GROUPES DE GALOIS DE TRINÔMES $X^p + aX + a$

Ch. L. BOUYACOUB
Laboratory of Arithmetic, LAC3
Faculty of Mathematics,U.S.T.H.B.
cbouyacoub@yahoo.fr

29 octobre 2017

Sommaire

Remerciements

La soutenance d'une thèse marque assurément la fin d'une étape dans la vie d'une personne. Je voudrais saisir cette occasion pour exprimer ma reconnaissance à tous ceux qui m'ont soutenue, encouragée à poursuivre ce travail et à le finir.

Je tiens tout d'abord et avant tout à exprimer mes profonds remerciements et toute ma gratitude à mon directeur de thèse, le professeur Alain SALINIER, qui m'a proposé ce travail. Durant ces quatres années, il n'a mesuré ni son son temps ni sa patience, il a dirigé ce travail avec beaucoup de compétence. Il a su grâce à sa science immense, m'orienter dans la bonne voie et m'obliger à aller toujours plus en avant. Ses conseils judicieux, encouragements et remarques m'ont permis de progresser et surtout de mener à bon terme cette thèse. Je voudrais juste lui dire à quel point j'ai adoré travailler sous sa direction. Qu'il trouve, dans l'aboutissement de ce travail, l'expression de mon infinie reconnaissance.

Mes sincères remerciements vont au professeur Rachid BEBBOUCHI. Notre histoire a commencé alors que j'étais toute jeune étudiante en 1984 sur les bancs de l'université d'Oran. Il a été un de mes premiers et meilleurs enseignants, je peux dire qu'il m' a particulièrement marqué, il avait le chic d'adopter ses étudiants et de les mettre très à l'aise. Il me fait l'honneur de présider ce jury et je l'en remercie chaleureusement.

Ce travail de thèse n'aurait jamais vu le jour sans mes collègues Farid BENCHERIF et Boualem BENSEBA. Ils n'ont pas ménagé leurs efforts lors du work shop de Novembre 2013, au moment où moi même j'avais baissé les bras pour reprendre les études, eux deux tenaient à ce que je m'inscrive en thèse.

De plus, directeurs respectifs du laboratoire LA3C, toutes les facilités m'ont été apportées à chaque fois que j'en ai eu besoin. Je ne pouvais soutenir sans que je leur témoigne toute ma reconnaissance, et je les remercie infiniment d'avoir accepter de faire partie du jury.

Je tiens à remercier tout particulièrement le professeur Omar KIHEL d'avoir accèpté de faire partie du jury sans hésitation aucune malgré son emploi du temps trés chargé. En effet, dès que je l'ai sollicité pour le jury et sans même pas savoir la date de soutenance, il était déjà d'accord. Qu'il trouve dans ces lignes mes sincères remerciements.

Je remercie profondément le professeur Abbas MOVAHHEDI, pour l'intêret qu'il a voulu porter à cette thèse en acceptant de la rapporter. J'ai été vraiment touchée par son accord immédiat de participer au jury malgré qu'il venait d'apprendre une triste nouvelle, je lui suis très reconnaissante.

Que ma petite famille, en particulier mon mari Mokhtar mes deux jeunes hommes Walid et Rafik ainsi que ma petite princesse Manel, trouvent ici toute ma reconnaissance pour leur compréhension, encouragement et patience qu'ils m'ont témoignés durant ces quatres années surtout à chaque fois que je devais, à leur grand supplice, me déplacer sur Limoges.

Je ne peux finir sans citer et remercier l'équipe du laboratoire XLIM pour l'indispensable support que leur personnel me fournissait avec compétence et gentillesse lors de tous mes stages sur Limoges. Je pense particulièrement au professeur et directeur Samir ADLY ainsi qu'à Annie Nicolas.

Mon adaptation à Limoges a été facilitée en partie grâce à Sylvie LAVAL chez qui je me sentais comme chez moi.

Pour finir, un merci particulier à ma collègue Fadila SI AHMED qui m'a supportée et surtout suppléée dans mes tâches pédagogiques à chaque fois que j'en avais besoin. Grâce à elle, je pouvais partir en stage tranquille.

Introduction

0.1 Position du problème

Un trinôme est la somme de 3 monômes non nuls de degrés distincts. l'objet de ce travail est de déterminer le groupe de Galois de trinômes à coefficients rationnels. Les trinômes constituent en un certain sens des polynômes les plus simples avec lesquels on peut espérer réaliser une liste pas trop réduite de groupes de Galois. Les monômes X^n, évidemment, mais aussi les binômes $X^n - a$, ne mènent pas à des situations très riches puisque les binômes à coefficients rationnels sont tous résolubles.

L'intérêt de l'étude de ces polynômes très particuliers peut être justifiée par plusieurs arguments.

En premier lieu, le calcul de leurs groupes de Galois nous fournit des polynômes simples ayant un groupe de Galois donné. Ainsi, étant donné un groupe fini G de permutations, chercher à le réaliser comme groupe de Galois d'un trinôme sur $\mathbb{Q}$ est une version à priori bien cernable par le calcul explicite du problème de Galois inverse. En fait, il est très difficile de réaliser effectivement des groupes primitifs autres que le groupe alterné A_n et le groupe symétrique S_n comme groupe de Galois d'un trinôme.

La deuxième motivation est la possibilité, grâce à la forme simple du polynôme envisagé, d'appliquer et d'illustrer les résultats de la théorie algébrique des nombres et de l'algèbre.

En troisième lieu, l'intéterêt le plus fort de l'étude des trinômes serait la résolution de la version algébrique du treizième problème de Hilbert [15] et plus

précisément de sa conjecture sextique, d'après laquelle l'équation générale du sixième degré ne peut être résolue par superposition de fonctions algébriques d'une variable.

La détermination du groupe de Galois sur $\mathbb{Q}$ du corps de décomposition d'un poynôme est un problème classique d'algèbre. Cette détermination repose sur le principe de Van der Waerden [44] basée essentielllement sur la ramification d'un nombre premier dans l'extension. Un théorème dû à cet auteur [44] affirmait qu'en dehors du groupe symétrique S_n, il est difficile de réaliser un sous-groupe strict de S_n comme groupe de Galois d'un polynôme unitaire à coefficients sur $\mathbb{Z}$. Par exemple, pour un nombre premier p impair et un entier a tel que $\sqrt[p]{a} \notin \mathbb{Z}$, le groupe de Galois du binôme $X^p - a$, qui est résoluble, est engendré par un cycle d'ordre p et un cycle d'ordre $(p-1)$, c'est donc le groupe affine $Aff(\mathbb{F}_p)$.

En fait les trinômes de degré n sur $\mathbb{Q}$ fournissent des exemples de polynômes de degré n à coefficients rationnels ayant pour groupe de Galois le groupe symétrique S_n : Par exemple Osada [30, 31] et Serre [38] ont montré indépendamment que le trinôme $X^n - X - 1$ a pour groupe de Galois S_n sur $\mathbb{Q}$ pour $n > 1$.

La facilité à établir que le groupe de Galois d'un trinôme à coefficients rationnels est S_n est liée à la propiété démontrée par Schinzel [34] : les trinômes génériques $X^n + t^r X^m + t^s$ avec n, m, r et s entiers naturels tels que $n > m > 0$ et $s(n-m) - rn = 1$, ont S_n pour groupe de Galois sur $\mathbb{Q}(t)$. En effet le théorème d'irréductibilité de Hilbert entraîne alors que le trinôme $X^n + t^r X^m + t^s$ a S_n pour groupe de Galois sur $\mathbb{Q}$ pour une infinité de valeurs du paramètre $t \in \mathbb{Q}^*$. Les travaux connus à ce jour semblent indiquer qu'il est très difficile de construire des exemples de trinômes irrèductibles de degré $n \geq 7$ ayant pour groupe de Galois sur $\mathbb{Q}$ un groupe de permutations ne contenant pas le groupe altèrné A_n. C'est ainsi qu' Angeli [2] a montré que si, $p \geq 7$ est un nombre premier fixé, il n'y a qu'un nombre fini d'orbites de trinômes irréductibles résolubles $f(X) = X^p + aX + b$ sous l'action $f(X) \longrightarrow k^p f(X/k)$ du groupe $\mathbb{Q}^*$.

La conjecture énoncée par Kölle et Schmid est la suivante :
si p est un nombre premier, et si a est un nombre entier tel que $v_p(a) = 1$, alors

le trinôme

$$f(X) = X^p + aX + a \tag{0.1.1}$$

a un groupe de Galois isomorphe au groupe symétrique S_p. Cette conjecture a été démontré par Gauckler [18] lorsque $p = 5$. D'autre part, on sait depuis l'article de Movahhedi [26] que, si trinôme (0.1.1) ne satisfait pas la conclusion de la conjecture, alors son groupe de Galois est nécessairement résoluble.

Dans cette thèse, nous nous intéressons à la possibilité de trouver un trinôme irréductible $f_0(X) = AX^p + BX + C$ $(ABC \neq 0)$ à coefficients rationnels de degré premier $p \geq 7$ qui soit résoluble. Pour un tel trinôme, il existe une valeur $k \in \mathbb{Q}^*$ telle que le trinôme $k^p f_0(X/k)$ soit de la forme

$$f(X) = X^p + ac^{p-2}X + ac^{p-1} \tag{0.1.2}$$

pour deux entiers rationnels a et c étrangers. C'est pourquoi nous nous limiterons à examiner des trinômes de cette forme (0.1.2).

0.2 Résumé de la littérature

Avant de citer les travaux relativement à la détermination de groupes de Galois de trinômes, nous allons essayer de parler en premier de cette détermination mais concernant des polynômes en général. La théorie de Galois est très utile dans plusieurs sphères des mathématiques telles que l'Arithmétique ainsi que l'Algèbre. Le théorème fondamental de cette théorie est inévitable lorsque vient le moment de faire l'éventail des sous corps d'une extension de $\mathbb{Q}$. En effet, elle transforme la chasse aux sous-corps en une chasse aux sous groupes.

Plusieurs auteurs se sont intéressés à la détermination de groupes de Galois de trinômes. Parmi les premiers travaux spécifiques aux trinômes, on peut citer Lalesco [22] qui dès 1907, montre que le polynôme $x^n - kaX + a$ a un groupe de Galois S_n sur $K(a)$, sous l'hypothèse que n est premier.

Dans le cas où le trinôme est de degré quelconque, nous pouvons citer les travaux [30, 31], [27] et [13, 14]. Nous pouvons aussi citer les travaux de Bishnoi et Khanduja [6] qui ont étendus ceux de Schur [35, 36]. Pour finir le cas des

trinômes de degré quelconque n, on cite [19] dans lequel les auteurs ont voulu aborder le problème inverse.

Dans le cas où l'entier p est premier, W. Feit [17] dresse la liste des groupes susceptibles de se réaliser comme groupe de Galois d'un trinôme de degré premier et irréductible sur le corps $\mathbb{Q}$. D'ailleurs il s'avère que très peu de groupes de permutations sont susceptibles de se réaliser comme groupe de Galois de tels trinômes. Dans ce cas, nous pouvons citer les articles [21], [26] ainsi que [4, 5].

D'autres résultats ultérieurs vont dans ce sens. Komatsu [21] donne des conditions suffisantes pour que le trinôme à coefficients entiers ait un groupe de Galois S_n ou A_n. A.Movahhedi étendra ces résultats dans [26].

S.D.Cohen, A.Movahhedi et A.Salinier montrent, sous des hypothèses pas très fortes, que le groupe de Galois d'un trinôme à coefficients entiers est A_n ou S_n [13, 14, 12].

Par ailleurs, A.Salinier et A.Hermez donnent explicitement et en tout degré des familles infinies de trinômes de groupes de Galois A_n [19].

En petit degré, des groupes de Galois plus petits sont réalisés. L'un des premiers exemples apparus dans la littérature est probablement le trinôme

$$X^7 - 7X + 3,$$

simple donc joli, qui réalise le groupe $PSL(3,2)$. Le fait fut remarqué par Trinks en 1968[41], et prouvé par Matzat quelques années plus tard. Plus récemment [10], N.D.Elkies et N.Bruin ont dressé la liste complète des trinômes de degré 7 réalisant $PSL(3,2)$, ajoutant à $X^7 - 154X + 99$, exhibé par Erbach, Fischer et McKay, deux nouveaux exemples.

Les outils essentiels utilisés dans la plus part des articles cités précédemment reposent presque tous sur les notions de ramification, de décomposition d'un nombre premier en produit d'idéaux premiers, de polygones de Newton et d'arithmétique de corps de nombres. Ces méthodes ont été reprises en détail dans l'article intitulé *The factorisation of polynomials over local fields* [12]. Dans

cet article, les auteurs ont non seulement apporté une démonstration moderne et accessible du théorème d'Ore [29] mais aussi étendu le domaine de validité de ces résultats. Cet article a posé les bases de nombreux travaux ultérieurs, nous pouvons citer par exemple les travaux menés à bien par l'école Barcelonaise [25].

Cependant, Gauckler dans son article [18] s'est distingué dans sa façon de s'y prendre pour prouver son résultat en passant par le polynôme résolvant [11].

Un second article original par ses techniques de démonstrations est du à Angeli [2]. En effet, en reprenant l'idée trouvée en premier chez Gauss [24], Angeli prouve alors que la détermination des paramètres t de trinômes de groupe de Galois G donné se ramène à la recherche de points rationnels sur une certaine courbe algébrique.

0.3 Résultats

Le premier chapitre se devait de rappeler et citer certaines notions de la théorie des nombres en particulier quelques éléments sur la théorie de Galois qui seront nos outils indispensables pour nos démonstrations. Nous avons voulu commencer par certains éléments incontournables et indispensables de la théorie de Galois en particulier les extensions, polynômes scindés, corps de rupture, corps de racines d'un polynôme séparable ainsi que le groupe de Galois d'un polynôme séparable. Les notions liées de ramification et polygône de Newton originellement exposés par Ore [29] puis reprises en mieux dans [12], ont été présentées. Ces notions, en combinaison avec le lemme d' Abhyankar [1], permettent d'identifier la structure du groupe d'inertie dans une extension N au dessus du corps des rationnels $\mathbb{Q}$. La détermination du groupe d'inertie nous renseigne sur la possible réalisation d'un groupe de permutations comme groupe de Galois du trinôme considéré.

Le deuxième chapitre est consacré aux groupes de Galois de trinômes.
Nous commençons par la notion du résultant de deux polynômes. La motivation de revisiter et au besoin démontrer les propriétés essentielles à cette notion,

inspirées de [39], nous est parue indispensable et nécessaire pour enfin arriver au lien liant le résultant au discriminant d'un polynôme apporté par la formule (2.2.4) de la définiton 20 . Tout ce ci pour enfin apporter une démonstration détaillée de la formule du discriminant d'un trinôme quelconque (2.2.6), formule que nous retrouvons dans [40]. La classification des trinômes s'imposant à nous y est ensuite présentée. Deux trinômes équivalents ont le même groupe de Galois d'où le problème de décrire ces classes et de trouver un représentant privilégié dans chaque classe.

Le chapitre 3 contient pour une part essentielle les résultats originaux auxquels nous sommes parvenus dans le cadre de cette thèse. Notre résultat principal est le théorème 3.1. Un cas particulier des trinômes que nous considérons dans le théorème 3.1, déjà traité dans la littérature [20, 26], est le cas $c = 1$, c'est à dire celui des trinômes $X^p + aX + a$, où a est un entier divisible par p exactement une fois. Soulignons de plus que Kölle et Schmid [20] conjecturent que le groupe de Galois de $f(X)$ est toujours S_p lorsque $c = 1$. Cependant, en général ceci a été prouvé seulement pour $p \leqslant 5$ à ce jour [18]. Nos méthodes de démonstrations sont proches de celles utilisées dans [20], et nous réctifions une petite erreur dans ce papier [20]. Le point 1 du théorème 3.1 a été démontré dans [20, pp.82-83] dans le cas particulier qui y est considéré, alors que les points 2 et 3 sont nouveaux : nous les déduisons à partir du théorème de Pellet-Stickelberger. L'idée principale dans nos démonstrations est la méthode locale. Dans le théorème 3.2, basé en partie sur le théorème 3.1 et aussi sur [20, 26], nous résumons les résultats connus sur les groupes de Galois du trinôme (0.1.2) lorsque $c = 1$. Enfin, nous déduisons par la loi de réciprocité quadratique et les théorèmes 3.1 et 3.2 le théorème 3.3 dont l'intérêt principal est de préciser la forme d'un contre exemple à la conjecture de Kölle-Schmid. Ces résultats ont fait l'objet d'un article intitulé *On the solvability of an Eisenstein trinomial of prime degree* [8].

Enfin, le dernier chapitre est consacré au cas particulier où l'entier premier p vaut 7.

Dans tout ce travail, nous emploierons le vocable de corps comme signifiant corps commutatif. De même, tout morphisme d'anneaux (en particulier

tout morphisme de corps) est supposé envoyer l'élément unité de la source sur l'élément unité du but. Il en résulte en particulier que tout morphisme de corps est injectif.

Chapitre 1

Groupes de Galois et ramification

1.1 Introduction

Nous avons voulu dans ce chapitre apporter certains éléments incontournables et indispensables de la théorie de Galois tels que les extensions, polynômes scindés, corps de rupture, corps de racines d'un polynôme séparable ainsi que le groupe de Galois d'un polynôme séparable. L'incontournable notion de ramification y est ensuite exposée, s'inspirant pour cela du livre de J.-P Serre [37]. S'en suivront, les notions liées de ramification et polygône de Newton originellement exposés par Ore [29] puis reprises en mieux dans [12]. Ces notions, en combinaison avec le lemme d' Abhyankar [1], permettent d'identifier la structure du groupe d'inertie dans une extension N au dessus du corps des rationnels $\mathbb{Q}$. La détermination du groupe d'inertie nous renseigne sur la possible réalisation d'un groupe de permutation comme groupe de Galois du trinôme considéré.

1.2 Éléments de la théorie de Galois

1.2.1 Rappels sur les extensions

Définition 1. Etant donné un corps F, on appelle *extension* de F un couple (E, j_E) constitué d'un corps E et d'un morphisme de corps $j_E : F \to E$. Le corps E est appelé le *corps essentiel* de l'extension (E, j_E), le corps F le *corps de base* et le morphisme j_E le *morphisme structural* ou *plongement* de l'extension.

Notation 1.1. La notation E/F est utilisée pour signifier que le corps E est le corps essentiel d'une extension du corps F.

Par abus de langage, on emploiera souvent des locutions telles que « l'extension E/F », omettant ainsi d'avoir à nommer le plongement $j_E : F \to E$ de l'extension. Ceci est surtout avantageux dans la situation où F est un sous-corps de E : il sera alors tacitement supposé par la notation E/F que j_E n'est autre que l'injection canonique de F dans E.

Exemple 1.2. Si A est une F-algèbre commutative, et si I est un idéal maximal de A, soit j^I le morphisme de source F et de cible l'algèbre quotient A/I obtenu par composition du morphisme structural de la F-algèbre A suivi par la surjection canonique de A dans A/I. Le couple $E_I = (A/I, j^I)$ est une extension de F.

Définition 2. Une extension (E, j_E) du corps F est dite *triviale* lorsque son morphisme structural j_E est surjectif (et donc bijectif).

Définition 3. Deux extensions (E, j_E) et $(E', j_{E'})$ du corps F sont dites *isomorphes* s'il existe un isomorphisme de corps $\phi : E \to E'$ tel que $\phi \circ j_E = j_{E'}$.

Définition 4. Étant données deux extensions E'/F et E/E' telles que le corps essentiel de la première est le corps de base de la seconde, donnés respectivement par les morphismes $j_{E'} : F \to E'$ et $j'_E : E' \to E$, on appelle *superposée* de ces deux extensions l'extension E/F donnée par le morphisme composé $j'_E \circ j_{E'} : F \to E$.

Lorsque E est une extension du corps F, le morphisme de corps $j_E : F \to E$ induit sur E une structure d'espace vectoriel sur F en posant pour tout élément a de F et pour tout élément x de E

$$a \cdot x = j_E(a)x \ .$$

Définition 5. Une extension E/F est dite *finie* lorsque E est un espace vectoriel sur F de dimension finie.

Ainsi une extension E/F donnée par le morphisme $j_E : F \to E$ est finie si et seulement s'il existe une partie finie $X \subset E$ telle que l'application $\phi_E : F^X \to E$ définie par

$$\forall \mathbf{a} = (a_x)_{x \in X} \in F^X, \qquad \phi_E(\mathbf{a}) = \sum_{x \in X} j_E(a_x)x$$

est surjective.

Proposition 1.1. *La superposée de deux extensions finies est une extension finie.*

Preuve. Soit E/F l'extension superposée de deux extensions finies E'/F et de E/E', supposées données respectivement par les morphismes $j_{E'} : F \to E'$ et $j'_E : E' \to E$. Puisque E'/F est finie, il existe une partie finie $X' \subset E'$ telle que l'application $\phi_{E'} : F^{X'} \to E'$ définie par

$$\forall \mathbf{a} = (a_{x'})_{x' \in X'} \in F^{X'}, \qquad \phi_{E'}(\mathbf{a}) = \sum_{x' \in X'} j_{E'}(a_{x'})x'$$

est surjective. De même, puisque l'extension E/E' est finie, il existe une partie finie X de E telle que l'application $\psi_E : E'^X \to E$ définie par

$$\forall \mathbf{b} = (b_x)_{x \in X} \in E'^X, \qquad \psi_E(\mathbf{b}) = \sum_{x \in X} j'_E(b_x)x$$

est surjective. Comme le produit cartésien d'ensembles finis est fini, l'ensemble

$$X'' = \{j'_E(x')x; (x, x') \in X \times X'\}$$

est une partie finie de E.

Soit alors un élément quelconque z de E : par la surjectivité de ψ_E, il existe un élément $\mathbf{b} = (b_x)_{x \in X}$ de E'^X tel que

$$z = \sum_{x \in X} j'_E(b_x)x \ .$$

Pour tout $x \in X$, par surjectivité de $\phi_{E'}$, il existe un élément $\mathbf{a}_x = (a_{x,x'})_{x' \in X'}$ de $F^{X'}$ tel que

$$b_x = \sum_{x' \in X'} j_{E'}(a_{x,x'})x' \ .$$

On en déduit que

$$z = \sum_{x \in X} \sum_{x' \in X'} (j'_E \circ j_{E'})(a_{x,x'})j'_E(x')x.$$

Ceci signifie que l'application ϕ_E de $F^{X''}$ dans E définie par

$$\forall \mathbf{a} = (a_{x''})_{x'' \in X''} \in F^{X''}, \qquad \phi_E(\mathbf{a}) = \sum_{x'' \in X''} (j'_E \circ j_{E'})(a_{x''})x''$$

est surjective. □

Définition 6. Soit E/F et E'/F deux extensions du même corps F. On dit que E'/F est une *sous-extension* lorsqu'il existe une extension E/E' du corps E' telle que E/F soit la superposée de E'/F et de cette extension E/E'. Une sous-extension E'/F d'une extension E/F est dite *propre* lorsque cette extension E/E' est non triviale.

Lorsque l'extension E'/F est une sous-extension de E/F, cela signifie donc par définition qu'on s'est donné un morphisme de corps $j'_E : E' \to E$.

Proposition 1.2. *Si E'/F est une sous-extension de l'extension finie E/F, alors les extensions E'/F et E/E' sont finies.*

Preuve. Notons $j_E : F \to E$ et $j_{E'} : F \to E'$ les morphismes structuraux respectifs des extensions E/F et E'/F. Puisque E'/F est supposée être une sous-extension de E/F, il existe un morphisme $j'_E : E' \to E$ tel que $j_E = j'_E \circ j_{E'}$, ce qui fait voir que l'application j'_E est F-linéaire. D'autre part, j'_E est injectif comme tout morphisme de corps. On dispose ainsi d'un morphisme F-linéaire injectif de E' dans E. Si E/F est finie, ceci montre que E' est un espace vectoriel de dimension finie sur F, c'est-à-dire que l'extension E'/F est finie.

Puisque E/F est finie, il existe une partie finie $X \subset E$ telle que l'application $\phi_E : F^X \to E$ définie par

$$\forall \mathbf{a} = (a_x)_{x\in X} \in F^X, \qquad \phi_E(\mathbf{a}) = \sum_{x\in X} j_E(a_x)x$$

est surjective. Pour tout $z \in E$, il existe donc un élément $(a_x)_{x\in X}$ de F^X tel que

$$z = \sum_{x\in X} j_E(a_x)x = \sum_{x\in X} j'_E(j_{E'}(a_x))x,$$

ce qui montre que l'application ψ_E de E'^X dans E définie par

$$\forall \mathbf{a} = (a_x)_{x\in X} \in E'^X, \qquad \phi_E(\mathbf{a}) = \sum_{x\in X} j'_E(a_x)x$$

est surjective. Ainsi l'extension E'/E est finie. □

Définition 7. Le *degré* d'une extension finie E/F est la dimension de E en tant qu'espace vectoriel sur F.

Notation 1.3. Pour toute extension finie E/F, le symbole $[E : F]$ désigne le degré de l'extension.

Exemple 1.4. Si $p(X) \in F[X]$ est un polynôme irréductible sur le corps F, alors l'anneau-quotient $F[X]/(p(X))$ est une extension finie de F, dont le degré est égal au degré du polynôme $p(X)$.

En effet, l'irréductibilité de $p(X)$ dans l'anneau $F[X]$ équivaut à la maximalité de l'idéal principal $I = (p(X))$ parmi tous les idéaux principaux de l'anneau $F[X]$. Puisque $F[X]$ est un anneau principal, ceci entraîne que I est un idéal maximal, et donc que $E = F[X]/I$ est un corps. Le morphisme structural de l'extension E/F est (exemple 1.2) le morphisme $j : F \to E$ donné par $j(a) = a + I$ pour tout élément a de F. De plus, une base du F-espace vectoriel E est donnée par la famille $(X^j + I)_{0 \leq j < \deg(p(X))}$ qui a précisément $\deg(p(X))$ éléments.

Proposition 1.3. *Si E'/F est une sous-extension de l'extension finie E/F, alors nous avons :*

$$[E : F] = [E : E'][E' : F]$$

Preuve. Par la proposition 1.2, on sait que les extensions E/E' et E'/F sont finies. Soit d le degré de l'extension E'/F et e le degré de l'extension E/E', de sorte qu'il existe dans le F-espace vectoriel E' une base $(x_1, \ldots, x_d)$ à d éléments, et dans le E'-espace vectoriel E une base $(y_1, \ldots, y_e)$ à e éléments. Notons $j_{E'}, j'_E$ et $j_E = j'_E \circ j_{E'}$ les morphismes structurels respectifs des extensions E'/F, E/E' et E/F. Alors tout élément z de E s'écrit de façon unique sous la forme d'une combinaison linéaire à coefficients dans E' des éléments $(y_1, \ldots, y_e)$, c'est-à-dire qu'il existe un unique $(b_1, \ldots, b_e) \in E'^e$ tel qu'on ait

$$z = \sum_{j=1}^{e} j'_E(b_j) y_j \ .$$

De même, tout élément de E' s'écrit de façon unique comme combinaison linéaire à coefficients dans E des éléments $(x_1, \ldots, x_d)$, de sorte que, pour tout indice $j \in \{1, \ldots, e\}$, il existe un unique $(a_{j,1}, \ldots, a_{j,d}) \in F^d$ tel que

$$b_j = \sum_{i=1}^{d} j_{E'}(a_{j,i}) x_i \ .$$

On en déduit

$$z = \sum_{j=1}^{e} \sum_{i=1}^{d} j'_E(j_{E'}(a_{j,i}))j'_E(x_i)y_j = \sum_{j=1}^{e} \sum_{i=1}^{d} j_E(a_{j,i})j'_E(x_i)y_j \ ,$$

par où l'on voit que la famille $(j'_E(x_i)y_j)_{1\leq i\leq d, 1\leq j\leq e}$ à de éléments engendre le F-espace vectoriel E, d'où l'inégalité $[E : F] \leq de$.

Si d'autre part on se donne une famille $(a_{j,i})_{1\leq i\leq d, 1\leq j\leq j}$ d'éléments de F telle que la combinaison linéaire

$$\sum_{j=1}^{e} \sum_{i=1}^{d} j_E(a_{j,i})j'_E(x_i)y_j = 0,$$

alors on peut écrire

$$\sum_{j=1}^{e} \sum_{i=1}^{d} j'_E(j_{E'}(a_{j,i})x_i)y_j = \sum_{j=1}^{e} j'_E(\sum_{i=1}^{d} j_{E'}(a_{j,i})x_i)y_j = 0.$$

Puisque la famille $(y_1, \ldots, y_e)$ est libre sur E', on en déduit que, quelque soit l'entier j tel que $1 \leq j \leq e$, on a

$$\sum_{i=1}^{d} j_{E'}(a_{j,i})x_i = 0 \ .$$

Puisque la famille $(x_1, \ldots, x_d)$ est libre sur F, on en conclut que tous les coefficients $a_{j,i}$ sont nécessairement nuls. Ceci montre que la famille $(j'_E(x_i)y_j)_{1\leq i\leq d, 1\leq j\leq e}$ est libre. Puisqu'on a déjà montré qu'elle est génératrice, c'est en fait une base du F-espace vectoriel E, d'où l'égalité $[E : F] = de$. □

Notation 1.5. Si E/F est une extension de morphisme structural $j_E = F \to E$, et si Y est une partie de E, on note $F(Y)$ le plus petit sous-corps de E contenant la partie $j_E(F) \cup Y \subseteq E$.

1.2.2 Polynômes scindés

Définition 8. Soit $f(X) \in F[X]$ un polynôme non nul à coefficients dans un corps F. On dit que $f(X)$ est *scindé* sur F lorsque tout diviseur irréductible de $f(X)$ dans $F[X]$ est de degré 1.

On peut donc affirmer qu'un corps F est algébriquement clos si et seulement si tout polynôme non nul de $F[X]$ est scindé sur F.

Propriété 1.4. *Si le polynôme $f(X)$ est scindé sur F et si le polynôme $g(X)$ divise $f(X)$ dans $F[X]$, alors $g(X)$ est scindé sur F.*

Preuve. En effet, tout diviseur irréductible du polynôme $g(X)$ dans $F[X]$ est aussi un diviseur irréductible de $f(X)$ dans $F[X]$. □

Propriété 1.5. *Si $f_1(X), f_2(X), \ldots, f_r(X)$ sont des polynômes non nuls scindés sur F, alors leur produit $f_1(X)f_2(X)\cdots f_r(X)$ est scindé sur F.*

Preuve. En effet, tout diviseur irréductible du produit $f_1(X)f_2(X)\cdots f_r(X)$ doit diviser au moins l'un des facteurs $f_1(X), f_2(X), \ldots, f_r(X)$, donc est de degré 1.

Notation 1.6. Si $j : R \to S$ est un morphisme d'anneaux, on note j^* l'unique morphisme de l'anneau de polynômes $R[X]$ dans $S[X]$ qui prolonge j et qui envoie l'indéterminée X de $R[X]$ sur l'indéterminée X de $S[X]$.

Définition 9. Si $f(X)$ est un polynôme non nul à coefficients dans un corps F, et si E/F est une extension de F, de morphisme structural $j_E : F \to E$, on dit que $f(X)$ *est scindé sur* E, lorsque le polynôme $j_E^*(f(X)) \in E[X]$ est scindé sur le corps E.

Proposition 1.6. *Soit $f(X) \in F[X]$ un polynôme non nul à coefficients dans un corps F. Si E'/F est une sous-extension de E/F, et si le polynôme $f(X)$ est scindé sur E', alors il est également scindé sur E.*

Preuve. Notons $j_E : F \to E$ et $j_{E'}$ les plongements respectifs des extensions E/F et E'/F. Puisque, par hypothèse, l'extension E'/F est une sous-extension de E/F, il existe un morphisme $j'_E : E' \to E$ tel que $j_E = j'_E \circ j_{E'}$. On a alors $j_E^*(f(X)) = {j'_E}^*(j_{E'}^*(f(X))$. Par hypothèse, le polynôme $f(X)$ est scindé sur E', c'est-à-dire que tout diviseur irréductible de $j_{E'}^*(f(X))$ dans $E'[X]$ est de degré 1. Puisque l'anneau $E'[X]$ est noethérien, on en déduit que $j_{E'}^*(f(X))$ est produit de polynômes de degré 1 à coefficients dans E'. Il en résulte que le polynôme $j_E^*(f(X)) = {j'_E}^*(j_{E'}^*(f(X))$ est lui aussi produit de polynômes de degré 1 à coefficients dans E. Puisque l'anneau $E[X]$ est factoriel, on en déduit que tout facteur irréductible de $j_E^*(f(X))$ doit diviser un polynôme de degré 1, il est donc forcément de degré 1. □

1.2.3 Corps de rupture d'un polynôme irréductible

Définition 10. Si $f(X)$ est un polynôme à coefficients dans un corps F, et si E/F est une extension de F, de morphisme structural $j_E : F \to E$, on dit que $f(X)$ *a une racine dans* E, lorsque le polynôme $j_E^*(f(X))$ admet dans $E[X]$ un diviseur de degré 1.

Définition 11. Soit $p(X) \in F[X]$ un polynôme irréductible à coefficients dans un corps F. On appelle *corps de rupture de* $p(X)$ *sur le corps* F toute extension E/F satisfaisant les conditions suivantes.

- Le polynôme $p(X)$ a une racine dans E.
- Si E'/F est une sous-extension propre de E/F, alors le polynôme $p(X)$ n'a pas de racine dans E'.

Théorème 1.7 (Existence du corps de rupture)**.** *Soit F un corps, et $p(X) \in F[X]$ un polynôme irréductible. On note $I = (p(Y))$ l'idéal de l'anneau $F[Y]$ engendré par le polynôme $p(Y)$, et on pose $E = F[Y]/I$. Alors E est un corps, et l'extension E/F est corps de rupture de $p(X)$. De plus, le degré de cette extension est égal au degré du polynôme $p(X)$.*

Preuve. Comme on l'a déjà observé (exemple 1.4), l'anneau E est un corps, et le plongement $j_E : F \to E$ tel que $j_E(a) = a + I$ pour tout élément a de F, fait de ce corps une extension du corps F, dont le degré est égal au degré du polynôme $p(X)$.
Soit $\theta = Y + I \in E$; vérifions que $X - \theta$ est diviseur de $j_E^*(p(X))$. Ecrivons $p(X) = a_0 + a_1X + \cdots + a_nX^n$, où $a_i \in F$. Alors, on a :

$$j_E^*(p(X)) = j(a_0) + j(a_1)X + \cdots + j(a_n)X^n,$$

et donc

$$j_E^*(p(X)) \equiv j(a_0) + j(a_1)\theta + \cdots + j(a_n)\theta^n \pmod{(X-\theta)E[X]}$$

Or

$$\begin{aligned} j(a_0) + j(a_1)\theta + \cdots + j(a_n)\theta^n &= (a_0 + I) + (a_1 + I)\theta + \ldots\ldots\ldots + (a_n + I)\theta^n \\ &= (a_0 + I) + (a_1 + I)(Y + I) + \ldots\ldots\ldots + (a_n + I)(Y + I)^n \end{aligned}$$

$$= (a_0 + I) + (a_1 Y + I) + ... + (a_n Y^n + I)$$
$$= a_0 + a_1 Y + ... + a_n Y^n + I$$
$$= p(Y) + I = I$$

car $I = (p(Y))$. Comme $I = 0 + I$ est l'élément nul de $F[Y]/I$, on en conclut que $j_E^*(p(X))$ est divisible par $X - \theta$, de sorte que $p(X)$ a une racine dans E.

Soit E'/F une sous-extension de E/F dans laquelle $p(X)$ a une racine. Nous notons $j_{E'}$ le morphisme structural de l'extension E'/F, et j'_E celui de l'extension E/E', de sorte que $j_E = j'_E \circ j_{E'}$. Dans $E'[X]$, le polynôme $j_{E'}^*(p(X))$ a un facteur de degré un $\alpha X - \beta$, où $\alpha \neq 0$ et β sont deux éléments de E'. Par définition de l'anneau $F[X]$, il existe un unique morphisme d'anneaux $\phi : F[X] \to E'$ tel que $\phi(a) = j_{E'}(a)$ pour tout a de F et $\phi(X) = \frac{\beta}{\alpha}$. On a alors

$$\phi(p(X)) = j_{E'}(a_0) + j_{E'}(a_1)\left(\frac{\beta}{\alpha}\right) + \cdots + j_{E'}(a_n)\left(\frac{\beta}{\alpha}\right)^n = 0$$

car

$$j_{E'}^*(p(X)) = j_{E'}(a_0) + j_{E'}(a_1)X + \cdots + j_{E'}(a_n)X^n$$

est par hypothèse divisible par $\alpha X - \beta$. Par conséquent, l'idéal I est contenu dans le noyau du morphisme ϕ, ce qui donne par passage au quotient un morphisme $\bar{\phi} : E \to E'$. Le composé $j'_E \circ \bar{\phi}$ est un endomorphisme de E dont il est facile de s'assurer qu'il est F-linéaire. Il est de plus injectif puisque c'est un morphisme de corps. Or on sait que tout endomorphisme injectif d'un espace vectoriel de dimension finie est aussi surjectif. Comme E est de dimension finie sur F, on en déduit que l'application $j'_E \circ \bar{\phi}$ est surjective. Par conséquent j'_E est surjective, ce qui signifie que l'extension E/E' est triviale. □

Proposition 1.8 (Unicité du corps de rupture)**.** *Pour tout corps de rupture E/F du polynôme irréductible $p(X) \in F[X]$, l'extension E/F est isomorphe à l'extension $(F[X]/(p(X)))/F$.*

Preuve. Notons $j_E = F \to E$ le morphisme structural de l'extension E/F. Par définition du corps de rupture, on sait que le polynôme $j_E^*(p(X))$ a dans l'anneau $E[X]$ un facteur de degré un $\alpha X - \beta$, où $\alpha \neq 0$ et β sont deux éléments de E. Alors, par définition de l'anneau des polynômes $F[X]$, il existe un unique morphisme ϕ d'anneaux de $F[X]$ dans E tel que $\phi(a) = j_E(a)$ pour tout élément a de $F \subset F[X]$ et $\phi(X) = \frac{\beta}{\alpha}$. Le noyau du morphisme ϕ contient le polynôme

$p(X)$ qui, étant irréductible, engendre un idéal maximal de l'anneau principal $F[X]$. Par conséquent, le noyau de ϕ est égal à l'idéal I de $F[X]$ engendré par $p(X)$. On en déduit par passage au quotient un morphisme $\bar{\phi} : F[X]/I \to E$. Le morphisme structural j^I de l'extension $(F[X]/I)/F$ est (exemple 1.2) obtenu en composant l'injection canonique de F dans $F[X]$ avec la projection modulo I, de sorte que $j_E = \bar{\phi} \circ j^I$. En tant que morphisme de corps, l'application $\bar{\phi}$ est injective. Pour montrer qu'elle est également surjective, on introduit le sous-corps E' de E qui est l'image de $F[X]/I$ par $\bar{\phi}$, c'est-à-dire l'image de $F[X]$ par ϕ. On voit que $\frac{\beta}{\alpha} \in E'$. Puisque $X - \frac{\beta}{\alpha}$ est un polynôme unitaire à coefficients dans E' qui divise $j_E^*(p(X))$ dans l'anneau $E[X]$, il le divise également dans $E'[X]$, de sorte que $p(X)$ a une racine dans E'. Par définition du corps de rupture, l'extension E/E' est triviale, c'est-à-dire que $E' = E$, de sorte que l'application ϕ est surjective. Ainsi ϕ réalise un isomorphisme entre les extensions $(F[X]/I)/F$ et E/F. □

1.2.4 Corps de racines d'un polynôme

Définition 12. Soit $f(X) \in F[X]$ un polynôme non nul à coefficients dans un corps F. On appelle corps de racines de $f(X)$ toute extension E/F telle que $f(X)$ est scindé sur E, mais ne l'est pas sur toute sous-extension propre.

Propriété 1.9. *Si E est corps de racines de $f(X) \in F[X] \setminus \{0\}$, alors $E = F(Rac(f))$ où $Rac(f) = \{r \in E / f(r) = 0\}$.*

Preuve. Notons $j_E : F \to E$ le plongement de l'extension E/F, et posons $E' = F(Rac(f))$. Le corps E' est par définition le plus petit sous-corps de E qui contient à la fois $j_E(F)$ et l'ensemble $Rac(f)$. On peut factoriser le polynôme scindé $j_E^*(f(X))$ de $E[X]$ sous la forme

$$j_E^*(f(X)) = j_E(A) \prod_{r \in Rac(f)} (X - r)^{k_r}$$

pour des entiers $k_r \geq 1$, où $A \in F^*$ est le coefficient dominant du polynôme $f(X)$. Par conséquent, tout diviseur irréductible de $j_E^*(f(X))$ est associé à un polynômes de la forme $X - r$, où $r \in Rac(f) \subset E'$. Par conséquent, le polynôme $f(X)$ est scindé dans l'extension E'/F, ce qui par définition du corps de racines, montre que $E = E'$. □

Théorème 1.10 (Kronecker)**.** *Soit $f(X) \in F[X] \setminus \{0\}$ où F est un corps. Il existe une extension E/F telle que $f(X)$ est scindé sur E.*

Preuve. On raisonne par récurrence sur le degré de $f(X)$. Si $f(X)$ est de degré ≤ 1, alors $E = F$ convient. Si $f(X)$ est de degré strictement plus grand que 1, nous écrivons $f(X) = p(X)g(X)$, où $p(X)$ est irréductible. Comme $\deg(p(X)) \geq 1$, on a $\deg(g(X)) < \deg(f(X))$. Par récurrence, il existe une extension E_1/F telle que $g(X)$ est scindé sur E_1. Par la propriété 1.5, on est ramené à montrer l'existence d'une extension E/E_1 telle que $p(X)$ est scindé sur E. Si $p(X)$ est de degré 1, alors $E = E_1$ convient. Si le degré de $p(X)$ est strictement plus grand que 1, alors le théorème 1.7 nous fournit une extension B/E_1 sur laquelle $p(X)$ a une racine. Par conséquent $p(X) = (X - \theta)q(X)$ dans $B[X]$. Par récurrence, il y a une extension E/E_1 telle que $q(X)$, donc $f(X)$, est scindé sur E. □

Théorème 1.11 (Existence d'un corps de racines)**.** *Tout polynôme non nul $f(X) \in F[X]$ admet un corps de racines.*

Preuve. En vertu du théorème de Kronecker, on sait qu'il existe une extension K/F telle $f(X)$ est scindé sur K. On pose alors $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$, où $\alpha_1, \alpha_2, ..., \alpha_n$ sont les racines de $f(X)$ dans K. Il est évident que $f(X)$ est scindé sur E et que $f(X)$ ne peut être scindé sur une quelconque sous-extension propre de E/F. □

Propriété 1.12. *Si E est un corps de racines de $f(X) \in F[X] \setminus \{0\}$, alors l'extension E/F est finie.*

Cette propriété se justifie immédiatement par une récurrence sur le degré de $f(X)$.

Définition 13. Une extension E/F est dite *normale* lorsque tout polynôme irréductible $p(X) \in F[X]$ ayant une racine dans E est scindé sur E.

Propriété 1.13. *Si E est un corps de racines d'un polynôme non nul $f(X) \in F[X]$, alors l'extension E/F est normale.*

Preuve. Notons $j_E : F \to E$ le plongement de l'extension E/F. On a vu que $E = F(Rac(f))$, où $Rac(f) = \{\theta_1, \ldots, \theta_n\}$ est l'ensemble des racines de $j_E^*(f(X))$ dans E. Soit $p(X)$ un polynôme irréductible dans $F[X]$ et supposons que $p(X)$ a une racine dans E, c'est-à-dire que le polynôme $j_E^*(p(X))$ a dans

l'anneau $E[X]$ un diviseur de degré un $\alpha X - \beta$, avec $\alpha \neq 0$ et β deux éléments de E. Posons alors $K = F\left(\frac{\beta}{\alpha}\right)$ qui est un sous-corps de E, et soit $j_K : F \to K$ le morphisme structural de l'extension K/F. Soit E' un corps de racines de $j_K^*(p(X)) \in K[X]$ sur K, et $j'_{E'}$ le morphisme structural de l'extension E'/K. On a alors dans $E'[X]$ la factorisation

$$j'^{*}_{E'}(j_K^*(p(X))) = q_1(X)q_2(X)\cdots q_d(X)$$

avec $\deg(q_j(X)) = 1$, $q_j(X) \in E'[X]$. On peut, quitte à multiplier les facteurs $q_j(X)$ par des constantes non nulles, imposer $q_1(X) = X - j'_{E'}\left(\frac{\beta}{\alpha}\right)$. Puisque $E = F(Rac(f))$, il existe dans l'anneau $F[X_1, \ldots, X_n]$ un polynôme P tel que $\frac{\beta}{\alpha} = j_E^*(P)(\theta_1, ..., \theta_n)$. Considérons alors le polynôme

$$g(X) := \prod_{\sigma \in S_n} (X - j_E^*(P)(\theta_{\sigma(1)}, ..., \theta_{\sigma(n)}))$$

qui est visiblement scindé sur E. En vertu du théorème des fonctions symétriques, les coefficients de $g(X)$ appartiennent au corps $j_E(F)$. Comme $p(X)$ est supposé irréductible dans $F[X]$, le polynôme $j_E^*(p(X))$ est irréductible dans l'anneau $j_E(F)[X]$. Comme il n'est pas premier à $g(X)$, il en est un diviseur dans $j_E(F)[X]$, donc $p(X)$ est scindé sur E. □

Théorème 1.14 (Unicité du corps des racines)**.** *Si E_1 et E_2 sont deux corps de racines de $f(X) \in F[X]$, alors E_1/F et E_2/F sont des extensions isomorphes de F.*

Preuve. cf corollaire 33 dans Rotman [33]. □

1.2.5 Corps de racines d'un polynôme séparable

Définition 14. Un polynôme non nul $f(X) \in F[X]$ est dit *séparable* lorsque tout facteur irréductible de $f(X)$ dans $F[X]$ est premier à sa dérivée.

Propriété 1.15. *Tout diviseur dans $F[X]$ d'un polynôme séparable est aussi séparable.*

Preuve. Tout facteur irréductible d'un quelconque diviseur de $f(X)$ est un facteur irréductible de $f(X)$. □

Définition 15. Soit E/F une extension, et $a \in F$. Le *polynôme minimal* de a sur E est le générateur unitaire, s'il existe, de l'idéal de $F[X]$ constitué des polynômes $g(X) \in F[X]$ tels que $j_E(g(X))^*(a) = 0$. Un élément a de E est dit *séparable* sur F si et seulement si il a un polynôme minimal séparable.

Définition 16. Une extension E/F est dite séparable si n'importe quel élément de E est séparable sur F.

Propriété 1.16. *Si $f(X) \in F[X]$ est séparable, alors tout corps de racines de $f(X)$ sur F est une extension séparable de F.*

Preuve. On peut utiliser un résultat connu [39, Theorem 14.12(b)] d'après lequel toute extension de la forme $F(S)/F$ est séparable dès que S est un ensemble d'éléments d'une extension donnée de F qui sont tous séparables sur F. Or, si N est corps des racines d'un polynôme séparable $f(X)$, alors on a vu (propriété 1.9) que $N = F(Rac(f))$. Notre résultat vient alors par la propriété 1.15. □

Propriété 1.17. *Si x est un élément d'une extension E/F, si x est algébrique et séparable sur F, et si $g(X)$ est le polynôme minimal de x sur F, alors tout corps de racines N/F de $g(X)$ sur F est une extension séparable de F.*

Preuve. Cas particulier de la propriété précédente. □

1.2.6 Groupe de Galois d'un polynôme séparable

Une *permutation* d'un ensemble X est une application bijective de X sur X. Pour tout ensemble X, on note $S(X)$ le *groupe symétrique sur* X, c'est-à-dire le groupe dont les éléments sont les permutations de X. Rappelons qu'on entend par *groupe de permutations* la donnée d'un triplet (G, X, π) constitué d'un groupe G, d'un ensemble X et d'un morphisme de groupes $\pi : G \to S(X)$. Un *isomorphisme de groupe de permutations* du groupe de permutations (G, X, π) sur un autre groupe de permutations (G', X', π') est la donnée de deux applications bijectives $\phi : G \to G'$ et $f : X \to X'$ telles que ϕ est un (iso)morphisme de groupes vérifiant l'identité $f \circ \pi(g) = \pi'(\phi(g)) \circ f$ pour tout élément $g \in G$.

Un F-automorphisme d'une extension E/F, de morphisme structural $j_E : F \to E$, est un automorphisme ρ du corps E tel que $\rho \circ j_E = j_E$, c'est-à-dire laissant fixes tous les éléments du sous-corps image $j_E(F)$ de F dans E.

Si $f(X)$ est un polynôme non nul à coefficients dans un corps F, et si E/F est une extension, notons $R_E(f)$ l'ensemble des racines du polynôme $j_E^*(f(X))$ dans E. On remarque que, lorsque ρ est un F-automorphisme de E, alors l'ensemble $R_E(f) \subset E$ est stable par l'application ρ. Le groupe G des F-automorphismes de l'extension E/F peut donc être utilisé pour construire un groupe de permutations $(G, R_E(f), \pi_f)$, où $\pi_f(\rho)$ est la permutation $a \mapsto \rho(a)$ des racines de $f(X)$ dans E. Ce groupe de permutations est appelé le *groupe des F-automorphismes de E agissant sur les racines de $f(X)$*.

Définition 17. Soit $f(X) \in F[X]$ un polynôme non nul séparable, et N/F un corps des racines de $f(X)$ sur le corps F. Le *groupe de Galois de $f(X)$ sur F* est la classe d'isomorphie de groupe de permutations du groupe des F-automorphismes de N agissant sur les racines $\theta_1, \ldots, \theta_n$ de $f(X)$ dans N.

Du fait que deux corps de racines sont isomorphes, il s'en suit que la classe d'isomorphie de groupe de permutations du groupe des F-automorphismes d'un corps de racines N agissant sur les racines de $f(X)$ dans N est déterminée de façon unique. Ce fait justifie la définition que nous venons de donner du groupe de Galois du polynôme $f(X)$.

1.3 Ramification

1.3.1 Corps valués

On appelle *corps valué* tout couple (F, v) où F est un corps, et où $v : F^* \to \mathbb{Z}$ est un morphisme de groupes satisfaisant l'*inégalité ultramétrique* : si a et b sont deux éléments non nuls de F, et si $a \neq b$, alors

$$v(a - b) \geq \min(v(a), v(b)) \; . \tag{1.3.1}$$

Un morphisme de groupes $v : F^* \to \mathbb{Z}$ satisfaisant (1.3.1) est aussi appelé une *valuation* du corps F. On supposera toujours que les valuations d'un corps F sont prolongées à F tout entier en posant $v(0) = +\infty$, de sorte que (1.3.1) reste vraie si $a = 0$, ou si $b = 0$, ou si $a = b$.

L'exemple de corps valué qui sera pratiqué dans le présent mémoire est celui de la *valuation p-adique* sur le corps $\mathbb{Q}$ des nombres rationnels, où p est un

nombre premier. Cette valuation, notée v_p, est définie par l'équivalence

$$v_p(x) = m \Longleftrightarrow \exists (a,b) \in (\mathbb{Z} \setminus p\mathbb{Z})^2, \qquad x = p^m a/b \tag{1.3.2}$$

pour tout $(x,m) \in \mathbb{Q}^* \times \mathbb{Z}$.

Lorsque v est l'application nulle de F^* dans $\mathbb{Z}$, on dit que la valuation v est *triviale*. Lorsque $v : F^* \to \mathbb{Z}$ est surjective, on dit que la valuation v est *normalisée*. Toute valuation non triviale $v : F^* \to \mathbb{Z}$ peut s'écrire de manière unique sous la forme $v = ew$, où $e \geq 1$ est un entier naturel, et où w est une valuation normalisée.

À tout corps valué (F, v), sont associés trois objets algébriques fondamentaux :

- l'*anneau des entiers* $\mathcal{O}_F$ (parfois aussi noté F°) : ses éléments sont les éléments $x \in F$ tels que $v(x) \geq 0$;

-l'*idéal maximal* $\mathfrak{m}_F$: ses éléments sont les éléments $x \in F$ tels que $v(x) > 0$;

-le *corps résiduel* : c'est l'anneau quotient $\bar{F} = \mathcal{O}_F/\mathfrak{m}_F$ de l'anneau des entiers par son idéal maximal.

Si (F, v) est un corps valué, on peut lui attacher la *distance* d_v définie par

$$\forall (a,b) \in k^2, \qquad d_v(a,b) = 2^{-v(a-b)} \, . \tag{1.3.3}$$

Le corps valué (F, v) est dit *complet* lorsque toute suite de points de F, qui est de Cauchy au sens de la distance d_v, converge, aussi au sens de la distance d_v, vers une limite appartenant à F.

À tout corps valué (F, v) est associé un *complété* obtenu en ajoutant aux éléments de F les limites des suites de Cauchy à valeurs dans F. On obtient ainsi un corps valué complet $(\hat{F}, \hat{v})$ tel que F est un sous-corps dense de $\hat{F}$, et v est la restriction à F de $\hat{v}$. Ce procédé de complétion est tout-à-fait analogue à celui par lequel on construit le corps des réels $\mathbb{R}$ à partir du corps des rationnels $\mathbb{Q}$. En particulier, quand on l'applique au corps $\mathbb{Q}$ muni de la valuation p-adique, où p est un nombre premier, on obtient le corps $\mathbb{Q}_p$ des nombres p-adiques. Dans ce procédé de complétion, le corps résiduel ne change pas, c'est-à-dire que l'application naturelle $x + \mathfrak{m}_F \mapsto x + \mathfrak{m}_{\hat{F}}$ est un isomorphisme entre le corps résiduel $\bar{F} = \mathcal{O}_F/\mathfrak{m}_F$ du corps valué F et le corps résiduel $\bar{\hat{F}} = \mathcal{O}_{\hat{F}}/\mathfrak{m}_{\hat{F}}$ du corps valué $\hat{F}$.

D'autre part, il y a unicité du completé du corps valué F, en ce sens que si le corps valué (F, v) est un sous-corps dense de deux corps valués complets

$(\hat{F}, \hat{v}$ et $(\tilde{F}, \tilde{v})$, tels que les restrictions des valuations $\hat{v}$ et $\tilde{v}$ au sous-corps F sont toutes deux égales à v, alors il existe un unique isomorphisme ϕ de $\hat{F}$ sur $\tilde{F}$, isométrie au sens où $\tilde{v} \circ \phi = \hat{v}$, et fixant tous les points de F.

1.3.2 Extensions d'un corps valué

Soit (F, v) un corps commutatif, et $E \supseteq F$ un surcorps de F. Si $w : E \to \mathbb{Z} \cup \{+\infty\}$ est une valuation normalisée de E, sa restriction v à F est évidemment une valuation de F, pas toujours normalisée. Lorsque v est normalisée, on dit que l'extension E/F de corps valués est *non ramifiée en* w. Plus généralement, dans le cas où v est non triviale, on peut l'écrire de manière unique sous la forme $v = ev_0$, où v_0 est normalisée. L'entier $e \geq 1$ est alors appelé l'*indice de ramification en* w de l'extension E/F. Dans le cas où v serait triviale, on posera $e = +\infty$.

Proposition 1.18. *Une extension E/F de corps valués est non ramifiée si et seulement si son indice de ramification est égal à 1.*

On définit aussi la notion d'*extension finie totalement ramifiée* : ce sont les extensions finies de corps valués dont l'indice de ramification est égal au degré.

Dans les hypothèses précédentes, le corps résiduel $\bar{F} = \mathcal{O}_F/\mathfrak{m}_F$ du corps de base F se plonge dans le corps résiduel $\bar{E} = \mathcal{O}_E/\mathfrak{m}_E$ par le plongement $\bar{\jmath}$ défini par

$$\forall x \in \mathcal{O}_F, \qquad \bar{\jmath}(x + \mathfrak{m}_F) = x + \mathfrak{m}_E \ .$$

On obtient ainsi une extension $\bar{E}/\bar{F}$, appelée l'*extension résiduelle* de l'extension E/F de corps valués. Le degré de cette extension résiduelle est appelé le *degré résiduel* de l'extension E/F de corps valués.

Dans le cas où l'extension E/F est finie et galoisienne, on définit le *groupe de décomposition* de w dans l'extension E/F, noté $D(w/v)$, par

$$D(w/v) = \{\sigma \in \mathrm{Aut}_F(E), \sigma(\mathcal{O}_E) \subseteq \mathcal{O}_E\} \ .$$

On définit de même le *groupe d'inertie* de w dans l'extension E/F, noté $I(w/v)$, par

$$I(w/v) = \{\sigma \in \mathrm{Aut}_F(E), \forall x \in \mathcal{O}_E, \ \ \sigma(x) - x \in \mathfrak{m}_E\} \ .$$

Le groupe d'inertie est évidemment un sous-groupe du groupe de décomposition.

Théorème 1.19. *L'ordre du groupe d'inertie $I(w/v)$ est égal à l'indice de ramification en w de l'extension E/F.*

Preuve. Une démonstration se trouve dans la monographie de Serre sur les corps locaux [37, pp. 31-32].

On a alors un morphisme $\sigma \mapsto \bar{\sigma}$ du groupe de décomposition $D(w/v)$ sur le groupe $\mathrm{Aut}_{\bar{F}}(\bar{E})$ défini par l'identité

$$\forall x \in \mathcal{O}_E, \qquad \bar{\sigma}(x + \mathfrak{m}_E) = \sigma(x) + \mathfrak{m}_E \ .$$

Ce morphisme est surjectif, de noyau égal au groupe d'inertie. Par conséquent, le groupe d'inertie $I(w/v)$ est un sous-groupe distingué du groupe de décomposition $D(w/v)$. Comme le morphisme $\sigma \mapsto \bar{\sigma}$ est surjectif, le quotient $D(w/v)/I(w/v)$ est isomorphe au groupe $\mathrm{Aut}_{\bar{F}}(\bar{E})$ des $\bar{F}$-automorphismes de $\bar{E}$ (ceci est démontré dans Serre [37, Proposition 20, p. 32]).

Proposition 1.20. *Soit (E, w) un corps valué tel que la valuation w de E est normalisée, soit F un sous-corps de E tel que l'extension E/F est finie galoisienne, et soit v la restriction de w à F. Si le corps résiduel du corps valué (F, v) est fini, alors le quotient $D(w/v)/I(w/v)$ est cyclique.*

Preuve. Toute extension finie d'un corps fini est cyclique. □

Corollaire 1.21. *Soit (E, w) un corps valué tel que la valuation w de E est normalisée, soit F un sous-corps de E tel que l'extension E/F est finie galoisienne, et soit v la restriction de w à F. Si l'extension E/F de corps locaux est non ramifiée en w, et si le corps résiduel du corps valué (F, v) est fini, alors le groupe de décomposition $D(w/v)$ est cyclique.*

Lorsque le corps valué (F, v) est complet, et si E/F est une extension finie, on montre que (E, w) doit être également complet. De plus, tout automorphisme σ de E doit alors être une isométrie du corps (E, w), au sens que $w \circ \sigma = w$. Par conséquent, lorsque l'on suppose de plus que l'extension E/F est galoisienne, le groupe de décomposition $D(w/v)$ est dans cette situation égal au groupe $\mathrm{Aut}_F(E)$ de tous les automorphismes de E fixant les points de F.

Plus généralement, pour toute extension finie E/F de corps telle que $E \supseteq F$, si w est une valuation normalisée sur E, de restriction v à F, on peut plonger E dans son complété $\hat{E}$, et considérer l'*extension locale* $\hat{E}/\bar{F}$, où $\bar{F}$ est

l'adhérence de F dans $\hat{E}$. On sait par la propriété d'unicité du complété que $\bar{F}$ est isomorphe au completé $\hat{F}$ de F, de sorte que l'extension locale peut aussi être vue comme l'extension des complétés. Dans la situation où l'on suppose de plus que l'extension E/F est galoisienne, alors le groupe de décomposition $D(w/v)$ s'identifie au groupe des $\bar{F}$-automorphismes de $\hat{E}$.

Dans la situation où (F, v) est un corps valué, on peut se poser réciproquement la question de prolonger v en une valuation du surcorps $E \supseteq F$. Ce n'est pas toujours possible à cause de la ramification. C'est pourquoi nous reformulons le problème sous la forme suivante. Etant donné le corps valué (F, v), où v est normalisée, et le surcorps $E \supseteq F$, trouver un entier $e \geq 1$ et une valuation w de E tels que la restriction de w à F s'écrive ev. Lorsque F est complet pour v, et que l'extension E/F est finie, on a un résultat particulièrement simple.

Théorème 1.22. *Soit (F, v) un corps valué complet, où v est une valuation normalisée de F, et $E \supseteq F$ un surcorps de F. Si l'extension E/F est finie, et si la valuation v est non triviale, alors il existe un unique entier $e \geq 1$ et une unique valuation normalisée w de E telle que la restriction de w à F est égale à ev. On a la* relation fondamentale

$$[E : F] = ef \ ,$$

où f est le degré résiduel de l'extension E/F de corps valués.

1.3.3 Polygones de Newton

Nous décrivons ici une méthode, originellement exposée par Ore [29], qui permet, à partir de certains polygones, de décrire partiellement la factorisation sur un corps valué complet d'un polynôme unitaire. Elle fournit aussi des renseignements assez précis sur la ramification des extensions du corps en question qui sont engendrées par des racines du polynôme considéré.

Soit $f(X)$ un polynôme unitaire de degré $n \geq 1$ à coefficients dans un corps valué complet (K, v). Pour un quelconque polynôme unitaire $\varphi(X) \in \mathcal{O}_K[X]$, dont la projection $\bar{\varphi}(X)$ est irréductible sur le corps résiduel de K, on écrit par divisions euclidiennes successives le $\varphi(X)$-développement de $f(X)$ sous la forme

$$f(X) = \sum_{j=0}^{t} Q_j(X)\varphi(X)^{t-j} \ , \tag{1.3.4}$$

où $\deg(Q_j(X)) < \deg(\varphi(X))$. On note alors v_j le minimum des valuations de tous les coefficients de $Q_j(X)$. Le *nuage de Newton* de $f(X)$ relativement à K et $\varphi(X)$ est l'ensemble des points du plan de la forme (j, v_j) pour $j \in [0..t]$. Le (K, φ)-*polygone* de $f(X)$ est la frontière de l'enveloppe convexe supérieure des points du nuage de Newton, privée des deux côtés verticaux : c'est une figure du plan réunion d'un ou plusieurs segments dont les pentes vont en croissant strictement de gauche à droite. Un tel segment est appelé un *côté* du polygone de Newton. Lorsqu'on suppose de plus que tous les coefficients de $f(X)$ sont éléments de $\mathcal{O}_K$, tout côté du polygone de Newton a une pente ≥ 0 : il peut exister ou non un côté horizontal, c'est-à-dire de pente 0. La *partie principale* du polygone de Newton de $f(X)$ est constituée par les côtés non horizontaux de ce polygone. Soit S un côté de la partie principale du (K, φ)-polygone du polynôme unitaire $f(X) \in \mathcal{O}_K[X]$. On attache à ce côté un *polynôme associé* $F_S(X, Y) \in \mathcal{O}_K[X, Y]$, qui en fait n'interviendra dans nos résultats qu'à travers sa classe modulo $\pi\mathcal{O}_K[X, Y] + \varphi(X)\mathcal{O}_K[X, Y]$. Cette classe peut être calculée de la manière suivante [12, Proposition 3.4]. On choisit un élément π de K tel que $v(\pi) = 1$, et on commence par calculer la pente $\rho > 0$ du côté S, qu'on exprime sous la forme du quotient $\rho = \frac{\kappa}{\lambda}$ de deux entiers strictement positifs premiers entre eux, puis on munit le corps $K(X)$ de la valuation $w : K(X) \to \mathbb{Z} \cup \{+\infty\}$ telle que

$$w(\sum_j Q_j(X)\varphi(X)^j) = \min_j(v(Q_j(\zeta)) + j\rho) \ ,$$

où tous les polynômes $Q_j(X)$ sont de degrés strictement moindres que le degré de $\varphi(X)$, et où v est l'unique prolongement de la valuation de K à un corps E de rupture de $\varphi(X)$ sur K, la notation ζ désignant une racine de $\varphi(X)$ dans E. Soit L la somme de toutes les longueurs des projections horizontales des côtés de pente strictement supérieure à ρ, et H la somme de toutes les longueurs des projections verticales des côtés de pente inférieure ou égale à ρ. On vérifie que l'application w donne au quotient

$$\frac{f(X)}{\varphi(X)^L \pi^H}$$

une image nulle. En réduisant ce polynôme modulo l'idéal maximal de la valuation w, on obtient un polynôme en $Y = \frac{X^\lambda}{\pi^\kappa}$ à coefficients dans le corps résiduel de l'extension $K(\zeta)$. On divise ce polynôme par son coefficient dominant, obte-

nant un polynôme en Y, qui est la classe désirée du polynôme $F_S(X,Y)$ associé au côté S.

Le côté S est dit *régulier* si la classe du polynôme associé $\pi\mathcal{O}_K[X,Y] + \varphi(X)\mathcal{O}_K[X,Y]$, qui est un polynôme en Y à coefficients dans le corps résiduel de $K(\zeta)$, est premier à sa dérivée par rapport à Y.

On a alors le résultat suivant.

Théorème 1.23. *[12, Theorem 1.5] Soit $f(X) \in \mathcal{O}_K[X]$ un polynôme unitaire. Si on a la factorisation*

$$f(X) \equiv \varphi_1(X)^{a_1} \dots \varphi_s(X)^{a_s} \pmod{\pi\mathcal{O}_K[X]},$$

où chaque polynôme $\varphi_\nu(X)$ est irréductible modulo π et est choisi de sorte que $\varphi_\nu(X)$ ne divise pas $f(X)$, alors on en déduit la factorisation suivante de $f(X)$.

$$f(X) = \Phi_1(X) \cdots \Phi_s(X),$$

où $\Phi_s(X)$ est un polynôme unitaire à coefficients dans $\mathcal{O}_K$, tel que

$$\Phi_\nu(X) \equiv \varphi_\nu(X)^{a_\nu} \pmod{\pi\mathcal{O}_K[X]}.$$

Supposons que la partie principale du (K,φ_ν)-polygone de Newton est composé de k côtés $S_1,\dots,S_k$. Pour chaque indice $i \in [1..k]$, on considère les entiers ℓ_i et h_i qui sont les longueurs des projections respectivement horizontale et verticale du côté S_i, et on pose $\lambda_i = \frac{\ell_i}{\operatorname{pgcd}(\ell_i,h_i)}$. On factorise le polynôme associé $F_i(X,Y)$ au côté S_i sous la forme

$$F_i(X,Y) \equiv F_1^{(i)}(X,Y)^{a_1^{(i)}} \cdots F_{t_i}^{(i)}(X,Y)^{a_{t_i}^{(i)}} \pmod{\pi\mathcal{O}_K[X,Y]+\varphi(X)\mathcal{O}_K[X,Y]},$$

où la classe de $F_j^{(i)}(X,Y)$ modulo $\pi\mathcal{O}_K[X,Y] + \varphi(X)\mathcal{O}_K[X,Y]$ est irréductible en tant qu'élément de l'anneau $\overline{K(\zeta)}[Y]$. Alors on a

$$\Phi_\nu(X) = \prod_{i=1}^{k} \prod_{j=1}^{t_i} \Phi_j^{(i)}(X)$$

où le facteur $\Phi_j^{(i)}(X)$ est un polynôme unitaire à coefficients dans $\mathcal{O}_K$, de degré

$$\deg(\phi_\nu(X)) \deg_Y(F_j^{(i)}(X,Y)) a_j^{(i)} \lambda_i,$$

tel que l'indice de ramification de l'extension $K(\alpha)/K$ est divisible par λ_i pour toute racine α du facteur $\Phi_j^{(i)}(X)$.

Si de plus le côté S_i est régulier, alors les polynômes $\Phi_j^{(i)}(X)$ sont irréductibles dans $K[X]$, et l'indice de ramification de l'extension $K(\alpha)/K$ est égal à λ_i pour toute racine α du facteur $\Phi_j^{(i)}(X)$.

Chapitre 2

Groupes de Galois de trinômes

2.1 Introduction

Dans ce chapitre, nous commençons par la notion du résultant de deux polynômes. Nous avons voulu apporter et démontrer certaines propriétés concernant cette notion [39, 3]. Cette notion conduira ensuite à la formule du discriminant d'un polynôme en général pour arriver enfin à celui d'un trinôme qui est l'objet de notre chapitre. Il s'en suit la classification des trinômes.

2.2 Le discriminant d'un trinôme

2.2.1 Résultant de deux polynômes

Soit A un anneau unitaire, commutatif et intègre, m et n deux entiers naturels. Considérons deux polynômes $f(X), g(X) \in A[X]$, de degrés respectivement $\leq m$ et $\leq n$:

$$f(X) = \sum_{i=0}^{m} a_i X^{m-i} \quad , \quad g(X) = \sum_{i=0}^{n} b_i X^{n-i}.$$

Pour tout entier naturel k, on introduit le A-module libre de rang k, noté A_k, dont les éléments sont les polynômes de $A[X]$ ayant un degré $< k$. On observe que, par division euclidienne par le monôme X^n, tout élément de A_{m+n} s'écrit de façon unique sous la forme $u(X) + X^n v(X)$, où $u(X)$ et $v(X)$ sont des polynômes de degré respectivement moindres que n et m. On dispose alors de l'endomorphisme κ du module A_{m+n}, dépendant des choix à la fois des polynômes $f(X)$ et $g(X)$ et des entiers $m \geq \deg(f(X)$ et $n \geq \deg(g(X))$, défini

par la relation

$$\kappa(u(X) + X^n v(X)) = u(X)f(X) + v(X)g(X) \ . \tag{2.2.1}$$

En particulier, pour $1 \leq j \leq n$, on a

$$\kappa(X^{j-1}) = X^{j-1}f(X) = \sum_{i=0}^{m} a_i X^{m-i+j-1} = \sum_{k=j}^{m+j} a_{m+j-k} X^{k-1} \ ,$$

alors que, pour $n+1 \leq j \leq m+n$, on a

$$\kappa(X^{j-1}) = X^{j-n-1}g(X) = \sum_{i=0}^{n} b_i X^{j-i-1} = \sum_{k=j-n}^{j} b_{j-k} X^{k-1} \ .$$

Par conséquent, en rapportant le A-module libre A_{m+n} à la base $(X^{j-1})_{1\leq j\leq m+n}$, l'application linéaire κ a pour matrice la transposée de la *matrice de Sylvester* de f et g, notée $\mathrm{Syl}_{m,n}(f,g)$, c'est-à-dire, la matrice carrée de taille $m+n$, à coefficients dans A, telle que :

$$\mathrm{Syl}_{m,n}(f,g) = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_m & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_m & a_{m-1} & a_{m-2} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_n & \cdots & b_2 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & b_n & b_{n-1} & b_{n-2} & \cdots & b_0 \end{pmatrix}$$

Définition 18. Le *résultant de type* (m,n) *de* $f(X)$ *et* $g(X)$, noté $\mathrm{Res}_{m,n}(f,g)$, est le déterminant de l'endomorphisme κ, c'est-à-dire le déterminant de la matrice de Sylvester de f et g :

$$\mathrm{Res}_{m,n}(f,g) = \det(\mathrm{Syl}_{m,n}(f,g)) \in A.$$

Remarque 2.1. Il convient de remarquer que la plupart des auteurs [23, 3, 7] définissent la matrice de Sylvester de façon légèrement différente en écrivant les coefficients des deux polynômes $f(X)$ et $g(X)$ suivant l'ordre décroissant des degrés en allant de gauche à droite. Ceci revient à modifier la définition du résultant de deux polynômes $f(X)$ et $g(X)$ en leur substituant leurs polynômes réciproques. Mais la définition de l'endomorphisme κ serait moins directe si l'on devait y faire intervenir les polynômes réciproques, d'où le choix ici fait d'une convention différente. On verra d'ailleurs ci-dessous que ceci ne change que le signe du résultant dans certaines situations (en fait uniquement si les deux entiers m et n sont tous deux impairs).

Exemple 2.2. Si f et g sont deux constantes, on peut prendre $m = n = 0$, de sorte que le module A_{m+n} se réduit au module nul. Dans ce cas, on applique la convention usuelle selon laquelle le déterminant de l'unique endomorphisme du module nul est égal à 1. On a donc $\mathrm{Res}_{0,0}(f, g) = 1$ pour deux polynômes constants f et g.

Exemple 2.3. Plus généralement, si l'un des polynômes f ou g est une constante, on peut prendre respectivement $m = 0$ ou $n = 0$. On vérifie dans ce cas que l'endomorphisme κ est une homothétie dont le rapport est la constante en question, de sorte qu'on a $\mathrm{Res}_{0,n}(a, g) = a^n$ pour tout polynôme constant $f = a$ et pour tout polynôme $g(X)$ de degré au plus n, et aussi $\mathrm{Res}_{m,0}(f, a) = a^m$ pour tout polynôme $f(X)$ de degré au plus m et pour tout polynôme constant $g = a$.

Exemple 2.4. Si $f(X)$ est une constante a, et si $g(X) = b_0X^n + \cdots + b_n$, on a

$$\forall j \in [1..m+n], \qquad \kappa(X^{j-1}) = \begin{cases} aX^{j-1} & \text{si } j \leq n \\ X^{j-1-n}g(X) & \text{si } j \geq n+1 \end{cases}.$$

Ecrivant la matrice de Sylvester, qui est ici une matrice triangulaire inférieure, on voit que $\mathrm{Res}_{m,n}(a, g) = a^n b_0^m$.

Dans ce qui suit, nous allons énoncer et établir quelques propriétés du résultant que nous venons de définir. Ces propriétés sont bien connues, mais la démarche des preuves est originale : il s'agit de tout justifier par des propriétés convenables des endomorphismes κ ou de leurs diverses variantes.

Théorème 2.1. *Soit deux entiers naturels m et n, et $f(X), g(X)$ deux polynômes tels que* $\deg(f(X)) \leq m, \deg(g(X)) = n$, *avec le coefficient dominant*

b_0 de $g(X)$ inversible dans l'anneau A. On définit sur l'algèbre $A[X]/(g(X))$ l'endomorphisme γ « de multiplication par $f(X)$ » :

$$\forall F(X) \in A[X], \qquad \gamma(F(X) + (g(X)) = F(X)f(X) + (g(X)) \ .$$

On a alors la formule de Poisson

$$\mathrm{Res}_{m,n}(f, g) = b_0^m \det(\gamma) \ .$$

Preuve. On introduit les endomorphismes suivants du A-module libre A_{m+n}.

Si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa(u(X)+X^n v(X)) = u(X)f(X)+v(X)g(X)$

Si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa_0(u(X)+X^n v(X)) = u(X)+v(X)g(X)$.

Par définition du résultant, on a $\mathrm{Res}_{m,n}(f, g) = \det(\kappa)$. De plus, les hypothèses faites sur $g(X)$ entraînent la bijectivité de l'endomorphisme κ_0, et que tout élément de A_{m+n} s'écrit de façon unique sous la forme $u(X) + v(X)g(X)$, où $\deg(u(X)) < n$ et $\deg(v(X)) < m$. Par conséquent, on peut caractériser l'endomorphisme $\kappa \circ \kappa_0^{-1}$ par le fait qu'il envoie un polynôme de la forme $u(X) + v(X)g(X)$, avec $\deg(u(X)) < n$ et $\deg(v(X)) < m$, sur le polynôme $u(X)f(X)+v(X)g(X)$. On a d'autre part la suite exacte courte de A-modules :

$$0 \longrightarrow A_m \longrightarrow A_{m+n} \longrightarrow A[X]/(g(X)) \longrightarrow 0,$$

où l'injection $A_m \to A_{m+n}$ est la multiplication par $g(X)$. Observons que le terme de droite $A[X]/(g(X))$ dans cette suite exacte admet la base $(X^k + (g(X)))_{0 \le k < n}$: c'est donc un module libre de rang n, ce qui permet de définir le déterminant d'un endomorphisme, par exemple γ. On s'assure immédiatement que l'endomorphisme $\kappa \circ \kappa_0^{-1}$ du terme central A_{m+n} de cette suite exacte induit sur le terme de droite l'endomorphisme γ, et sur le terme de gauche l'identité. Donc on a $\det(\kappa \circ \kappa_0^{-1}) = \det(\gamma)$. Comme $\det(\kappa_0) = \mathrm{Res}_{m,n}(1, g) = b_0^m$, le résultat voulu est démontré. □

Exemple 2.5. Si $g(X) = X - r$ est un polynôme unitaire de degré 1, dont $r \in A$ est racine, on peut choisir $n = 1$. D'après la formule de Poisson, $\mathrm{Res}_{m,1}(f, X - r) = \det(\gamma)$, où γ est l'endomorphisme de l'algèbre quotient $A[X]/(X - r)$ qui envoie la classe d'un polynôme $F(X) \in A[X]$ sur la classe du polynôme $F(X)f(X)$. Or le morphisme d'anneaux qui à $F(X) \in A[X]$ associe $F(r)$ induit

un isomorphisme de A-algèbres de l'algèbre quotient $A[X]/(X-r)$ sur A. Par conséquent, tout endomorphisme de $A[X]/(X-r)$ est une homothétie, et son déterminant est le rapport de cette homothétie. Pour l'endomorphisme γ, du fait que $f(X) \equiv f(r) \pmod{X-r}$, le rapport est égal à $f(r)$. On a donc

$$\mathrm{Res}_{m,1}(f, X-r) = f(r)\ . \tag{2.2.2}$$

Propriété 2.2. *Soit $\phi : A \to A'$ un morphisme d'anneaux, m et n deux entiers naturels, $f(X) \in A[X]$ et $g(X) \in A[X]$ deux polynômes à coefficients dans A, avec $\deg(f(X)) \leq m$ et $\deg(g(X)) \leq n$. On note ϕ^* l'unique morphisme d'anneaux de $A[X]$ dans $A'[X]$ prolongeant ϕ et tel que $\phi^*(X) = X$. On a alors la* formule de spécialisation

$$\mathrm{Res}_{m,n}(\phi^*(f), \phi^*(g)) = \phi(\mathrm{Res}_{m,n}(f,g))\ .$$

Preuve. La matrice de Sylvester $\mathrm{Syl}_{m,n}(\phi^*(f), \phi^*(g))$ a pour éléments les coefficients des polynômes $\phi^*(f)(X)$ et $\phi^*(g)(X)$, qui sont les images par le morphisme ϕ des coefficients analogues des polynômes $f(X)$ et $g(X)$, où l'on reconnaît les éléments de la matrice $\mathrm{Syl}_{m,n}(f,g)$. La propriété de naturalité du déterminant par rapport aux morphismes d'anneaux donne alors la formule de spécialisation. □

Lemme 2.3. *Soit $f^*(X) = X^m f(X^{-1})$ et $g^*(X) = X^n g(X^{-1})$ les polynômes « réciproques »de $f(X)$ et de $g(X)$. L'endomorphisme κ^* défini par le couple $(f^*(X), g^*(X))$ en degrés m et n est conjugué à l'endomorphisme κ_1 défini par le couple $(g(X), f(X))$ en degrés n et m.*

Preuve. Explicitement, on a d'après (2.2.1)

si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa^*(u(X)+X^n v(X)) = u(X)f^*(X)+v(X)g^*(X$

si $\deg(u_1(X)) < m$ et $\deg(v_1(X)) < n$, alors $\kappa_1(u_1(X)+X^m v_1(X)) = u_1(X)g(X)+v_1(X$

On introduit alors l'application $\rho : A_{m+n} \to A_{m+n}$ définie par

$$\forall F(X) \in A_{m+n}, \qquad \rho(F(X)) = X^{m+n-1} F(X^{-1})\ .$$

Un calcul direct montre que $\rho \circ \kappa^* = \kappa_1 \circ \rho$. Comme ρ est une involution de A_{m+n}, donc bijective, le résultat voulu s'ensuit. □

Propriété 2.4. *Avec les notations précédentes, on a l'égalité*

$$\mathrm{Res}_{m,n}(f^*, g^*) = \mathrm{Res}_{n,m}(g, f) \ .$$

Preuve. Deux endomorphismes conjugués ont le même déterminant. □

Lemme 2.5. *Soit σ la permutation de l'ensemble $\{1, \ldots, m+n\}$ des $m+n$ premiers entiers strictement positifs définie par*

$$\sigma(j) = \begin{cases} j+m & \text{si } j \leq n \\ j-n & \text{si } j \geq n+1 \end{cases} \ .$$

La permutation σ a exactement mn inversions.

Preuve. Un couple (j, j') d'entiers tels que $1 \leq j < j' \leq m+n$ est une inversion de σ si et seulement si on a à la fois $1 \leq j \leq n$ et $n+1 \leq j' \leq m+n$. □

Propriété 2.6. *Pour deux polynômes $f(X)$ et $g(X)$ et deux entiers naturels m et n tels que* $\deg(f(X)) \leq m$ *et* $\deg(g(X)) \leq n$, *on a la* formule d'échange

$$\mathrm{Res}_{m,n}(f, g) = (-1)^{mn}\mathrm{Res}_{n,m}(g, f) \ .$$

Preuve. On introduit les endomorphismes κ, κ_1, τ du A-module libre A_{m+n} définis comme suit.

Si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa(u(X)+X^n v(X)) = u(X)f(X)+v(X)g(X)$

Si $\deg(u_1(X)) < m$ et $\deg(v_1(X)) < n$, alors $\kappa_1(u_1(X)+X^m v_1(X)) = u_1(X)g(X)+v_1(X$

Si $\deg(u(X)) < m$ et $\deg(v(X)) < m$, alors $\tau(u(X)+X^n v(X)) = v(X)+X^m u(X)$.

Par la définition du résultant, on a $\mathrm{Res}_{m,n}(f, g) = \det(\kappa)$ et $\mathrm{Res}_{n,m}(g, f) = \det(\kappa_1)$. On vérifie immédiatement la relation $\kappa = \kappa_1 \circ \tau$, d'où il suit l'égalité $\det(\kappa) = \det(\kappa_1)\det(\tau)$. Ainsi pour conclure à l'égalité désirée, il suffira de montrer que $\det(\tau) = (-1)^{mn}$. Pour calculer ce déterminant, on considére la base de A_{m+n} constituée par les monômes X^{j-1}, où j décrit l'ensemble des entiers entre 1 et $m+n$. On s'assure facilement que

$$\forall j \in [1..m+n], \qquad \tau(X^{j-1}) = X^{\sigma(j)-1} \ ,$$

où σ est la permutation introduite dans l'énoncé du lemme 2.5. Par conséquent, la matrice de τ dans la base considérée s'identifie à la matrice de la permutation σ, et $\det(\tau)$ est donc la signature de σ. On conclut en utilisant le lemme 2.5. □

En rapprochant les propriétés 2.4 et 2.6, on obtient immédiatement l'énoncé qui suit.

Propriété 2.7. *Pour deux polynômes $f(X)$ et $g(X)$ et deux entiers naturels m et n tels que* $\deg(f(X)) \leq m$ *et* $\deg(g(X)) \leq n$*, si $f^*(X) = X^m f(X^{-1})$ et $g^*(X) = X^n g(X^{-1})$, alors on a l'égalité*

$$\mathrm{Res}_{m,n}(f^*, g^*) = (-1)^{mn}\mathrm{Res}_{m,n}(f, g) \ .$$

Propriété 2.8. *Soit deux polynômes $f(X)$ et $g(X)$ et deux entiers naturels m et n tels que $m \geq n$,* $\deg(f(X)) \leq m$ *et* $\deg(g(X)) \leq n$*. Si on a $f(X) = q(X)g(X)+r(X)$, avec* $\deg(q(X)) \leq m-n$ *(et donc* $\deg(r(X)) \leq m$*), alors on a la* formule de Laplace

$$\mathrm{Res}_{m,n}(f, g) = \mathrm{Res}_{m,n}(r, g) \ .$$

Preuve. On introduit les endomorphismes κ, κ_1, τ du A-module libre A_{m+n} définis comme suit.

Si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa(u(X)+X^n v(X)) = u(X)f(X)+v(X)g(X)$

Si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa_1(u(X)+X^n v(X)) = u(X)r(X)+v(X)g(X)$

Si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\tau(u(X)+X^n v(X)) = u(X)+X^n(v(X)-q(X)$

Par définition du résultant, on a $\det(\kappa) = \mathrm{Res}_{m,n}(f, g)$ et $\det(\kappa_1) = \mathrm{Res}_{m,n}(r, g)$. On vérifie immédiatement l'égalité $\kappa_1 = \kappa \circ \tau$, de sorte qu'on est ramené à montrer que le déterminant de τ est égal à 1. On vérifie grâce à la définition de l'endomorphisme τ que, pour tout entier $j \in [1..n+m]$, la différence $\tau(X^{j-1})-X^{j-1}$ est divisible par X^j. Ceci signifie que la matrice de τ dans la base $\left(X^{j-1}\right)_{1\leq j\leq m+n}$ est une matrice triangulaire inférieure dont tous les coefficients diagonaux valent 1. Une telle matrice est évidemment de déterminant égal à 1. □

Propriété 2.9. *Soit deux polynômes $f(X)$ et $g(X)$ et trois entiers naturels h, m et n, tels que $h < m$,* $\deg(f(X)) \leq m-h$ *et* $\deg(g(X)) \leq n$*. Alors on a la* formule de changement de type

$$\mathrm{Res}_{m,n}(f, g) = b_0^h \ \mathrm{Res}_{m-h,n}(f, g) \ ,$$

où b_0 est le coefficient du terme de degré n dans $g(X)$.

Preuve. Par récurrence, il suffit de traiter le cas où $h = 1$. On considère les endomorphismes κ_{m+n} et κ_{m-1+n}, respectivement des A-modules libres A_{m+n} et A_{m-1+n} définis par :

si $\deg(u(X)) < n$ et $\deg(v(X)) < m$, alors $\kappa_{m+n}(u(X)+X^n v(X)) = u(X)f(X)+v(X)g($

si $\deg(u(X)) < n$ et $\deg(v(X)) < m-1$, alors $\kappa_{m-1+n}(u(X)+X^n v(X)) = u(X)f(X)+v($

On remarque que κ_{m+n} laisse stable le sous-module A_{m-1+n}, et qu'il induit sur ce sous-module l'endomorphisme κ_{m-1+n}. Un supplémentaire S de ce sous-module dans A_{m+n} est le module engendré par X^{m-1+n}. Or

$$\kappa_{m+n}(X^{m-1+n}) = X^{m-1}g(X) = \sum_{j=m-1}^{m-1+n} b_{m-1+n-j}X^j \,,$$

a une composante $b_0 X^{m-1+n}$ dans le supplémentaire S. Il en résulte que $\det(\kappa_{m+n}) = \det(\kappa_{m-1+n})b_0$, c'est-à-dire $\mathrm{Res}_{m,n}(f,g) = b_0\,\mathrm{Res}_{m-1,n}(f,g)$. □

Propriété 2.10. *Soit deux polynômes $f(X)$ et $g(X)$ et trois entiers naturels h, m et n, tels que $h < n$, $\deg(f(X)) \leq m$ et $\deg(g(X)) \leq n-h$. Alors on a la* (deuxième) formule de changement de type

$$\mathrm{Res}_{m,n}(f,g) = a_0^h\,(-1)^{hm}\mathrm{Res}_{m,n-h}(f,g)\,,$$

où a_0 est le coefficient du terme de degré m dans $f(X)$.

Preuve. Résulte immédiatement des propriétés 2.6 et 2.9. □

Propriété 2.11. *Soient trois polynômes $f_1(X), f_2(X), g(X)$ et trois entiers naturels m_1, m_2 et n tels que $\deg(f_1(X)) \leq m_1, \deg(f_2(X)) \leq m_2$ et $\deg(g(X)) \leq n$. On a alors la* formule de multiplicativité

$$\mathrm{Res}_{m_1+m_2,n}(f_1f_2,g) = \mathrm{Res}_{m_1,n}(f_1,g)\mathrm{Res}_{m_2,n}(f_2,g)\,.$$

Preuve. Soit b_0 le coefficient du terme de degré n dans le polynôme $g(X)$. Il existe un anneau A'', un sous-anneau A' de A'', un morphisme $\phi : A' \to A$, et un élément b_0' de A' inversible dans A'' tels que $\phi(b_0') = b_0$. Par conséquent, en utilisant la formule de spécialisation, il suffit de vérifier la multiplicativité quand b_0 est inversible. Dans ce cas, on peut utiliser la formule de Poisson, d'après laquelle

$$\mathrm{Res}_{m_1+m_2,n}(f_1f_2,g) = b_0^{m_1+m_2}\det(\gamma),$$

où γ est l'endomorphisme de multiplication par $f_1(X)f_2(X)$ dans l'algèbre quotient $A_g := A[X]/(g(X))$. De même, on a, pour $i \in \{1,2\}$

$$\mathrm{Res}_{m_i,n}(f_i,g) = b_0^{m_i}\det(\gamma_i)\,,$$

où γ_i est l'endomorphisme de multiplication par $f_i(X)$ dans A_g. Il est immédiat que $\gamma = \gamma_1 \circ \gamma_2$, d'où le résultat. □

Propriété 2.12. *Soient trois polynômes $f(X), g_1(X), g_2(X)$ et trois entiers naturels m, n_1 et n_2 tels que* $\deg(f(X)) \leq m, \deg(g_1(X)) \leq n_1$ *et* $\deg(g_2(X)) \leq n_2$. *On a alors la* (deuxième) formule de multiplicativité

$$\mathrm{Res}_{m,n_1+n_2}(f, g_1 g_2) = \mathrm{Res}_{m,n_1}(f, g_1)\mathrm{Res}_{m,n_2}(f, g_2) \ .$$

Preuve. Résulte immédiatement des propriétés 2.6 et 2.11. □

Exemple 2.6. Soient deux entiers m et n, et $d \geq 1$ leur plus grand diviseur. On pose $r = \frac{m}{d}$ et $s = \frac{n}{d}$. Alors

$$\mathrm{Res}_{m,n}(X^m - a, X^n - b) = (-1)^n \left(a^s - b^r\right)^d . \tag{2.2.3}$$

En effet, par utilisation de la formule de spécialisation, il suffit de se placer dans le cas où l'anneau A est un corps de caractéristique nulle, tel que le polynôme $X^n - b$ est scindé sur A. Lorsque $n = 1$, la formule (2.2.3) est vérifiée en vertu de (2.2.2). Lorsque $n > 1$, on utilise la deuxième formule de multiplicativité, en utilisant la factorisation

$$X^n - b = \prod_{i=1}^{n} (X - \zeta^i \beta) \ ,$$

où β est une racine dans A du binôme $X^n - b$, et où $\zeta \in A$ est une racine de l'unité primitive d'ordre n. De cette factorisation de $X^n - b$ résulte alors que

$$\begin{aligned}
\mathrm{Res}_{m,n}(X^m - a, X^n - b) &= \prod_{i=1}^{n} \mathrm{Res}_{m,1}(X^m - a, X - \zeta^i \beta) \\
&= \prod_{i=1}^{n} [(-1)(a - \zeta^{mi} \beta^m) \\
&= (-1)^n \prod_{i=1}^{n} (a - \zeta^{mi} \beta^m) \ .
\end{aligned}$$

Comme on sait que ζ^m est une racine de l'unité primitive d'ordre $s = \frac{n}{d}$, la différence $a - \zeta^{mi}\beta^m$ ne dépend que de la classe de i modulo s. Par conséquent, on obtient

$$\mathrm{Res}_{m,n}(X^m - a, X^n - b) = (-1)^n \left[\prod_{i=1}^{s} (a - \zeta^{mi} \beta^m) \right]^d \ .$$

Or $a^s - b^r = a^s - \beta^{nr} = a^s - (\beta^m)^s = \prod_{i=1}^{s} (a - \zeta^{mi}\beta^m)$, ce qui achève d'établir (2.2.3).

2.2.2 Discriminant d'un polynôme

Soit $n \geq 1$ un entier. Commençons par le cas où l'anneau A est un anneau de polynômes $A = \mathbb{Z}[a_0, \ldots, a_n]$ en les $n+1$ indéterminées $a_0, \ldots, a_n$, et où $f(X) = \sum_{i=0}^{n} a_{n-i} X^i$ est le polynôme « générique » de degré n. On note $f'(X) = \sum_{i=1}^{n} a_{n-i} i X^{i-1}$ son polynôme dérivé, qui est de degré $n-1$.

Lemme 2.13. *Le résultant* $\mathrm{Res}_{n,n-1}(f, f')$ *est un élément de* A *divisible par* a_0.

Preuve. Soit le morphisme $\phi : A \to A$ tel que $\phi(F(a_0, \ldots, a_n)) = F(0, a_1, \ldots, a_n)$. En vertu de la formule de spécialisation, on a $\phi\left(\mathrm{Res}_{n,n-1}(f, f')\right) = \mathrm{Res}_{n,n-1}(\phi^*(f), \phi^*(f'))$, où $\phi^* : A[X] \to A[X]$ est l'unique endomorphisme prolongeant ϕ et envoyant X sur lui-même. On remarque que le polynôme $\phi^*(f)(X) = \sum_{i=0}^{n-1} a_{n-i} X^i$ est de degré $n-1$, et la formule de changement de type donne alors

$$\mathrm{Res}_{n,n-1}(\phi^*(f), \phi^*(f')) = b_0 \mathrm{Res}_{n-1,n-1}(\phi^*(f), \phi^*(f')) \ ,$$

où b_0 est le coefficient de X^{n-1} dans le polynôme $\phi^*(f')$. Or $\phi^*(f')(X) = \sum_{i=1}^{n-1} a_{n-i} i X^{i-1}$, de sorte que $b_0 = 0$. Ainsi le résultant $\mathrm{Res}_{n,n-1}(\phi^*(f), \phi^*(f'))$ est nul, ce qui montre que $\mathrm{Res}_{n,n-1}(f, f')$ appartient au noyau du morphisme ϕ, c'est-à-dire à l'idéal de A engendré par a_0. □

Définition 19. Le *discriminant générique en degré* n est l'élément

$$D_n = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} \mathrm{Res}_{n,n-1}(f, f')$$

de l'anneau $A = \mathbb{Z}[a_0, \ldots, a_n]$.

Définition 20. Si A est un anneau (commutatif) quelconque, et si $f(X)$ est un polynôme de degré n à coefficients dans A, le *discriminant* $D(f)$ de $f(X)$ est la valeur prise par le polynôme D_n quand on y substitue simultanément chaque indéterminée a_j par le coefficient de X^{n-j} dans $f(X)$.

Par spécialisation, on a pour tout polynôme $f(X)$ de degré n l'égalité

$$\mathrm{Res}_{n,n-1}(f, f') = (-1)^{\frac{n(n-1)}{2}} \mathrm{cd}(f) D(f) \ , \tag{2.2.4}$$

où $\mathrm{cd}(f)$ est le coefficient dominant du polynôme $f(X)$.

Proposition 2.14. *Soit $f(X)$ un polynôme unitaire de degré $n \geq 1$, à coefficients dans un corps K. Si le polynôme $f(X)$ est scindé sur K, de sorte que $f(X) = \mathrm{cd}(f)\prod_{i=1}^{n}(X-\alpha_i)$ pour certains éléments α_i de K, où la notation $\mathrm{cd}(f)$ représente le coefficient dominant de $f(X)$, son discriminant est alors*

$$D(f) = \mathrm{cd}(f)^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

Preuve. Par la formule de multiplicativité, nous avons

$$\mathrm{Res}_{n,n-1}(f,f') = \mathrm{Res}_{0,n-1}(\mathrm{cd}(f),f')\prod_{i=1}^{n}\mathrm{Res}_{1,n-1}(X-\alpha_i,f').$$

D'après l'exemple 2.3, on a $\mathrm{Res}_{0,n-1}(\mathrm{cd}(f),f') = \mathrm{cd}(f)^{n-1}$. Par ailleurs, par la formule de l'échange et l'équation (2.2.2), on a $\mathrm{Res}_{1,n-1}(X-\alpha_i,f') = (-1)^{n-1}f'(\alpha_i)$. On a donc

$$\mathrm{Res}_{n,n-1}(f,f') = \mathrm{cd}(f)^{n-1}\prod_{i=1}^{n}f'(\alpha_i)\ .$$

Par les propriétés usuelles de la dérivation, on sait que $f'(\alpha_i) = \mathrm{cd}(f)\prod_{1\leq j\leq n, j\neq i}(\alpha_i-\alpha_j)$, donc

$$\mathrm{Res}_{n,n-1}(f,f') = \mathrm{cd}(f)^{2n-1}\prod_{(i,j),1\leq i\leq n,1\leq j\leq n,i\neq j}(\alpha_i-\alpha_j)\ .$$

Comme il y exactement $\frac{n(n-1)}{2}$ couples d'entiers (i,j) tels que $n\geq i>j\geq 1$, le produit pour $i\neq j$ de tous les facteurs $\alpha_i-\alpha_j$ est égal au produit de $(-1)^{\frac{n(n-1)}{2}}$ par le produit des carrés des facteurs pour $i<j$. Comme $\mathrm{Res}_{n,n-1}(f,f') = (-1)^{\frac{n(n-1)}{2}}\mathrm{cd}(f)D(f)$, la proposition est démontrée. □

2.2.3 Discriminant d'un trinôme

Définition 21. Pour un couple (n,m) d'entiers naturels tels que $n>m>0$, et k un corps commutatif, on appelle (n,m)-trinôme sur k tout polynôme de la forme

$$f(X) = aX^n - bX^m + c, \tag{2.2.5}$$

où les coefficients a,b,c sont des éléments non nuls de k.

Nous allons maintenant calculer le discriminant d'un trinôme.

Théorème 2.15. *On considère un couple (n, m) tels que $n > m > 0$. On pose $d = \mathrm{pgcd}(n, m)$, $n_1 = \frac{n}{d}$ et $m_1 = \frac{m}{d}$. Alors*

$$D(aX^n - bX^k + c) = (-1)^{n(n-1)/2} a^{n-m-1} c^{m-1} [n^{n_1} a^{m_1} c^{n_1-m_1} - m^{m_1}(n-m)^{n_1-m_1} b^{n_1}]^d \quad (2.2.6)$$

Preuve. En utilisant la propriété de spécialisation, on peut supposer que la caractéristique du corps de base est nulle. Par application de la relation (2.2.4) au trinôme $X^n + aX^k + b$, il s'ensuit que :

$$\begin{aligned} D(aX^n - bX^m + c) &= (-1)^{n(n-1)/2} a^{-1} \mathrm{Res}_{n,n-1}(aX^n - bX^m + c, naX^{n-1} - bmX^{m-1}) \\ &= (-1)^{n(n-1)/2} a^{-1} \mathrm{Res}_{n,n-1}(aX^n - bX^m + c, X^{m-1}(naX^{n-m} - bm)) \end{aligned}$$

Par la propriété de multiplicativité, on sait que

$$\begin{aligned} &\mathrm{Res}_{n,n-1}(aX^n - bX^m + c, X^{m-1}(naX^{n-m} - bm)) = \\ &(\mathrm{Res}_{n,1}(aX^n - bX^m + c, X))^{m-1} \, \mathrm{Res}_{n,n-m}(aX^n - bX^m + c, naX^{n-m} - bm) \, . \end{aligned}$$

Or, d'après (2.2.2), on a $\mathrm{Res}_{n,1}(aX^n - bX^m + c, X) = c$, d'où

$$D(aX^n - bX^m + c) = (-1)^{n(n-1)/2} a^{-1} c^{m-1} \mathrm{Res}_{n,n-m}(aX^n - bX^m + c, naX^{n-m} - bm) \, .$$

On a l'égalité de polynômes

$$aX^n - bX^m + c = n^{-1} X^m (naX^{n-m} - bm) - bn^{-1}(n-m)X^m + c \, .$$

Comme dans cette relation le degré du quotient partiel $n^{-1}X^m$ ne dépasse pas la différence des degrés du dividende $aX^n - bX^m + c$ et du diviseur $naX^{n-m} - bm$, on est en position d'appliquer la formule de Laplace, d'où l'on déduit :

$$D(aX^n - bX^m + c) = (-1)^{n(n-1)/2} a^{-1} c^{m-1} \mathrm{Res}_{n,n-m}(-bn^{-1}(n-m)X^m + c, naX^{n-m} - bm) \, .$$

Puisque le degré du polynôme $-bn^{-1}(n-m)X^m + c$ est $m < n$, on applique alors la formule de changement de type, pour obtenir :

$$D(aX^n - bX^m + c) = (-1)^{n(n-1)/2} a^{n-m-1} c^{m-1} n^{n-m} \mathrm{Res}_{m,n-m}(-bn^{-1}(n-m)X^m + c, naX^{n-m} -$$

Posons alors $\mathbf{a} = nc(n-m)^{-1}b^{-1}$ et $\mathbf{b} = n^{-1}ma^{-1}b$. Avec cette notation, on a

$$\mathrm{Res}_{m,n-m}(-bn^{-1}(n-m)X^m + c, naX^{n-m} - bm) = \mathrm{Res}_{m,n-m}(-bn^{-1}(n-m)(X^m - \mathbf{a}), na(X^{n-}$$

Par multiplicativité, on en déduit :

$$D(aX^n-bX^m+c) = (-1)^{n(n-1)/2}a^{n-1}(-b)^{n-m}c^{m-1}n^m(n-m)^{n-m}\mathrm{Res}_{m,n-m}(X^m-\mathbf{a}, X^{n-m}-\mathbf{b}$$

Par (2.2.3), on voit que

$$\begin{aligned}&\mathrm{Res}_{m,n-m}(X^m-\mathbf{a}, X^{n-m}-\mathbf{b}) = (-1)^{n-m}\left(\mathbf{a}^{n_1-m_1}-\mathbf{b}^{m_1}\right)^d\\ &= (-1)^{n-m}n^{-m}(n-m)^{-(n-m)}a^{-m}b^{-(n-m)}\left(n^{n_1}a^{m_1}c^{n_1-m_1}-m^{m_1}(n-m)^{n_1-m_1}b^{n_1}\right)^d\ .\end{aligned}$$

Par conséquent, on obtient

$$D(aX^n-bX^m+c) = (-1)^{n(n-1)/2}a^{n-m-1}c^{m-1}\left(n^{n_1}a^{m_1}c^{n_1-m_1}-m^{m_1}(n-m)^{n_1-m_1}b^{n_1}\right)^d\ ,$$

comme on l'avait annoncé.

2.3 Classification des trinômes

2.3.1 Position du problème

Définition 22. Soit k un anneau commutatif intègre, et k^* le groupe de ses éléments inversibles. On fait agir le groupe k^{*2} sur l'ensemble $T_{n,m}(k)$ des (n,m)-trinômes à coefficients dans k en posant

$$(\lambda,\mu)\cdot f(x) = \lambda f(\mu x).$$

De manière équivalente, en assimilant $T_{n,m}(k)$ à k^{*3}, ceci revient à

$$(\lambda,\mu)\cdot(a,b,c) = (\lambda\mu^n a, \lambda\mu^m b, \lambda c).$$

On a en particulier

$$Disc((\lambda,\mu)\cdot f) = \lambda^{2n-2}\mu^{n(n-1)}Disc(f).$$

Définition 23. Une orbite dans cette action est appelée une *classe de trinômes* (plus exactement, il faudrait parler de classes de k-trinômes). Deux trinômes sont dits *k-équivalents*, ou s'il n'y a pas d'ambiguïté, *équivalents*, lorsqu'ils appartiennent à la même classe.

Lorsque k est un corps, on remarque que deux trinômes k-équivalents ont le même groupe de Galois sur k. Dans cette section, nous nous posons le problème de décrire ces classes et de trouver un représentant privilégié dans chaque classe.

2.3.2 Classification sur un corps commutatif

Dans cette sous-section, nous supposons que k est un corps commutatif.

Définition 24. Le *paramètre* du trinôme (2.2.5) est l'élément

$$t = \frac{a^m c^{n-m}}{b^n} \tag{2.3.1}$$

de k^*.

Proposition 2.16. *Deux trinômes équivalents ont le même paramètre. Réciproquement, lorsque les entiers n et m sont premiers entre eux, alors deux (n, m)-trinômes de même paramètre sont équivalents.*

Preuve. En effet, prenons un premier trinôme $f(x) = ax^n - bx^m + c$, puis considérons le trinôme $f_1(x) = a_1x^n - b_1x^m + c_1$ tel que $f_1(x) = (\lambda, \mu) \cdot f(x) = \lambda f(\mu x)$. Il en résulte que $a_1 = \lambda\mu^n a, b_1 = \lambda\mu^m b, c_1 = \lambda c$. Sans grande difficulté, nous vérifions que $a^m b^{-n} c^{n-m} = a_1^m b_1^{-n} c_1^{n-m}$, c'est-à-dire que les trinômes $f(x)$ et $f_1(x)$ ont le même paramètre.

Réciproquement, si $f(x) = ax^n - bx^m + c$ et $f_1(x) = a_1x^n - b_1x^m + c_1$ sont deux trinômes à coefficients dans k ayant même paramètre, c'est–à-dire tels que $a^m b^{-n} c^{n-m} = a_1^m b_1^{-n} c_1^{n-m}$, alors on pose $\lambda = \frac{c_1}{c}$. Puisque n et m sont supposés premiers entre eux, il existe des entiers r et s tels que $s(n-m) - rn = 1$. En utilisant ces entiers r et s, on pose $\mu = a_1^{s-r} b_1^{-s} c_1^r a^{-(s-r)} b^s c^{-r}$. Un calcul direct montre alors que $(\lambda, \mu) \cdot f(x) = f_1(x)$. □

Les nombres s et r qui interviennent dans la démonstration de la proposition précédente ont une certaine importance. Il est possible d'en faire un choix bien déterminé comme suit. On suppose que les entiers n et m sont premiers entre eux. Soit s l'unique entier appartenant à $[1..n-1]$ tel que $-sm \equiv 1 \pmod{n}$). Soit r l'unique entier appartenant à $[0..n-m-1]$ tel que $-rn \equiv 1 \pmod{n-m}$. Les entiers $s(n-m)$ et $1+rn$ sont alors tous deux congrus à 1 modulo n et à 0 modulo $n-m$. Comme ils appartiennent tous deux à l'intervalle $[1..n(n-m)-1]$, on en conclut qu'ils sont égaux. On a donc les conditions

$$s(n-m) - rn = 1, 0 \leqslant r \leqslant n-m-1, 1 \leqslant s \leqslant n-1.$$

Ce choix des entiers r et s permet à son tour la définition suivante.

Définition 25. Supposons que les entiers r, s, m, n vérifient $s(n-m)-rn=1$, avec $0 \leqslant r \leqslant n-m-1, 1 \leqslant s \leqslant n-1$. Le multiplicateur du trinôme (2.2.5) est l' élément

$$u = \frac{a^{s-r}c^r}{b^s} \tag{2.3.2}$$

de k^*.

Proposition 2.17. *On suppose que les entiers n et m sont premiers entre eux. Soit t et u le paramètre et le multiplicateur du trinôme $f(X) = aX^n - bX^m + c$. Alors :*

(a) on a $b = \frac{at^r}{u^{n-m}}$ et $c = \frac{at^s}{u^n}$.

(b) le multiplicateur de $(\lambda, \mu) \cdot f$ est μu.

Preuve. (a) En effet

$$\frac{at^r}{u^{n-m}} = a^{1-(s-r)(n-m)+mr} b^{s(n-m)-nr} c^{-r(n-m)+r(n-m)} = a^0 b^1 c^0 = b$$

et

$$\frac{at^s}{u^n} = a^{1-(s-r)n+ms} b^{sn-sn} c^{-rn+s(n-m)} = a^0 b^0 c^1 = c$$

(b) On sait que $(\lambda, \mu) \cdot f$ est le trinôme $a_1 X^n - b_1 X^m + c_1$, avec $a_1 = \lambda \mu^n a, b_1 = \lambda \mu^m b, c_1 = \lambda c$. En tenant compte de la relation $s(n-m) - rn = 1$, il est alors facile de vérifier que le multiplicateur $a_1^{s-r} b_1^{-s} c_1^r$ de ce nouveau trinôme est le produit de μ par $a^{s-r} b^{-s} c^r$. □

Définition 26. Supposons que les entiers r, s, m, n vérifient $s(n-m)-rn=1$, avec $0 \leqslant r \leqslant n-m-1, 1 \leqslant s \leqslant n-1$. Un (n,m)-trinôme est dit *réduit* s'il est de la forme $f(x) = x^n - t^r x^m + t^s$ pour un $t \in k^*$.

Un trinôme réduit est unitaire et de multiplicateur 1. Réciproquement, en vertu de la proposition 2.17, tout trinôme unitaire de multiplicateur 1 est réduit.

Il en résulte que, dans toute classe de (n,m)-trinômes, il existe un et un seul trinôme réduit. Ceci résout le problème de la classification des (n,m)-trinômes sur un corps commutatif, à condition que les entiers n et m soient premiers entre eux.

2.4 Groupes de Galois de trinômes sur le corps des nombres rationnels

La détermination du groupe de Galois sur $\mathbb{Q}$ du corps de décomposition d'un poynôme à coefficients dans $\mathbb{Z}$ est un problème classique d'algèbre. Cette détermination repose sur le principe de Van der Waerden [44] basée essentiellllement sur la ramification d'un nombre premier dans l'extension. Un théorème dû à cet auteur [44] affirmait qu'en dehors du groupe symétrique S_n, il est difficile de réaliser un sous-groupe strict de S_n comme groupe de Galois d'un polynôme unitaire à coefficients sur $\mathbb{Z}$. Par exemple, pour un nombre premier p impair et un entier a tel que $\sqrt[p]{a} \notin \mathbb{Z}$, le groupe de Galois du binôme $X^p - a$, qui est résoluble, est engendré par un cycle d'ordre p et un cycle d'ordre $(p-1)$, c'est donc le groupe affine $Aff(\mathbb{F}_p)$.
Suivant les conditions nécessaires observées par Feit [17], et en supposant que le groupe de Galois G d'un $\mathbb{Q}$-trinôme contienne une involution fixant au plus 3 racines, très peu de groupes de permutations sont susceptibles de se réaliser comme groupes de Galois de tels trinômes.
Plusieurs auteurs se sont intéressés à la caractérisation des trinômes ayant pour groupe de Galois G le groupe symétrique S_n. C'est ainsi qu' Osada [30, 31] a montré que G est isomorphe à S_n sous les hypothèses suivantes :

1. $A = ac^n, B = bc^n$ où a, b et c sont des entiers relatifs tels que $pgcd(nb, acs(n-s)) = 1$.
2. $\mid D_0 \mid$ n'est pas un carré, où $\mid D_0 \mid = n^n b^{n-s} + (-1)^{n-1} s^s (n-s)^{n-s} a^n c^{ns}$.
3. Il existe un nombre premier p qui divise b sans que p^2 divise b.

En fait la question de la primitivité du groupe de Galois G joue un rôle essentiel. En effet dans [27], les auteurs ont montré que dans le cas où G est primitif, les conditions 1. et 2. précédentes suffisent pour que G soit isomorphe à S_n.
En 1997, dans [13] les auteurs ont étudié le groupe de Galois d'un trinôme irréductible $f(X) = X^n + aX^s + b$ à coefficients entiers $(1 \leq s \leq n-1, ab \neq 0)$ et ils montrent que sous des hypothèses convenables mais pas trop restrictives, quand n et s sont premiers entre eux, le groupe de Galois est doublement transitif. Ces résultats étendent ceux d' Osada mais on peut remarquer que les hypothèses des théorèmes dans [13] n'excluent pas la possibilité que certains premiers se ramifient sauvagement dans l'extension de $\mathbb{Q}$ obtenue par adjonc-

tion d'une racine du trinôme considéré. De plus le théorème 1.2 [13] donne une condition suffisante de double transitivité du groupe de Galois lorsque $n-s$ est une puissance d' un nombre premier divisant b.
Nous ne pouvions finir avec l'article [13] sans citer le suivant [14], fait par les mêmes auteurs, qui n'est qu'une suite directe du précédent. Dans [14], les auteurs obtiennent des critères simples et explicites pour que le groupe de Galois d'un trinôme pp irrèductible $X^n + aX^s + b$ à coefficients entiers, contienne le groupe alterné A_n. Ces critères étendent ceux d'Osada, mais permettent de couvrir des situations plus délicates. Notons que dans [14], on y a utilisé la classification des groupes de Jordan et celles des groupes multiplement transitifs, qui sont toutes deux conséquences de la classification des groupes finis simples.

Nous pouvons citer aussi les travaux de Bishnoi et Khanduja [6] qui ont étendu les résultats de Schur [35, 36] permettant ainsi la construction de trinômes de degré n pour tout n avec S_n pour groupe de Galois.
Pour finir le cas des trinômes de degré n quelconque, nous citons l'article [19] dans lequel les auteurs ont voulu aborder le problème inverse. Le principe de ce dernier, étant donné un groupe de permutations G de degré n, trouver un trinôme séparable de degré n qui le réalise sur un corps K. L'objectif de cet article a été de construire explicitement un nombre infini de familles de trinômes à coefficients rationnels dont le groupe de Galois soit isomorphe à A_n.
En utilisant la classification des groupes simples finis, W. Feit [17] dresse la liste des groupes susceptibles de se réaliser comme groupe de Galois d'un trinôme de degré premier, irréductible sur le corps $\mathbb{Q}$ des nombres rationnels.
K. Komatsu [21] a étudié le groupe de Galois d'un trinôme irrèductible de la forme $X^p + aX + a$ sur le corps $\mathbb{Q}$ où p est un entier premier et a un entier rationnel. Il a montré que G est le groupe symétrique S_p si p divise a exactement une fois et si a/p est un carré.
A. Movahhedi [26] a amélioré ce dernier résultat. En effet, A. Movahhedi a montré que si p divise exactement une fois l'entier a, alors le groupe G est, soit le groupe symétrique S_p, soit le groupe $Aff(\mathbb{F}_p)$ [26, Sect. 3, Theorem 3.1]. De plus, il montre que G est le groupe symétrique S_p dans chacun des cas suivants :

1. $a < 0$
2. $\dfrac{a}{p} \neq 1(modp)$

Lorsque p ne divise pas a, A. Movahhedi [26] a montré ce qui suit :

1. $G \simeq S_p$, si le discriminant du trinôme n'est pas un carré,
2. G est soit le groupe alterné A_p, soit le groupe projectif spécial linéaire $PSL_2(2^e)$. Ce dernier cas a lieu uniquement lorsque $p = 1 + 2^e$ est un premier de Fermat.

En 2008, dans [4], les auteurs ont généralisés les résultats de A. Movahhedi [26] aux trinômes de la forme $X^p + aX^s + a$. Dans [4], les auteurs ont montré sous des restrictions mineurs : $pgcd(sv_p(a), p-1) > 1$ et $sv_p(a) < p$, que si le groupe de Galois G n'est pas résoluble il est isomorphe à S_p ou A_p.
D' autre part en 2009 dans [5], les auteurs ont montré que le groupe de Galois G du trinôme irréductible $X^p + aX^{p-1} + a$ sur le corps $\mathbb{Q}$ est tout le groupe S_p.
Avant de finir, on citera de même les travaux de [42, 43].

2.5 Groupes de Galois de trinômes sur le corps des fractions rationnels

Concernant le goupe de Galois d'un trinôme sur le corps des fractions rationnels $\mathbb{Q}(T)$, nous pouvons citer essentielement les travaux de A. Schinzel [34] dans les quels l'auteur a montré que les trinômes génériques $X^n + T^r X^m + T^s$, avec n, m, r, s entiers naturels tels que $n > m > 0$ et $s(n-m) - rn = 1$, ont S_n pour groupe de Galois sur le corps $\mathbb{Q}(T)$.

Chapitre 3

Groupe de Galois d'un trinôme d'Eisenstein $X^p + ac^{p-2}X + ac^{p-1}$

3.1 Introduction

Puisque les binômes à coefficients rationnels sont tous résolubles, les trinômes fournissent les exemples les plus simples de polynômes de degré n à coefficients rationnels ayant pour groupe de Galois le groupe symétrique S_n : par exemple, Osada [30] et Serre [38, p. 52] ont montré indépendamment que le trinôme $X^n - X - 1$ a cette propriété pour tout entier $n > 1$. La facilité à établir que le groupe de Galois d'un trinôme à coefficients rationnels a pour groupe de Galois le groupe symétrique est liée à la propriété démontrée par Schinzel [34] les trinômes génériques $X^n + t^r X^m + t^s$, avec n, m, r, s entiers naturels tels que $n > m > 0$ et $s(n-m) - rn = 1$, ont S_n pour groupe de Galois sur $\mathbb{Q}(t)$. En effet le théorème d'irrèductibilité de Hilbert entraîne alors que le trinôme $X^n + t^r X^m + t^s$ a S_n pour groupe de Galois sur $\mathbb{Q}$ pour une infinité de valeurs du paramètre $t \in \mathbb{Q}^*$. En fait, les travaux connus à ce jour semblent indiquer qu'il est très difficile de construire des exemples de trinômes irréductibles de degré $n \geqslant 7$ ayant pour groupe de Galois sur $\mathbb{Q}$ un groupe de permutations ne contenant pas le groupe alterné A_n. C'est ainsi qu'Angeli [2] a montré que, si $p \geqslant 7$ est un nombre premier fixé, il n'y a qu'un nombre fini d'orbites de trinômes irréductibles résolubles $f(X) = X^p + aX + b$ sous l'action $f(X) \longmapsto k^p f(X/k)$ du groupe $\mathbb{Q}^*$.
Dans ce présent travail, nous nous intéressons précisément à la possibilité de trouver un trinôme irréductible $f_0(X) = Ax^p + Bx + C (ABC \neq 0)$ à coefficients

rationnels de degré premier $p \geqslant 7$ qui soit résoluble. Pour un tel trinôme, il existe une valeur $k \in \mathbb{Q}^*$ telle que le trinôme $k^p f_0(X/k)$ soit de la forme

$$f(X) = X^p + ac^{p-2}X + ac^{p-1} \tag{3.1.1}$$

pour deux entiers rationnels a et c mutuellement étrangers. C'est pourquoi nous nous limiterons à examiner des trinômes de cette forme (3.1.1). Pour assurer l'irréductibilité d'un tel trinôme, nous supposons qu'il est du type d'Eisenstein en p, c'est à dire que $a = pa_1$, où a_1 est un entier premier à p. De plus, nous aurons besoin pour nos démonstations de l'hypothèse supplémentaire que c est premier à $p-1$. Notre résultat principal est le suivant.

Théorème 3.1. *Soit $p \geq 7$ un nombre premier, et a_1, c deux entiers rationnels tels que $pgcd(a_1, pc) = pgcd(c, p(p-1)) = 1$. On pose $a = pa_1$ et*

$$D_0 = \frac{c}{\mid c \mid}(p^{p-1} + (p-1)^{p-1}a_1).$$

Pour que le groupe de Galois G du trinôme $f(X)$ de la forme (3.1.1) soit résoluble, les conditions suivantes sont nécessaires.

1. *L'entier D_0 est un carré dans $\mathbb{Z}$.*
2. *Si $p \equiv 1 \pmod 4$, alors l'entier $p \mid c \mid$ est résidu quadratique modulo tout diviseur premier de D_0.*
3. *Si $p \equiv 3 \pmod 4$, alors l'entier $\frac{p-1}{2}$ est résidu quadratique modulo tout diviseur premier de l'entier D_0.*

Un cas particulier des trinômes que nous considérons dans le théorème 3.1, déjà traité dans la littérature [20, 26], est le cas $c = 1$, c'est à dire celui des trinômes $X^p + aX + a$, où a est un entier divisible par p exactement une fois. Soulignons de plus que Kölle et Schmid [20] conjecturent que le groupe de Galois de $f(X)$ est toujours S_p lorsque $c = 1$. Cependant, en général ce ci a été prouvé seulement pour $p \leqslant 5$ à ce jour [18]. Nos méthodes de démonstrations sont proches de celles utilisées dans [20], et nous réctifions une petite erreur dans ce papier [20]. Le point 1 du théorème 3.1 a été démontré dans [20, pp.82-83] dans le cas particulier qui y est considéré, alors que les points 2 et 3 sont nouveaux : nous les déduisons à partir du théorème de Pellet-Stickelberger.
L'idée principale dans nos démonstrations est la méthode locale.

Notre lemme 3.5 peut être vu comme une étude locale en un premier à l'infini, c'est à dire au dessus du corps des réels $\mathbb{R}$, par contre les lemmes suivants représentent l'étude locale en un entier premier q divisant D_0. Dans cette étude, nous utilisons le théorème d'Ore ainsi que le polygone de Newton pour la factorisation de polynômes [29, 38]. Cependant les travaux antérieurs, excèpté de [20], ont utilisé l'étude locale en des entiers premiers ramifiés dans des extensions engendrées par des racines du trinôme, il est remarquable qu'une telle étude générale soit faisable, car les entiers premiers divisant D_0 ne sont pas nécessairement ramifiés dans de telles extensions.
Dans le théorème suivant, basé en partie sur le théorème 3.1 et aussi sur [20, 26], nous résumons les résultats connus sur les groupes de Galois du trinôme $f(X)$ lorsque $c = 1$.

Théorème 3.2. *Soit $p \geqslant 7$ un entier premier et $a_1 \in \mathbb{Z}/p\mathbb{Z}$. Posons $a = pa_1$, $f(X) = X^p + aX + a$ et $D_0 = p^{p-1} + (p-1)^{p-1}a_1$. Le groupe de Galois au dessus de $\mathbb{Q}$ du trinôme $f(X)$ est isomorphe soit au groupe symétrique S_p soit au groupe affine $AGL(1, p)$, ce dernier survient précisément lorsqu'un corps des racines de $f(X)$ au dessus de $\mathbb{Q}$ contient une racine p-ème de l'unité. Le groupe de Galois G est S_p dans les cas suivants :*

1. *D_0 n'est pas un carré dans $\mathbb{Z}$;*
2. *a_1 est un carré dans $\mathbb{Z}$;*
3. *$a_1 \not\equiv 1 \pmod{p}$;*
4. *$a_1 < p$;*
5. *Il existe un diviseur premier q de D_0 tel que $q \not\equiv \pm 1 (mod p)$;*
6. *Il existe un diviseur premier q de D_0 avec $q \equiv 1(mod p)$ tel que $-p(p-1)/2$ n'est pas résidu quadratique modulo q ;*
7. *Il existe un diviseur premier q de D_0 avec $q \equiv -1(mod q)$ tel que $-p(p-1)/2$ est résidu quadratique modulo q ;*
8. *a est impaire ;*
9. *$a \equiv 2(mod 3)$;*
10. *$p \equiv 2(mod 3)$ et $a \equiv 1(mod 3)$.*

En outre, on déduit par la loi de réciprocité quadratique et les théorèmes 3.1 et 3.2 le résultat suivant dont l'intérêt principal est de préciser la forme d'un contre exemple à la conjecture de Kölle-Schmid.

Théorème 3.3. *Etant donné un entier premier $p \equiv 7(mod 8)$ tel que $l = \frac{p-1}{2}$ est aussi premier, et un entier $a_1 \in \mathbb{Z}$ premier à p, pour que le trinôme d'Einsenstein*

$$f(X) = X^p + pa_1X + pa_1 \tag{3.1.2}$$

soit résoluble, il est nécessaire qu'il existe un entier $\mu \equiv -4v \pm 2(modp)$ tel que

$$a_1 = (v + 2^{2l-2}\mu)(u + l^{2l}\mu), \tag{3.1.3}$$

où (u, v) est l' unique couple d'entiers naturels tel que $u2^{2l-2} - vl^{2l} = p^l$ et $u < l^{2l}$.

3.2 Etude locale

Nous partons de l'énoncé bien connu suivant [16, p. 91].

Lemme 3.4. *Tout groupe de permutations transitif et résoluble de degré premier p est isomorphe à un sous-groupe du groupe affine $AGL(1, p)$.*

Lemme 3.5. *Si le trinôme $f(X)$ est résoluble, alors l'entier D_0 est strictement positif.*

Preuve. Le discriminant du trinôme $f(X)$ est [40] :

$$D(f) = (-1)^{\frac{p-1}{2}} p^p a_1^{p-1} |\ c\ |^{p(p-2)} D_0. \tag{3.2.1}$$

Comme p et $(p-1)a_1$ sont premiers entre eux, on a certainement $D_0 \neq 0$, de sorte que le trinôme $f(X)$ est séparable. D'après la règle de Descartes [32, p. 41], notre trinôme $f(X)$ admet au plus trois racines réelles. Si f admettait exactement trois racines réelles, la conjugaison complexe induirait une permutation de G qui aurait exactement trois points fixes. D'autre part, notre trinôme $f(X)$ étant irréductible (car d'Eisenstein), résoluble et de degré premier p, on sait par le lemme 3.4 que son groupe de Galois G est isomorphe à un sous-groupe du groupe affine $AGL(1, p)$. Or, le groupe affine $AGL(1, p)$ [1] ne comprend pas de

permutation ayant exactement trois points fixes. Donc f ne peut avoir qu'une seule racine réelle, de sorte que le nombre r_2 de paires de plongements conjugués imaginaires du corps de rupture du trinôme $f(X)$ est exactement $\frac{p-1}{2}$. Sachant que $D(f)(-1)^{r_2} > 0$ [9], on déduit de la formule (3.2.1) que D_0 est positif. □

Pour tout nombre premier q, le symbole v_q désigne la valuation q-adique sur le corps $\mathbb{Q}$ des rationnels.

Lemme 3.6. *Soit q un diviseur premier de D_0. Le $(\mathbb{Q}_q, X+1)-$polygone de Newton du polynôme*

$$f^*(X) = (\frac{p-1}{pc})^p f(\frac{pc}{p-1}X)$$

est composé de deux côtés : un côté horizontal de longueur $p-2$ et un côté oblique (S) joignant les points $(p-2, 0)$ et $(p, v_q(D_0))$.

Preuve. Comme pc et $(p-1)a_1$ sont premiers entre eux, Le diviseur q de D_0 ne divise pas $p(p-1)c$. Considérons le polynôme $f^*(X) = (\frac{p-1}{pc})^p f(\frac{pc}{p-1}X)$. Par la formule de Taylor appliquée à f^* au voisinage de -1, nous avons :

$$f^*(X) = \sum_{k=0}^{p} \frac{f^{*(k)}(-1)}{k!}(X+1)^k$$

Pour

$$k = 0 \quad : \quad f^*(-1) = \frac{-D_0}{\mid c \mid p^{p-1}}, \qquad k = 1 : \quad f^{*'}(-1) = \frac{D_0}{\mid c \mid p^{p-2}},$$

$$2 \leq k \leq p : \quad \frac{f^{*(k)}(-1)}{k!} = \binom{p}{k}(-1)^{p-k}.$$

D'où :

$$f^*(X) = \sum_{j=0}^{p-2} \binom{p}{j}(-1)^j(X+1)^{p-j} + \frac{D_0}{\mid c \mid p^{p-2}}(X+1) - \frac{D_0}{\mid c \mid p^{p-1}}. \quad (3.2.2)$$

Par conséquent, le nuage de Newton est constitué des $p+1$ points : $(0,0)$, $\left(j, v_q\left(\binom{p}{j}\right)\right)$ pour j entier entre 1 et $p-2$, $(p-1, v_q(D_0))$ et $(p, v_q(D_0))$.

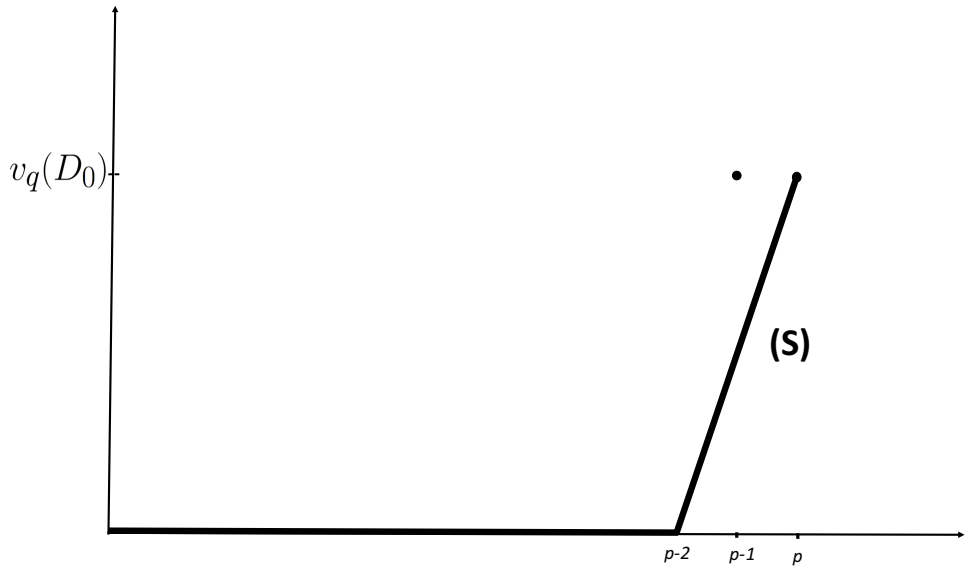

FIGURE 3.1 – $(X+1, \mathbb{Q}_q)$-polygone de Newton de $f^*(X)$

Observons en particulier que, puisque le nombre q est premier à $p(p-1)$, le point $(p-2, 0)$ est élément de ce nuage. On constate que tous les points de ce nuage sont au dessus de l'axe des abscisses qui passe au moins par les points $(0, 0)$ et $(p-2, 0)$ qui appartiennent au nuage.
On constate de même que tous les points du nuage sont au-dessus de la droite d'équation $y = \frac{v_q(D_0)}{2}(X-(p-2))$ qui passe par les deux points $(p-2, 0)$ et $(p, v_q(D_0))$ qui appartiennent au nuage.

Lemme 3.7. *Si $g(X) = X^p + aX + b \quad (ab \neq 0)$ est un trinôme à coefficients dans un corps K dont la caractéristique est différente de p, le degré du pgcd de $g(X)$ et de sa dérivée $g'(X)$ est au plus égal à 1.*

Preuve. En effet, on a $g'(X) = pX^{p-1} + a$ et $g(X) = g'(X)\frac{X}{p} + \frac{p-1}{p}aX + b$. Par conséquent le pgcd de $g(X)$ et de $g'(X)$ doit diviser le polynôme $\frac{p-1}{p}aX + b$ qui est non nul et de degré au plus 1.

Lemme 3.8. *Pour tout diviseur premier q de D_0, le trinôme $f^*(X)$ du lemme 3.6 se factorise dans l'anneau $\mathbb{Z}_q[X]$ sous la forme*

$$f^*(X) = f_{p-2}(X)f_2(X), \tag{3.2.3}$$

où $f_{p-2}(X)$ est un polynôme unitaire de degré $p-2$ dont la réduction modulo q n'a pas de racine multiple, et où $f_2(X)$ est un polynôme unitaire de degré 2 dont le $(\mathbb{Q}_q, X+1)$-polygone de Newton est le translaté à l'origine du côté oblique (S). Le corps des racines du polynôme $f_{p-2}(X)$ sur $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$.

Preuve. La factorisation (3.2.3) résulte immédiatement du lemme 3.6 et du théorème d'Ore [29]. A partir de la relation (3.2.3), on obtient dans l'anneau $\mathbb{F}_q[X]$ la factorisation

$$\overline{f^*}(X) = \overline{f_{p-2}}(X)(X+1)^2, \tag{3.2.4}$$

où la notation $\overline{g}(X)$ représente la réduction modulo q du polynôme $g(X) \in \mathbb{Z}_q[X]$. Comme q est premier à p, il résulte de la factorisation (3.2.4) du trinôme et du lemme 3.6 que $\overline{f_{p-2}}(X)$ est séparable sur $\mathbb{F}_q$. En utilisant [28, lemma 5.24, p.222] on en déduit que, pour toute racine α du polynôme $f_{p-2}(X)$, l'extension $\mathbb{Q}_q(\alpha)/\mathbb{Q}_q$ est non ramifiée. Par conséquent tout corps F des racines du polynôme $f_{p-2}(X)$ sur le corps $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$.

Lemme 3.9. *On suppose que le groupe de Galois G du trinôme $f(X)$ sur $\mathbb{Q}$ est résoluble. Si q est un diviseur premier de D_0, alors l'entier $v_q(D_0)$ est pair.*

Preuve. Supposons au contraire que la valuation $v_q(D_0)$ soit impaire. En utilisant le lemme 3.5, on voit que la longueur de la projection horizontale du côté oblique (S) est $\ell = 2$, et que la longueur de sa projection verticale est $h = v_q(D_0)$. Comme, dans ce cas, les longueurs ℓ et h sont premières entre elles, il résulte de [12, Theorem 1.5] que, si β est l'une des deux racines β de $f_2(X)$, alors l'indice de ramification de l'extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$ est pair. Puisque le polynôme $f_2(X)$ est de degré 2, on voit que l'extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$ est totalement ramifiée de degré 2, et est le corps des racines de $f_2(X)$ sur $\mathbb{Q}_q$.

Soit N_q le corps des racines de $f(X)$ (ou de $f^*(X)$) sur $\mathbb{Q}_q$, et F celui du facteur $f_{p-2}(X)$ de la relation (3.2.3). D'après la relation (3.2.3), le corps N_q est le composé du corps F avec le corps $\mathbb{Q}_q(\beta)$. Comme l'extension $F/\mathbb{Q}_q$ est non ramifiée, le lemme d'Abhyankar [28, Corollary 4, p. 229] entraîne que l'indice de ramification de l'extension $N_q/\mathbb{Q}_q$ est égal à 2.

Soit N le sous-corps de N_q engendré par les racines du trinôme $f(X)$ (ou de $f^*(X)$). Comme N est un corps des racines de $f(X)$ sur $\mathbb{Q}$, le groupe de

Galois G s'identifie au groupe des automorphismes de N. Il résulte de ce qui précède que le groupe d'inertie I de la place de N induite par l'idéal maximal de N_q est d'ordre 2, et que son générateur laisse fixes les racines de $f_{p-2}(X)$. Par conséquent, le groupe I est engendré par une transposition. Comme $AGL(1,p)$ ne contient pas de transposition, le groupe de Galois G ne peut être isomorphe à un sous-groupe du groupe $AGL(1,p)$ et donc, d'après le lemme 3.4, n'est pas résoluble.

Lemme 3.10. *Si le groupe de Galois G du trinôme $f(X)$ est résoluble, et $f_2(X)$ et $f_{p-2}(X)$ sont comme dans le lemme 3.8, alors, pour tout diviseur premier q de D_0, nous avons :*

(a) le corps $\mathbb{Q}_q\left(\sqrt{-\frac{p(p-1)|c|}{2}}\right)$ est un corps de racines sur $\mathbb{Q}_q$ du polynôme $f_2(X)$;

(b) Tout facteur irréductible sur $\mathbb{Q}_q$ de $f^*(X)$ est de degré au plus 2 et le nombre r de facteurs irréductibles sur $\mathbb{Q}_q$ du polynôme $f_{p-2}(X)$ est donné par

$$r = \begin{cases} p-2 & \text{si } -\frac{p(p-1)|c|}{2} \text{ est résidu quadratique modulo } q\ ; \\ \frac{p-1}{2} & \text{sinon.} \end{cases} \tag{3.2.5}$$

Preuve. D'après le lemme 3.9, on sait que $v_q(D_0)$ est paire. Dans ce cas, la longueur de la projection horizontale du côté (S) est $\ell = 2$, et la longueur de sa projection verticale est $h = v_q(D_0)$ qui est un nombre pair. Par [12, Proposition 1.4], le polynôme associé au côté (S) est

$$F(Y) = Y^2 + \frac{2D_0^*}{\mid c \mid p^p.(p-1)} \tag{3.2.6}$$

où $D_0^* = \frac{D_0}{q^{v_q(D_0)}}$ est la partie première à q de l'entier D_0. D'après le lemme 3.8, le trinôme $f^*(X)$ se factorise sous la forme (3.2.3), où $f_{p-2}(X)$ est un polynôme de degré $p-2$ dont le corps des racines F sur $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$. Comme q ne divise pas $p(p-1)$, le polynôme $F(Y)$ est séparable modulo q, et donc on sait, par [12, Théorème 1.5], qu'un corps des racines du polynôme $f_2(X)$ sur $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$. D'autre part, aussi par [12, Théorème 1.5], la factorisation dans $\mathbb{Q}_q[X]$ du polynôme $f_2(X)$ est analogue à celle dans $\mathbb{F}_q[Y]$ de la réduction $\overline{F}(Y)$ modulo q du polynôme associé $F(Y)$. Comme on sait par les lemmes 3.5 et 3.8 que D_0^* est un carré dans $\mathbb{Z}$, la relation

(3.2.6) montre que la factorisation du polynôme $\overline{F}(Y)$ dépend uniquement du caractère quadratique de $-\frac{p(p-1)|c|}{2}$ modulo q. Le degré d'un corps des racines sur $\mathbb{Q}_q$ de $f_2(X)$ est donc 1 ou 2 selon que $-\frac{p(p-1)}{2}$ est ou non un résidu quadratique modulo q. Comme q est premier à $p(p-1)$, le corps $\mathbb{Q}_q\left(\sqrt{-\frac{p(p-1)|c|}{2}}\right)$ est une extension non ramifiée de $\mathbb{Q}_q$ ayant le même degré que le corps des racines sur $\mathbb{Q}_q$ du polynôme $f_2(X)$; or deux extensions non ramifiées de même degré de $\mathbb{Q}_q$ sont isomorphes, ce qui prouve le premier point.

En outre, le corps des racines N_q sur $\mathbb{Q}_q$ du trinôme $f^*(X)$, en tant que composé de deux extensions non ramifiées de $\mathbb{Q}_q$, en est aussi une extension non ramifiée. Donc le groupe de Galois sur $\mathbb{Q}_q$ du trinôme $f^*(X)$ est cyclique. On distingue deux cas.

Cas 1. L'entier $-\frac{p(p-1)|c|}{2}$ est résidu quadratique modulo q. Dans ce cas, la réduction $\overline{F}(Y)$ modulo q du polynôme associé $F(Y)$ se factorise en 2 polynômes de degré 1 dans $\mathbb{F}_q[Y]$. Par conséquent $f_2(X)$ se factorise en 2 facteurs de degré 1 dans $\mathbb{Q}_q[X]$, et donc tout élément du groupe de Galois sur $\mathbb{Q}_q$ doit laisser fixes les deux racines du facteur $f_2(X)$. Comme G est supposé résoluble et que la seule permutation de $AGL(1,p)$ qui laisse fixes deux points est l'identité, on voit par le lemme 3.4 que $f_{p-2}(X)$ est scindé sur $\mathbb{Q}_q$, donc a $p-2$ facteurs irréductibles dans $\mathbb{Q}_q[X]$.

Cas 2. L'entier $-\frac{p(p-1)|c|}{2}$ n'est pas résidu quadratique modulo q. Alors la réduction $\overline{F}(Y)$ modulo q du polynôme associé $F(Y)$ est irréductible dans $\mathbb{F}_q[Y]$, et donc $f_2(X)$ est irréductible sur $\mathbb{Q}_q$. Un générateur du groupe de Galois G_q sur $\mathbb{Q}_q$ du trinôme $f^*(X)$ agit donc en échangeant les 2 racines de $f_2(X)$, et est donc d'ordre pair. Comme on sait par le lemme 3.4 que G, et donc aussi G_q, est isomorphe à un sous-groupe du groupe affine $AGL(1,p)$, on conclut que ce générateur de D possède exactement un point fixe, qui est forcément une racine de $f_{p-2}(X)$. En examinant les permutations appartenant au groupe $AGL(1,p)$, on voit que les seules permutations dans ce groupe qui possèdent exactement un point fixe et un cycle de longueur 2 sont les produits de $\frac{p-1}{2}$ transpositions deux à deux disjointes. Par conséquent, le polynôme $f_{p-2}(X)$ se factorise sur $\mathbb{Q}_q$ en $\frac{p-1}{2}$ facteurs irréductibles : un de degré 1 et $\frac{p-3}{2}$ de degré 2.

3.3 Preuve du théorème 3.1 :

Supposons G résoluble. Les lemmes 3.5 et 3.9 suffisent à montrer que l'entier D_0 est un carré dans $\mathbb{Z}$. Par conséquent, on voit par les relations (3.2.1) et (3.2.3) qu'il existe un élément non nul x du corps $\mathbb{Q}_q$ tel que

$$D(f_{p-2})D(f_2) = (-1)^{\frac{p-1}{2}} p \mid c \mid x^2, \tag{3.3.1}$$

où on note $D(f_{p-2})$ et $D(f_2)$ pour les discriminants des polynômes respectivement $f_{p-2}(X)$ et $f_2(X)$ figurant dans la relation (3.2.3). Le corps des racines sur $\mathbb{Q}_q$ de $f_2(X)$ étant isomorphe à $\mathbb{Q}_q\left(\sqrt{-\frac{p(p-1)|c|}{2}}\right)$, on a $-\frac{p(p-1)|c|}{2}D(f_2) \in \mathbb{Q}_q^{*2}$, et ceci, en vertu de la relation (3.3.1), signifie que $D(f_{p-2}) \in (-1)^{\frac{p+1}{2}}\frac{p-1}{2}\mathbb{Q}_q^{*2}$.

Notons par r le nombre de facteurs irréductibles du polynôme $f_{p-2}(X)$ dans $\mathbb{Q}_q[X]$. D'après un théorème de Pellet-Stickelberger [40, Theorem 1, p. 1100], et puisqu'on sait par l'argument donné dans la Démonstration du lemme 3.9 que la réduction $\overline{f_{p-2}}(X)$ du polynôme $f_{p-2}(X)$ modulo q est séparable, on a

$$(-1)^{r+1} = \left(\frac{D(f_{p-2})}{q}\right) . \tag{3.3.2}$$

Supposons en premier que $p \equiv 1(mod 4)$, pour que $D(f_{p-2})$ soit dans $-\frac{p-2}{2}\mathbb{Q}_q^{*2}$. Le lemme 3.10 montre que le nombre r de facteurs irréductibles de $f_{p-2}(X)$ dans $\mathbb{Q}_q[X]$ est impair lorsque $-\frac{p(p-1)|c|}{2}$ est résidu quadratique modulo q, et est pair sinon. Utilisant le théorème de Pellet-Stickelberger, on voit que $-\frac{p-1}{2}$ est un carré dans $\mathbb{Q}_q^*$ si et seulement si $-\frac{p(p-1)|c|}{2}$ l'est. Alors, le produit de ces deux éléments inversibles de $\mathbb{Z}_q$ est toujours un carré dans $\mathbb{Q}_q^*$. Alors $p \mid c \mid$ est toujours un carré dans $\mathbb{Q}_q^*$, donc, l'entier $p \mid c \mid$ est résidu quadratique modulo q.
Supposons maintenant $p \equiv 3 \pmod 4$. On a vu alors que $D(f_{p-2}) \in \frac{p-1}{2}\mathbb{Q}_q^{*2}$, et le lemme 3.10 montre que le nombre r de facteurs irréductibles de $f_{p-2}(X)$ dans $\mathbb{Q}_q[X]$ est impair, indépendamment du caractère quadratique de $-\frac{p(p-1)|c|}{2}$ modulo q. Nous déduisons alors par le théorème de Pellet-Stickelberger que $\frac{p-1}{2}$ est résidu quadratique modulo q.

3.4 Preuve du théorème 3.2

Notons par G le groupe de Galois du trinôme $f(X) = X^p + aX + a$ sur $\mathbb{Q}$. On suppose que $a = pa_1$, avec $a_1 \in \mathbb{Z}$ premier à p. Pour la preuve du théorème 3.2, nous comptons sur les résultats connus. Nous observons d'abords que Movahhedi a montré que G est soit S_p soit AGL(1,p) [26, Théorème 1]. L'équivalence entre la solvabilité de $f(X)$ et le fait que la p^{ieme} racine primitive de l'unité fasse partie du corps des racines de $f(X)$ sur $\mathbb{Q}$ résultent des travaux classiques de Wegener and Hasse, cités dans [20]. Movaheddi a redémontré ce résultat dans une meilleure version que celle dans [26, Théorème 2.2].
Le point (a) du théorème 3.2 est simplement le point 1 du théorème 3.1, et (c) est un résultat de Movahhedi [26, Théorème 4.3].
Pour le point (b), on peut argumenter comme suit. Supposons que $a_1 = h^2$ est le carré d'un entier h et que $f(X)$ n'est pas à groupe de Galois S_p. Alors, par le théorème 3.1, $D_0 = p^{(p-1)} + (p-1)^{(p-1)}h^2$ doit être carré d'un entier. En utilisant le fait que h et p sont premiers entre eux, on voit facilement que l'on doit avoir $p(p-1) = 2(p-1)^{\frac{p-1}{2}}h + 1$, montrant que $\pm 2h + 1 \equiv 0(modp)$. mais par (c) nous avons $h \equiv \pm 1(modp)$. Alors $\pm 2 + 1$ est divisible par p, ce qui n'est pas le cas.
Pour (d), on peut distinguer trois cas ; le cas $a_1 < 0$ est traité par Movahhedi [26, Théorème 4.5], le cas $a_1 = 1$ est un cas particulier de (b), et le cas $1 < a_1 < p$ est impliqué par (c).
Il a été prouvé par Kölle et Schmid [20, p.83] que si G est le groupe affine et q divise D_0, alors $q \equiv 1(modp)$ si le groupe de décomposition en q est trivial, et $q \equiv -1(modp)$ sinon. Ce qui justifie (e) du théorème 3.2. Quand on prend en compte le lemme 3.10, les points (f) et (g) s'en déduisent.
Les points (h), (h') et (h") sont observés par Kölle et Schmid [20, p.83].

3.5 Preuve du théorème 3.3

Soit $p \geq 7$ un entier premier et considérons $l = \frac{(p-1)}{2}$. Si le trinôme $f(X) = X^p + pa_1X + pa_1$ est résoluble, avec p ne divisant pas a_1, alors les lemmes 3.5 et 3.9 montrent l'existence de $y \in \mathbb{Z}$ tel que

$$D_0 = p^{2l} + (2l)^{2l}a_1 = y^2. \tag{3.5.1}$$

En remplaçant y par son opposé si nécessaire, on peut supposer que y est positif. Evidemment y doit être impair, pour que $w = \frac{(y+p^l)}{2}$ et $w' = \frac{(y-p^l)}{2}$ soient des entiers. Comme p ne divise pas a_1, ces entiers sont premiers. D' après (3.5.1), nous avons aussi $ww' = 2^{2l-2}l^{2l}a_1$, pour que 2^{2l-2} divise un et un seul entre w et w'. On pose en conséquence

$$\frac{y+\varepsilon p^l}{2} = 2^{2l-2}x, \tag{3.5.2}$$

où $\varepsilon \in \{-1, 1\}$ et $x \in \mathbb{Z}$. Alors $\frac{(y-\varepsilon p^l)}{2} = 2^{2l-2}x - \varepsilon p^l$, par conséquent $ww' = 2^{2l-2}x(2^{2l-2}l^{2l}a_1$, ce qui entraine

$$x(2^{2l-2}x - \varepsilon p^l) = l^{2l}a_1. \tag{3.5.3}$$

Supposons maintenant que l est premier et $p \equiv 7(mod 8)$, et rappelant que G est résoluble, on veut montrer que l ne divise pas x. Supposons le contraire. Puisque l est premier à $p = 2l+1$, il est premier à $2^{2l-2}x - \varepsilon p^l$, pour que (3.5.3) montre l'existence de $\mu \in \mathbb{Z}$ tel que

$$x = l^{2l}\mu. \tag{3.5.4}$$

De (3.5.2) et (3.5.3),

$$y = 2^{2l-1}l^{2l}\mu - \varepsilon p^l. \tag{3.5.5}$$

Comme l'exposant $2l - 1 \geq 5$ et l impair, nous avons $y \equiv \varepsilon(mod 4)$. De plus, puisque $f(X)$ est supposé résoluble, le point 3 du théorème 3.1 montre que l est résidu quadratique modulo tout entier divisant y ; alors le symbole de Jacobi $(\frac{l}{y})$ est 1. Alors la loi de réciprocité quadratique et la congruence $l \equiv 3(mod 4)$ entraine

$$(\frac{y}{l}) = (-1)^{\frac{(y-1)}{2}} = (-1)^{\frac{(\varepsilon-1)}{2}}. \tag{3.5.6}$$

A présent, d'après (3.5.5), et puisque $p \equiv 1(mod l)$, nous avons $(\frac{y}{l}) = (\frac{-\varepsilon}{l}) = (-1)^{\frac{l-1}{2}}.\frac{\varepsilon+1}{2} = (-1)^{\frac{\varepsilon+1}{2}}$. Par conséquent, $\frac{\varepsilon-1}{2} \equiv \frac{\varepsilon+1}{2}$ (mod 2), contradiction.
Puisque l'entier premier l ne divise pas x, (3.5.3) montre que l^{2l} doit diviser l'entier $2^{2l-2}x - \varepsilon p^l$, afin que nous puissions écrire

$$2^{2l-2}x - \varepsilon p^l = l^{2l}\lambda(\lambda \in \mathbb{Z}). \tag{3.5.7}$$

Considérons l'unique entier $u \in \left]0, l^{2l}\right[$ tel que $u2^{2l-2} \equiv p^l (mod l^{2l})$. En posant $v = \frac{(u2^{2l-2}-p^l)}{l^{2l}}$, on obtient un entier $v \in \left]0, 2^{2l-2}\right[$ tel que $u2^{2l-2} - vl^{2l} = p^l$. Substituant cette expression de p^l dans (3.5.7), nous obtenons $2^{2l-2}(x - u\varepsilon) = l^{2l}(\lambda - v\varepsilon)$, ce qui prouve l'existence de $\mu \in \mathbb{Z}$ tel que $x - u\varepsilon = l^{2l}\mu$ et $\lambda = v\varepsilon + 2^{2l-2}\mu$. En substituant cette expression de λ dans (3.5.7), puis par application de (3.5.3), on trouve après simplification

$$a_1 = (v\varepsilon + 2^{2l-2}\mu)(u\varepsilon + l^{2l}\mu),$$

qui est exactement (3) pour $\varepsilon = 1$. Lorsque $\varepsilon = -1$, alors la procédure conduit à la même equation (3) après remplacement du paramètre μ par son opposé.
En outre, le point (1) du théorème 3.1 ainsi que le point (e) du théorème 3.2 entrainent que $D_0 \equiv 1(modp)$. Comme, $D_0 \equiv a_1(modp)$, on choisit l'entier μ tel que $(v + 2^{2l-2}\mu)(u + l^{2l}\mu \equiv 1(modp)$. La classe résiduelle $\overline{\mu}$ de μ modulo l'entier premier p est alors racine de l'equation quadratique, et c'est facile de vérifier dirèctement que les classes des deux entiers $-4v \pm 2$ sont deux solutions dans le corps $\mathbb{Z}/p\mathbb{Z}$, alors elles sont les seules solutions, ce qui prouve que $\mu \equiv -4v \pm 2(modp)$.

Chapitre 4

Groupe de Galois du trinôme d'Einsenstein $X^7 + aX + a$

4.1 Introduction

Dans ce chapitre, nous nous intéressons au cas particulier où notre trinôme (3.1.1) est de la forme

$$f(X) = X^7 + aX + a. \tag{4.1.1}$$

On ne pouvait finir de rédiger les travaux entrepris dans le cadre de cette thèse sans parler de ce cas particulier. En fait c'est par ce cas là que toute notre étude a commencé, voulant suivre le chemin emprunté par Gauckler [18] par lequel l'auteur prouva la conjecture de Kölle et Schmid.
le trinôme $f(X)$ (4.1.1) étant d'Eisenstein assure alors que le groupe de Galois qui lui est associé sur le corps des rationnels $\mathbb{Q}$ est un sous-groupe transitif de S_7. A conjugaison près, il n'existe que 7 sous-groupes transitifs de S_7, à savoir : C_7, D_7, F_{21}, F_{42}, G_{168}, A_7 et S_7.
Notons que G_{168} est le groupe simple d'ordre 168, il est isomorphe au groupe $PSL_2(\mathbb{F}_7)$. Remarquons également que F_{21} et F_{42} sont respectivement les groupes de Frobenius d'ordre 21 et 42.
Nous avons ensuite voulu appliquer la méthode de la résolvante, utilisée par Gauckler, présentée dans le livre de Cohen [11, Algorithme 6.3.11, p. 325]. Cet algorithme se divise en trois parties :

1. La construction de la résolvante de f.
2. L'analyse des facteurs irréductibles du polynôme résolvant.

3. L'étude du cas où la résolvante est irréductible.

Dans notre cas, le polynôme appelé résolvante est de la forme :

$$P(x) = \Pi_{1\leq i<j<k\leq 7}\,(x - (\theta_i + \theta_j + \theta_k))$$

où les θ_i sont les racines de $f(X)$, il est de degré 35. En utilisant Maple, nous l'avons calculé, le reste de la démarche est assez direct. Il suffit de factoriser cette résolvante en facteurs irréductibles et de comparer la liste des degrés avec la liste des longueurs d'orbites des actions des groupes transitifs de degré 7 [11]. Mais dans note cas la factorisation modulo un certain nombre d'entiers n'a pas pu nous renseigner sur son irréductibilité. Ce qui justifia le fait de ne pas avoir prouvé notre résultat utilisant cette méthode.

Ce ci étant, apportons les lemmes qui nous ont conduits aux conditions necessaires à la résolubilité du trinôme (4.1.1).

4.2 Lemmes de préparation

Lemme 4.1. *Si le trinôme $f(X)$ est résoluble, alors l'entier D_0 est strictement positif.*

Preuve. Le discriminant du trinôme $f(X)$ est [40] :

$$D(f) = -7^7 a_1^6 D_0. \tag{4.2.1}$$

Comme 7 ne divise pas a_1, on a certainement $D_0 \neq 0$, de sorte que le trinôme $f(X)$ est séparable. D'après la règle de Descartes [32, p.41], notre trinôme $f(X)$ admet au plus 3 racines réelles.
Si f admettait exactement trois racines réelles, il y aurait dans le groupe de Galois G la conjugaison complexe qui aurait exactement trois points fixes. D'autre part notre trinôme $f(X)$ étant irréductible (car d'Eisenstein), résoluble et de degré premier 7, on sait par le lemme 3.4 que son groupe de Galois G est isomorphe à un sous-groupe du groupe affine $AGL(1,7)$. Dans $AGL(1,7)$ [1], il n'y a pas de permutation ayant exactement trois points fixes. Donc f ne peut admettre 3 racines réelles, par conséquent il n'en possède qu'une seule.
Sachant que $D(f).(-1)^{r_2} > 0$ [9], où r_2 est le nombre de paires de plongements

conjugués imaginaires du corps de rupture du trinôme $f(X)$, on en conclut que $D(f)$ est négatif.
D'après (4.2.1), on voit que l'entier D_0 est positif. □
Pour tout nombre premier q, le symbole v_q désigne la valuation q-adique sur le corps $\mathbb{Q}$ des rationnels.

Lemme 4.2. *Soit q un diviseur premier de D_0. Le $(\mathbb{Q}_q, X+1)-$polygone de Newton du polynôme $f^*(X) = \frac{6^7}{7^7} f(\frac{7}{6}X)$ est composé de deux côtés : un côté horizontal de longueur 5 et un côté oblique (S) joignant les points $(5,0)$ et $(7, v_q(D_0))$.*

Preuve. Puisque q divise D_0, nécessairement $q \notin \{2,3,7\}$. Considérons le polynôme $f^*(X) = \frac{6^7}{7^7} f(\frac{7}{6}X)$. Par la formule de Taylor appliquée à f^* au voisinage de -1 , nous avons :

$$f^*(X) = \sum_{j=0}^{7} \frac{f^{*(7-j)}(-1)}{(7-j)!}(X+1)^{7-j}$$

Pour

$$j = 7 \ : \ f^*(-1) = \frac{-D_0}{7^6}, \qquad j = 6 : \ f^{*'}(-1) = \frac{D_0}{7^5},$$
$$0 \le j \le 5 : \ \frac{f^{*(7-j)}(-1)}{(7-j)!} = \binom{7}{j}(-1)^j.$$

D'où :

$$f^*(X) = \sum_{j=0}^{5} \binom{7}{j}(-1)^j (X+1)^{7-j)} + \frac{D_0}{7^5}(X+1) - \frac{D_0}{7^6}. \tag{4.2.2}$$

Par conséquent, le nuage de Newton est constitué des points : $\left(j, v_q\left(\binom{7}{j}\right)\right)$ pour j entier entre 0 et 5, $(6, v_q(D_0))$ et $(7, v_q(D_0))$. On constate que tous les points de ce nuage sont au dessus de l'axe des abscisses qui passe au moins par les points $(0,0)$ et $(5,0)$ qui appartiennent au nuage.
On constate de même que tous ces points sont au-dessus de la droite d'equation $y = \frac{v_q(D_0)}{2}(X-5)$ qui passe par les deux points $(5,0)$ et $(7, v_q(D_0))$ qui

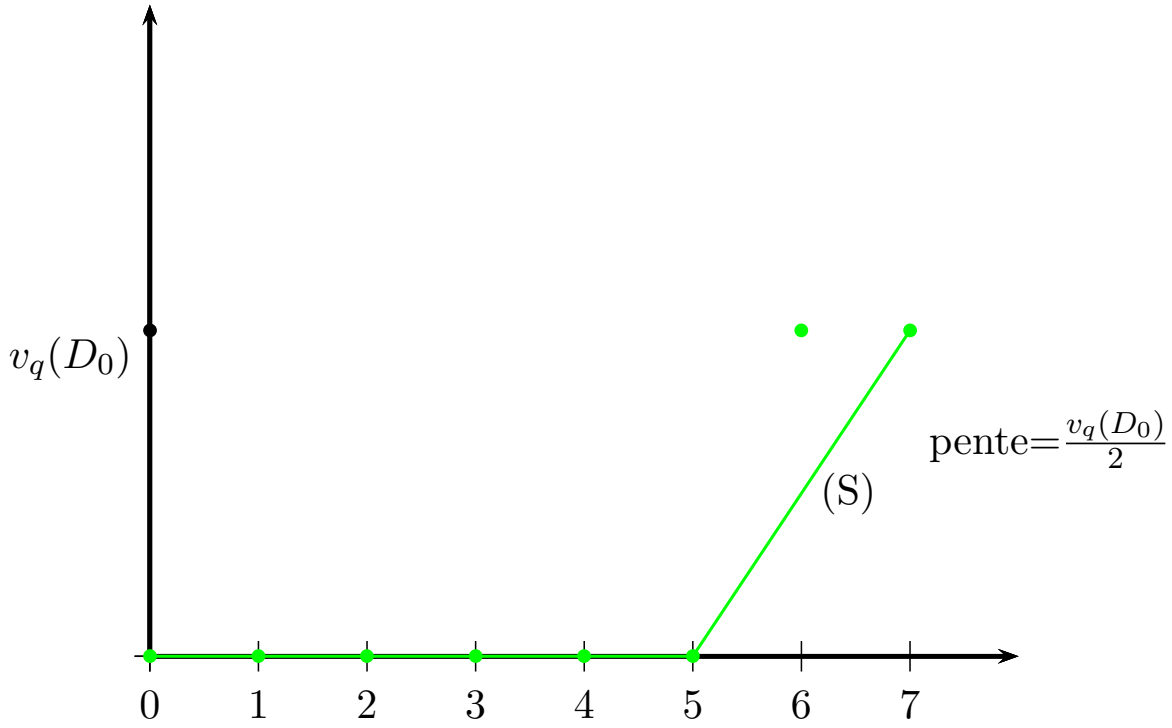

FIGURE 4.1 – $(X+1, \mathbb{Q}_q)$ polygone de Newton

appartiennent au nuage.

Lemme 4.3. *Si $g(X) = X^7 + aX + b \quad (ab \neq 0)$ est un trinôme à coefficients dans un corps K dont la caractéristique est différente de 7, le degré du pgcd de $g(X)$ et de sa dérivée $g'(X)$ est au plus égal à 1.*

Preuve. En effet, on a $g'(X) = 7X^6 + a$ et $g(X) = g'(X)\frac{X}{7} + \frac{6}{7}aX + b$. Par conséquent le pgcd de $g(X)$ et de $g'(X)$ doit diviser le polynôme $\frac{6}{7}aX + b$ qui est de degré au plus 1.

Lemme 4.4. *On suppose que G est résoluble. Si q est un diviseur premier de D_0, alors l'entier $v_q(D_0)$ est pair.*

Preuve. D' après le lemme 2 et le théorème d'Ore [5], le polynôme $f^*(X)$ se factorise dans l'anneau $\mathbb{Z}_q[X]$ sous la forme

$$f^*(X) = f_5(X)f_2(X), \tag{4.2.3}$$

où f_5 est un polynôme unitaire de degré 5 dont le $(\mathbb{Q}_q, X+1)$-polygone de Newton est le côté horizontal du polygone décrit par le lemme 2, et où $f_2(X)$ est un polynôme unitaire de degré 2 dont le $(\mathbb{Q}_q, X+1)$-polygone de Newton est le translaté à l'origine du côté oblique (S).
A partir de la relation (4.2.3), on obtient dans l'anneau $\mathbb{F}_q[X]$ la factorisation

$$\overline{f^*}(X) = \overline{f_5}(X)(X+1)^2, \tag{4.2.4}$$

où la notation $\overline{g}(X)$ représente la réduction modulo q du polynôme $g(X)$. Par le lemme 3, il en résulte que $\overline{f_5}(X)$ est séparable sur $\mathbb{F}_q$. En utilisant [10, lemme 5.24, p. 222] on en déduit que, pour toute racine α du polynôme $f_5(X)$, l'extension $\mathbb{Q}_q(\alpha)/\mathbb{Q}_q$ est non ramifiée. Par conséquent le corps F des racines du polynôme $f_5(X)$ sur le corps $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$.

Supposons maintenant que la valuation $v_q(D_0)$ soit impaire. On remarque que la longueur de la projection horizontale du côté (S) est $\ell = 2$, et que la longueur de sa projection verticale est $h = v_q(D_0)$. Comme dans ce cas, ℓ et h sont premiers entre eux, il résulte de [5, Theorem 1.5] que l'indice de ramification de l'extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$ est divisible par 2 pour chacune des deux racines β de $f_2(X)$. Puisque le polynôme $f_2(X)$ est de degré 2 et que $q \neq 2$, on voit que l'extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$ est totalement et modérément ramifiée de degré 2, et est le corps des racines de $f_2(X)$ sur $\mathbb{Q}_q$.

Soit N_q le corps des racines de $f(X)$ (ou de $f^*(X)$) sur $\mathbb{Q}_q$. D'après la relation (4.2.3), le corps N_q est le composé du corps F avec le corps $\mathbb{Q}_q(\beta)$. Comme l'extension $N_q/\mathbb{Q}_q$ est non ramifiée et que l'extension $\mathbb{Q}_q(\beta)/\mathbb{Q}_q$ est modérément ramifiée, le lemme d'Abhyankar [10, Corollary 4, p. 229] entraîne que l'indice de ramification de l'extension $N_q/\mathbb{Q}_q$ est égal à 2.

Soit N le corps des racines du trinôme $f(X)$ (ou de $f^*(X)$) sur le corps $\mathbb{Q}$ des nombres rationnels. Il résulte de ce qui précède que le groupe d'inertie I d'une place de N au-dessus du nombre premier q est d'ordre 2 et que son générateur laisse fixes les racines de $f_5(X)$. Par conséquent, le groupe I est engendré par une transposition. Comme $AGL(1,7)$ ne contient pas de transposition, le groupe de Galois G ne peut être contenu dans le groupe $AGL(1,7)$ et, d'après le lemme 0, n'est pas résoluble.

Lemme 4.5. *Si G est résoluble, alors tout diviseur premier q de D_0 est congru à $\pm 1[12]$.*

Preuve. D'après le lemme 4, on sait que $v_q(D_0)$ est paire. Dans ce cas, la longueur de la projection horizontale du côté (S) est $\ell = 2$, et la longueur de sa projection verticale est $h = v_q(D_0)$ qui est un nombre pair. Par [5, Definition 1.4], le polynôme associé au côté (S) est

$$F(Y) = Y^2 + \frac{D_0^*}{7^7.3} \tag{4.2.5}$$

où $D_0^* = \dfrac{D_0}{q^{v_q(D_0)}}$ est la partie première à q de l'entier D_0. Par les mêmes arguments que dans la démonstration du lemme 4, le trinôme $f^*(X)$ se factorise sous la forme (4.2.3), où $f_5(X)$ est un polynôme de degré 5 dont le corps des racines F sur $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$. Comme $q \notin \{2, 3, 7\}$, le polynôme $F(Y)$ est séparable modulo q, et donc on sait, par [5, Theorem 1.5], que le corps des racines du polynôme $f_2(X)$ sur $\mathbb{Q}_q$ est une extension non ramifiée de $\mathbb{Q}_q$. Il en résulte en particulier que le groupe de décomposition D d'une place au-dessus de q du corps des racines N du trinôme $f^*(X)$ est cyclique. D'autre part, aussi par [5, Theorem 1.5], la factorisation dans $\mathbb{Q}_q[X]$ du polynôme $f_2(X)$ est analogue à celle dans $\mathbb{F}_q[X]$ de la réduction $\overline{F}(Y)$ modulo q du polynôme associé $F(Y)$. Comme on sait par les lemmes 1 et 4 que D_0^* est un carré dans $\mathbb{Z}$, la relation (4.2.5) montre que la factorisation du polynôme $\overline{F}(Y)$ dépend uniquement du caractère quadratique de -21 modulo q. Ceci conduit à distinguer deux cas.

Cas 1 $-\bar{21} \in \mathbb{F}_q^2$, dans ce cas $\overline{F}(Y)$ se factorise en 2 polynômes de degré 1 dans $\mathbb{F}_q[X]$. Par conséquent $f_2(X)$ se factorise en 2 facteurs de degré 1 dans $\mathbb{Q}_q[X]$, et donc un générateur de D doit laisser fixes les 2 racines de $f_2(X)$. Comme G est supposé résoluble et que la seule permutation de $AGL(1, 7)$ qui laisse fixes deux points est l'identité, on voit par le lemme 0 que D est trivial et par conséquent $f_5(X)$ est scindé sur $\mathbb{Q}_q$.

Cas 2 $-\bar{21} \notin \mathbb{F}_q^2$. Alors la réduction $\overline{F}(Y)$ modulo q du polynôme associé $F(Y)$ est irréductible dans $\mathbb{F}_q[X]$, et donc $f_2(X)$ est irréductible sur $\mathbb{Q}_q$. Un générateur de D agit donc en échangeant les 2 racines de $f_2(X)$, ce qui montre qu'il est d'ordre pair, donc a exactement un point fixe, qui est forcément une racine de $f_5(X)$. En examinant les permutations éléments du groupe $AGL(1, 7)$, on voit que les seules permutations dans ce groupe qui possèdent un point fixe et un cycle de longueur 2 sont des triples transpositions. Comme conséquence du

lemme 0, le polynôme $f_5(X)$ se factorise sur $\mathbb{Q}_q$ en trois facteurs irréductibles : un de degré 1 et deux de degré 2.

Dans les deux cas, on voit que le polynôme $f_5(X)$ a un nombre impair de facteurs irréductibles dans $\mathbb{Q}_q[X]$: notons par r ce nombre de facteurs. D'après un théorème de Pellet-Stickelberger [16, Theorem 1, p. 1100], et puisqu'on sait par l'argument donné dans la preuve du lemme 4 que la réduction $\overline{f_5}(X)$ du polynôme $f_5(X)$ modulo q est séparable, on en déduit que $r \equiv 5 \pmod 2$ si et seulement si le discriminant $D(f_5)$ du polynôme $f_5(X)$ est un carré dans $\mathbb{Q}_q$. Or, par les relations (4.2.1) et (4.2.3), on sait qu'il existe un élément x du corps $\mathbb{Q}_q$ tel que

$$D(f_5)D(f_2) = -7x^2, \tag{4.2.6}$$

où $D(f_2)$ est le discriminant du polynôme $f_2(X)$. Le corps des racines de $f_2(X)$ étant une extension non ramifiée de $\mathbb{Q}_q$, de degré 1 ou 2 selon que -21 est ou non résidu quadratique modulo q, est forcément égale à $\mathbb{Q}_q(\sqrt{-21})$. Donc $-21D(f_2) \in \mathbb{Q}_q^{*2}$, et ceci, en vertu de la relation (4.2.6), signifie que $D(f_5) \in 3\mathbb{Q}_q^{*2}$. Puisque $q \notin \{2, 3\}$, on a donc $\left(\frac{3}{q}\right) = 1$, où on a employé la notation usuelle $\left(\frac{m}{q}\right)$ pour le symbole de Legendre qui vaut 1 ou -1 selon que l'entier m, supposé premier à q, est ou non un résidu quadratique modulo le nombre premier q. Par la loi de réciprocité quadratique, on en déduit l'égalité

$$\left(\frac{q}{3}\right) = (-1)^{\frac{q-1}{2}},$$

qui équivaut à $q \equiv \pm 1 \pmod{12}$.

4.3 Théorème

les lemmes cités ci dessus sont nos outils de démonstrations du résultat final résumé dans :

Théorème 4.6. *Soit $f(X) = X^7 + aX + a$ où a est un entier de la forme $a = 7a_1$, avec a_1 entier premier à 7.*
On note $D_0 = 7^6 + 6^6 a_1$.
Pour que le groupe de Galois G de f soit résoluble, il est nécessaire que :

1. *D_0 soit un carré dans $\mathbb{Z}$.*
2. *Tout diviseur premier q de D_0 soit congru à $\pm 1[12]$.*

Conclusion et perspectives

Suite essentiellement à la conjecture de Kölle et Schmid, qui a été prouvée par Gauckler pour $p = 5$ [18], notre intention première a été de tenter de l' élargir au cas $p = 7$.

Nous nous sommes ensuite intéressés plus généralement à un trinôme de la forme

$$f(X) = X^p + ac^{p-2}X + ac^{p-1},$$

où p est un nombre premier et où a et c sont deux entiers rationnels mutuellement étrangers. On suppose que ce trinôme est d'Eisenstein en p, c'est-à-dire que $v_p(a) = 1$. Nous avons déterminé des conditions nécessaires pour que le groupe de Galois de ce trinôme soit résoluble, et ceci permet de rétrécir le champ des contre-exemples possibles à la conjecture de Kölle et Schmid.

En posant $D_0 = \dfrac{c}{\mid c \mid}(p^{p-1}c + (p-1)^{p-1}a_1)$, où $a_1 = \dfrac{a}{p}$, les conditions nécessaires ainsi obtenues se laissent décrire comme suit.

1. l'entier D_0 est un carré dans $\mathbb{Z}$.
2. Si $p \equiv 1(mod 4)$, alors l'entier $p \mid c \mid$ est résidu quadratique modulo tout diviseur premier de D_0.
3. Si $p \equiv 3(mod 4)$, alors l'entier $\dfrac{p-1}{2}$ est résidu quadratique modulo tout diviseur premier de D_0.

Dans le cas où $p \equiv 7(mod 8)$ et où $\dfrac{p-1}{2}$ est un nombre premier et en exploitant la loi de réciprocité quadratique, nous avons établi qu'un éventuel contre-exemple à cette conjecture est de la forme

$$f(X) = X^p + pa_1X + pa_1,$$

avec a_1 de la forme

$$a_1 = (v + 2^{p-3}\mu)(u + (\frac{p-1}{2})^{p-1}\mu),$$

où (u, v) est un couple d'entiers positifs satisfaisant à la relation $u2^{p-3} = v(\frac{p-1}{2})^{p-1} + p^l$, avec $u < (\frac{p-1}{2})^{p-1}$, et où μ est un entier tel que $\mu \equiv -4v \pm 2 (mod\, p)$.
Hélas, l'étendue de la théorie de Galois est bien trop vaste pour être couverte dans ce modeste mémoire, dans lequel nous en avons présenté quelques aspects.

Nous pouvons envisager le prolongement du travail entrepris dans cette thèse en examinant les conséquences de la théorie du corps de classes sur les groupes de Galois des trinômes.

Bibliographie

[1] S.S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. **27**, No. 1(1992), 68-133.

[2] J. Angeli, *Trinômes irréductibles résolubles sur un corps de nombres*, Acta Arith. **127** (2007), 169-178.

[3] F. Apéry et J-P. Jouanolou, *Élimination : Le cas d'une variable*, Collection Méthodes, HERMANN (2006).

[4] B. Bensebaa, A. Movaheddi et A. Salinier, *The Galois group of* X^p+aX^s+a, Acta Arith. **134** (2008), 55-65.

[5] B. Bensebaa, A. Movahhedi et A. Salinier, *The Galois Group of* $X^p + aX^{p-1} + a$, Journal of Number Theory, **129**, 4, (2009), 824-830.

[6] A. Bishnoi and S.K.Khanduja, *A class of trinomals with Galois Group* S_n, Algebra Colloquium **19** (2012), 905-911.

[7] N. Bourbaki, *Éléments de Mathématiques*, Livre II Algèbre, Deuxième Edition, Hermann.

[8] Ch. Bouyacoub et A. Salinier, *On the solvability of an Eisenstein trinomial of prime degree*, Acta Arith. **178**, No. 4 (2017), 385-396.

[9] A. Brill, *Ueber die Discriminante*, Math. Ann. **12** (1877), 87-89.

[10] N. Bruin et N.D. Elkies, *Trinomials* ax^7+bx+c *and* ax^8+bx+c *with Galois groups of order 168 and 8.168. In Algorithmic number theory.* (Sydney, 2002), volume 2369 of Lecture Notes in Comput. Sci., 172-188. Springer, Berlin, 2002.

[11] H. Cohen, *A course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics. Springer-Verlag, 1993.

[12] S.D. Cohen, A. Movahhedi and A. Salinier,*Factorization over local fields and the irreducibility of generalized difference polynomials*, Mathematika, **14** (2000), 173-196.

[13] S. D. Cohen, A. Movahhedi and A. Salinier, *Double Transitivity of Galois Groups of Trinomials*, Acta Arith. LXXXII (1997), 1-15.

[14] S. D. Cohen, A. Movahhedi and A. Salinier, *Galois Groups of Trinomials*, Journal of Algebra **222** (1999), 561-573.

[15] J. Dixmier, *Histoire du* 13^e *problème de Hilbert* Cahiers Sem. Hist. Math. Ser. 2 **3** (1993), 85-94.

[16] J.D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163, Springer-Verlag, Berlin/New York, 1996.

[17] W. Feit, *Some consequences of the classification of finite simple groups*, Proc. sympos. Pure Math, **37** (1980), 175-181.

[18] L. Gauckler, *The Galois group of the Eisenstein polynomial* $X^5 + aX + a$, Arch. Math. **90** (2008), 136-139.

[19] A. Hermez et A. Salinier, *Rational Trinomials with the Alternating Group as Galois Group*, Journal of Number Theory **90** Fasc 1, (2001), 113-129.

[20] M. Kölle et P.Schmid, *Computing Galois groups by means of Newton polygons*, Acta Arith. **115**(2004), 71-84.

[21] K. Komatsu, *On the Galois group of* $X^p + aX + a = 0$, Tokyo J. Math. **15**, No 1 (1991), 227-229.

[22] T. Lalesco, *Sur les groupes des équations trinômes*, Bull. Soc. Math. France. **35**(1907), 75-76.

[23] S. LANG, *Algebra*, Second Edition, Addition-Wesley Publishing Company, Inc, (2002), California.

[24] Literatur-Berichte, *Lehrbuch der Algebra*, Monatsh. Math. Phys., **6**, (1) : A15-A19, 1895. Heinrich Weber. In zwei Bänden. I. Band. Friedrich Vieweg und Sohn, Braunschweig. 1895. XV+653 S. gr. 8 o. Ladenpreis 16 M.

[25] J. Montes Peral, *Poligonos de Newton de orden superior y aplicaciones arithméticas*, Memoria presentada para optar al grado de Doctor en Matematicas, Universitat de Barcelona(1999).

[26] A. Movahhedi, *Galois group of $X^p + aX + a$*, J. Algebra. **180** (1996), 966-975.

[27] A. Movahhedi and A. Salinier, *The primitivity of the Galois group of trinomial*, J. London Math. Soc. (2) **53** (1996), 433-440.

[28] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed, Springer, Berlin, and PWN-Polish Scientific Publ, Warszawa, 2006.

[29] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Korper*, Meth. Ann. **99** (1928), 84-117.

[30] H. Osada, *The Galois groups of polynomials $x^n + ax^s + b$* , J. Number Th. **25**(1987),230-238.

[31] H. Osada, *The Galois groups of polynomials x^n+ax^s+b*, II, Tôhoku Math.J. **39** (1987), 437-445.

[32] G. Polya, G. Szegö, *Problems and theorems in Analysis, Tome 2.*

[33] J. Rotman, *Galois Theory*, Second Edition, Springer-Verlag New York (1998).

[34] A.Schinzel,*On Reducible trinomials*, Dissertations Mat,**329** (1993), 83pp.

[35] I. Schur, *Einige Satze Uber Primzahlen mit Annendungen and Irreduzibilitts fragen I*, Gesammelte Abhandlungen, Band III **64** (1929) 140-151.

[36] I. Schur, *Gleichungen ohne Affekt*, Gesammelte Abhandlungen, Band III **67** (1930) 191-197.

[37] J.-P. Serre, *Corps locaux*, troisième ed. Hermann, 1968.

[38] J.-P. Serre, *Topics in Galois Theory*, Jones and Barlett, Boston, MAA, 1992.

[39] K. Spindler, *Abstract Algebra with Applications*, Marcel Dekker, Inc, New York (1994).

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

[41] W. Trinks, *Ein Beispiel eines Zahlkörpers mit der Galoisgruppe PSL(3,2) über* $\mathbb{Q}$, manuscrit, Univ. Karlsruhe, (1968).

[42] K. Uchida, *Galois groups of unramified solvable extensions*, Tôhoku Math.Journ. **34** (1982), 311-317.

[43] K. Uchida, *Galois groups of an equation* $X^n - aX + b = 0$, Tôhoku Math.Journ. **22** (1970), 670-678.

[44] B.L.Van der Waerden,*Die Seltenheit der Gleichungen mit Affect*, Math.Ann., **109**, (1934), 13-16.