Université Polytechnique HAUTS-DE-FRANCE

Mémoire pour obtenir

L'Habilitation à Diriger des Recherches

Spécialité : **Mathématiques Pures**

Quelques contributions à l'arithmétique des corps et des polynômes

Présenté et soutenu le 27 mai 2022 par

Salah NAJIB

devant le jury composé de :

Rapporteurs
Abdelmejid Bayad, Maître de Conférences HDR, Université Paris-Saclay
Nigel Byott, Professeur, Université d'Exeter (Angleterre)
Bruno Deschamps, Professeur, Le Mans Université

Examinateurs
Philippe Cassou-Noguès, Professeur, Université de Bordeaux
Pierre Dèbes, Professeur, Université de Lille
Aziz El Kacimi, Professeur, Université Polytechnique Hauts-De-France

Directeur
Bouchaïb Sodaïgui, Professeur, Université Polytechnique Hauts-De-France

Avant-Propos

Ce mémoire comprend deux parties. La première est consacrée à une présentation détaillée de mon CV. La seconde est une synthèse de mes articles publiés dans différentes revues depuis la fin de ma thèse de Doctorat. Pour un exposé complet, incluant démonstrations et détails techniques, on pourrait consulter les articles mentionnés ci-dessous.

La liste complète de mes articles se trouve dans la section 1.4.1 de mon CV. Voici les travaux présentés dans ce rapport :

– **Autour d'un théorème de Stein,** *Extracta Math.,* 23(2) (2008), 173–180.
– **Irréductibilité et spécialisation des polynômes,** *Port. Math.,* 65(3) (2008), 339–343
– **Irreducibility of hypersurfaces,** *Comm. Algebra,* 37(6) (2009), 1884–1900. [Avec A. Bodin et P. Dèbes].
– **Indecomposable polynomials and their spectrum,** *Acta Arith.,* 139(1) (2009), 79–100. [Avec A. Bodin et P. Dèbes].
– **Indecomposability of polynomials via jacobian matrix,** *J. Algebra,* 324(1) (2010). [Avec G. Chèze].
– **Noether's forms for the study of non-composite rational functions and their spectrum,** avec L. Busé et G. Chèze, *Acta Arith.,* 147(3) (2011), 217–231.
– **Indecomposability of multivariate polynomials over finite extensions,** *Intern. J. Algebra,* 5(8) (2011), 309–314.
– **Families of polynomials and their specializations,** *J. Number Theory,* 170 (2017), 390–408. [Avec A. Bodin et P. Dèbes].
– **The Schinzel Hypothesis for Polynomials,** *Trans. Amer. Math. Soc.,* 373(12) (2020), 8339-8364 . [Avec A. Bodin et P. Dèbes].
– **The spectrum of a rational function,** *Algebra Colloq.,* 27(3) (2020), 477–482.
– **Prime and coprime values of polynomials,** *Enseig. Math.,* 373(1-2) (2020), 173–182 [Avec A. Bodin et P. Dèbes].
– **The Hilbert-Schinzel specialization property,** *J. Reine Angew. Math.* (2022), à paraître. [Avec A. Bodin et P. Dèbes et J. Koenig].

Table des matières

1. Curriculum Vitae 4
1.1. Parcours Professionnel 4
1.2. Parcours académique 4
1.3. Activités d'Enseignement 5
1.4. Activités de Recherche 6
2. Synthèse des travaux de recherche 11
2.1. Introduction - Thème de recherche 11
2.2. Résultats de ma thèse 13
2.3. Déformation d'un polynôme 13
2.4. Indécomposabilité d'un polynôme 17
2.5. Spectre d'un polynôme 21
2.6. Indécomposabilité d'une fraction rationnelle 22
2.7. Spectre d'une fraction rationnelle 23
2.8. Fixer à l'avance des valeurs spectrales d'une fraction rationnelle 24
2.9. La propriété de la conservation d'irréductibilité d'un polynôme après spécialisation 24
2.10. Nombres premiers et polynômes irréductibles 26
Références 32

1. Curriculum Vitae

Etat-civil et coordonnées

- *Date et lieu de Naissance :* 01 janvier 1974 à Khouribga
- *Nationalité :* Marocaine
- *Adresse professionnelle :* Faculté Polydisciplinaire de Khouribga, Université Sultan Moulay Slimane ; BP.145, Hay Ezzaytoune, Khouribga, Maroc.
- *Tél :* (00212) 0622846758
- *E-mail :* slhnajib@gmail.com

1.1. **Parcours Professionnel.** • **Depuis** 2014 **:** Maître de conférences, Université Sultan Moulay Slimane,
Faculté Polydisciplinaire de Khouribga (FPK).

• **2010 – 2014 :** Professeur Assistant d'Enseignement Supérieur, Faculté Polydisciplinaire de Khouribga.
• **2009 – 2010 :** Enseignant contractuel, IUT du Limousin, Brive.
• **01 Mars 2008 – 31 Août 2009 :** Position chercheur, Université de Lille 1.
• **01 Janvier – 29 Février 2008 :** Séjour de recherche, Institut de Max-Planck, Bonn, Allemagne.
• **05 Septembre 2006 – 04 Décembre 2007 :** Séjour post-doctoral, Abdus Salam International Center of Theoritical Physics (ICTP), Trieste, Italie.
• **Septembre 2005 – Août 2006 :** Position chercheur, Université de Lille 1.
• **2004 – 2005 :** Attaché temporaire à l'enseignement et la recherche (ATER, mi-temps), Université de Lille 1.
• **2003 – 2004 :** Attaché temporaire à l'enseignement et la recherche (ATER, temps plein), Université de Lille 3.
• **2001 – 2003 :** Tutorat et Vaccations de Mathématiques, Universités de Lille 1 et Lille 3.

1.2. **Parcours académique.** • **2001 – 2005 :** Thèse de Doctorat de Mathématiques Pures, Université de Lille 1 :
"Factorisation des polynômes $P(X_1, \ldots, X_n) - \lambda$
et théorème de Stein". Soutenue le *18 Mars 2005*.
Sous la direction de Mohamed Ayad et Pierre Dèbes ;
• **2000 – 2001 :** D.E.A. de Maths Pures, Université de Lille 1.

• **1994 – 1999 :** Licence et maîtrise de Mathématiques,
Université Chouaïb Doukkali, El Jadida, Maroc.

1.3. **Activités d'Enseignement.**

1.3.1. **Enseignements effectués. Cours enseignés :**
– Topologie (SMA, S5) ;
– Analyse des données (SMI, S5)
– Algèbre 1 (SMPC, S1) ;
– Algèbre 2 (SMPC, S2) ;
– Algèbre 3 (SMIA, S2) ;
– Algèbre 5 (SMA, S4) ;
– Arithmétique des Polynômes ; Master d'Analyse Mathématique Avancé, (S2, FST de Béni-Mellal) ;
– Introduction à la Théorie de Galois ; Master de Mathématiques et leurs Applications (S2, FP de Khouribga).

1.3.2. Production pédagogique

• **Polycopies : exercices corrigés, examens corrigés**
– Examens et contrôles corrigés d'Algèbre 1 SMPC (S1) ; édition 2016 ;
– Examens et contrôles corrigés d'Algèbre 1 SMPC (S1) ; édition 2019 ;
– Exercices corrigés d'Algèbre 3 SMIA (S2) ;
– Exercices corrigés d'Algèbre SEG (S2).

• **Polycopies cours**
– Cours d'Algèbre 3 SMIA(S2) ;
– Cours d'Algèbre 2 SMPC (S2) ;
– Cours d'Algèbre 5 SMA (S4) ;
– Cours d'Arithmétique des polynômes ; Master d'Analyse Mathématique
Avancé (S2, FST Béni-Mellal) ;
– Cours d'Introduction à la Théorie de Galois ; Master de Mathématiques
et leurs Applications (S2, FP Khouribga).

1.3.3. Projets de Fin d'étude Master co-encadrés

– 03 projets pour les étudiants du Master Matière et Rayonnement (FP Khouribga, soutenus en Octobre 2020).
(*Co-encadrés avec Abdellatif Hassnaoui et Khalid Sbai*).

– 01 projet pour les étudiants du Master d'Analyse Mathématique Avancé (FST Béni-Mellal, soutenu en Septembre 2018).
(Co-encadré avec Said El Baghdadi).
– 01 projet pour les étudiants du Master de Mathématiques et leurs Applications (FP Khouribga, soutenu en Octobre 2021).
(*Co-encadré avec Khalid Iskafi*).

1.4. **Activités de Recherche.**

1.4.1. *Publications.* • **Articles parus ou à paraître :**

1. *The Hilbert-Schinzel specialization property.*
J. Reine Angew. Math., 2022, à paraître.
[Avec A. Bodin, P. Dèbes et J. Koenig].
2. *The Schinzel Hypothesis for Polynomials.*
Transactions of the American Mathematical Society,
Vol. 373, Number 12 (2020), 8339–8364.
[Avec A. Bodin et P. Dèbes].
3. *The Spectrum of a Rational Function.*
Algebra Colloquium 27 : 3 (2020) 477–482.
4. *Prime and coprime values of polynomials.*
L'Enseignement Mathématique (2) 66 (2020), 169–182.
[Avec A. Bodin et P. Dèbes].
5. *Families of polynomials and their specializations.*
J. Number Theory, Vol. 170 (2017), 390–408.
[Avec A. Bodin et P. Dèbes].
6. *Indecomposability of multivariate polynomials over finite extensions.* International J. of Algebra,
Vol. 5, (2011), no. 7, 309–314.
7. *Noether's forms for the study of non-composite rational functions and their spectrum.* Acta Arith. 147(3) (2011), 217–231.
[Avec L. Busé et G. Chèze].
8. *Indecomposability of polynomials via jacobian matrix.*
J. of Algebra 324(1) (2010), 1–11. [Avec G. Chèze].
9. *Indecomposable polynomials and their spectrum.*
Acta Arith. 139 (2009), 79–100. [Avec A. Bodin et P. Dèbes.]
10 *Irreducibility of hypersurfaces.*
Comm. in Algebra , Volume 37, Issue 6 (2009), 1884–1900.
[Avec A. Bodin et P. Dèbes].
11. *Autour d'un théorème de Stein.*

Extracta Math. 23(2) (2008), 173–180.
12. *Irréductibilité et spécialisation des polynômes.*
Portugal. Math. (N.S.) Vol. 65, Fasc. 3, (2008), 339–343.
13. *Un raffinement du caractère hilbertien du corps $K(X)$.*
Manuscripta Math. 120, no. 4, (2006), 415–418.
14. *Une généralisation de l'inégalité de Stein-Lorenzini.*
J. of Algebra, 292, No. 2 (2005), 566–573.
15. *Sur le spectre d'un polynôme à plusieurs variables.*
Acta Arithmetica, 114, No. 2 (2004), 169–181.

• **Preprints et articles en préparation :**
1. *A note on the spectrum of a rational function.* Soumis.
[Avec Mohammed Benelmekki].
2. *Indécomposable univariate polynomials.*
[Avec Mohammed Benelmekki et Bouchaïb Sodaïgui].

1.4.2. Conférences – Communications Orales

• **02 – 03 Novembre 2021 :** *Des entiers vers les polynômes.*
Colloque "Journées de Théorie des Nombres et Cryotographie de Valenciennes", Université Polytechnique Hauts-De-France.
• **28 – 29 Février 2020 :** *Spectre d'une fraction rationnelle.*
"3^{nd} International Conference on Mathematics and its Applications (ICMACASA 2020)", Faculté des Sciences Ain Chock, Casablanca.
• **29 – 30 Mars 2019 :** *The finiteness of the ring of constants problem.* "1^{st} International Conference on Research in Applied Mathematics and Computer Sciences (ICRAMCS 2019)", Faculté des Sciences Ben M'Sick, Casablanca.
• **02 – 05 Juillet 2018 :** *Constructing indecomposable rational function with prescribed Spectrum.*
"International Conference on Algebra and Related Topics (ICART)", Université de Mohamed V, Rabat.
• **03 – 07 Juillet 2017 :** *Reduction and Specialization of a Polynomials Family.* "30èmes Journées Arithmétiques", Université de Caen.
• **26 – 27 Décembre 2018 :** *"Les 3èmes Journées d'Algèbre et de Géométrie".* Faculté des Sciences, Kenitra.
• **23 – 25 Juin 2010 :** "21èmes Rencontres Arithmétiques Université de Caen".
• **06 – 10 Juillet 2009 :** "26èmes Journées Arithmétiques", Université de Saint-Etienne.

- **23 – 28 Juin 2008 :** "5th International Fez Conference on Commutative Algebra and Applications", Fez.
- **27 – 31 Août 2007 :** "18th Czech and Slovak International Conference on Number Theory Congress Center of the Slovak Academy of Sciences", Smolenice.
- **02 – 06 Juillet 2007 :** "25èmes Journées Arithmétiques", Edinburgh.

1.4.3. Participation à des conférences sans communication orale

- **30 Juin – 04 Juillet 2009 :** Activités additives et Analytiques, Université de Lille 1.
- **09 – 26 Juillet 2007 :** Summer School and Conference on Automorphic Forms and Shimura Varieties, Institut ICTP.
- **14 – 25 Mai et 28 Mai – 01 Juin 2007 :** School and Conference on Algebraic K -Theory and its Applications, Institut ICTP.
- **23 Avril – 11 Mai 2007 :** School and Conference on Analytic Number Theory, Institut ICTP.
- **09 – 27 Octobre 2006 :** School and Conference on Nolinear Differential Equations, Institut ICTP.
- **22 – 23 Juin 2006 :** Conférence "Approximation and Iterative Methods", Université de Lille 1.
- **15 – 17 Juin 2006 :** Conférence "Théorie des nombres et analyse harmonique", Université de Lille 1.
- **05 – 11 Février 2006 :** Conférence "The Arithmetic of Fields", Oberwolfach (Allemagne).

1.4.4. Exposés à des séminaires

- **16 Mai 2014 :** Séminaire de mathématique, Faculté des Sciences et Techniques, Béni-Mellal (Maroc).
- **01 Avril 2010 :** Séminaire calcul formel, Limoges.
- **09 Novembre 2009 :** Séminaire Théorie des Nombres, Limoges.
- **28 Janvier 2008 :** Séminaire Galois - und Zahlentheorie, Universität Düsseldorf.
- **23 Janvier 2008 :** Séminaire Number theory lunch, Institut Max Planck, Bonn.
- **20 Septembre 2007 :** Séminaire d'Arithmétique, Lille 1.
- **26 Juin 2007 :** Séminaire de Mathématique, Institut ICTP.
- **20 Juin 2007 :** Séminaire d'Algèbre, Univ. Udine (Italie)
- **20 Février 2007 :** Institut de Mathématiques, Toulouse 2.
- **26 Septembre 2006 :** Séminaire de Mathématique, Institut ICTP.

- **24 Mars 2006 :** Séminaire de Théorie des Nombres, Caen.
- **06 Juin 2005 :** Séminaire de Théorie des Nombres, Amiens.
- **08 Aril 2005 :** Séminaire de Théorie des Nombres, Bordeaux 1.
- **07 Aril 2005 :** Séminaire de Théorie des Nombres, Toulouse 2.
- **21 Mars 2005 :** Séminaire de Théorie des Nombres, Limoges.

1.4.5. Quelques séjours de recherche

- **01 – 31 Octobre 2018 :** Laboratoire Paul Painlevé, Université de Lille 1.
- **12 Juin – 12 Juillet 2014 :** Laboratoire Paul Painlevé, Université de Lille 1.
- **Durant Janvier 2008 :** Universität Düsseldorf.
- **Durant Juillet 2007 :** B-IT Bonn-Aachen International Center for Information Technology Department of Computer Security, Bonn.
- **Durant Juin 2007 :** Université Udine.
- **Durant Février 2007 :** Équipe Algorithmes, Institut de Mathématiques, Toulouse.

1.4.6. Encadrements de Thèse de Doctorat

- L'étudiant Mohamed Benelmekki (*Thèse en cours :*) *"Décomposition et irréductibilité des polynômes à plusieurs indéterminées".* (*Co-encadré avec Said EL Baghdadi*).

1.4.7. Jury de Thèses

- Thèse de Brahim Boulayat (*soutenue en Octobre 2021*) : *"La propriété de Schreier et factorisation dans les anneaux de semi-groupes".* FST Béni-Mellal.
- Thèse de Abdelhadi Hachlaf (*soutenue en Octobre 2020*) : *"Modélisation mathématique et analyse numérique de quelques problèmes de contact avec frottement en thermo-piézoélectricité".* FP Khouribga.

1.4.8. Contribution à l'organisation d'activités de rayonnement de l'établissement

- **04–09 Mai 2022 :** Membre organisateur de la Conférence internationale "Arithmetic and Polynomials", Laboratoire Paul Painlevé, Univ. de Lille 1.
- **09 – 13 Novembre 2021 :** Membre organisateur de l'École

internationale IBRO School 2021, FP Khouribga.
• **15 – 19 Juin 2019 :** Membre organisateur de l'École internationale IBRO School 2019, FP Khouribga.
• **13 – 17 Mai 2015 :** Membre organisateur de l'École internati-onale IBRO School 2015, FP Khouribga.
• **20 Mai 2017 :** Membre organisateur de la Journée Scientifique "Méthodes numériques et aide à la décision", FP Khouribga ;
• **25 Mai 2016 :** Membre organisateur de la Journée Scientifique "Mathématiques et Applications", FP Khouribga.

Rapporteur/Reviewer

- *Reviewer* pour Zentralblatt MATH. *(depuis 2007).*
- *Reviewer* pour American Mathematical Society "MathScinet" *(depuis 2016).*

Autres

• Admissible à l'écrit du Concours d'Agrégation Externe de Mathématiques (France). Session 2012.
• Qualifications (France) pour le corps maître de conférences. Section 25- Mathématiques, Campagnes 2006 et 2010.

2. Synthèse des travaux de recherche

2.1. **Introduction - Thème de recherche.** Dans cette synthèse, les corps sont commutatifs. Dans toute la suite, $\mathbb{K}$ désigne un corps commutatif.

Mes travaux concernent l'arithmétique des corps et des polynômes, notamment la réductibilité et la décomposabilité de ces derniers.

Un polynôme est décomposable sur un corps s'il peut s'écrire non trivialement comme composé de deux polynômes à coefficients dans ce corps. Comme la propriété soeur de réductibilité, il s'agit d'une propriété de base qui pose de nombreuses questions : critères, invariance par morphisme (en particulier par réduction modulo un premier p), comptage, etc. Une littérature importante est consacrée à ce sujet, citons par exemple les travaux de Ruppert, Stein, Cygan, Vistoli et Lorenzini.

Plus précisément, soit $P(\underline{x}) := P(x_1, \ldots, x_n)$, $n \geq 2$, un polynôme non constant en les indéterminées (qu'on appellera parfois variables) $x_1, \ldots, x_n$ à coefficients dans $\mathbb{K}$; $P(\underline{x})$ est dit *décomposable* sur $\mathbb{K}$ s'il existe deux polynômes $H(\underline{x}) \in \mathbb{K}[\underline{x}]$ et $u(t) \in \mathbb{K}[t]$ de degré ≥ 2 tels que $P(\underline{x}) = u(H(\underline{x}))$; dans le cas contraire, P est dit *indécomposable*.

L'ensemble des valeurs λ appartenant à une clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$ pour lesquelles le polynôme $P - \lambda$ est réductible sur $\overline{\mathbb{K}}$ est appelé le *spectre* de P ; on le note $Sp(P)$. Cet ensemble est un objet central de mes travaux.

La notion d'indécomposabilité est classiquement liée à celle du spectre d'un polynôme. Une première information qu'on obtient à partir du théorème de Bertini-Krull est : si P est indécomposable sur $\overline{\mathbb{K}}$, alors l'ensemble $Sp(P)$ est fini. En 1989, Stein a donné une première majoration du cardinal de $Sp(P)$ dans la situation où le corps de base $\mathbb{K}$ est algébriquement clos, non dénombrable et de caractéristique nulle. De façon précise, il a montré que si $P(x, y)$ est indécomposable sur $\mathbb{K}$, alors $\mathrm{card}(Sp(P)) \leq \deg(P) - 1$; géométriquement : si $P(x, y)$ est indécomposable sur $\mathbb{K}$, alors le nombre de fibres réductibles du polynôme P est $\leq \deg(P) - 1$.

En 1992, Cygan a étendu l'inégalité de Stein sur $\mathbb{K} = \mathbb{C}$ au cas d'un nombre $n \geq 2$ quelconque d'indéterminées (par réduction au cas $n = 2$). Dans la même année, Kaliman a développé l'interprétation géométrique ci-dessus du résultat de Stein sur $\mathbb{K} = \mathbb{C}$ et pour le cas de deux indéterminées ($n = 2$). Le résultat de Kaliman donne une première amélioration de la borne démontrée par Stein.

Un peu plus tard, en 1993, Vistoli a prouvé le résultat dans le cas d'un corps algébriquement clos de caractéristique nulle et $n \geq 2$. En 1993, Lorenzini a considéré d'une part, pour la première fois le cas de caractéristique quelconque, pour $n = 2$; il a donné d'autre part une deuxième amélioration de la borne qui figure dans l'inégalité originale.

Notons que si $P(\underline{x}) \in \mathbb{K}[\underline{x}]$ est indécomposable alors $P(\underline{x}) + t$ est irréductible dans $\overline{\mathbb{K}(t)}[\underline{x}]$, et pour toute spécialisation t^* de t dans $\mathbb{K}$, le polynôme spécialisé $P(\underline{x}) + t^*$ reste irréductible sauf peut-être pour au plus $\deg(P) - 1$ valeurs de $t^* \in \mathbb{K}$; il s'agit d'une interprétation arithmétique. Nous renvoyons à [Na4, Théorème 1.1] et les références citées dedans pour plus de détail.

Dans [BDN3], avec A. Bodin et P. Dèbes, nous avons étudié un problème plus général d'irréductibilité et spécialisation dont l'objet du spectre devient un cas particulier.

Récemment, avec A. Bodin et P. Dèbes, dans les travaux [BDN4] et [BDN5], nous avons considéré une conjecture appelée l'*hypothèse (H)*. Cette dernière a paru dans un premier temps dans le travail de Schinzel-Sierpinski [SS]. Elle concerne la primalité des valeurs d'une famille finie $(P_1, ..., P_s)$ de polynômes à coefficients entiers ; elle est toujours ouverte. Elle implique plusieurs conjectures, par exemple celle des nombres premiers jumeaux et celle de Goldbach. Nous avons étudié notamment l'analogue de cette hypothèse sur un anneau de polynômes. Puis dans la continuité de ces travaux, nous avons considéré avec J. Koenig dans [BDKN] la version *"relative"* de l'hypothèse (H), c'est-à-dire demander - sous certaines conditions - que les valeurs $P_1(n), ..., P_s(n)$ soient premiers entre eux pour une infinité de $n \in \mathbb{Z}$.

Je vais présenter ce thème en différentes sous-parties.

Après avoir donné un résumé des résultats de ma thèse de Doctorat dans §2.2, je présenterai dans la sous-partie §2.3 le problème de déformation d'un polynôme. Les travaux de Stein [St], Kaliman [Ka], Cygan [Cy], et mes articles [Na1], [Na2] concernent la perturbation du coefficient constant. Quant au problème de modifier plusieurs coefficients, il a été étudié, par exemple par Ruppert [Ru1], Lorenzini [Lo], Vistoli [Vi], Bodin [Bo1] et les auteurs de [BDN1].

La sous-partie §2.4 introduit mes contributions (seul ou en collaboration) au sujet de la décomposition d'un polynôme, notamment le critère de l'indécomposabilité d'un polynôme en utilisant son polygône de Newton, l'indécomposabilité et invariance par morphisme d'anneaux (en prticulier, l'indécomposabilité et la réduction modulo un premier p puis l'indécomposabilité et spécialisation) et l'ensemble et le nombre de polynômes indécomposables sur un corps fini.

Dans la sous-partie §2.5, je présenterai mes travaux (après le Doctorat) sur le spectre d'un polynôme. Puis les sous-parties §2.6 à §2.9 seront respectivement cosacrées à l'indécomposabilité d'une fraction rationnelle, à son spectre et à la fixation par avance d'une partie finie de ce dernier. Ensuite, dans la sous-partie §2.9 j'introduirai la propriété (à la *Bertni-Noether* et *Hilbert*) de la conservation d'irréductibilité d'un polynôme à plusieurs inéterminées après en avoir spécialisé une ou plusieurs ; plus précisément, je présenterai mon travail [Na5] et celui avec A. Bodin et P. Dèbes [BDN3] qui généralise le problème de déformation d'un polynôme.

Enfin, la dernière sous-partie sera consacrée à la présentation des récents travaux [BDN4], [BDN5] et [BDKN] qui concernent l'Hypothèse (H), notamment son analogue sur un anneau de polynômes, ses versions relative et modulaire, et une version "*entière*" du théorème d'irréductibilité de Hilbert.

2.2. **Résultats de ma thèse.** Dans [Na2], j'ai donné une nouvelle démonstration qui prouve la meilleure inégalité, celle de Lorenzini, sur un corps de caractéristique quelconque et pour un nombre $n \geq 2$ quelconque d'indéterminées ; j'ai procédé par réduction au cas $n = 2$.

Je me suis également intéressé à la question suivante : étant donné un ensemble fini $S \subset \mathbb{K}$, peut-on construire un polynôme indécomposable P dont le spectre soit l'ensemble S ? J'ai répondu par l'affirmative dans [Na1]. Plus précisément, j'ai montré qu'on peut fixer à l'avance les éléments λ du spectre ainsi que le nombre de facteurs irréductibles des $P-\lambda$, et même, dans une certaine mesure tous les facteurs irréductibles des $P - \lambda$ sauf un. Ce résultat a été établi sur un corps $\mathbb{K}$ infini, de caractéristique quelconque et pour un nombre $n \geq 2$ quelconque d'indéterminées. Pour le prouver, j'ai utilisé comme ingrédient principal le caractère "*hilbertien*" raffiné du corps $\mathbb{K}(x)$ figurant dans mon article [Na3] dont une grande partie se trouve dans ma thèse.

2.3. **Déformation d'un polynôme.**

2.3.1. **Modification du coefficient constant.** Étant donnés un corps $\mathbb{K}$ et un polynôme non constant $P \in \mathbb{K}[\underline{x}]$, modifier le coefficient constant de P revient à étudier l'irréductibilité des polynômes $(P - \lambda)_{\lambda \in \overline{\mathbb{K}}}$. À cette question sont liés l'indécomposabilité et le spectre de P. Ces deux notions étaient l'objet de plusieurs travaux comme ceux de Stein [St], Cygan [Cy] et mes articles [Na1, Na2]. Dans les lignes qui suivent, je vais présenter ma contribution [Na4].

La méthode suivie par Stein dans [St] pour montrer que "*lorsque* $\mathbb{K}$ *est algébriquement clos, non dénombrable et de caractéristique nulle, si* $P(x,y) \in \mathbb{K}[x,y]$ *est indécomposable sur* $\mathbb{K}$*, alors le nombre des valeurs* $\lambda \in \mathbb{K}$ *pour lesquelles* $P(x,y)-\lambda$ *est réductible sur* $\mathbb{K}$ *est* $\leq \deg(P)-1$," utilise la notion de "dérivation" d'une $\mathbb{K}-$algèbre, notamment quelques propriétés des noyaux de "dérivations jacobiennes" de $\mathbb{K}[x,y]$ et de leur prolongement à $\mathbb{K}(x,y)$. (Ces propriétés figurent aussi dans les travaux de Ayad [Ay] et Nowicki [Now]). Dans [Na4], j'ai repris la preuve de Stein en éliminant l'aspect "dérivation jacobienne" ; de plus, j'en ai profité pour apporter quelques autres simplifications.

2.3.2. Modification de plusieurs coefficients

Soient $\mathbb{K}$ un corps et $P, Q \in \mathbb{K}[\underline{x}]$ deux polynômes non constants premiers entre eux. L'étude de l'irréductibilité des polynômes $(P-\lambda Q)_{\lambda \in \overline{\mathbb{K}}}$ mène à une majoration du cardinal du spectre de la fraction rationnelle P/Q si elle est indécomposable. Les deux notions indécomposabilité et spectre d'une fraction rationnelle seront précisées dans §2.6 et §2.7 ci-dessous.

Dans ce contexte, j'ai considéré avec A. Bodin et P. Dèbes dans [BDN1] la déformation d'un polynôme par plusieurs monômes. Notamment, pour un polynôme $P \in K[\underline{x}]$ donné, nous avons caractérisé les monômes $Q_i \in K[\underline{x}]$ qui, pour un choix générique de $(\lambda_1, \ldots, \lambda_\ell)$, rendent le polynôme $P + \lambda_1 Q_1 + \ldots + \lambda_\ell Q_\ell$ irréductible.

2.3.2.1. Motivations et définitions

Prenons $P(x,y) = \sum_{i,j} a_{i,j} x^i y^j$ un polynôme à deux indéterminées sur $\mathbb{K}$. Fixons un indice (i_0, j_0). Nous avons montré un théorème dont j'énonce informellement un corollaire ainsi : $P(x,y) + \lambda x^{i_0} y^{j_0}$ *est irréductible pour tout* $\lambda \in \mathbb{K}$ *sauf un nombre fini et sauf des cas particuliers de* P.

Nous avons généralisé ce résultat pour un nombre quelconque fini d'indéterminées en autorisant des déformations par plusieurs monômes. Des résultats bien connus sur le cardinal d'une fraction rationnelle indécomposable nous ont permis de borner le nombre fini des valeurs λ exceptionnelles.

De plus, nous avons donné une description explicite et complète des polynômes P pour lesquels ce résultat n'est pas vrai. Par exemple : si $P(x,y)$ est homogène de degré $d = i_0 + j_0$, alors $P(x,y) + \lambda x^{i_0} y^{j_0}$ est réductible pour tout $\lambda \in \mathbb{K}$.

Passons maintenant à la situation générale. Soient $\mathbb{K}$ un corps algébriquement clos de caractéristique quelconque et $P \in \mathbb{K}[\underline{x}]$, où

$\underline{x} = (x_1, \ldots, x_n)$ et $n \geq 2$. Soient $\ell \geq 1$ un entier et $Q_1, \ldots, Q_\ell \in \mathbb{K}[\underline{x}]$ des monômes de degré inférieur ou égal au degré de P. Nous supposons que les Q_i sont distincts et que $\text{pgcd}(P, Q_1, \ldots, Q_\ell) = 1$. Notons

$$\Sigma = \{(\lambda_1, \ldots, \lambda_\ell) \in \mathbb{K}^\ell \,|P+\lambda_1 Q_1+\cdots+\lambda_\ell Q_\ell \text{ est réductible dans } \mathbb{K}[\underline{x}]\}.$$

On dit que $\{Q_1, \ldots, Q_\ell\}$ est un lieu de réductibilité pour P si l'ensemble Σ contient un ouvert non vide de la topologie de Zariski sur $\mathbb{K}^\ell$.

Voici deux exemples lorsque $\ell = 1$: pour $Q_1 \in \mathbb{K}$, $\Sigma = Sp(P)$: le spectre de P ; pour $Q_1 \in \mathbb{K}[\underline{x}]$, $\Sigma = Sp(P/Q_1)$: le spectre de la fraction rationnelle P/Q_1.

Je présente maintenant les cas particuliers dont j'ai parlé ci-dessus.

Un polynôme non constant $P(\underline{x}) \in \mathbb{K}[\underline{x}]$ est dit homogène en deux monômes $m_1, m_2 \in \mathbb{K}[\underline{x}]$ s'il existe $h \in \mathbb{K}[u, v]$ homogène de degré ≥ 2 tel que

$$P = h(m_1, m_2).$$

Si de plus la fraction m_1/m_2 est indécomposable, on dira qu'une telle décomposition est maximale.

Si P est homogène en deux monômes, alors il existe une décomposition maximale ; cela revient à exiger que le degré de h est maximal parmi toutes les décompositions homogènes en deux monômes. Par exemple, $P(x, y, z) = x^6 - (yz)^4 = h(x, yz)$, où $h(u, v) = u^6 - v^4$, est une décomposition maximale en deux monômes.

Si $P = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$ admet une décomposition homogène en deux monômes, alors le *support* de P

$$\text{supp}(P) = \{(i_1, \ldots, i_n) \in \mathbb{Z}^n \mid a_{i_1,\ldots,i_n} \neq 0\}$$

est inclus dans une droite de $\mathbb{Z}^n$.

2.3.2.2. Quelques énoncés

Soit $P \in \mathbb{K}[\underline{x}]$ qui n'est pas un monôme, ni une puissance pure dans $\mathbb{K}[\underline{x}]$ (c'est-à-dire, il n'existe pas $S \in \mathbb{K}[\underline{x}]$ et un entier $e > 1$ tels que $P = S^e$).

1) **Quels sont les lieux de réductibilité ?**

(1.1) Si P est homogène en deux monômes et $P = h(m_1, m_2)$ est une décomposition maximale, où m_1, m_2 sont deux monômes et h homogène de degré $d \geq 2$, alors les lieux de réductibilité sont les parties de

$$\{m_1^k m_2^{d-k},\ 0 \leq k \leq d \text{ et } deg(m_1^k m_2^{d-k}) \leq deg(P)\}.$$

(1.2) Si P n'est pas homogène en deux monômes, alors les seuls lieux possibles de réductibilité sont des singletons ($\ell = 1$) de la forme

$$\{m^k\},$$

où m est un monôme premier avec P et $k \geq 2$.
Que se passe-t'il si $\{Q_1, \ldots, Q_\ell\}$ n'est pas un lieu de réductibilité pour P ?

Pour les autres cas, $\{Q_1, \ldots, Q_\ell\}$ n'est pas un lieu de réductibilité pour P et Σ est inclus dans un fermé propre de Zariski. De plus, pour toutes valeurs $\lambda_i, 1 \leq i \leq \ell$, sauf au plus $\deg(P)^2 - 1$ valeurs, $P + \lambda_1 Q_1 + \cdots + \lambda_\ell Q_\ell$ est irréductible.

Remarques :
(1) Dans le cas où le polynôme $P(\underline{x})$ est un monôme et une puissance pure dans $\mathbb{K}[\underline{x}]$, les lieux de réductibilité de P sont aussi décrits dans [BDN1].
(2) Nous avons vu que si $supp(P)$ n'est pas inclus dans une droite, alors nous sommes dans la situation (1.2). Si de plus $\ell \geq 2$, alors nous sommes directement dans la situation 2).

Comme conséquences, on peut citer :

Le polynôme $P(\underline{x}) + \lambda_1 x_1 + \ldots + \lambda_n x_n$ est irréductible pour des valeurs génériques de $\lambda_1, \ldots, \lambda_n$.

Le polynôme $P(\underline{x}) + \lambda Q(\underline{x})$ est irréductible pour toutes sauf $\deg(P)^2 - 1$ valeurs de $\lambda \in \mathbb{K}$ dans les situations suivantes :
(1) $P \notin \mathbb{K}[x_1]$ et non divisible par x_1, et $Q = x_1$.
(2) P n'est pas divisible par $x_1 x_2$ et $Q \in \{x_1, x_2\}$.
(3) $n = 2$, $P(x, y) \in \mathbb{K}[x, y]$ est homogène de degré $d \geq 2$ mais n'est pas une puissance pure, et $Q = x^i y^j$ est un monôme de degré $i + j < d$ avec $pgcd(P, Q) = 1$.

Pour prouver ces corollaires nous avons utilisé aussi les énoncés dans lesquels P est un monôme ou une puissance pure.

Remarque : on note aussi qu'il y a la contre partie topologique du problème de déformation ; citons par exemple les travaux : [AHS], [BT] et [LR].

2.4. **Indécomposabilité d'un polynôme.** Rappelons qu'on dit q'un polynôme non constant $P(\underline{x}) \in \mathbb{K}[\underline{x}]$ est *décomposable* sur $\mathbb{K}$ s'il existe deux polynômes $H(\underline{x}) \in \mathbb{K}[\underline{x}]$ et $u(t) \in \mathbb{K}[t]$ de degré ≥ 2 tels que $P(\underline{x}) = u(H(\underline{x}))$; sinon, P est dit *indécomposable*.

Il y a eu beaucoup de travaux dont l'objet était de donner des critères ou étudier l'invariance par homomorphisme (notamment spécialisation et réduction modulo un premier p) d'irréductibilité (absolue) d'un polynôme ; citons par exemple ceux de Bertini [Be], Noether [No], Krull [Kr], Ostrowski [Os], Fried-Jarden [FJ], Kaltofen [Kal], Ruppert [Ru2], Zannier [Za], Gao [Ga] et Gao-Rodrigues [GR]. De plus, il est bien connu qu'un "*un polynôme absolument irréductible (c'est-à-dire irréductible sur une clôture algébrique) est indécomposable*" ; motivé par ce lien, dans [CN], j'ai étudié avec G. Chèze des analogues de célèbres théorèmes sur l'irréductibilité absolue dans le cas de l'indécomposabilité tout en donnant un critère - assez géométrique - de cette dernière notion.

2.4.1. Critères d'indécomposabilité

On appele *polygône de Newton* du polynôme P, et l'on note $N(P)$, l'envelope convexe de $supp(P) \cup \{(0, \ldots, 0)\}$. Dans [CN], nous avons démontré :

Soient $P, H \in \mathbb{K}[\underline{x}]$ et $u \in \mathbb{K}[t]$ tels que $P = u \circ H$. Si $(i_1, \ldots, i_n)$ est un sommet de $N(P)$, alors on peut écrire $(i_1, \ldots, i_n) = (r.j_1, \ldots, r.j_n)$, avec $r = \deg(u)$ et $(j_1, \ldots, j_n)$ est un sommet de $N(H)$.

À l'aide de ce résultat, on peut tester si un polynôme P est décomposable ou non :

Soint $P \in \mathbb{K}[\underline{x}]$ un polynôme non constant et $({i_1}^{(j)}, \ldots, {i_n}^{(j)})$, $1 \leq j \leq k$, les sommets de $N(P)$. Si $pgcd({i_l}^{(j)}, 1 \leq l \leq n, 1 \leq j \leq k) = 1$, alors P est indécomposable.

Remarque : si on n'ajoute pas $(0, 0, \ldots, 0)$ au $supp(P)$, l'énoncé de notre critère est faux. En effet, considérons $H(x, y) = x^4y^2 + x^5y^5 + x^2y$ et $P(x, y) = H^2 - H$. Alors $(2, 1), (8, 4), (10, 10), (5, 5)$ sont les sommets de $N(P)$ et $pgcd(2, 1, 8, 4, 10, 5) = 1$, cependant P est décomposable.

Signalons que d'autes critères d'indécomposabilité sont aussi présentés dans les articles [BDN2] (à la *critère d'Eiseinstein pour l'irréductibilité*), [Bo2] et [Na6].

2.4.2. Indécomposabilité et invariance par homomorhpisme

Dans cette sous-section, j'introduis la conservation de l'indécomposabilité d'un polynôme par application d'un homomorphisme d'anneaux, en particulier : la réduction modulo p *"effective"* à la *Ostrowski* et la spécialisation à la *Bertini-Noether* ([FJ], [Sc]).

2.4.2.1. Indécomposabilité et réduction modulo p

L'étude de l'indécomposabilité d'un polynôme après réduction modulo un entier premier p était motivée d'une part par le lien "absolue irréductible, indécomposable", et d'autre part par le théorème d'Ostrowski [Os] et ses versions effectives qui étaient l'objet de plusieurs travaux comme ceux de Ruppert [Ru2], Zannier [Za] et Gao-Rodrigues [GR].

Cette étude était l'un des thèmes de nos articles [BDN2] et [CN].

Étant donné $P(\underline{x}) \in \mathbb{K}[\underline{x}]$ un polynôme non constant, on note :

• $D = \text{pgcd}(i_1^{(1)}, \ldots, i_n^{(1)}, \ldots, i_1^{(k)}, \ldots, i_n^{(k)})$, où $(i_1^{(\alpha)}, \ldots, i_n^{(\alpha)})$, $1 \leq \alpha \leq k$, sont les sommets de $N(P)$,

• D_{min} le plus petit diviseur premier de D,

• $N(P)_{D_{min}}$ le polygône de sommets $(\frac{i_1^{(\alpha)}}{D_{min}}, \ldots, \frac{i_n^{(\alpha)}}{D_{min}})$, $1 \leq \alpha \leq k$.

Dans [CN], nous avons montré la version effective suivante.

Soient $P = \sum_{i,j} c_{i,j} x^i y^j \in \mathbb{Z}[x, y]$ *un polynôme indécomposable de degré* d *et* $H(P) =: \max_{i,j} |c_{i,j}|$ *la hauteur de* P.

Si $D = 1$, *alors pour tout premier* $p > H(P)$ *le polynôme réduit* $\tilde{P}$ *de* P *modulo* p *est indécomposable.*

Si $D \neq 1$, *alors* $\tilde{P}$ *est indécomposable pour tout premier* p *tel que* $p > \max[\frac{d^2}{d_{min}}, (\frac{d^2}{D_{min}} ||P||_2)^{T'}]$, *où* T' *est le nombre de points entiers dans* $N(P)_{D_{min}}$.

Dans cette direction, une certaine variante a été présentée dans [BDN2, Theorem 3.1].

2.4.2.2. Indécomposabilité et spécialisation

Le thème de ce paragraphe sera présenté en lien avec le spectre d'un polynôme dans le paragraphe §2.5 ci-dessous.

2.4.3. Indécomposabilité et extension de corps

Lorsque la caractéristique de $\mathbb{K}$ est nulle, l'équivalence suivante est bien connue : $P(\underline{x})$ *est indécomposable sur* $\mathbb{K} \Leftrightarrow P(\underline{x})$ *est indécomposable sur toute extension de* $\mathbb{K}$. Cette dernière est fausse en caractéristique positive (voir par exemple [Ay]).

Dans cette section, nous allons étudier cette équivalence dans le cas de caractéristique positive. En particulier, préciser les polynômes pour lesquels elle n'est pas vérifiée.

Dans [BDN2], nous avons montré :

Soit $E/\mathbb{K}$ une extension algébrique, purement inseparable et de caractéristique $p > 0$. Soit $P(\underline{x}) \in \mathbb{K}[\underline{x}]$. Supposons que $P(\underline{x})$ ne soit pas de la forme $bG(\underline{x}) + c$, où $G(\underline{x}) \in E[\underline{x}]$ et $b, c \in \mathbb{K}$. Alors, $P(\underline{x})$ est indécomposable sur $\mathbb{K}$ si et seulement s'il est indécomposable sur E.

Remarques :
(1) L'analogue de ce résultat sans aucune condition sur $P(\underline{x})$, mais pour une extension E/K purement séparable, a été demontré par Arzhan tsev-Petravchuk dans [AP]. De plus, comme toute extension est une extension algébrique purement inséparable d'une certaine extension purement séparable, nous avons précisé ce résultat dans [BDN2].
(2) *Cas d'une seule indéterminée :* si on adopte la définition ci-dessus d'un polynôme décomposable, alors tout polynôme en une seule indéterminée de degré ≥ 2 est décomposable. On la modifie par la définition suivante : $P(x) \in \mathbb{K}[x]$ est dit *strictement décomposable* sur $\mathbb{K}$ si $P(x) = u(H(x))$, où $H(x) \in \mathbb{K}[x]$ et $u(t) \in K[t]$ avec $\deg(u) \geq 2$ et $\deg(H) \geq 2$. Ce cas à été étudié par exemple dans [Ri1, Ri2], [Fr2], [DF], [FM], [AA], [Na1], [DG], [Gu] et [BCD].
(3) En utilisant la notion de stricte décomposabilité, nous avons aussi caractérisé dans [BDN2] les polyñomes d'une seule indéterminée dont l'équivalence en question n'est pas vérifiée.

Une certaine variante du problème "indécomposabilité et extension de corps" a été considérée dans [Na6]. Plus précisément, étant donnés $\mathbb{K}$ de caractéristique nulle et $L/\mathbb{K}$ une extension finie de degré ≥ 2, un polynôme $P \in L[\underline{x}]$ est dit $(L - \mathbb{K})-$décomposable s'il existe deux polynômes $Q \in \mathbb{K}[\underline{x}]$ et $u(t) \in L[t]$ de degré ≥ 2 tels que $P(\underline{x}) = u(Q(\underline{x}))$. Il est évident que si $P \in L[\underline{x}]$ est $(L-\mathbb{K})-$décomposable, alors P est $L-$décomposable. Par contre, la réciproque n'est pas toujours vraie (par exemple, $\mathbb{K} = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ et $P(x, y) = (y + x\sqrt{2})^2$). Entre autres, j'ai démontré dans [Na6] :

Il existe une infinité de valeurs $a \in L$ tels que $P(\underline{x}) - a$ possède un diviseur non constant dans $\mathbb{K}[\underline{x}]$ si et seulement si P est $(L - \mathbb{K})-$décomposable. De plus, si P n'est pas $(L-\mathbb{K})-$décomposable, alors le nombre de telles valeurs a est $\leq \deg(P) - 1$.

2.4.4. Ensemble et nombre de polynômes indécomposables sur un corps fini

Dans cette section, les travaux [BDN2] et [CN] seront présentés.

2.4.4.1. Ensemble de polynômes indécomposables

Dans [CN], nous avons montré que l'ensemble des polynômes décomposables est inclus dans une variété algébique (*formes de Noether de l'indécomposabilité*).

En particulier, nous avons obtenu le théorème suivant.

Soient $d,\ n \geq 2$ *des entiers et* $P = \sum_{|\underline{e}|\leq d} c_{\underline{e}} x_1^{e_1} \dots x_n^{e_n} \in \mathbb{K}[\underline{x}]$ *un polynôme non constant, où* $\underline{e} = (e_1, \dots, e_n)$ *et* $|\underline{e}| = e_1 + ...e_n$. *Supposons que* $p = 0$ *ou* $p > d^2/d_{min}$, *où* p *est la caractéristique de* $\mathbb{K}$ *et* d_{min} *est le plus petit premier divisant le degré de* P. *Alors :*

P *est décomposable ou* $\deg(P) < d \iff \Big($*il existe une famille de polynômes*

$$\Phi_1, \dots, \Phi_N \in \mathbb{Z}[X_{\underline{e}}, |\underline{e}| \leq d],\ \textit{si } p = 0\ \textit{(resp. } \mathbb{Z}/p\mathbb{Z}[X_{\underline{e}}, |\underline{e}| \leq d],\ \textit{si } p \neq 0\textit{)}$$

avec les $X_{\underline{e}}$ *sont des indéterminées (dont le nombre est égal à celui des* c_e*), et* $N \geq 2$ *un entier, avec la propriété :* $\Phi_t(c_{\underline{e}}, |\underline{e}| \leq d) = 0$ *pour tout* $t = 1, \dots, N\Big)$

De plus,

$$\deg(\Phi_t) \leq 1 + \tfrac{1}{2}(\tfrac{d}{d_{min}} + 1)(\tfrac{d}{d_{min}} + 2) =: \mathfrak{B}$$

pour tout $t = 1, \dots, N$.

Remarque :

La borne $\mathfrak{B}$ donnée dans ce résultat est meilleure que celle de la factorisation absolue. Par exemple, si on a un polynôme de degré $d = 10$, alors le degré de nos formes est 22. Cependant le degré des formes de Noether de l'absolue irréductibilité est $d^2 - 1 = 99$ ([Ru1], [Sc2]). Mais on ne sait pas si notre borne $\mathfrak{B}$ est optimale.

Comme conséquence de ce résultat, avec G. Chèze, dans [CN] nous avons obtenu :

Soient $\mathbb{K}$ *un corps de caractéristique* 0 *ou* $p > d^2/d_{min}$, $P(\underline{x}) = \sum_{|\underline{e}|\leq d} c_{\underline{e}} x_1^{e_1} \dots x_n^{e_n} \in \mathbb{K}[\underline{x}]$ *et* S *un sous-ensemble fini de* $\mathbb{K}$.

Pour un choix équiprobable des $c_{\underline{e}}$ *dans* S, *la probabilité*

$$\mathbf{P}(f \textit{ est indécomposable et } \deg(f) = d \textit{ et } c_{\underline{e}} \in S) \geq 1 - \mathfrak{B}/card(S)$$

Nous avons raffiné ces résultats dans [BDN2].

2.4.4.2. Nombre de polynômes indécomposabes sur un corps fini

Pour un entier $d \geq 1$, on note N_d le nombre des éléments de $\mathbb{F}_q[\underline{x}]$ de degré $\leq d$ et I_d (resp. D_d) le nombre parmi les N_d polynômes qui sont indécomposables (resp. décomposables) de sorte que $N_d = I_d + D_d$.

Dans [BDN2], nous avons montré l'assertion suivante :

Supposons que $n = 2$. Alors, I_d/N_d tend vers 1 dans les deux situations : lorsque $d \to \infty$ avec q fixé, et quand $q \to \infty$ avec d fixé.

Remarques :

(1) En distinguant les cas $d = p$, $d = p^2$ (avec p premier), d est produit de deux premiers, et d'autres, nous avons aussi pu calculer le nombre D_d.

(2) Un résultat dans ce sens a été démontré dans [vzG] dans le cas général de n indéterminées.

(3) Sous la condition $pgcd(d, q) = 1$ et en utilisant les deux théorèmes de Ritt [Ri1, Ri2] (ou [Sc, §1.3, theorem 7] et [Sc, §1.4, theorem 8]), un résultat similaire a été donné dans [BDN2] dans le cas particulier d'une seule indéterminée ($n = 1$).

2.5. **Spectre d'un polynôme.** Soient $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$ et $P \in \mathbb{K}[\underline{x}]$ un polynôme non constant. Le spectre de P est le sous-ensemble de $\overline{\mathbb{K}}$ défini par :

$$Sp(P) = \{\lambda \in \overline{\mathbb{K}} : P(\underline{x}) - \lambda \text{ est réductible sur } \overline{\mathbb{K}}\}.$$

Je vais présenter ici nos contributions dans [BDN2] à l'invariance par homomorphisme de l'indécomposabilité et le spectre d'un polynôme, en particulier par spécialisation et réduction modulo un premier p.

Soit A un anneau intégralement clos ayant un corps de fractions parfait $\mathbb{K}$. Le résultat suivant donne une conclusion à la *Bertini-Noether.*

Soit $P(\underline{x}) \in A[\underline{x}]$ un polynôme indécomposable sur $\overline{\mathbb{K}}$. Alors, il existe un élément non-nul $h_P \in A$ tel que pour tout homomorphisme σ de A dans un corps algébriquement clos k, si $\sigma(h_P) \neq 0$, alors $\sigma(P)(\underline{x})$ est indécomposable dans $k[\underline{x}]$ et $\sigma(Sp(P)) = Sp(\sigma(P))$.

Remarque :

Une généralisation pour une fraction rationnelle (avec une version effective) a été démontrée dans [BCN] et sera présentée dans les sous-parties §2.6 et §2.7 ci-dessous.

Voici deux applications.

Situation 1. $A = \mathbb{Z}$, $\sigma : \mathbb{Z} \to \overline{\mathbb{F}_p}$ l'homomorphisme de réduction modulo un nombre premier p.

Pour tout p assez grand, le polynôme réduit $\tilde{F}(\underline{x})$ est indécomposable dans $\overline{\mathbb{F}_p}[\underline{x}]$ et $Sp(\tilde{F}) = \widetilde{Sp(F)}$.

Situation 2. $A = k[\underline{t}]$, avec k un corps algébriquement clos et $\underline{t}$ sont des indéterminées. Notons $P(\underline{t}, \underline{x})$ le polynôme $P(\underline{x})$ de notre énoncé général. En appliquant notre résultat avec $\sigma : k[\underline{t}] \to k$ l'homomorphisme de spécialisation qui envoie $\underline{t} = (t_1, \ldots, t_r)$ en un $r-$uplet $\underline{t^*} = (t_1^*, \ldots, t_r^*) \in k^r$, on obtient :

Pour tout $\underline{t^*}$ en dehors d'un fermé propre de Zariski de k^r, le polynôme spécialisé $P(\underline{t^*}, \underline{x})$ est indécomposable dans $k[\underline{x}]$, et son spectre est obtenu en spécialisant celui de $P(\underline{t}, \underline{x})$.

Remarque : Une certaine variante du problème "indécomposabilité et invariance par homomorphisme" a été considérée dans [BCD].

2.6. **Indécomposabilité d'une fraction rationnelle.** Dans ce paragraphe, je présente notre étude dans [BCN] concernant l'indécomposabilité d'une fraction rationnelle après spécialisation et réduction modulo un premier p.

Une fraction rationnelle $\mathcal{R}(\underline{x}) \in K(\underline{x})$ est dite décomposable sur $\mathbb{K}$ s'il existe deux fractions $H(\underline{x}) \in \mathbb{K}(\underline{x})$ et $u(t) \in K(t)$ de degré ≥ 2 telles que $\mathcal{R}(\underline{x}) = u(H(\underline{x}))$; sinon, $\mathcal{R}$ est dite *indécomposable.*

Convention : le degré d'une fraction rationnelle $\frac{A}{B} \in K(\underline{x})$ est $\deg(\frac{A}{B}) := \max(\deg(A), \deg(B))$.

Dans la suite, j'énoncerai quelques résultats montrés dans [BCN].

Si la caractéristique de $\mathbb{K}$ est $> \deg(\mathcal{R})^2$, alors $\mathcal{R}(\underline{x})$ $(\in \mathbb{K}(\underline{x}))$ est décomposable sur $\mathbb{K}$ si et seulement si $\mathcal{R}(\underline{x})$ est décomposable sur toute extension de K.

Soit $\mathcal{R} = P/Q \in \mathbb{Z}(\underline{x})$ une fraction rationnelle non constante, réduite et indécomposable de degré $d > 1$. Soient $H(P)$ et $H(Q)$ les hauteurs de P et Q. Alors, pour tout premier $p > \mathcal{H}$, la réduction $\tilde{\mathcal{R}}$ de $\mathcal{R}$ modulo p est indécomposable et réduite, où

$$\mathcal{H} = d^{3d^2-3}(\binom{n+d}{n} 2^d)^{d^2-1} \binom{d^2-1}{\lfloor (d^2-1)/2 \rfloor} \max(H(P), H(Q))^{d^2-1}.$$

Soient d, k deux entiers positifs et $\mathbb{K}$ un corps parfait de caractéristique 0 ou $p \geq d^2$. Soit $\mathcal{R} = P/Q \in K[\underline{Z}](\underline{x})$ une fraction rationnelle, non constante, réduite et telle que $0 < \deg_{\underline{x}}(\mathcal{R}) \leq d$, $0 < \deg_{\underline{Z}}(\mathcal{R}) \leq k$. Si $\mathcal{R}$ est indécomposable sur $K(\underline{Z})$, alors pour un choix équiprobable et uniforme des variables $z_1, \ldots, z_s$ dans un sous-ensemble fini S de K, la probabilité pour que la spécialisation $\mathcal{R}(z_1, \ldots, z_s, \underline{x})$ soit indécomposable sur $\mathbb{K}$ est $\geq 1 - k(d^2-1)/card(S)$.

2.7. **Spectre d'une fraction rationnelle.** Soient $P, Q \in \mathbb{K}[\underline{x}]$ deux polynômes non constants et premiers entre eux. Le spectre de la fraction rationnelle (réduite) $\mathcal{R} = P/Q$, est le sous-ensemble de $\overline{K}$ donné par

$$Sp(\mathcal{R}) = \{\lambda \in \overline{K} : P(\underline{x}) - \lambda\, Q(\underline{x}) \text{ est réductible sur } \overline{K}\}.$$

Comme conséquence du théorème de Bertini-Krull, on a : $\mathcal{R}$ est indécomposable si et seulement si $Sp(\mathcal{R})$ est fini. De plus, si $\mathcal{R}$ est indécomposable de degré d, alors $\text{card}(Sp(\mathcal{R})) \leq d^2 - 1$. Cette estimation est une extension de l'inégalité de Stein-Lorenzini raffinée dans [Na2]. Elle a été démontrée par Ruppert [Ru1] en caractéristique 0 et par Vistoli [Vi] pour $n \geq 3$ indéterminées, ensuite a été étendue par Lorenzini [Lo] en caractéristique quelconque (mais seulement pour $n = 2$) ; et finalement a été généralisée pour $n \geq 3$ par Bodin [Bo1]. Dans ce contexte, il y a aussi l'article [IP].

Ce paragraphe présente nos contributions dans [BCN] concernant l'invariance de ce spectre par homomorphisme, notamment par spécialisation et réduction modulo un premier p, à savoir :

Soit $\mathcal{R} = P/Q \in \mathbb{Z}(\underline{x})$. Pour tout premier $p > \mathcal{B}$, on a $Sp(\tilde{\mathcal{R}}) = \widetilde{Sp(\mathcal{R})}$, où $\mathcal{B}$ est une constante qui dépend de d et de la quantité $\mathcal{H}$ introduite ci-dessus.

Comme conséquence de ce résultat : *si $Sp(\mathcal{R}) = \emptyset$, alors $Sp(\tilde{\mathcal{R}}) = \emptyset$ pour tout premier $p > \mathcal{B}$.*

Maintenant, si on considère une fraction rationnelle $\mathcal{R} = P/Q \in k[\underline{t}](\underline{x})$, avec k un corps algébriquement clos, $\underline{t}$ des indéterminées sur

k et $\sigma : k[\underline{t}] \to k$ l'homomorphisme de spécialisation qui envoie $\underline{t} = (t_1, \ldots, t_r)$ en un $r-$uplet $\underline{t^*} = (t_1^*, \ldots, t_r^*)$, on obtient :

Supposons que $\max(\deg(P), \deg(Q)) \leq d$ *et* $\max(\deg_{\underline{x}}(P), \deg_{\underline{x}}(Q)) \leq e$. *Alors, il existe une collection finie* (ϕ_i) *de polynômes dans* $k[\underline{t}]$ *de degré* $< 2\ e(d^2-1)^2$ *vérifiant : si* $\sigma(\phi_i) \in k$ *sont non tous nuls, alors* $\sigma(Sp(\mathcal{R})) = Sp(\sigma(\mathcal{R}))$.

2.8. **Fixer à l'avance des valeurs spectrales d'une fraction rationnelle.** Dans la continuité des travaux présentés dans les sections 2.6 et 2.7, j'ai démontré dans l'article [Na7] que l'on peut fixer à l'avance certaines valeurs spectrales d'une fraction rationnelle $\mathcal{R} = P/Q$ et certains facteurs irréductibles des polynômes $P - \lambda Q$ (pour toute valeur spectrale λ). Il s'agit d'un certain analogue de la version polynômiale (spectre d'un polynôme indécomposable) présentée dans [Na1]. Plus précisément, on a l'énoncé suivant.

Soit $\mathbb{K}$ *un corps infini. Étant donnés :*
– $s \geq 1$ *un entier et* $\{t_1^*, ..., t_s^*\}$ *un ensemble fini d'éléments distincts de* $\mathbb{K}$,
– $f_1, ..., f_s$ *des polynômes de* $\mathbb{K}[\underline{x}]$ *tels que* $(f_i) + (f_j) = \mathbb{K}[\underline{x}]$ *si* $i \neq j$,
– $Q \in \mathbb{K}[\underline{x}]$ *tel que* Q *et* f_i *sont premiers entre eux pour tout* $i = 1, ..., s$.
Alors, il existe une infinité de polynômes $P \in \mathbb{K}[\underline{x}]$ *premiers avec* Q *et tels que* $P - t_i^* Q = f_i H_i$, *avec* $H_i \in \mathbb{K}[\underline{x}]$ *irréductible sur* $\mathbb{K}$ *et ne divisant pas* f_i *pour tout* $i = 1, ..., s$. *De plus, pour tout* $j = 1, ..., n-1, \deg_{x_j}(P)$ *peut être choisi assez grand, en particulier* $\deg(P) > \deg(Q)$ *et* $\deg(P) > \sum_{i=1}^{s} \deg(f_i)$.

D'une part, cet énoncé affirme que pour tout ensemble fini $\{t_1^*, ..., t_s^*\}$ d'éléments de $\mathbb{K}$, on peut construire une fraction rationnelle $\mathcal{R}$ telle que $\{t_1^*, ..., t_s^*\} \subset Sp(\mathcal{R})$; de plus on peut fixer à l'avance les facteurs irréductibles des polynômes $P - t_i^* Q$. D'autre part, il offre une réponse partielle au problème (b) soulevé dans [BDN3, §3.1.1].

Une autre variante de l'énoncé ci-dessus a été démontrée dans [BDN4, §5.5].

2.9. **La propriété de la conservation d'irréductibilité d'un polynôme après spécialisation.**

2.9.1. **Une variante à la Hilbert.** Le problème d'étudier l'irréductibilité d'un polynôme à plusieurs indéterminées (au moins deux) après en avoir spécialisé une ou plusieurs a fait l'objet de beaucoup de travaux, notamment ceux de Hilbert [Hi], Bertini [Be], Noether [No], Schmidt [Sch], Schinzel [Sc], Dèbes-Fried [DF] et Müller [Mü]. L'un des célèbre théorèmes est dû à Hilbert ; on l'appelle *le théorème d'irréductibilité de Hilbert* ([Hi, Fr1, Sc]). Dans ce contexte, j'ai étudié dans [Na5] une question qui a lien avec ce dernier après avoir donné un critère d'irréductibilité de polynômes à deux indéterminées.

Dans [BFO] le résultat suivant a été démontré : *soit $n \geq 2$ un entier premier et $n = \sum_{i=0}^{m} a_i b^i$ sa décomposition dans la base b (b entier naturel ≥ 1). Alors le polynôme $P(x) = \sum_{i=0}^{m} a_i x^i$ est irréductible dans $\mathbb{Z}[x]$.*

Dans [Na5], j'ai généralisé ce résultat pour donner un critère d'irréductibilité de polynômes à deux indéterminées.

Avant d'énoncer la généralisation commençons par un rappel. Soient $b(x) \in \mathbb{K}[x]$ et $f(x) \in \mathbb{K}[x]$ des polynômes non constants. On peut décomposer $f(x)$ dans la base $b(x)$ de la manière suivante : $f(x) = \sum_{i=0}^{m} a_i(x) b(x)^i$, où $a_m(x) \neq 0$ et $\deg(a_i) < \deg(b)$ pour $i = 0, \ldots, m$.

Dans [Na5], j'ai montré :

Soit $f(x)$ un polynôme irréductible dans $\mathbb{Q}[x]$ et $f(x) = \sum_{i=0}^{m} a_i(x) b(x)^i$ sa décomposition dans la base $b(x)$. Alors le polynôme $P(x, y) = \sum_{i=0}^{m} a_i(x) y^i$ est irréductible dans $\mathbb{Q}[x, y]$.

Ensuite, j'ai étudié la réciproque de ce dernier résultat, laquelle a un lien avec le théorème d'irréductibilité de Hilbert. J'ai obtenu :

Supposons $\mathbb{K}$ hilbertien et soit $P(x, y)$ un polynôme irréductible dans $\mathbb{K}[x, y]$. Alors il existe une infinité de polynômes $b(x) \in \mathbb{K}[x]$, avec $\deg(b) > \deg_x(F)$ et tels que $F(x, b(x))$ sont irréductibles dans $\mathbb{K}[x]$.

Remarques :

(1) On peut définir un corps hilbertien comme un corps dont le théorème d'irréductibilité de Hilbert est vérifié (par exemple $\mathbb{Q}$, $\mathbb{K}(x)$; en revanche, un corps algébriquement clos n'est pas hilbertien) ; [FJ], [Sc].

(2) La différence entre ce résultat et le caractère hilbertien de $\mathbb{K}$ est que l'indéterminée y est spécialisée dans $\mathbb{K}[x]$ au lieu de $\mathbb{K}$.

(3) Il est évident que l'énoncé de ce résultat n'est plus valable si $\mathbb{K}$ est supposé algébriquement clos.

2.9.2. Une variante plus générale

Dans un contexte plus général, certaines variantes des résultats présentés ci-dessus ont été étudiées dans [BDN3].

Soit $P(\underline{t},\underline{x}) \in \mathbb{K}[\underline{t},\underline{x}]$ un polynôme irréductible dans $\overline{\mathbb{K}(\underline{t})}[\underline{x}]$ (on dit que P est génériquement irréductible), où $\underline{t} = (t_1,...,t_s)$ et $\underline{x} = (x_1,...,x_n)$ sont des indéterminées, avec $s \geq 1, n \geq 2$. Le but principal de [BDN3] était l'étude de la réductibilité des polynômes spécialisés $P(\underline{t^*},\underline{x})$ pour $\underline{t^*} \in \mathbb{K}^s$. Ensuite, si P est génériquement irréductible, que peut-on dire de l'ensemble

$$Sp^*(P) = \{\underline{t^*} \in \mathbb{K}^s |\ P(\underline{t^*},\underline{x}) \text{ réductible dans } \mathbb{K}[\underline{x}]\} \ ?$$

Deux cas particuliers :

(a) $P = P(t,\underline{x}) = P_1(\underline{x}) - t$ avec $P_1(\underline{x}) \in \mathbb{K}[\underline{x}]$ non constant. Dans ce cas $Sp^*(P) = Sp(P)$.

(b) $P = P(t,\underline{x}) = P_1(\underline{x}) - tQ_1(\underline{x})$, avec $P_1, Q_1 \in \mathbb{K}[\underline{x}]$ non constants et premiers entre eux. Dans ce cas $Sp^*(P) = Sp(P_1/Q_1)$; de plus, $P = P_1(\underline{x}) - t$ *(resp.* $P = P_1(\underline{x}) - tQ_1(\underline{x})$*) est génériquement irréductible si et seulement si* P_1 *(resp.* P_1/Q_1*) est indécomposable.*

Dans [BDN3], entre autres, on a démontré le résultat suivant.

Soit $P(\underline{t},\underline{x}) \in \mathbb{K}[\underline{t},\underline{x}]$ *un polynôme génériquement irréductible. Supposons* $\mathbb{K}$ *de caractéristiqe nulle ou* $p > 2(\deg(F))^3$*. Alors, il existe un polynôme* $\mathcal{B}_F \in \mathbb{K}[\underline{t},\underline{x}]$ *tel que* $P(\underline{t^*},\underline{x})$ *est irréductible dans* $\mathbb{K}[\underline{x}]$ *pour tout* $\underline{t^*} \in \mathbb{K}^s$ *satisfaisant* $\mathcal{B}_P(\underline{t^*},\underline{x}) \neq 0$*.*

2.10. **Nombres premiers et polynômes irréductibles.** Récemment, motivé par le problème de l'irréductibilité des polynômes $P(t,\underline{x}) = P_1(\underline{x}) - tQ_1(\underline{x})$, en collaboration avec A. Bodin et P. Dèbes, nous avons établi un lien avec l'Hypothèse (H).

Cette hypothèse, parue et notée (H) dans le travail de Schinzel-Sierpinski [SS], est en fait une conjecture.

2.10.1. L'hypothèse (ou conjecture) (H)

(H) : *Soient* $P_1(x),...,P_s(x)$ *des polynômes irréductibles de* $\mathbb{Z}[x]$*. Supposons qu'aucun nombre premier ne divise tous les produits* $\prod_{i=1}^s P_i(n)$*,* n *parcourant* $\mathbb{Z}$*. Alors, il existe une infinité de* $n \in \mathbb{Z}$ *tels que* $P_1(n),...,P_s(n)$ *soient tous des nombres premiers.*

Cette hypothèse est toujours ouverte. En particulier, elle implique les conjectures bien connues suivantes :

– *Il existe une infinité de nombres premiers de la forme* $n^2 + 1$.

– *Il existe une infinité de nombres premiers jumeaux ; c'est-à-dire une infinité de nombres premiers p tels que $p+2$ soit aussi premier (utiliser $P_1(x) = x$ et $P_2(x) = x+2$).*

Remarque (seul cas connu de la validité de (H) : *Théorème de Dirichlet relatif à une progression arithmétique).*

Soit $P(x) = ax + b$. Si $pgcd(a, b) = 1$, alors il existe une infinité de $n \in \mathbb{Z}$ tels que les $P(n)$ soient premiers.

2.10.2. Des entiers vers les polynômes

Nous allons formuler un analogue de (H) pour les polynômes en utilisant les correspondances suivantes :

– à l'anneau $\mathbb{Z}$ correspond l'anneau $Z = \mathbb{Z}[y_1, ..., y_m] = \mathbb{Z}[\underline{y}]$,

– à la donnée $P(x) \in \mathbb{Z}[x]$ correspond $P(x, \underline{y}) \in Z[x] = \mathbb{Z}[x, \underline{y}]$,

– à la valeur $P(n)$ correspond $P(N(\underline{y}), \underline{y}) \in Z = \mathbb{Z}[\underline{y}]$, où $N(\underline{y}) \in Z$.

– à la conclusion $P(n)$ premier correspond $P(N(\underline{y}), \underline{y})$ irréductible dans $\mathbb{Z}[\underline{y}]$,

– à une infinité de $n \in \mathbb{Z}$ correspond un ensemble Zariski dense.

Version simple de (H) pour les polynômes (VS).

(VS) : *Soit $P(x, y) \in \mathbb{Z}[x, y]$ un polynôme irréductible satisfaisant $\deg_x(P) \geq 1$. Alors, il existe au moins $N(y) \in \mathbb{Z}[y]$ tel que $P(N(y), y)$ est irréductible dans $\mathbb{Z}[y]$.*

Remarques.

(1) (VS) est fausse si on exige $N(y) \in \mathbb{Z}$. Par exemple, si $P(x, y) = x(x+1) + y(x(x+1)+2)$, $P(n, y) = n(n+1)(1+y) + 2y$ est toujours divisible par 2.

(2) Si dans (VS) on remplace $\mathbb{Z}$ par le corps à deux éléments $\mathbb{F}_2$, l'énoncé obtenu est faux. En effet, on a l'exemple de Swan [Sw] : pour $P(x, y) = x^8 + y^3$, le polynôme $N(y)^8 + y^3$ est réductible dans $\mathbb{F}_2[y]$ pour tout $N(y) \in \mathbb{F}_2[y]$.

(3) De même, si l'anneau $\mathbb{Z}$ est remplacé par un corps algébriquement clos dans (VS), l'énoncé obtenu est faux.

Version plus générale.

Soient R un anneau factoriel et $Z = R[y_1, ..., y_m] = R[\underline{y}]$. On suppose que le corps des fractions $K = Frac(R)$ de R a une formule du produit et il est imparfait si $car(K) = p > 0$ (c'est-à-dire $K \neq K^p$).

Dans [BDN4], nous avons montré le résultat suivant :

Soient $P_1, ..., P_s \in R[x, \underline{y}]$ *des polynômes irréductibles tels que* $\deg_x P_i \geq 1$ *pour tout* $i = 1, ..., s$. *Alors, pour tout* $\underline{d} = (d_1, ..., d_n) \in (\mathbb{N}^*)^n$ *vérifiant* $d_1 + ... + d_n \geq \max_{1 \leq i \leq s} \deg_{\underline{y}}(P_i) + 2$, *l'ensemble* $\{N(\underline{y}) \in R[\underline{y}] \mid P_i(N(\underline{y}), \underline{y})$ irréductible dans $R[\underline{y}]$ pour tout $i\}$ est Zariski dense dans $\{M \in R[\underline{y}] \mid \deg_{y_i}(M_i) \leq d_i$ pour tout $i\}$.

Stratégie. Esquissée pour un polynôme ($s = 1$) et une indéterminée à spécialiser.

On écrit $P(x, \underline{y}) = \sum_{\underline{i}} A_{\underline{i}}(x)\underline{y}^{\underline{i}}$. On trouve une spécialisation $x = x^*$ telle que $A_1(x^*), ..., A_n(x^*)$ soient premiers entre eux dans Z, et $P(x^*, \underline{y})$ soit irréductible dans $Q[\underline{y}]$ en utilisant le théorème d'irréductibilité de Hilbert.

Remarques :

(1) D'après l'exemple de Swan ci-dessus, cet énoncé devient faux si $m = 1$ et R est remplacé par $\mathbb{F}_2$.

(2) Quelques exemples de R vérifiant les hypothèses de l'énoncé :

– $R = \mathbb{Z},\ R = \mathbb{K}[u_1, ..., u_r]$, où $r \geq 1$.

– R est un corps ayant une formule du produit et imparfait si $car(R) = p > 0$; par exemple : $R = \mathbb{Q},\ R = \mathbb{K}(u_1, ..., u_r)$ et ses extensions finies, où $r \geq 1$.

Comme corollaires du résultat précédent, on a :

(1) **Théorème de Dirichlet polynômial :**
Soit $P(x, \underline{y}) = A(\underline{y}) + xB(\underline{y}) \in R[x, \underline{y}]$, *avec* $pgcd(A, B) = 1$. *Alors, il existe des polynômes* $N(\underline{y}) \in R[\underline{y}]$ *tels que* $P(N(\underline{y}), \underline{y}) = A(\underline{y}) + N(\underline{y})B(\underline{y})$ *soient irréductibles dans* $R[\underline{y}]$.

(2) **Polynômes irréductibles "jumeaux" :**
Il existe des polynômes irréductibles $N(\underline{y}) \in R[\underline{y}]$ *tels que* $N(\underline{y}) + 2$ *soient aussi irréductibles.*

(3) **Problème de Goldbach polynômial :**
Tout polynôme non constant $Q(\underline{y})$ *peut s'écrire comme la somme de deux polynômes irréductibles* (prendre $P_1(x, \underline{y}) = x$ et $P_2(x, \underline{y}) = -x + Q(\underline{y})$).

Remarque :

Nos résultats ne couvrent pas le cas "$R = \mathbb{F}_2$ et $m \geq 2$". D'où la question : *quel est le nombre de polynômes* $N(\underline{y}) \in \mathbb{F}_2[\underline{y}]$ *tels que* $P(N(\underline{y}), \underline{y})$ *est irréductible dans* $\mathbb{F}_2[\underline{y}]$ *?* Cependant le théorème de Dirichlet est valable lorsque $R = \mathbb{F}_2$ et $m = 1$.

2.10.3. L'hypothèse (H) relative (sur $\mathbb{Z}$)

L'hypothèse (H) relative est une version modifiée de (H) (voir corollaire 1 ci-dessous).

Soient

• $P_1(x), ..., P_s(x) \in \mathbb{Z}[x]$ (où $s \geq 2$) des polynômes non nuls et premiers entre eux dans $\mathbb{Q}[X]$ (i.e, leur pgcd est 1),

• $d_n = pgcd(P_1(n), ..., P_s(n))$,

• $\mathcal{D} = \{d_n; n \in \mathbb{Z}\}$.

Avec A. Bodin et P. Dèbes, nous avons montré dans [BDN5] le résultat suivant :

La suite $(d_n)_{n\in\mathbb{Z}}$ est périodique et $\mathcal{D}$ est un ensemble fini, stable par pgcd et ppcm.

Remarque :

Ce résultat s'étend sur un anneau principal mais pas sur un anneau factoriel [BDKN, \$2.5].

Comme applications de l'énoncé précédent on a les corollaires suivants.

Corollaire 1 (L'hypothèse (H) relative).

Avec les hypothèses et notations précédentes, supposons en plus qu'aucun premier ne divise tous les entiers $P_1(n), ..., P_s(n)$, n parcourant $\mathbb{Z}$. Alors il existe une infinité de $m \in \mathbb{Z}$ tels que les entiers $P_1(m), ..., P_s(m)$ soient premiers entre eux.

En effet : l'entier d^*, défini comme étant le *pgcd* de tous les d_n, est aussi le *pgcd* de toutes les valeurs $P_1(n), ..., P_s(n)$, n parcourant $\mathbb{Z}$. Par l'hypothèse du corollaire, on a $d^* = 1$; de plus comme $\mathcal{D}$ est stable par pgcd, on a $1 \in \mathcal{D}$. Donc il existe $m \in \mathbb{Z}$ tel que $P_1(m), ..., P_s(m)$ soient premiers entre eux. En vertu de la périodicité de la suite $(d_n)_{n\in\mathbb{Z}}$, l'ensemble de tels m est infini.

Le corollaire suivant est une application du corollaire 1 et du théorème de Dirichlet.

Corollaire 2. *Soient $P_1(x), P_2(x) \in \mathbb{Z}[x]$ deux polynômes premiers entre eux. Supposons qu'aucun premier ne divise les entiers $P_1(n)$ et $P_2(n)$, n parcourant $\mathbb{Z}$. Alors, pour une infinité de $n \in \mathbb{Z}$, il existe une infinité de $\ell \in \mathbb{Z}$ tel que $P_1(n) + \ell P_2(n)$ soit un nombre premier.*

L'hypothèse (H) modulo m.

Soient $m > 0$ un entier et $P_1(x), ..., P_s(x) \in \mathbb{Z}[x]$ des polynômes premiers entre eux. Supposons qu'aucun premier ne divise tous les produits $\prod_{i=1}^{s} P_i(n)$, n parcourant $\mathbb{Z}$. Alors, il existe $n \in \mathbb{Z}$ tel que les $P_i(n)$ sont congrus à des nombres premiers modulo m.

En fait, on a plus : *il existe une infinité de $n \in \mathbb{Z}$ vérifiant pour chaque $i = 1, ..., s$, il existe une infinité de nombres premiers p_i tels que $P_i(n) \equiv p_i \mod m$.*

Exemples d'applications.

(1) **Nombres premiers jumeaux modulo m.**
Soit $m > 0$ un entier. Il existe une infinité de nombres premiers p et q tels que $q \equiv p + 2 \mod m$.

En effet : Prenons $P_1(x) = x$, $P_2(x) = x + 2$, et les valeurs $n = 1$ et $n = 2$. On a $P_1(1)P_2(1) = 3$ et $P_1(2)P_2(2) = 8$, de sorte qu'aucun nombre premier p ne divise $P_1(n)P_2(n)$ pour tout $n \in \mathbb{Z}$. On conclut en utilisant l'hypothèse (H) modulo m.

(2) **Théorème de Goldbach modulo m.**
Soient m et ℓ des entiers naturels non nuls. Il existe une infinité de nombres premiers p et q tels que $p + q \equiv 2\ell \mod m$.

Pour une démonstration : prendre $P_1(x) = x$ et $P_2(x) = 2\ell - x$ et ensuite appliquer l'hypothèse (H) modulo m.

2.10.5. L'hypothèse (H) relative (version générale)

Un anneau intègre Z est dit **presque factoriel** *si tout élément non nul de Z a un nombre fini de diviseurs premiers, et si tout élément non inversible a au moins un diviseur premier.*

Notons qu'on a :
– un anneau factoriel est presque factoriel ;
– un anneau presque factoriel et Noethérien est factoriel ;
– dans un anneau presque factoriel tout élément irréductible est premier.

Avec A. Bodin, P. Dèbes et J. Koenig, dans [BDKN] nous avons montré le résultat suivant.

Soient Z un anneau presque factoriel, ou de Dedekind, et $Q = Frac(Z)$. Soient $P_1(t), ..., P_s(t)$ des polynômes premiers entre eux dans $Q[t]$. Supposons qu'aucun non inversible de Z divise toutes les

valeurs $P_1(z), ..., P_s(z)$, z parcourant $\mathbb{Z}$. Alors, il existe $m \in Z$ tel que $P_1(m), ..., P_s(m)$ sont premiers entre eux dans Z.

Remarques :

(1) Ce résultat était connu pour $Z = \mathbb{Z}$ dans l'article de Schinzel [Sc1], et pour $Z = \mathbb{F}_q[u]$ dans celui de Poonen [Po].

(2) L'énoncé précédent reste vrai avec plusieurs indéterminées $\underline{t} = (t_1, ..., t_k)$, si Z est presque factoriel. Il l'est aussi en prenant Z l'anneau des fonctions entières. Cependant, il n'est pas vrai pour $Z = \mathbb{Z}[\sqrt{5}]$.

2.10.5. Parties Hilbertiennes

Soient Z un anneau intègre, $Q = Frac(Z)$, $\underline{x} = (x_1, ..., x_k)$ et $\underline{y} = (y_1, ..., y_n)$ des indéterminées. Soient $P_1(\underline{x}, \underline{y}), ..., P_s(\underline{x}, \underline{y})$ des polynômes irréductibles dans $Q[\underline{x}, \underline{y}]$ satisfaisant $\deg_{\underline{y}}(P_i) \geq 1$.

On appelle partie hilbertienne de Q^k associée aux P_i, et l'on note $H_Q(P_1, ..., P_s)$, l'ensemble des spécialisations $\underline{x^*} \in Q^k$ telles que les $P_i(\underline{x^*}, \underline{y})$ soient irréductibles dans $Q[\underline{y}]$.

Un résultat bien connu de Weissauer [We] affirme que : toutes les parties hilbertiennes $H_Q(P_1, ..., P_s)$ *sont Zariski-denses dans Q^k (autrement dit Q est Hilbertien).*

Le cas $Q = \mathbb{Q}$ est le théorème d'irréductibilité de Hilbert.

On dit que Z est un anneau *hilbertien* si l'ensemble $H_Q(P_1, ..., P_s)$ contient une spécialisation $\underline{x^*}$ de Z^k.

2.10.6. Le théorème d'irréductibilité de Hilbert pour un anneau

Soient Z un anneau intègre et $Q = Frac(Z)$. Supposons que Q est de caractéristique 0 ou imparfait. Soient $P_1, ..., P_s \in Z[\underline{t}, \underline{y}]$ tels que chaque P_i est irréductible dans $Q[\underline{t}, \underline{y}]$, $\deg_{\underline{y}}(P_i) \geq 1$ et P_i est primitif vu comme polynôme dans $Z[\underline{t}][\underline{y}]$; ici $\underline{t} = (t_1, ..., t_k)$.

Supposons aussi que $P = P_1...P_s$ n'a pas de diviseur fixe dans Z en $\underline{t}$ (c'est-à-dire qu'il n'existe pas de $a \in Z$ tel que $P(\underline{m}, \underline{y}) \equiv 0 \mod a$ pour tout $\underline{m} \in Z^k$).

Notons que P_i est primitif vu comme polynôme dans $Z[\underline{t}][\underline{y}]$ signifie que ces coefficients dans $Z[\underline{t}]$ sont premiers entre eux.

Nous avons montré dans [BDKN] le résultat suivant.

Avec les notations et les hypothèses ci-dessus, supposons en plus que Z est un anneau hilbertien. Alors il existe un Zariski dense $H \subset Z^k$ tel que pour tout $\underline{m} \in H$, les polynômes $P_i(\underline{m}, \underline{y})$ sont irréductibles dans $Z[\underline{y}]$ pour :
– Z presque factoriel et $k, n, s \geq 1$,
– Z un anneau de Dedekind, $k = 1$ et $n, s \geq 1$, ou $s = 1$ et $k, n \geq 1$.

Références

[AA] Ayad, M., Ali, N., *On composite polynomials,* Int. J. Algebra **2** (2008), no. 5/8, 315–326.

[AHS] Abhyankar, S. S., Heinzer, W. J., Sathaye, A., *Translates of polynomials,* Reprinted from A Tribute to Seshadri. Perspectives in Geometry and Representation Theory, Chennai, (2002). Trends Math. Birkhäuser, Basel, (2003), pp. 51–124.

[AP] Arzhantsev, I. V., Petravchuk, A. P., *Closed polynomials algebras,* Ukraïn. Math. Zh. **59** (2007), no. 12, 1783–1790.

[Ay] Ayad, M., *Sur les polynômes $f(X, Y)$ tels que $K[f]$ est intégralement fermé dans $K[X, Y]$,* Acta Arith. **105** (2002), 9–28.

[BCD] Bodin, A., Chèze, G., Dèbes, P., *Spécializations of indecomposable polynomials,* Manuscripta Math. **139** (2012), no. 3-4, 391–403.

[BCN] Busé, L., Chèze, G., Najib, S., *Noether's forms for the study of non-composite rational functions and their spectrum,* Acta Arith. **147** (2011), no. 3, 217–231.

[BDKN] Bodin, A., Dèbes, P., Koenig, J., Najib, S., *The Hilbert-Schinzel specialization property,* À paraître dans J. Reine Angew. Math. (2022).

[BDN1] Bodin, A., Dèbes, P., Najib, S., *Irreducibility of hypersurfaces,* Comm. Algebra **37** (2009), no. 6, 1884–1900.

[BDN2] Bodin, A., Dèbes, P., Najib, S., *Indecomposable polynomials and their spectrum,* Acta Arith. **139** (2009), no. 1, 79–100.

[BDN3] Bodin, A., Dèbes, P., Najib, S., *Families of polynomials and their specializations,* J. Number Theory **170** (2017), 390–408.

[BDN4] Bodin, A., Dèbes, P., Najib, S., *The Schinzel hypothesis for polynomials,* Transactions Amer. Math. Soc. **139** (2020), no. 1, 79–100.

[BDN5] Bodin, A., Dèbes, P., Najib, S., *Prime and coprime values of polynomials,* L'Enseignement Mathématique **66** (2020), no. 2, 169–182.

[Be] Bertini, E., *Sui sistemi lineari,* Rend. Ist. Lombardo (2) **15** (1882), 24–28.

[BFO] Brillhart, J., Filaseta, M., Odlyzko, A., *On an irreducibility theorem of A. Cohn,* Canad. J. Math. **33** (1981), 1055–1059.

[Bo1] Bodin, A., *Reducibility of rational functions in several variables,* Isr. J. Math. **164** (2008), 333–347.

[Bo2] Bodin, A., *Decomposition of polynomials and approximate roots,* Proc. Amer. Math. Soc. **138** (2010), no. 6, 1989–1994.

[BT] Bodin, A., Mihai, T., *Topological equivalence of complex polynomials,* Adv. Math. **199** (2006), 136–150.

[CN] Chèze, G., Najib, S., *Indecomposability of polynomails via jacobian matrix*, J. Algebra. **324** (2010), no. 1, 1–11.

[Cy] Cygan, E., *Factorization of polynomials,* Bull. Polish Acad. Sci. Math. **40** (1992), no. 1, 45–52.

[DF] Dèbes, P., Fried, M., *Integral specialisation of families of rational functions,* Pacific J. Math. **190** (1999), no. 1, 45–52.

[DG] Dujella, A., Gusić, I., *Indecomposability of polynomials and related diophantine equations,* Quart. J. Math. Oxford Ser. **498** (2005), 173–199.

[Fr1] Fried, M., *On Hilbert's irreducibility theorem,* J. Number Theorey **6** (1974), 211–231.

[Fr2] Fried, M., *Variables separated polynomials, the genus* 0 *problem and moduli spaces,* in Number Theory in Progress, Procedings of the Number Theory Conference in Zakopane (1999), 75–102.

[FJ] Fried, M., Jarden, M., *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, **11**, Springer-Verlag, (2004).

[FM] Fried, M., MacRae, R., *On the invariance of chains of fields,* Illinois J. Math. **13** (1969), 165–171.

[Ga] Gao, S., *Factoring multivariate polynomials via partial differential equations,* Math. Comput. **72** (2002), no. 242, 801–822.

[GR] Gao, S., Rodrigues, V., *Irreducibility of polynomials modulo p via Newton polytopes,* J. Number Theory **101** (2003), 32–47.

[Gu] Gusić, I., *On decomposition of polynomials over rings,* Glas. Mat. Ser. III. **43** (2008), 7–12.

[Hi] Hilbert, D., *Uber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten,* J. Reine Angew. Math. **110** (1892), 104–129.

[IP] Iena, O. G., Petravchuk, A. P., *On closed rational functions in several variables,* Algebra and Discrete Math. (2007), no. 2, 115–124.

[Jo] Jouanolou, J. P., *Théorèmes de Bertini et applications,* Birkhäuser, Boston (1983).

[Ka] Kaliman, S., *Two remarks on polynomials in two variables,* Pacific J. Math. **154** (1992), 285–295.

[Kal] Kaltofen, E., *Effective Noether irreducibility forms and applications,* Symposuim on the theory of Computing (New Orleans, LA, 1991). J. Comput. System Sci. **50** (1995), no. 2, 274–295.

[Kr] Krull, W., *Uber einen Irreduzibilitätssatz von Bertini,* J. Reine Angew. Math. **177** (1937), 94–104.

[Lo] Lorenzini, D., *Reducibility of polynomials in two variables*, J. Algebra **156** (1993), 65–75.

[LR] Lê, D. T., Ramanujam, C. P., *The invariance of Milnor's number implies the invariance of the topological type,* Amer. J. Math. **98** (1976), 67–78.

[Mü] Müller, P., *Hilbert's irreducibility theorem for polynomials of prime degree and for generic polynomials,* Isr. J. Math. **109** (1999), 319–337.

[Na1] Najib, S., *Sur le spectre d'un polynôme à plusieurs variables,* Acta Arith. **114** (2004), no. 2, 169–181.

[Na2] Najib, S., *Une généralisation de l'inégalité de Stein-Lorenzini,* J. Algebra **292** (2005), no. 3, 566–573.

[Na3] Najib, S., *Un raffinement du caractère hilbertien du corps $K(X)$,* Manusc. Math. **120** (2006), no. 4, 415–418.

[Na4] Najib, S., *Autour d'un théorème de Stein,* Extracta Math. **23** (2008), no. 2, 173–180.

[Na5] Najib, S., *Irrédictibilité et spécialisation des polynômes,* Portugaliae Math. (N.S.) **65** (2008), no. 3, 339–343.

[Na6] Najib, S., *Indecomposability of multivariate polynomials over finite extensions,* Int. J. Algebra. **5** (2011), no. 7, 309–314.

[Na7] Najib, S., *The spectrum of a rational function,* Algebra Colloquium **27** (2020), no. 3, 477–482.

[No] Noether, E., *Ein algebaisches Kriterium für absolute Irreduzibiltät,* Math. Ann. **85** (1922), 26–33.

[Now] Nowicki, A., *Polynomial derivations and their rings of constants,* Toruń, 1994.

[Os] Ostrowski, A., *Zur arithmetischen Theorie der algebraischen Grössen,* Nachr. K. Ges. Wiss. Göttingen, (1919), 273–298.

[Pl] Ploski, A., *On the irreducibility of polynomials in several complexe variables,* Bull. Pol. Ac. : Math. **39** (1991), 241–247.

[Po] Poneen, B., *Squarefree values of multivariate polynomials,* Duke Math. J., **118**(2) (2003), 353–373.

[Ri1] Ritt, J. F., *Prime and composite polynomials,* Trans. Amer. Math. Soc. **23** (1922), 51–66.

[Ri2] Ritt, J. F., *Permutable rational functions,* Ibid **24** (1923), 399–448.

[Ru1] Ruppert, W., *Reduzibilität Ebener Kurven,* J. Reine Angew. Math. **369** (1986), 167–191.

[Ru2] Ruppert, W., *Reducubility of polynomials $f(x, y)$ modulo p,* J. Number Theory **77** (1999), 62–70.

[Sc1] Schinzel, A., *A property of polynomials with an application to Siegel's lemma,* Monatsh Math., **137**(3) (2002), 239-251.

[Sc2] Schinzel, A., *Slected topics on polynomials,* Ann Arbor Publications, University of Michigan Press, (1982).

[SS] Schinzel, A., Sierpinski, W., *Sur certaines hypothèses concernant les nombres premiers,* Acta Arith. **4** (1958), 185–208 ; erratum 5 (1958), 259.

[Sch] Schmidt, W. M., *Equations over finite fields, an elementary approach*, Springer-Verlag (1976).

[St] Stein, Y., *The total reducibility order of a polynomial in two variables*, Isr. J. Math. **68** (1989), 109–122.

[Sw] Swan, R. G., *Factorization of polynomials over finite fields,* Pacific J. Math. **12** (1962), 1099–1106.

[Vi] Vistoli, A., *The number of reducible hypersurfaces in a pencil,* Invent. math. **112** (1993), 247–262.

[vzG] von zur Gathen, J., *Counting decomposable mulivariate polynomials,* Appl. Algebra Engrg. Comm. Comput. **22(3)** (2011), 165–185.

[We] Weissauer, R., *Der Hilbertsche Irreduzibilitatssatz,* J. Reine Angew. Math. **334** (1982), 203–220.

[Za] Zannier, U., *On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$,* Arch. Math. **68** (1997), 129–138.