22, 2022. (Cité en pages 5, 6, 8, 48, 53, 63, 64, 65 et 68.)

[110] A. Poteaux and M. Weimann. A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$. *Journal of Computational Complexity*, 31 :1–52, 2022. (Cité en pages 5, 40 et 61.)

[111] W. M. Ruppert. Reduzibilität ebener kurven. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, pages 167 – 191, 1986. (Cité en pages 4, 40, 44 et 45.)

[112] D. Rupprecht. Semi-numerical absolute factorization of polynomials with integer coefficients. *Journal of Symbolic Computation*, 37(5) :557–574, 2004. (Cité en pages 39 et 41.)

[113] T. Sakai. On the gonality of singular plane curves ii. *Proc. Symposium on Algebraic Geometry at Sado 2006*, pages 32–48, 2007. (Cité en page 85.)

[114] G. Salmon. *A treatise on the analytic geometry of three dimensions. Vol. II.* 1865. reprinted fifth edition at Chelsea Publishing Co., 1965. (Cité en pages 6 et 74.)

[115] T. Sasaki and M. Sasaki. A unified method for multivariate polynomial factorizations. *Japan Journal of Industrial and Applied Mathematics*, 10 :21–39, 1993. (Cité en page 40.)

[116] T. Sasaki, M. Suzuki, M. Kolar, and M. Sasaki. Approximate factorization of multivariate polynomials and absolute irreducibility testing. *Japan J. Indust. Appl. Math.*, 8 :357–375, 1991. (Cité en page 40.)

[117] J. Schicho, F.-O. Schreyer, and M. Weimann. Computational aspects of gonal maps and radical parametrization of curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(5) :313–341, Nov. 2013. (Cité en pages 7, 79, 80, 81, 82, 84 et 85.)

[118] J. Schicho and D. Sevilla. Effective radical parametrization of trigonal curves. *arXiv e-prints*, page arXiv :1104.2470, Apr. 2011. (Cité en page 80.)

[119] F.-O. Schreyer. Syzygies of canonical curves and special linear series. *Mathematische Annalen*, 275(1) :105–137, 1986. (Cité en pages 80 et 81.)

[120] J. R. Sendra and D. Sevilla. Radical parametrizations of algebraic curves by adjoint curves. *Journal of Symbolic Computation*, 46(9) :1030–1038, 2011. (Cité en page 80.)

[121] J.-P. Serre. *Algèbre locale. Multiplicités*, volume 11 of *Lecture Notes in Math.* Springer-Verlag, second edition, 1965. (Cité en page 51.)

[122] M. Sharir and N. Solomon. Incidences between points and lines on two- and three-dimensional varieties. *Discrete Comput. Geom.*, 59 :88–130, 2018. (Cité en page 73.)

[123] A. Shchuplev, A. Tsikh, and A. Yger. Residual kernels with singularities on coordinate planes. *Proc. Steklov Inst. Math.*, 253 :256–274, 2006. (Cité en page 25.)

[124] D. Simon. Construction de polynômes de petits discriminants. *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics*, 329(6) :465–468, 1999. (Cité en page 54.)

[125] D. Simon and M. Weimann. Plane curves with minimal discriminant. *Journal of Commutative Algebra*, 10(4) :559–598, Aug. 2018. (Cité en pages 4, 5, 48, 54 et 55.)

[126] M. Sombra. A sparse effective nullstellensatz. *Advances in Applied Mathematics*, 22(2) :271–295, 1999. (Cité en page 23.)

[127] A. J. Sommese, J. Verschelde, and C. W. Wampler. Numerical decomposition of the solution sets of polynomial systems into irreducible components. *SIAM Journal on Numerical Analysis*, 38(6) :2022–2046, 2001. (Cité en page 40.)

[128] T. Tao. The Monge-Cayley-Salmon theorem via classical differential geometry. blog entry at `https://terrytao.wordpress.com/2014/03/28/`, 2014. (Cité en page 73.)

[129] J. Tate. Residues of differentials on curves. *Ann. Sci. École Norm. Sup. (4)*, 1 :149–159, 1968. (Cité en page 51.)

[130] M. van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation*, 18 :353–363, 1994. (Cité en page 60.)

[131] M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *Journal of Symbolic Computation*, 23(2-3) :209–227, 1997. (Cité en page 61.)

[132] M. Vaquié. Extensions de valuation et polygone de newton. *Annales de l'institut Fourier*, 58(7) :2503–2541, 2008. (Cité en page 67.)

[133] A. Vidras and A. Yger. *Multidimensional Residue Theory and Applications*, volume 275 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2023. (Cité en page 23.)

[134] M. Weimann. *La trace en géométrie projective et torique*. These, Université Sciences et Technologies - Bordeaux I, Juin 2006. (Cité en pages 3, 12, 15, 17, 18, 19, 26 et 28.)

[135] M. Weimann. Trace et calcul résiduel : une nouvelle version du théorème d'Abel inverse, formes abéliennes. *Annales de la faculté des sciences de Toulouse Mathématiques*, 16(2) :397–424, 2007. (Cité en pages 3, 12, 14 et 15.)

[136] M. Weimann. An interpolation theorem in toric varieties. *Annales de l'Institut Fourier*, 58(4) :1371–1381, 2008. (Cité en pages 3, 4, 12, 15, 19 et 29.)

[137] M. Weimann. A lifting and recombination algorithm for rational factorization of sparse polynomials. *Journal of Complexity*, 26(6) :608–628, 2010. (Cité en pages 4, 12, 31, 34, 40, 44, 45, 46 et 47.)

[138] M. Weimann. Algebraic Osculation and Application to Factorization of Sparse Polynomials. *Journal of Foundations of Computational Mathematics*, 12(2) :173–201, 2012. (Cité en pages 4, 8, 31, 40, 43 et 44.)

[139] M. Weimann. Concavity, Abel transform and the Abel-inverse theorem in smooth complete toric varieties. *Collectanea Mathematica*, 64(1) :111–133, Jan. 2013. (Cité en pages 3, 12, 15, 18, 19, 27 et 28.)

[140] M. Weimann. Factoring bivariate polynomials using adjoints. *Journal of Symbolic Computation*, 58 :77–98, 2013. (Cité en pages 4, 5, 8, 12, 40, 50, 51, 52 et 53.)

[141] M. Weimann. Bivariate factorization using a critical fiber. *Journal of Foundations of Computational Mathematics*, pages 1–45, 2016. (Cité en pages 4, 5, 40, 47, 48, 49, 50 et 60.)

[142] V. Williams, Y. Xu, Z. Xu, and R. Zhou. New bounds for matrix multiplication : from alpha to omega. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 3792–3835, 2024. (Cité en page 46.)

[143] J. Wood. Osculation by algebraic hypersurfaces. *J. Differential Geometry*, 18 :563–573, 1983. (Cité en page 33.)

[144] J. Wood. A simple criterion for an analytic hypersurface to be algebraic. *Duke Mathematical Journal*, 51(1) :235–237, 1984. (Cité en page 14.)

[145] E. Wulcan. Products of residue currents of cauchy-fantappiè-leray type. *Arkiv för Matematik*, 45 :157–78, 2007. (Cité en page 25.)

[146] O. Zariski. Studies in equisingularity i equivalent singularities of plane algebroid curves. *American Journal of Mathematics*, 87(2) :507–536, 1965. (Cité en page 62.)

[147] H. Zassenhaus. On hensel factorization, i. *Journal of Number Theory*, 1(3) :291–311, 1969. (Cité en page 39.)

Résumé : Ce mémoire d'habilitation porte sur des problèmes de géométrie algébrique effective et de calcul formel. Il se compose de trois parties.
La première partie porte sur mes travaux dans la lignée de ma thèse, à l'interface de l'analyse complexe et la géométrie torique. Son but est de donner au lecteur un aperçu de l'utilité du calcul résiduel multivarié dans les problèmes de prolongement algébrique d'objets analytiques dans les variétés toriques compactes complexes.
La seconde partie, à visée plus algorithmique, concerne la complexité de la factorisation des polynômes, problème fondamental du calcul formel. On décrit dans un premier temps des méthodes de factorisation bivariée basées sur la géométrie torique, conduisant à des algorithmes polynomiaux en le volume du polytope de Newton. On s'intéresse ensuite aux méthodes de factorisation bivariée basées sur la résolution des singularités des courbes planes. Enfin on s'intéresse à la factorisation des polynômes univariés sur les anneaux de valuations discrètes complets.
La dernière partie du manuscrit concerne deux autres problèmes relativement transverses. L'un porte sur le calcul du degré et de l'équation du lieu flex des hypersurfaces projectives *via* la théorie des résultants multivariés, et l'autre porte sur le calcul de la gonalité des courbes algébriques *via* l'étude des syzygies du modèle canonique.

Mots clés : Polynômes, variétés toriques, polytopes, résidus, résultants, factorisation, singularités, séries de Puiseux, corps locaux, algorithmes, complexité.