THÈSE de DOCTORAT de l'UNIVERSITÉ PARIS 6

Spécialité : INFORMATIQUE

Présentée par

Gaétan HACHÉ

pour obtenir le titre de

DOCTEUR DE L'UNIVERSITÉ PARIS 6

Titre de la thèse :

Construction Effective des Codes Géométriques

Soutenue le 19 septembre 1996, devant le jury composé de :

Daniel LAZARD	*Président*
Dominique DUVAL	*Rapporteur*
Jacques WOLFMANN	*Rapporteur*
Dominique Le BRIGAND	*Directeur*
Pascale CHARPIN	*Examinateur*
Tom HØHOLDT	*Examinateur*
Jean-Jacques RISLER	*Examinateur*

Remerciements

Mes remerciements vont tout d'abord à Bernard Courteau qui le premier m'a initié à la recherche en mathématiques. C'est a lui que je dois d'avoir commencé mes études doctorales.

J'exprime ma gratitude la plus sincère à Dominique Le Brigand pour avoir dirigé cette thèse avec une patience infinie. Je la remercie aussi pour l'amitié et le soutien qu'elle m'a prodigués tout au long de cette thèse.

J'adresse mes plus sincères remerciements à Dominique Duval et Jacques Wolfmann pour avoir accepté la lourde tâche de rapporteur. J'en suis très honoré.

Pour avoir rendu possible ma venue au projet CODES, je remercie Paul Camion et Pascale Charpin.

Merci à Daniel Lazard d'avoir présidé le jury.

Mange tak til Tom Høholdt som sad i bedømmelsesudvalget.

Je remercie Jean-Jacques Risler pour sa participation au jury et pour m'avoir aidé dans la démonstration de la Proposition 4.2.1.

À Daniel Augot, je lui dit sincèrement merci. Je le remercie d'avoir toujours su m'écouter et répondre à mes questions. Je le remercie pour son aide expérimentée en Axiom. Travailler à ses cotés fut pour moi une chance inouïe.

Merci à Guy Chassé. J'ai toujours su profiter de ses talents de géomètre.

Merci à Ruud Pellikaan, Tom Høholdt et Henning Stichtenoth pour l'intérêt qu'a suscité en eux mes travaux sur la construction effective des codes sur des extensions du type d'Artin-Schreier.

J'aimerais tout particulièrement remercier encore une fois Ruud Pellikaan pour l'accueil chaleureux qu'il m'a prodigué lors de mon séjour de trois mois au département de mathématiques discrètes de l'Université d'Eindhoven.

Tak til Kaj Laursen, pour le vif intérêt qu'il porte à l'égard de mes travaux de recherches et tout spécialement pour mon implantation de l'algorithme de Brill-Noether : il m'a beaucoup aidé en y ajoutant les fonctionnalités relatives au calcul de la fonction Zéta.

Mes remerciements à tous les membres du projets CODES que je n'ai pas déja nommés : Nicolas Sendrier, Anne Canteaut, Caroline Fontaine, Grégoire Bommier et Christelle Guiziou qui effectue toujours nos travaux de secrétariat avec le sourire. Grâce à eux, on y travaille dans la bonne humeur. Je salue aussi les anciens, Françoise Levy-dit-Vehel et Hervé Chabanne.

Enfin, merci à Gaëtane d'avoir partagé les joies et les peines qui ont constitué ma vie de thésard.

Introduction

En 1981, V.D. Goppa introduit une nouvelle construction de codes correcteurs qu'on appelle maintenant *codes de Goppa géométriques* (ou simplement codes géométriques). Ces codes sont construits à partir d'une courbe algébrique lisse ou, de façon équivalente, à partir d'un corps de fonctions algébriques à une variable. C'est en particulier grâce au Théorème de Riemann-Roch que l'on peut déterminer les paramètres de ces codes. Dès lors, la rencontre [1] de la théorie des codes correcteurs et celle de la géométrie algébrique n'a cessé d'apporter de nouveaux résultats aux deux théories : parmi les plus remarquables citons celui dû à M. Tsfasman, S. Vlăduţ et T. Zink [44] qui ont donné la première construction d'une classe de codes dépassant la borne de Varshamov-Gilbert.

Ce mémoire traite de la construction effective des codes géométriques et de son implantation sur ordinateur. Le problème le plus difficile pour construire un code géométrique est celui de calculer une base de l'espace vectoriel associé à un diviseur d'un corps de fonctions. Dans le cas où on connaît un modèle plan du corps de fonctions, c'est-à-dire une courbe plane dont le corps des fonctions est isomorphe au corps de fonctions initial, il existe essentiellement deux méthodes pour calculer une telle base : la première est inspirée de la théorie des nombres et ne s'applique qu'aux courbes affines planes n'ayant aucune ramification à l'infini (cf. [2, 46]). L'autre méthode consiste à appliquer l'algorithme de Brill-Noether et fait appel à la notion d'éclatement de points et de courbes adjointes : cette dernière est proposée par Goppa ([14, 15]) dans le cas particulier où la courbe n'a que des singularités ordinaires qui est l'unique cas dans lequel l'algorithme est classiquement présenté [2] (voir aussi [10, 24]). C'est cette dernière méthode qui a été choisie car en fait, comme l'ont montré D. Le Brigand et J.J. Risler [28], l'algorithme de Brill-Noether se généralise à toutes courbes planes quelle que soit la nature de leurs singularités.

L'objectif principal de mon travail de thèse a été de réaliser un logiciel qui im-

1. Notons que V.D. Goppa avait déjà souligné en 1977 ([12]) que la rencontre des deux théories était inévitable.

2. Théoriquement, l'une ou l'autre des deux méthodes est suffisante car toute courbe plane $\mathcal{C}$ est birationnelle à une courbe plane $\mathcal{C}'$ adéquate pour la méthode choisie.

plante l'algorithme de Brill-Noether comme décrit par D. Le Brigand et J.J. Risler [28]. Ces travaux ont donné lieu à la publication de deux articles : le premier [19] se veut un prolongement de [28] et a été écrit en collaboration avec D. Le Brigand. Il utilise un point de vue géométrique et donne une version précise des procédures sous-jacentes à l'algorithme de Brill-Noether. Le deuxième [17] reprend le premier en utilisant un point de vue strictement algébrique ce qui à mon avis rend plus aisé le passage de la théorie à l'implantation.

Voici comment ce mémoire est organisé. Le premier chapitre rappelle les notions de base de la théorie des corps de fonctions algébriques à une variable qui caractérisent les corps des fonctions des courbes algébriques. On choisit donc d'emblée l'approche algébrique pour définir les codes géométriques. Bien que moins intuitive que l'approche géométrique, l'approche algébrique se veut plus naturelle car elle permet de considérer un corps de base non algébriquement clos et en l'occurrence les corps finis. On retrouvera aux Sections 1.2 à 1.4 les notions d'anneaux de valuation, de places, de diviseurs et d'espace vectoriel associés à un diviseur. La Section 1.5 est consacrée au Théorème de Riemann-Roch qui permet de déterminer les paramètres des codes géométriques. Ceux-ci seront définis à la Section 1.6 et on terminera le chapitre avec quelques remarques liées à la construction effective de tels codes.

Le Chapitre 2 présente l'algorithme de Brill-Noether. Cet algorithme utilise à la fois les propriétés locales et globales des courbes planes. L'étude des propriétés locales d'une courbe correspond à celle des anneaux locaux des points. À la Section 2.1, on montre le lien existant entre les anneaux locaux de points et les places du corps des fonctions d'une courbe affine plane. On sera alors en mesure à la Section 2.2 de définir les éclatements de points en utilisant une approche algébrique inspirée de celle que l'on retrouve dans l'article de H. Hironaka [22]. Seront définis ensuite les diviseurs exceptionnels de points en fonction desquels sont fait la plupart des calculs liés à l'algorithme de Brill-Noether. À la Section 2.4 on se situe dans le plan projectif pour étudier les propriétés globales des courbes. On y trouvera en particulier une variante du Théorème de Bézout formulée en fonction des diviseurs d'intersection de polynômes homogènes avec une courbe projective plane. En utilisant à la fois cette variante et le Théorème de Bézout, on montrera que le degré du diviseur exceptionnel d'un point est égal à la multiplicité du point. On en déduira une preuve simple du fait bien connu qu'un nombre fini d'éclatements suffisent à désingulariser une courbe plane dans un voisinage d'un point singulier. Vient ensuite la notion d'arbre de désingularisation et plus particulièrement celle de diviseur d'adjonction d'une courbe projective plane (Sections 2.5 et 2.6). Dès lors, on a tous les outils nécessaires pour définir l'algorithme de Brill-Noether (Section 2.7). La Section 2.8

termine le Chapitre 2 en expliquant comment appliquer l'algorithme de Brill-Noether dans le cas particulier d'une courbe projective plane définie sur un corps fini.

Le Chapitre 3 est consacré à l'implantation de l'algorithme de Brill-Noether dans le système de calcul formel Axiom. Chacune des sections traite d'un algorithme particulier sous-jacent à l'algorithme de Brill-Noether. Les algorithmes seront généralement donnés sous forme de pseudo-codes. Cependant, en fonction de leur nature, certains algorithmes seront donnés tels qu'ils ont été codés dans le langage Axiom. À la première section, j'introduis la notion *d'extension dynamique d'un corps fini* qui est inspirée de la clôture algébrique dynamique d'un corps définie par D. Duval [8]. L'utilisation des extensions dynamiques est nécessaire pour la raison suivante : pour appliquer l'algorithme de Brill-Noether à une courbe projective plane définie sur $\mathbb{F}_q$, on est presque toujours obligé d'étendre le corps de base $\mathbb{F}_q$. Or, il est difficile, voire impossible, de déterminer à l'avance le degré de la plus petite extension de $\mathbb{F}_q$ qui sera nécessaire pour mener à bien les calculs. Au mieux, on peut montrer qu'une extension suffisante aura un degré de l'ordre de $\text{ppcm}(\{1, 2, \ldots, n^2\})$ ce qui, on en convient, est beaucoup trop élevé. On utilisera donc les extensions dynamiques pour construire au fur et à mesure les extensions successives de $\mathbb{F}_q$ qui seront nécessaires à l'aboutissement des calculs. Il y a aussi un autre avantage non négligeable à l'utilisation des extensions dynamiques : je montrerai comment les utiliser pour répartir les calculs dans un nombre fini d'extensions $\mathbb{F}_{q^{r_i}}$ telles que $r_i \leq N$ et $N \simeq O(n^2 + d)$ où n est le degré de la courbe et d est le degré diviseur pour lequel on veut calculer une base de l'espace vectoriel associé. Je terminerai ce chapitre en donnant quelques exemples d'utilisations de mon logiciel. On y retrouvera entre autre une construction de codes géométriques quasi auto-duaux que j'ai obtenue en m'inspirant d'un article de W. Scharlau [39] (voir aussi [18]).

Le Chapitre 4 n'utilise pas l'algorithme de Brill-Noether. Il concerne une construction effective d'une classe de codes géométriques qui dépasse la borne de Varshamov-Gilbert et qui a été obtenue tout récemment par A. Garcia et H. Stichtenoth [11]. Cette classe est construite en utilisant des extensions de corps

$$F_1 \subset F_2 \subset \ldots \subset F_n \subset \ldots$$

où chacun des corps F_n est un corps de fonctions algébriques à une variable de la forme $F_n := \mathbb{F}_{q^2}(x_1, x_2, \ldots, x_n)$ et tel que F_n est une extension du type d'Artin-Schreier de F_{n-1}. Dans les cas particuliers où $n = 1, 2, 3$, T. Høhold et C. Voss [23] donnent une formulation explicites de ces codes mais, comme ils le soulignent eux-mêmes, il ne semble pas possible de la généraliser. Pour $n \geq 4$ le problème est toujours ouvert. À défaut d'une formulation explicite, on considère donc une construction effective. Malheureusement, il ne suffit pas d'appliquer l'algorithme de Brill-Noether : pour le corps de fonctions F_n, le degré d'une courbe plane $\mathcal{C}_n$ telle que $\mathbb{F}_{q^2}(\mathcal{C}_n) \cong F_n$ est d'ordre $O(q^{n/2})$ et les calculs s'avèrent alors d'une trop grande complexité. Néanmoins, pour les cas $q \leq 3$ et $n \leq 3$, il est possible d'appliquer l'algorithme et de construire des codes avec des temps de calculs raisonnables. Les résultats de ces premiers calculs expérimentaux m'ont permis de déduire une méthode de construction effective particulière aux codes géométriques définis sur les corps F_n. En voici les grandes lignes. Pour certains diviseurs particuliers D de F_n, je démontrerai que l'espace vectoriel associé $\mathcal{L}(D)$ possède une base contenue dans l'anneau $\mathbb{F}_{q^2}[x_1, x_2, \ldots, x_n]$. Ensuite, pour toute place $\mathfrak{P}$ de F_n qui est un zéro ou un pôle de x_1 j'expliquerai comment calculer pour chacune des fonctions x_i, $i = 1, 2, \ldots, n$, la série $\mathfrak{P}$-adique en fonction d'un paramètre local de $\mathfrak{P}$. On sera alors en mesure d'établir un système d'équations linéaires exprimant les conditions nécessaires et suffisantes pour qu'un élément de $\mathbb{F}_{q^2}[x_1, x_2, \ldots, x_n]$ appartienne à $\mathcal{L}(D)$. Pour finir, je montrerai comment utiliser ce système d'équations linéaires pour obtenir une base de $\mathcal{L}(D)$ avec laquelle on construira un code géométrique. On trouvera à la fin du chapitre un exemple d'application de cette méthode.

Table des matières

Chapitre 1

Notions de base

Dans ce chapitre, je rappelle les notions de base de la théorie des corps de fonctions algébriques à une variable. Cette théorie permet de définir les codes géométriques (cf. Section 1.6). Je me réfère essentiellement au livre de Henning Stichtenoth "Algebraic Function Fields and Codes" ([43]), et dans la mesure du possible, j'utilise les mêmes notations.

1.1 Corps de fonctions algébriques à une variable

Dans tout ce qui suit, K est un corps commutatif quelconque et $\overline{K}$ une clôture algébrique de K.

DÉFINITION 1.1.1 *Un* corps de fonctions algébriques à une variable F/K *est une extension de corps* $F \supset K$ *telle qu'il existe* $x \in F$ *transcendant sur* K *pour lequel* F *est une extension finie de* $K(x)$*. Le corps* K *est appelé* corps de base *de* F/K *et la clôture algébrique de* K *dans* F*,*

$$\overline{K}^c := \{\, \alpha \in F \mid \alpha \text{ est algébrique sur } K \,\},$$

est appelée corps des constantes *de* F/K*.*

Dans le but d'alléger le texte, on désignera simplement par corps de fonctions un corps de fonctions algébriques à une variable.

REMARQUE 1.1.2 On démontre aisément que $z \in F$ est transcendant sur K si et seulement si $[F : K(z)] < \infty$.

EXEMPLE 1.1.3 Soit x transcendant sur K. Alors $K(x)/K$ est un corps de fonctions appelé corps rationnel sur K. Il est facile de voir que le corps des constantes de

$K(x)/K$ est égal au corps de base K. Observons aussi que tout élément $z \in K(x) \setminus \{0\}$ admet une factorisation unique

$$z = \alpha \prod_{i=1}^{r} p_i(x)^{n_i} \tag{1.1}$$

où $\alpha \in K \setminus \{0\}$, $n_i \in \mathbb{Z}$ et les polynômes $p_i \in K[x]$ sont irréductibles, unitaires et deux à deux distincts.

Remarque 1.1.4 Le corps de base d'un corps de fonctions n'est pas toujours égal au corps des constantes. Par exemple, soient $K := \mathbb{F}_2$ et

$$C := X^2 + XY + Y^2 \in \mathbb{F}_2[X, Y].$$

Le polynôme C est irréductible dans l'anneau $\mathbb{F}_2[X, Y]$, mais il est réductible dans $\overline{\mathbb{F}}_2[X, Y]$. L'anneau quotient

$$R := \mathbb{F}_2[X, Y]/\langle C \rangle$$

est intègre. Soit F le corps des fractions de R. Il est clair que F/K est un corps de fonctions. Maintenant, soient x et y les images résiduelles respectives de X et Y dans F. Alors

$$\left(\frac{x}{y}\right)^2 + \frac{x}{y} + 1 = \frac{x^2 + xy + y^2}{y^2} = 0,$$

d'où $x/y \in \overline{K}^c$. En fait, $\overline{K}^c$ se plonge dans le corps $\mathbb{F}_{2^2}$ et le corps F est isomorphe au corps rationnel sur $\mathbb{F}_{2^2}$.

Proposition 1.1.5 *Soit F/K un corps de fonctions où K est parfait. Alors il existe $x, y \in F$ tels que $F = K(x, y)$.*

Démonstration : Stichtenoth [43, Proposition III.9.2].

Si F/K est un corps de fonctions, il existe donc $x, y \in F$ tels que $F = K(x, y)$, et il est clair que y est algébrique sur $K(x)$. Posons $n := [F : K(x)]$ et soit

$$\varphi(Y) := Y^n + a_1(x)Y^{n-1} + \cdots + a_n(x) \in K(x)[Y]$$

le polynôme minimal de y sur $K(x)$. Pour $i = 1, 2, \ldots, n$, soient $G_i(X), H_i(X) \in K[X]$ tels que

$$a_i(x) = G_i(x)/H_i(x)$$

et supposons sans perte de généralité que $G_i(X)$ et $H_i(X)$ n'ont pas de facteur commun et que chacun des polynômes H_i est unitaire. Soit $B(X) \in K[X]$ le plus petit commun multiple des polynômes $H_i(X)$, $i = 1, 2, \ldots, n$. Soit le polynôme

$$C(X, Y) := B(X) \left(Y^n + \frac{G_1(X)}{H_1(X)} Y^{n-1} + \cdots + \frac{G_n(X)}{H_n(X)} \right) \in K[X, Y].$$

Il est clair que

$$C(x,y)=0.$$

En utilisant le fait que les polynômes $G_i(X)$ et $H_i(X)$ n'ont pas de facteur commun, on vérifie aisément que l'irréductibilité de $\varphi(Y)$ entraîne celle de $C(X,Y)$. Il est aussi aisé de montrer que si $C' \in K[X,Y]$ est un autre polynôme irréductible tel que $C'(x,y)=0$, alors il existe $\alpha \in K$ tel que $C=\alpha C'$. Rappelons qu'un polynôme $C \in K[X,Y]$ est dit **absolument irréductible** si C est irréductible dans l'anneau $\overline{K}[X,Y]$.

PROPOSITION 1.1.6 *Soit F/K un corps de fonctions où K est parfait. Soit $\overline{K}^c$ le corps des constantes de F/K. Soient $x,y \in F$ tels $F=K(x,y)$ et soit $C \in K[X,Y]$ un polynôme irréductible tel que $C(x,y)=0$. Alors*

$$K=\overline{K}^c \iff C \text{ est absolument irréductible.}$$

Démonstration : Stichtenoth [43, Corollaire III.6.7].

1.2 Anneaux de valuation et places

Soient $K(x)/K$ le corps rationnel, $z \in K(x) \setminus \{0\}$ et $\alpha \in K$. En considérant la factorisation de z comme en (1.1), il est clair qu'il existe $g,h \in K[x]$ premiers entre eux tels que $z=g/h$. Si $h(\alpha)\neq 0$, on peut alors évaluer z en α en posant $z(\alpha):=g(\alpha)/h(\alpha)$. On dira que α est un *zéro* de z si $z(\alpha)=0$. Si $h(\alpha)=0$, alors z n'est pas défini en α et on dit alors que α est un *pôle* de z. Observons qu'il existe un unique entier $n \in \mathbb{Z}$ et un unique élément $u \in K(x)$ tels que $z=(x-\alpha)^n u$ et $u(\alpha)\neq 0$. Si $n>0$, alors $z(\alpha)=0$ et on dit que α est un *zéro d'ordre* n. Si par contre $n<0$, on dit alors que α est un *pôle d'ordre* n. On veut généraliser cette propriété à tout corps de fonctions F/K et pour ce faire on introduit les notions *d'anneaux de valuation* et *places* de F/K.

DÉFINITION 1.2.1 *Soit F/K un corps de fonctions. Un* **anneau de valuation** $\mathcal{O}$ *de F/K est un anneau tel que*

1. *$K \subsetneq \mathcal{O} \subsetneq F$,*
2. *pour tout $x \in F$, $x \notin \mathcal{O} \Longrightarrow x^{-1} \in \mathcal{O}$.*

EXEMPLE 1.2.2 Soient le corps rationnel $K(x)/K$ et $p \in K[x]$ un polynôme irréductible. Il est clair que

$$\mathcal{O}_p := \{\, g/h \mid g,h \in K[x], p \text{ ne divise pas } h \,\}$$

est un anneau de valuation de $K(x)/K$. Aussi, on vérifiera facilement que

$$\mathcal{O}_\infty := \{\, g/h \mid g, h \in K[x], \deg g \leq \deg h \,\}$$

est un anneau de valuation de $K(x)/K$. De plus, on peut montrer que

$$\{\, \mathcal{O}_p \mid p \in K[x], p \text{ est irréductible} \,\} \cup \{\, \mathcal{O}_\infty \,\}$$

est exactement l'ensemble de tous les anneaux de valuation de $K(x)/K$ (cf. Stichtenoth [43, Section I.2]).

PROPOSITION 1.2.3 *Soit $\mathcal{O}$ un anneau de valuation du corps de fonctions F/K. Alors*

1. *$\mathcal{O}$ est un anneau local ; son unique idéal maximal est $\mathfrak{P} := \mathcal{O} \setminus \mathcal{O}^*$, où $\mathcal{O}^*$ est le groupe des éléments inversibles de $\mathcal{O}$,*
2. *pour $0 \neq x \in F$, on a $x \in \mathfrak{P} \iff x^{-1} \notin \mathcal{O}$,*
3. *$\overline{K}^c \subset \mathcal{O}$ et $\overline{K}^c \cap \mathfrak{P} = \{\, 0 \,\}$ où $\overline{K}^c$ est le corps des constantes de F/K.*

Démonstration : Stichtenoth [43, Proposition I.1.5].

DÉFINITION 1.2.4 *Une* place *$\mathfrak{P}$ d'un corps de fonctions F/K est l'idéal maximal d'un anneau de valuation $\mathcal{O}$ de F/K. On désigne par $\mathbb{P}_F$ l'ensemble de toutes les places de F/K.*

THÉORÈME 1.2.5 *Soient $\mathcal{O}$ un anneau de valuation du corps de fonctions F/K et $\mathfrak{P}$ l'unique idéal maximal de $\mathcal{O}$. L'anneau $\mathcal{O}$ est principal : plus précisément, si $I \neq \{\, 0 \,\}$ est un idéal de $\mathcal{O}$ et $t \in \mathfrak{P}$ est tel que $\mathfrak{P} = t\mathcal{O}$, alors il existe $n \in \mathbb{N}$ tel que $I = t^n\mathcal{O}$. L'entier n dépend uniquement de l'idéal I et non du choix de l'élément t tel que $\mathfrak{P} = t\mathcal{O}$.*

Démonstration : Stichtenoth [43, Théorème. I.1.6]

DÉFINITION 1.2.6 *Soit $\mathfrak{P}$ une place du corps de fonctions F/K. Tout élément $t \in \mathfrak{P}$ tel que $\mathfrak{P} = t\mathcal{O}$ est appelé* paramètre local *de la place $\mathfrak{P}$.*

D'après la Proposition 1.2.3, tout anneau de valuation $\mathcal{O}$ d'un corps de fonctions F/K est uniquement déterminé par son unique idéal maximal $\mathfrak{P}$ puisque $\mathcal{O} := \{\, z \in F \mid z^{-1} \notin \mathfrak{P} \,\}$. On appelle donc $\mathcal{O}_\mathfrak{P} := \mathcal{O}$ l'anneau de valuation de la place $\mathfrak{P}$.

DÉFINITION 1.2.7 *Une* valuation discrète *d'un corps L est une application surjective*

$$\nu : L \to \mathbb{Z} \cup \{ \infty \}$$

telle que

1. $\nu(x) = \infty \iff x = 0$,
2. $\nu(xy) = \nu(x) + \nu(y)$ *quels que soient* $x, y \in L$,
3. $\nu(x+y) \geq \min \{ \nu(x), \nu(y) \}$ *quels que soient* $x, y \in L$ *(*inégalité du triangle*).*

Soit K un sous-corps de L. On dit que ν est triviale *sur K si quel que soit $x \in K \setminus \{ 0 \}$ on a $\nu(x) = 0$.*

LEMME 1.2.8 (INÉGALITÉ STRICTE DU TRIANGLE) *Soient ν une valuation discrète d'un corps L et $x, y \in L$. Si $\nu(x) \neq \nu(y)$ alors $\nu(x+y) = \min \{ \nu(x), \nu(y) \}$.*

Démonstration : D'après 1.2.7(2), on a $\nu(-1) = \nu((-1)^3) = 3\nu(-1)$ d'où $\nu(-1) = 0$. Par conséquent, pour tout $x \in L$, on a $\nu(-x) = \nu(-1) + \nu(x) = \nu(x)$. Maintenant, soient $x, y \in L$ tels que $\nu(x) \neq \nu(y)$ et supposons sans perte de généralité que $\nu(x) > \nu(y)$. Supposons qu'on ait $\nu(x+y) \neq \min \{ \nu(x), \nu(y) \}$. On a donc $\nu(x+y) > \nu(y)$ d'après 1.2.7(3). Mais alors $\nu(y) = \nu((x+y) - x) \geq \min \{ \nu(x+y), \nu(x) \} > \nu(y)$ ce qui est impossible. □

Soient $\mathfrak{P}$ une place d'un corps de fonctions F/K, t un paramètre local de $\mathfrak{P}$ et $x \in F \setminus \{ 0 \}$. En vertu du Théorème 1.2.5, il existe $u \in \mathcal{O}_{\mathfrak{P}}^*$ et un unique entier $n \in \mathbb{Z}$ tels que

$$x = t^n u.$$

En particulier, l'application $\nu_{\mathfrak{P}} : F \to \mathbb{Z} \cup \{ \infty \}$ donnée par

$$\nu_{\mathfrak{P}}(x) := \begin{cases} n & \text{si } x \neq 0 \text{ et } x = t^n u \text{ où } u \in \mathcal{O}_{\mathfrak{P}}^*, \\ \infty & \text{si } x = 0 \end{cases} \tag{1.2}$$

est bien définie et ne dépend pas du choix du paramètre local de la place $\mathfrak{P}$.

THÉORÈME 1.2.9 *Soient $\mathfrak{P}$ une place de F/K et $\nu_{\mathfrak{P}}$ l'application définie en (1.2). Alors*

1. *l'application $\nu_{\mathfrak{P}}$ est une valuation discrète de F triviale sur K et*

$$\begin{aligned} \mathcal{O}_{\mathfrak{P}} &= \{ z \in F \mid \nu_{\mathfrak{P}}(z) \geq 0 \}, \\ \mathcal{O}_{\mathfrak{P}}^* &= \{ z \in F \mid \nu_{\mathfrak{P}}(z) = 0 \}, \\ \mathfrak{P} &= \{ z \in F \mid \nu_{\mathfrak{P}}(z) > 0 \}. \end{aligned}$$

Un élément $x \in F$ est un paramètre local de $\mathfrak{P}$ si et seulement si $\nu_{\mathfrak{P}}(x) = 1$.

2. *Réciproquement, soit ν une valuation discrète de F triviale sur K. Alors il existe une et une seule place $\mathfrak{P}$ de F/K telle que $\nu(x) = \nu_{\mathfrak{P}}(x)$ pour tout $x \in F$.*

3. *Tout anneau de valuation de F/K est un sous-anneau maximal propre de F.*

Démonstration : Stichtenoth [43, Théorème I.1.12].

EXEMPLE 1.2.10 Soient $K(x)/K$ le corps rationnel et $p \in K[x]$ un polynôme irréductible. Notons $\mathfrak{P}_p$ la place de l'anneau de valuation $\mathcal{O}_p$ défini à l'Exemple 1.2.2. On a

$$\mathfrak{P}_p = \{\, g/h \mid g, h \in K[x], p \text{ ne divise pas } h, p \text{ divise } g \,\}.$$

Il est clair alors que p est un paramètre local de $\mathfrak{P}_p$. De plus, pour $z \in K(x)$, il est aisé de calculer la valuation $\nu_{\mathfrak{P}_P}(z)$ si l'on sait factoriser z comme en (1.1).

Soit $\mathcal{O}_{\mathfrak{P}}$ l'anneau de valuation d'une place $\mathfrak{P}$ du corps de fonctions F/K. Puisque $\mathfrak{P}$ est un idéal maximal de $\mathcal{O}_{\mathfrak{P}}$, l'anneau quotient $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ est un corps. D'après la Proposition 1.2.3, on a $K \subseteq \overline{K}^c \subset \mathcal{O}_{\mathfrak{P}}$ et $\overline{K}^c \cap \mathfrak{P} = \{\,0\,\}$. Par suite, K et $\overline{K}^c$ se plongent dans $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ via l'application canonique

$$\begin{array}{ccc} \mathcal{O}_{\mathfrak{P}} & \longrightarrow & \mathcal{O}_{\mathfrak{P}}/\mathfrak{P} \\ x & \mapsto & x + \mathfrak{P}. \end{array}$$

DÉFINITION 1.2.11 *Soit $\mathfrak{P}$ une place du corps de fonctions F/K. On appelle $F_{\mathfrak{P}} := \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ le* corps résiduel *de la place $\mathfrak{P}$ et $\deg \mathfrak{P} := [F_{\mathfrak{P}} : K]$ le* degré *de la place $\mathfrak{P}$. Si $x \in \mathcal{O}_{\mathfrak{P}}$, alors $x(\mathfrak{P}) := x + \mathfrak{P}$ est appelé* évaluation *de x à la place $\mathfrak{P}$.*

DÉFINITION 1.2.12 *Soit $z \in F \setminus \{\,0\,\}$ et $\mathfrak{P} \in \mathbb{P}_F$. On dit que $\mathfrak{P}$ est un* zéro *de z si $\nu_{\mathfrak{P}}(z) > 0$. On dit que $\mathfrak{P}$ est un* pôle *de z si $\nu_{\mathfrak{P}}(z) < 0$.*

PROPOSITION 1.2.13 *Soient F/K un corps de fonctions et $\mathfrak{P} \in \mathbb{P}_F$. Alors quel que soit $x \in \mathfrak{P} \setminus \{\,0\,\}$, on a*

$$\deg \mathfrak{P} \leq [F : K(x)] < \infty.$$

Démonstration : Stichtenoth [43, Proposition I.1.14].

REMARQUE 1.2.14 Soit $\mathfrak{P}$ une place du corps de fonctions F/K. Si $\deg \mathfrak{P} = 1$, alors $K \cong F_{\mathfrak{P}}$. On identifiera donc à K tout corps résiduel d'une place de degré 1. Soulignons au passage que si K est algébriquement clos, alors toutes les places de F/K sont de degré 1 (c'est une conséquence immédiate de la proposition précédente).

Puisque le corps des constantes $\overline{K}^c$ d'un corps de fonctions F/K se plonge dans le corps $F_{\mathfrak{P}}$ quelle que soit la place $\mathfrak{P} \in \mathbb{P}_F$, on a le corollaire suivant :

Corollaire 1.2.15 *Soit $\overline{K}^c$ le corps des constantes de F/K. Alors*

$$[\overline{K}^c : K] < \infty.$$

Avant de continuer, il faut s'assurer qu'il existe des places de F/K.

Proposition 1.2.16 *Soit le corps de fonctions F/K. Soient un anneau R tel que $K \subsetneq R \subsetneq F$ et I un idéal propre de R. Alors il existe une place $\mathfrak{P} \in \mathbb{P}_F$ telle que $R \subseteq \mathcal{O}_{\mathfrak{P}}$ et $I \subseteq \mathfrak{P}$. En particulier, si I est un idéal premier, alors $I = \mathfrak{P} \cap R$.*

Démonstration : Stichtenoth [43, Théorème I.1.18]. Pour la dernière assertion voir Chevalley [5, Remarque 2, page 8].

Corollaire 1.2.17 *Soient le corps de fonctions F/K et $z \in F$ transcendant sur K. Alors z possède au moins un zéro et un pôle. En particulier, $\mathbb{P}_F \neq \emptyset$.*

Démonstration : Pour trouver un zéro de z, il suffit d'appliquer la proposition précédente à l'anneau $K[z] \subset F$ et à l'idéal $I := zK[z]$. Pour trouver un pôle de z on applique le même argument avec z^{-1}. □

Remarque 1.2.18 Soient le corps de fonctions F/K et $z \in F \setminus \{0\}$. Alors

$$z \in \overline{K}^c \setminus \{0\} \iff z \text{ n'a ni zéro ni pôle.}$$

En effet, l'implication ($\Rightarrow$) est immédiate du fait que $\overline{K}^c \cap \mathfrak{P} = \{0\}$ pour tout $\mathfrak{P} \in \mathbb{P}_F$ et la réciproque est équivalente au corollaire précédent car si $z \notin \overline{K}^c$, alors z est transcendant sur K.

Proposition 1.2.19 *Dans un corps de fonctions F/K, tout élément $z \in F \setminus \{0\}$ possède au plus un nombre fini de zéros et de pôles.*

Démonstration : Stichtenoth [43, Corollaire I.3.4].

1.3 Diviseurs

Soient F/K un corps de fonctions et son corps des constantes $\overline{K}^c$. Puisque

$$[\overline{K}^c : K] < \infty,$$

on peut considérer F comme un corps de fonctions sur $\overline{K}^c$. De plus, puisqu'un anneau de valuation de F/K contient le corps des constantes, l'ensemble de tous les anneaux de valuation de $F/\overline{K}^c$ est exactement le même que l'ensemble de tous les anneaux de valuation de F/K.

> *Dans tout ce qui suit, quel que soit le corps de fonctions considéré, on supposera le corps de base égal au corps des constantes.*

Soit F/K un corps de fonctions. On note $\mathcal{D}_F$ le groupe abélien libre engendré par $\mathbb{P}_F$. Un élément $D \in \mathcal{D}_F$ est appelé diviseur de F/K. On a donc

$$D = \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \mathfrak{P}$$

où $n_{\mathfrak{P}} \in \mathbb{Z}$ et $n_{\mathfrak{P}} = 0$ sauf pour au plus un nombre fini de places. On note $\nu_{\mathfrak{P}}(D) := n_{\mathfrak{P}}$ le coefficient de la place $\mathfrak{P}$ dans le diviseur D. L'ensemble $\mathrm{supp} D := \{\, \mathfrak{P} \in \mathbb{P}_F \mid \nu_{\mathfrak{P}}(D) \neq 0 \,\}$ est le support de D. L'élément neutre du groupe $\mathcal{D}_F$ est noté 0. Si

$$D := \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \mathfrak{P} \quad \text{et} \quad D' := \sum_{\mathfrak{P} \in \mathbb{P}_F} n'_{\mathfrak{P}} \mathfrak{P}$$

alors

$$D + D' := \sum_{\mathfrak{P} \in \mathbb{P}_F} (n_{\mathfrak{P}} + n'_{\mathfrak{P}}) \mathfrak{P}.$$

Le groupe $\mathcal{D}_F$ est muni d'une relation d'ordre partiel définie par :

$$(D, D' \in \mathcal{D}_F) \quad D \geq D' \iff \nu_{\mathfrak{P}}(D) \geq \nu_{\mathfrak{P}}(D') \text{ pour tout } \mathfrak{P} \in \mathbb{P}_F.$$

On dit d'un diviseur D qu'il est effectif si $\nu_{\mathfrak{P}}(D) \geq 0$ pour tout $\mathfrak{P} \in \mathrm{supp} D$ (on écrit alors $D \geq 0$). On remarquera que tout diviseur D peut s'écrire de façon unique comme différence de deux diviseurs effectifs ayant des supports disjoints :

$$D = D_+ - D_-,$$

où $D_+ \geq 0$ et $D_- \geq 0$. Les diviseurs D_+ et D_- sont respectivement appelés partie positive et négative de D. Le degré d'un diviseur D est défini par

$$\deg D := \sum_{\mathfrak{P} \in \mathbb{P}_F} \nu_{\mathfrak{P}}(D) \deg \mathfrak{P}.$$

Puisque tout élément $x \in F \setminus \{0\}$ possède au plus un nombre fini de zéros et de pôles (voir Proposition 1.2.19), on peut associer un diviseur à tout élément x non nul de F :

DÉFINITION 1.3.1 *Soient $x \in F \setminus \{0\}$ et $\mathcal{Z}_x$ (respectivement $\mathcal{N}_x$) l'ensemble de ses zéros (respectivement pôles). On définit*

1. *le* diviseur des zéros *de x par*

$$(x)_0 := \sum_{\mathfrak{P} \in \mathcal{Z}_x} \nu_{\mathfrak{P}}(x)\mathfrak{P},$$

2. *le* diviseur des pôles *de x par*

$$(x)_\infty := -\sum_{\mathfrak{P} \in \mathcal{N}_x} \nu_{\mathfrak{P}}(x)\mathfrak{P},$$

3. *et le* diviseur principal *de x par*

$$(x) := (x)_0 - (x)_\infty.$$

Soit $x \in F \setminus \{0\}$. D'après la Remarque 1.2.18, on a

$$x \in K \setminus \{0\} \iff (x) = 0.$$

Soient $x, y \in F \setminus \{0\}$. Puisque $\nu_{\mathfrak{P}}(xy) = \nu_{\mathfrak{P}}(x) + \nu_{\mathfrak{P}}(y)$ pour tout $\mathfrak{P} \in \mathbb{P}_F$, il est clair que l'ensemble $\mathrm{Pr}_F := \{(x) \mid x \in F \setminus \{0\}\} \subset \mathcal{D}_F$ est un sous-groupe du groupe $\mathcal{D}_F$. On a donc la relation d'équivalence suivante:

$$(D, D' \in \mathcal{D}_F) \quad D \equiv D' \iff D - D' \in \mathrm{Pr}_F.$$

PROPOSITION 1.3.2 *Soit $x \in F \setminus \{K\}$. Alors*

$$\deg(x)_0 = \deg(x)_\infty := [F : K(x)].$$

En particulier, $\deg(x) = 0$.

Démonstration : Stichtenoth [43, Th. I.4.11].

1.4 L'espace vectoriel $\mathcal{L}(D)$

La définition qui suit joue un rôle fondamental pour la théorie des corps de fonctions et est essentielle à celle des codes géométriques (cf. Section 1.6).

DÉFINITION 1.4.1 *Soit F/K un corps de fonctions. À tout diviseur $D \in \mathcal{D}_F$ est associé l'ensemble*

$$\mathcal{L}(D) := \{ x \in F \setminus \{ 0 \} \mid (x) + D \geq 0 \} \cup \{ 0 \} .$$

Les éléments de $\mathcal{L}(D)$ sont des éléments de F/K qui ont des pôles au plus aux places du support de D ; plus précisément, si $x \in \mathcal{L}(D)$ et $\mathfrak{P}$ est un pôle de x, alors $\mathfrak{P} \in \mathrm{supp} D$ et $\nu_{\mathfrak{P}}(x) \geq -\nu_{\mathfrak{P}}(D)$. De plus, on déduit aisément de la Proposition 1.3.2 que x a au plus $\deg D$ zéros à l'extérieure de $\mathrm{supp} D$.

LEMME 1.4.2 *Soit $D \in \mathcal{D}_F$. Alors $\mathcal{L}(D)$ est un espace vectoriel sur K.*

Démonstration : Stichtenoth [43, Lemme I.4.6].

PROPOSITION 1.4.3 *Soit D un diviseur d'un corps de fonctions F/K. Le K-espace vectoriel $\mathcal{L}(D)$ est de dimension finie et on note $\ell(D) := \dim_K \mathcal{L}(D)$.*

Démonstration : Stichtenoth [43, Prop. I.4.9].

PROPOSITION 1.4.4 *Il existe un entier $\gamma \in \mathbb{Z}$ tel que, pour tout diviseur $D \in \mathcal{D}_F$,*

$$\deg D - \ell(D) \leq \gamma.$$

Démonstration : Stichtenoth [43, Proposition I.4.14].

Grâce à la proposition précédente la définition suivante a un sens.

DÉFINITION 1.4.5 *Soit F/K un corps de fonctions. On appelle* genre *de F/K l'entier*

$$g := \max \{ \deg D - \ell(D) + 1 \mid D \in \mathcal{D}_F \} .$$

REMARQUE 1.4.6 Le genre d'un corps de fonctions F/K est un entier non négatif : en effet, on a, en vertu de la Remarque 1.2.18,

$$\mathcal{L}(0) = \{ x \in F \setminus \{ 0 \} \mid (x) \geq 0 \} \cup \{ 0 \} = K,$$

et donc $g \geq \deg 0 - \ell(0) + 1 = 0$.

THÉORÈME 1.4.7 (RIEMANN) *Soit F/K un corps de fonctions de genre g. Alors*

1. *pour tout diviseur $D \in \mathcal{D}_F$,*

$$\ell(D) \geq \deg D - g + 1,$$

2. *il existe un entier c, ne dépendant que de F/K, tel que si* $\deg D \geq c$, *alors*

$$\ell(D) = \deg D - g + 1.$$

Démonstration : Stichtenoth [43, Th. I.4.17]

1.5 Théorème de Riemann-Roch

C'est le Théorème de Riemann-Roch qui permet de calculer la dimension de l'espace vectoriel $\mathcal{L}(D)$ où D est un diviseur de F/K. Ce théorème fait appel à la notion de *diviseurs canoniques* de F/K qui sont les diviseurs associés aux éléments du *module des différentielles de Weil* de F/K. Les diviseurs canoniques ne seront utilisés que pour énoncer le Théorème de Riemann-Roch et afin de ne pas alourdir le texte, ils ne seront pas considérés plus en détail. Le lecteur se reportera à [43] pour plus de précisions.

THÉORÈME 1.5.1 (RIEMANN-ROCH) *Soit W un diviseur canonique d'un corps de fonctions F/K de genre g. Pour tout $D \in \mathcal{D}_F$, on a*

$$\ell(D) = \deg D - g + 1 + \ell(W - D).$$

Démonstration : Stichtenoth [43, I.5.15].

COROLLAIRE 1.5.2 *Quel que soit le diviseur canonique W, on a*

$$\deg W = 2g - 2 \text{ et } \ell(W) = g.$$

Démonstration : Stichtenoth [43, Corollaire 1.5.16].

COROLLAIRE 1.5.3 *Soient W et W' deux diviseurs canoniques de F/K. Alors $W \equiv W'$.*

Démonstration : En appliquant le Théorème de Riemann-Roch au diviseur W', on a

$$g = \ell(W') = \deg W' - g + 1 + \ell(W - W') = g - 1 + \ell(W - W')$$

et donc $\ell(W-W')=1$. Il existe donc $x\neq 0$ tel que $(x)+(W-W')\geq 0$. En fait, $(x)+(W-W')=0$ car $\deg((x)+(W-W'))=0$. Par conséquent, $W'-W=(x)\in \mathrm{Pr}_F$ d'où $W\equiv W'$. □

Si A est un diviseur de degré $\deg A<0$, on déduit aisément de la Proposition 1.3.2 que $\ell(A)=0$. Le théorème qui suit est donc une conséquence du Théorème de Riemann-Roch et du Corollaire 1.5.2.

Théorème 1.5.4 *Si D est un diviseur de degré $\deg D\geq 2g-1$, alors*

$$\ell(D)=\deg D-g+1.$$

Corollaire 1.5.5 *Soit $\mathfrak{P}\in\mathbb{P}_F$. Il existe $u\in F$ tel que $\mathfrak{P}$ est l'unique zéro (resp. pôle) de u.*

Démonstration : D'après le théorème précédent, il existe un entier $n\in\mathbb{N}$ assez grand tel que $\ell(n\mathfrak{P})\geq 2$ et par conséquent, il existe $v\in\mathcal{L}(n\mathfrak{P})$ tel que $v\notin K$. Mais dans ce cas $\mathfrak{P}$ est l'unique pôle de v par définition de $\mathcal{L}(n\mathfrak{P})$. Il est clair alors que $\mathfrak{P}$ est l'unique zéro de v^{-1}. □

1.6 Codes géométriques

Dans toute cette section $K=\mathbb{F}_q$.

Les codes géométriques ont été inventés par Goppa en 1981 dans son article "Codes on algebraic curves" ([13]). En voici une définition (on trouvera à l'Annexe A un court rappel sur les codes correcteurs).

Définition 1.6.1 *Soit F/K un corps de fonction où $K=\mathbb{F}_q$. Supposons que $\mathbb{P}_F$ contient n places $\mathfrak{P}_1,\dots,\mathfrak{P}_n$ de degré 1 deux à deux distinctes et posons*

$$\mathcal{P}:=\mathfrak{P}_1+\cdots+\mathfrak{P}_n.$$

Soit D un diviseur de F/K ayant un support disjoint de celui de $\mathcal{P}$. Le code géométrique *$C_{\mathcal{L}}(F,\mathcal{P},D)$ est l'image de l'application K-linéaire*

$$\begin{array}{rccc} ev_{\mathcal{P}}: & \mathcal{L}(D) & \longrightarrow & K^n \\ & u & \mapsto & (u(\mathfrak{P}_1),\dots,u(\mathfrak{P}_n)). \end{array}$$

Proposition 1.6.2 *Soient F/K, $\mathcal{P}$ et D comme dans la définition précédente. Alors le code $C_{\mathcal{L}}(F,\mathcal{P},D)$ est un $[n,k,d]_q$-code où*

$$k=\ell(D)-\ell(D-\mathcal{P})$$

et

$$d := d(C_{\mathcal{L}}(F, \mathcal{P}, D)) \geq n - \deg D.$$

En particulier, si $2g - 1 \leq \deg D < n$, *alors*

$$k = \deg D - g + 1.$$

Démonstration : L'application $ev_{\mathcal{P}}$ étant une application K-linéaire, on a

$$k := \dim_K ev_{\mathcal{P}}(\mathcal{L}(D)) = \ell(D) - \dim_K \ker ev_{\mathcal{P}}.$$

D'autre part, il est aisé de vérifier que $ev_{\mathcal{P}}(z) = 0$ si et seulement si $z \in \mathcal{L}(D - \mathcal{P})$. On a donc $k = \dim_K ev_{\mathcal{P}}(\mathcal{L}(D)) = \ell(D) - \ell(D - \mathcal{P})$. Soit maintenant $u \in \mathcal{L}(D)$. Par définition de $\mathcal{L}(D)$, la fonction u a au plus $\deg D$ zéros à l'extérieur du support de D. Il est clair alors qu'il existe au moins $n - \deg D$ places du support de D qui ne sont pas des zéros de u, d'où le poids $w := w(ev_{\mathcal{P}}(u))$ du mot $ev_{\mathcal{P}}(u)$ est tel que $w \geq n - \deg D$, montrant ainsi que $d \geq n - \deg D$. Pour finir, puisque $\deg D < n = \deg \mathcal{P}$, on doit avoir $\mathcal{L}(D - \mathcal{P}) = \{ 0 \}$ et donc $k = \ell(D) = \deg D - g + 1$ d'après le Théorème 1.5.4 car $\deg D \geq 2g - 1$. □

La proposition suivante montre que le dual d'un code géométrique est un code géométrique.

Proposition 1.6.3 *Soient* F/K, D *et* $\mathcal{P}$ *comme dans la Définition 1.6.1. Il existe un diviseur canonique* W *de* F *tel que*

$$C_{\mathcal{L}}(F, \mathcal{P}, D)^{\perp} = C_{\mathcal{L}}(F, \mathcal{P}, \mathcal{P} - D + W))$$

Démonstration : Stichtenoth Prop. II.2.10 [43]. □

Remarque 1.6.4 Soient F/K, D et $\mathcal{P}$ comme dans la Définition 1.6.1. Dans [13], Goppa a introduit un code défini en fonction de D et $\mathcal{P}$ en utilisant l'espace vectoriel des différentielles de Weil du corps de fonctions F/K. Sans le définir, notons ce code $C_{\Omega}(F, \mathcal{P}, D)$ et soulignons seulement que $C_{\Omega}(F, \mathcal{P}, D)$ est le dual de $C_{\mathcal{L}}(F, \mathcal{P}, D)$. D'après la proposition précédente, le code $C_{\Omega}(F, \mathcal{P}, D)$ est donc un code géométrique au sens de la Définition 1.6.1.

1.6.1 Remarques sur la construction effective des codes géométriques

Soient F/K, D et $\mathcal{P}$ comme à la Définition 1.6.1. Soit $B := \{ f_1, f_2, \ldots, f_k \}$ une base de l'espace vectoriel $\mathcal{L}(D)$. Alors le code $C_{\mathcal{L}}(F, \mathcal{P}, D)$ admet pour matrice génératrice la matrice

$$G := \begin{bmatrix} f_1(\mathfrak{P}_1) & f_1(\mathfrak{P}_2) & \cdots & f_1(\mathfrak{P}_n) \\ f_2(\mathfrak{P}_1) & f_2(\mathfrak{P}_2) & \cdots & f_2(\mathfrak{P}_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(\mathfrak{P}_1) & f_k(\mathfrak{P}_2) & \cdots & f_k(\mathfrak{P}_n) \end{bmatrix}.$$

Par conséquent, pour construire le code $C_{\mathcal{L}}(F, \mathcal{P}, D)$, il faut essentiellement savoir

1. identifier les places de degré 1 de F pour construire le diviseur $\mathcal{P}$,
2. construire un diviseur D dont le support est disjoint de celui de $\mathcal{P}$ (le support de D peut contenir des places de degré supérieur à 1)
3. calculer une base $B = \{ f_1, f_2, \ldots, f_k \}$ de $\mathcal{L}(D)$,
4. évaluer les fonctions $f \in B$ en chacune des places du support de $\mathcal{P}$.

Chapitre 2

Algorithme de Brill-Noether

Pour ce chapitre on suppose connues les notions élémentaires de la théorie des courbes algébriques. Le lecteur se reportera à l'Annexe B pour plus de détails.

Ce chapitre a pour but de présenter l'algorithme de Brill-Noether qui calcule une base de $\mathcal{L}(D)$ où D est un diviseur du corps des fonctions d'une courbe plane. En théorie cet algorithme n'est défini que lorsque le corps de base est algébriquement clos. Il peut sembler alors que cet algorithme ne résout pas le problème posé à la Section 1.6.1 qui est de calculer une base de l'espace vectoriel associé à un diviseur d'un corps de fonctions F/K où $K = \mathbb{F}_q$. Or on sait, d'après les Propositions 1.1.5 et 1.1.6, qu'il existe $x, y \in F$ tels que $F = K(x, y)$ et que le polynôme irréductible $C \in K[X, Y]$ tel que $C(x, y) = 0$ est absolument irréductible. Ainsi, en considérant la courbe affine plane $\mathcal{C} := \{ C = 0 \}$ définie sur K, le corps F s'identifie au corps $K(\mathcal{C})$ qui est un sous-corps de $\overline{K}(\mathcal{C})$. On verra à la Section 2.8 qu'on peut associer à tout diviseur D du corps de fonctions $K(\mathcal{C})$ un diviseur D' du corps de fonctions $\overline{K}(\mathcal{C})$ qui est tel que

1. $\dim_K \mathcal{L}(D) = \dim_{\overline{K}} \mathcal{L}(D')$,

2. il existe une base de $\mathcal{L}(D')$ formée d'éléments de $K(\mathcal{C})$,

3. toute base de $\mathcal{L}(D')$ formée d'éléments de $K(\mathcal{C})$ est une base de $\mathcal{L}(D)$.

Ainsi, pour calculer une base de $\mathcal{L}(D)$, il suffira d'appliquer l'algorithme de Brill-Noether au diviseur D' et de faire en sorte que la base obtenue soit formée d'éléments de $K(\mathcal{C})$.

2.1 Points versus places

Dans cette section je m'intéresse au lien qui existe entre les points d'une courbe affine plane et les places du corps de fonctions de la courbe. On établit ce lien en étudiant les anneaux locaux des points. Parmi les propriétés locales d'un point $P \in \mathcal{C} := \{\, C = 0 \,\} \subset \mathbb{A}^2$, l'une des plus élémentaires est la *multiplicité* du point P : soient $P := (0,0) \in \mathbb{A}^2$ et un polynôme $G \in \overline{K}[X,Y]$. On peut écrire

$$G = G_{m_1} + G_{m_2} + \cdots + G_{m_d}, \quad m_1 < m_2 < \cdots < m_d,$$

où G_{m_i} est un polynôme homogène de degré m_i pour $i = 1, 2, \ldots, d$. On appelle G_{m_1} la **forme initiale** de G et on la note $\mathrm{Init}(G)$. La **multiplicité** du point $P = (0,0)$ sur G, notée $\mathrm{m}_P(G)$, est le degré de la forme initiale de G, c'est-à-dire $\mathrm{m}_{(0,0)}(G) := \deg \mathrm{Init}(G)$. Si $P = (a,b)$, alors la **multiplicité** du point P sur G est définie par $\mathrm{m}_P(G) := \mathrm{m}_{(0,0)}(G(X+a, Y+b))$. Clairement $G(P) = 0$ si et seulement si $\mathrm{m}_P(G) > 0$.

Remarque 2.1.1 Rappelons que tout polynôme homogène de $\overline{K}[X,Y]$ se factorise en un produit de formes linéaires. Si $P = (0,0)$ et $\mathrm{m}_P(G) > 0$, on peut donc écrire

$$\mathrm{Init}(G) = \prod_{i=1}^{l} (\alpha_i X + \beta_i Y)^{e_i}$$

où $\sum_{i=1}^{l} e_i = \mathrm{m}_P(G)$. Géométriquement, les facteurs distincts $L_i := \alpha_i X + \beta_i Y$ de $\mathrm{Init}(G)$ définissent les tangentes distinctes en P à la courbe affine plane $\mathcal{G} = \{\, G = 0 \,\}$.

Définition 2.1.2 *Soient* $\mathcal{C} := \{\, C = 0 \,\}$ *une courbe affine plane et* $P \in \mathcal{C}$. *On appelle* $\mathrm{m}_P(\mathcal{C}) := \mathrm{m}_P(C)$ *la* **multiplicité** *du point* P.

Soient $\mathcal{C} := \{\, C = 0 \,\}$ une courbe affine plane et $P := (a,b) \in \mathcal{C}$. Soient C_X et C_Y les dérivés usuelles de C par rapport à X et Y respectivement. On vérifie que

$$\mathrm{m}_P(\mathcal{C}) = 1 \iff C_X(a,b) \neq 0 \text{ ou } C_Y(a,b) \neq 0.$$

Le membre de droite de cette équivalence correspond exactement à la définition d'un point simple d'une courbe affine plane (cf. Annexe B.4.2). D'autre part, on sait qu'un point P est simple si et seulement si $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète (cf. Annexe B.4.5). En résumé, on a la proposition suivante :

Proposition 2.1.3 *Soient* $\mathcal{C} := \{\, C = 0 \,\}$ *une courbe affine plane et* $P := (a,b) \in \mathcal{C}$. *Les énoncés suivants sont équivalents :*

1. *P est simple.*

2. $C_X(a,b) \neq 0$ *ou* $C_Y(a,b) \neq 0$.

3. $\mathrm{m}_P(\mathcal{C}) = 1$.

4. $\mathcal{O}_P(\mathcal{C})$ *est un anneau de valuation discrète.*

Remarque 2.1.4 La multiplicité d'un point $P \in \mathcal{C}$ dépend uniquement de l'anneau local $\mathcal{O}_P(\mathcal{C})$. En effet, on peut montrer qu'il existe un entier N assez grand tel que pour tout $n \geq N$,

$$\mathrm{m}_P(\mathcal{C}) = \dim_{\overline{K}} \mathcal{M}_P(\mathcal{C})^n / \mathcal{M}_P(\mathcal{C})^{n+1}$$

où $\mathcal{M}_P(\mathcal{C})$ est l'unique idéal maximal de $\mathcal{O}_P(\mathcal{C})$ (voir par exemple Fulton [10, Théorème 2, page 71]).

> Pour tout le reste de ce chapitre, on fixe F/K un corps de fonctions, Φ une clôture algébrique du corps F et $\overline{K} \subset \Phi$ la clôture algébrique de K. On fixe aussi le compositum[1] $\overline{F} := \overline{K}F$.

Il est clair que $\overline{F}/\overline{K}$ est un corps de fonctions ayant $\overline{K}$ pour corps des constantes. D'un point vue algébrique et algorithmique, il sera utile de fixer le corps $\overline{F}$ et d'identifier à $\overline{F}$ tous les corps de fonctions de courbes affines planes $\overline{K}$-isomorphes à $\overline{F}$. Pour ce faire, j'utiliserai la définition suivante qui est apparentée à celle d'un point générique d'une courbe (cf. [9, Ch. 4, §1]).

Définition 2.1.5 *Un* ensemble de coordonnées *de* $\overline{F}/\overline{K}$ *est un ensemble* $\Gamma := \{x, y\} \subset \overline{F}$ *tel que* $\overline{F} = \overline{K}(x,y)$. *Le polynôme*[2] *irréductible* $C \in \overline{K}[X,Y]$ *tel que* $C(x,y) = 0$ *est appelé* polynôme de définition *de* Γ. *À l'ensemble de coordonnées* Γ *est associé la courbe affine plane*

$$\mathcal{C}_\Gamma := \{ (a,b) \in \mathbb{A}^2 \mid C(a,b) = 0 \}.$$

On dit que Γ *est* défini *sur* K *si* $C \in K[X,Y]$ *et* $F = K(x,y)$, *et on note alors* Γ/K.

Soit $\mathcal{C} := \{ C = 0 \}$ une courbe affine plane telle que $\overline{K}(\mathcal{C}) \cong \overline{F}$. Il existe une infinité d'isomorphismes de $\overline{K}(\mathcal{C})$ vers $\overline{F}$. Par contre, en choisissant un ensemble de coordonnées $\Gamma := \{x, y\}$ de $\overline{F}/\overline{K}$ tel que $\mathcal{C} = \mathcal{C}_\Gamma$, on peut fixer l'isomorphisme

$$\begin{array}{cccc} \varphi_\Gamma : & \overline{K}(\mathcal{C}) & \longrightarrow & \overline{F} \\ & \frac{G(x_1,y_1)}{H(x_1,y_1)} & \mapsto & \frac{G(x,y)}{H(x,y)} \end{array} \tag{2.1}$$

1. Le compositum de $\overline{K}$ et F est le plus petit sous-corps de Φ contenant à la fois les corps $\overline{K}$ et F.

2. Ce polynôme est unique à multiplication près par un élément de $\overline{K}$.

où x_1 et y_1 sont respectivement les images résiduelles de X et Y dans $\overline{K}[\mathcal{C}]$. Si Γ est défini sur K, on peut alors restreindre φ_Γ au corps $K(\mathcal{C})$ comme suit:

$$\begin{array}{cccc} \varphi_{\Gamma/K}: & K(\mathcal{C}) & \longrightarrow & F \\ & \frac{G(x_1,y_1)}{H(x_1,y_1)} & \longmapsto & \frac{G(x,y)}{H(x,y)}. \end{array}$$

Remarque 2.1.6 Il est clair que si Γ est un ensemble de coordonnées défini sur K, alors la courbe $\mathcal{C}_\Gamma$ est définie sur K. En revanche, la réciproque n'est pas vraie en général comme le montre l'exemple suivant: soient $K := \mathbb{F}_2$ et $C(X,Y) := Y^4 + Y + X^3 \in \overline{K}[X,Y]$. Le polynôme C est absolument irréductible. Considérons la courbe affine plane $\mathcal{C} := \{ C = 0 \}$. Posons $F := K(\mathcal{C})$, $\overline{F} := \overline{K}F = \overline{K}(\mathcal{C})$ et soient x et y les images résiduelles de X et Y dans $\overline{F}$. Il est clair que $\Gamma := \{ x, y \}$ est un ensemble de coordonnées de $\overline{F}/\overline{K}$ défini sur K. Soit maintenant $\alpha \in \overline{K}$ tel que $\alpha^4 + \alpha = 0$ et posons $\Gamma' := \{ x, y - \alpha \}$. Il est évident que Γ' est un ensemble de coordonnées de $\overline{F}/\overline{K}$, mais il n'est pas défini sur K car $\alpha \notin K$. Par contre, on a

$$C(X, Y + \alpha) = (Y + \alpha)^4 + (Y + \alpha) + X^3 = Y^4 + Y + X^3 \in K[X,Y]$$

et par conséquent $\mathcal{C}_{\Gamma'} = \mathcal{C}_\Gamma$.

Remarque 2.1.7 Soient $\Gamma := \{ x, y \}$ un ensemble de coordonnées de $\overline{F}/\overline{K}$ et $\mathcal{C} := \mathcal{C}_\Gamma$ sa courbe associée. Soient $R := (a,b) \in \mathcal{C}$ et $\mathcal{O}_R(\mathcal{C}_\Gamma)$ l'anneau local du point R. On vérifie aisément que

$$\langle x - a, y - b \rangle = \overline{K}[x,y] \cap \varphi_\Gamma(\mathcal{M}_R(\mathcal{C}))$$

où φ_Γ est le $\overline{K}$-isomorphisme défini en (2.1). Par conséquent, $\langle x - a, y - b \rangle$ est un idéal maximal de $\overline{K}[x,y]$ et

$$\varphi_\Gamma(\mathcal{O}_R(\mathcal{C})) = \overline{K}[x,y]_{\langle x-a, y-b \rangle}.$$

J'introduis ici la notion de point d'un corps de fonctions, en espérant que le lecteur me pardonnera cet abus de langage.

Définition 2.1.8 *Soit le corps de fonctions $\overline{F}/\overline{K}$. Un* point *de $\overline{F}/\overline{K}$ est le couple $P := (\, a, b \,;\, x, y \,)$ où $\Gamma := \{ x, y \}$ est un ensemble de coordonnées de $\overline{F}/\overline{K}$ et $(a,b) \in \mathcal{C}_\Gamma$. Le localisé de $\overline{K}[x,y]$ en l'idéal maximal $\langle x - a, y - b \rangle$,*

$$\mathcal{O}_P := \overline{K}[x,y]_{\langle x-a, y-b \rangle},$$

est appelé l'anneau local *du point P et on note $\mathcal{M}_P$ son unique idéal maximal. On appelle l'ensemble*

$$\mathcal{Z}(\Gamma) := \{ (\, a, b \,;\, x, y \,) \mid (a,b) \in \mathcal{C}_\Gamma \}$$

l'ensemble des points de $\overline{F}/\overline{K}$ définis en fonction *de Γ.*

Soient $\Gamma := \{\, x, y \,\}$ un ensemble de coordonnées de $\overline{F}/\overline{K}$ et $P = (\ a, b\ ;\ x, y\ ) \in \mathcal{Z}(\Gamma)$. Le point P hérite de toutes définitions et propriétés locales du point $(a, b) \in \mathcal{C}_\Gamma$. Par exemple, le point P est **simple** si $(a, b) \in \mathcal{C}_\Gamma$ est simple et la **multiplicité** du point P, noté m_P, est celle du point $(a, b) \in \mathcal{C}_\Gamma$. De plus, si $u \in \mathcal{O}_P$, alors il existe $G, H \in \overline{K}[X, Y]$ tels que $u = G(x, y)/H(x, y)$ et $H(a, b) \neq 0$. On pose alors $u(P) := G(a, b)/H(a, b)$ qu'on appelle **l'évaluation** de u au point P ; il est clair que $u(P)$ ne dépend pas du choix des polynômes G et H.

DÉFINITION 2.1.9 *Soient P et Q deux points de $\overline{F}/\overline{K}$. On dit que P est équivalent à Q, et on note $P \equiv Q$, si $\mathcal{O}_P = \mathcal{O}_Q$.*

Il est clair que $P \equiv Q$ est une relation d'équivalence. L'exemple le plus simple de points équivalents est le suivant : soit $\Gamma := \{\, x, y \,\}$ un ensemble de coordonnés de $\overline{F}/\overline{K}$. Quels que soient $a, b \in \overline{K}$, l'ensemble $\Gamma' := \{\, x - a, y - b \,\}$ est aussi un ensemble de coordonnées de $\overline{F}/\overline{K}$. Si $C \in \overline{K}[X, Y]$ est le polynôme de définition de Γ, alors Γ' admet $C'(X, Y) := C(X + a, Y + b)$ comme polynôme de définition. Par conséquent, si $P := (\ a, b\ ;\ x, y\ ) \in \mathcal{Z}(\Gamma)$, alors $P' := (\ 0, 0\ ;\ x - a, y - b\ ) \in \mathcal{Z}(\Gamma')$ et P est équivalent au point P'. Le passage du point P au point P' s'appelle **translation à l'origine** du point P.

Rappelons qu'un anneau local B d'idéal maximal M_B **domine** un anneau local A d'idéal maximal M_A si $B \supseteq A$ et $M_B \supseteq M_A$.

DÉFINITION 2.1.10 *Soient P et Q deux points du corps de fonctions $\overline{F}/\overline{K}$. On dit que Q* **domine** *le point P si $\mathcal{O}_Q$ domine $\mathcal{O}_P$ et on note $Q|P$. De même, si $\mathfrak{P}$ est une place de $\overline{F}/\overline{K}$, on dira que $\mathfrak{P}$* **domine** *le point P si $\mathcal{O}_\mathfrak{P}$ domine $\mathcal{O}_P$ et on note $\mathfrak{P}|P$. On dira que P est un* **représentant** *de la place $\mathfrak{P}$ si P est un point simple et $\mathcal{O}_P = \mathcal{O}_\mathfrak{P}$, et on note $P \equiv \mathfrak{P}$.*

REMARQUE 2.1.11 La relation "Q domine P" est une relation d'ordre partiel sur l'ensemble des points de $\overline{F}/\overline{K}$. En vertu du Théorème 1.2.9.(3), les points simples de $\overline{F}/\overline{K}$ sont des éléments maximaux pour cet ordre. Si P est un point de $\overline{F}/\overline{K}$ et $\mathfrak{P}$ une place dominant P, on verra à la Section 2.2 comment calculer une suite de points $P = Q_0, Q_1, Q_2, \ldots, Q_n$ tels que $Q_{i+1}|Q_i$ pour $i = 0, 1, \ldots, n-1$ et $Q_n \equiv \mathfrak{P}$.

LEMME 2.1.12 *Soient $P := (\ a, b\ ;\ x, y\ )$ un point de $\overline{F}/\overline{K}$ et $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ une place telle que $\mathfrak{P}|P$. Supposons que $\nu_\mathfrak{P}(x - a) \leq \nu_\mathfrak{P}(y - b)$. Alors*

$$\nu_\mathfrak{P}(x - a) = \min \{\, \nu_\mathfrak{P}(z) \ \mid\ z \in \mathcal{M}_P \,\}.$$

Démonstration : Soit $z \in \mathcal{M}_P$. Puisque $\langle x-a, y-b\rangle = \mathcal{M}_P$, il existe $g, h \in \overline{K}[x,y]$ tels que $z = (x-a)g + (y-b)h$. Or $g, h \in \mathcal{O}_{\mathfrak{P}}$ et puisque $\nu_{\mathfrak{P}}(x-a) \leq \nu_{\mathfrak{P}}(y-b)$, on a $z/(x-a) = g + h(y-b)/(x-a) \in \mathcal{O}_{\mathfrak{P}}$ d'où $\nu_{\mathfrak{P}}(x-a) \leq \nu_{\mathfrak{P}}(z)$ pour tout $z \in \mathcal{M}_P$. □

PROPOSITION 2.1.13 *Soit $P = (\, a, b \,;\, x, y \,)$ un point simple. Alors $x-a$ ou $y-b$ est un paramètre local de la place $\mathfrak{P} \equiv P$.*

Démonstration : C'est une conséquence du lemme précédent et du Théorème 1.2.9. □

PROPOSITION 2.1.14 *Soit $P := (\, a, b \,;\, x, y \,)$ un point du corps de fonctions $\overline{F}/\overline{K}$. Soit Q (resp. $\mathfrak{Q}$) un point (resp. une place) de $\overline{F}/\overline{K}$. Les propositions suivantes sont équivalentes :*

1. *$Q|P$ (resp. $\mathfrak{Q}|P$).*
2. *$\mathcal{O}_P \subseteq \mathcal{O}_Q$ (resp. $\mathcal{O}_P \subseteq \mathcal{O}_{\mathfrak{Q}}$).*
3. *$\mathcal{M}_P \subseteq \mathcal{M}_Q$ (resp. $\mathcal{M}_P \subseteq \mathfrak{P}$).*
4. *$x-a \in \mathcal{M}_Q$ et $y-b \in \mathcal{M}_Q$ (resp. $x-a \in \mathfrak{Q}$ et $y-b \in \mathfrak{Q}$).*

Démonstration : Montrons la proposition pour un point Q de $\overline{F}/\overline{K}$ (la proposition est similaire pour une place). Par définition on a (1) $\Leftrightarrow$ ((2) et (3)). Montrons donc (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (2).

((2) $\Rightarrow$ (3)). Supposons que $\mathcal{O}_P \subseteq \mathcal{O}_Q$ et considérons l'injection suivie de la surjection canonique

$$\varphi : \mathcal{O}_P \hookrightarrow \mathcal{O}_Q \to \mathcal{O}_Q/\mathcal{M}_Q \cong \overline{K}.$$

Le noyau $\ker\varphi$ est un idéal premier et il est clair que $\ker\varphi \neq \mathcal{O}_P$. De plus, $\ker\varphi \neq \{\,0\,\}$ car sinon l'application φ est injective et alors $\mathcal{O}_P$ s'identifie à un anneau contenu dans $\overline{K}$. Mais cela est impossible car le corps des fractions de $\mathcal{O}_P$ est égal à $\overline{F}$. D'autre part, $\{\,0\,\}$ et $\mathcal{M}_P$ sont les seuls idéaux premiers propres de $\mathcal{O}_P$ (cf. Annexe B.3.6). On a donc $\ker\varphi = \mathcal{M}_P$ d'où $\mathcal{M}_P \subseteq \mathcal{M}_Q$.

((3) $\Rightarrow$ (4)). C'est trivial car $\mathcal{M}_P = \langle x-a, y-b\rangle\mathcal{O}_P$.

((4) $\Rightarrow$ (2)). Soit $u \in \mathcal{O}_P$. L'anneau $\mathcal{O}_P$ est le localisé de $\overline{K}[x,y]$ en l'idéal maximal $M_P = \langle x-a, y-b\rangle$. Il existe donc $g, h \in \overline{K}[x,y]$ tels que $u = g/h$ et $h \notin M_P$. Par hypothèse $x-a, y-b \in \mathcal{M}_Q$. On a donc $\overline{K}[x,y] \subset \mathcal{O}_Q$ et $M_P = \overline{K}[x,y] \cap \mathcal{M}_Q$. En particulier, $g, h \in \mathcal{O}_Q$ et $h \notin \mathcal{M}_Q$ d'où $h^{-1} \in \mathcal{O}_Q$ et donc $u = gh^{-1} \in \mathcal{O}_Q$. □

COROLLAIRE 2.1.15 *Soit P un point du corps de fonctions $\overline{F}/\overline{K}$. Alors P est dominé par au moins une et au plus un nombre fini de places $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$.*

Démonstration : Qu'il existe au moins une place $\mathfrak{P}$ dominant le point P est une conséquence de la Proposition 1.2.16. Qu'il n'y en ait qu'un nombre fini est une conséquence immédiate du fait que, d'après la proposition précédente, toute place dominant un point $P = (\ a, b\ ;\ x, y\ )$ est un zéro de $x - a$ et $y - b$. Or $x - a$ et $y - b$ admettant chacun au plus un nombre fini de zéros, ils ont au plus un nombre fini de zéros en commun. $\square$

COROLLAIRE 2.1.16 *Soit* $\Gamma := \{\, x, y\,\}$ *un ensemble de coordonnées de* $\overline{F}/\overline{K}$. *Alors*

$$\mathcal{Z}(\Gamma) = \left\{\ (\ x(\mathfrak{P}), y(\mathfrak{P})\ ;\ x, y\ ) \in \mathbb{A}^2 \ \mid\ \mathfrak{P} \in \mathbb{P}_{\overline{F}} \text{ avec } x \in \mathcal{O}_{\mathfrak{P}} \text{ et } y \in \mathcal{O}_{\mathfrak{P}} \right\}.$$

Démonstration : Soient $P = (\ a, b\ ;\ x, y\ ) \in \mathcal{Z}(\Gamma)$, $\mathcal{O}_P$ son anneau local et $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ tel que $\mathfrak{P}|P$. Puisque $\mathcal{M}_P \subseteq \mathfrak{P}$, on a $x - a \in \mathfrak{P}$ et $y - b \in \mathfrak{P}$, d'où $(a, b) = (x(\mathfrak{P}), y(\mathfrak{P}))$. Réciproquement, soient C le polynôme de définition de Γ et $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ tel que $x, y \in \mathcal{O}_{\mathfrak{P}}$. On a

$$C(x(\mathfrak{P}), y(\mathfrak{P})) = C(x, y)(\mathfrak{P}) = 0(\mathfrak{P}) = 0$$

d'où $(\ x(\mathfrak{P}), y(\mathfrak{P})\ ;\ x, y\ ) \in \mathcal{Z}(\Gamma)$. $\square$

REMARQUE 2.1.17 Pour un ensemble de coordonnées fixé $\Gamma = \{\, x, y\,\}$ de $\overline{F}/\overline{K}$, il existe au moins une et au plus un nombre fini de places de $\overline{F}/\overline{K}$ qui ne dominent aucun point de $\mathcal{Z}(\Gamma)$. Ce sont toutes les places qui sont un pôle de x ou de y.

2.2 Éclatement de points

Soient P un point du corps de fonctions $\overline{F}/\overline{K}$ et $\mathfrak{P}$ une place dominant le point P. On a vu à la section précédente que si P est singulier, alors $\mathcal{O}_P \subsetneq \mathcal{O}_{\mathfrak{P}}$. Dans ce cas on peut alors se poser la question suivante : existe-t-il un point Q de $\overline{F}/\overline{K}$ tel que $Q \equiv \mathfrak{P}$? Si oui, comment peut-on le déterminer ? Ces deux questions sont liées au problème de *désingularisation des courbes* qui, étant donnée une courbe singulière $\mathcal{C}$, consiste à déterminer une courbe lisse birationnelle à $\mathcal{C}$. Pour résoudre ce problème, la méthode la plus classique, voire la plus simple, fait appel à la notion *d'éclatements de points* et cette section y est consacrée. On se contentera d'aborder cette notion d'un point de vue strictement algébrique en s'inspirant du point de vue de Hironaka [22]. Pour une approche géométrique, on se reportera par exemple à [20, 38, 40].

Soit $\{\, x, y\,\}$ un ensemble de coordonnées du corps de fonctions $\overline{F}/\overline{K}$ et posons $y_1 := y/x$. Puisque $y \in \overline{K}(x, y_1)$, l'ensemble $\{\, x, y_1\,\}$ est aussi un ensemble de coordonnées de $\overline{F}/\overline{K}$. L'ensemble de coordonnées $\{\, x, y_1\,\}$ est appelé transformé monoïdale de $\{\, x, y\,\}$ de coordonnée exceptionnelle x. De la même façon, on définit le transformé monoïdale de $\{ x, y \}$ de coordonnée exceptionnelle y comme étant l'ensemble de coordonnées $\{ x_1, y \}$ où $x_1 := x/y$. Soient maintenant $G \in \overline{K}[X, Y]$ et $m := \deg \mathrm{Init}(G)$. Il est aisé de montrer que m est le plus grand entier tel que X^m divise $G(X, XY) \in \overline{K}[X, Y]$. De même, m est le plus grand entier tel que Y^m divise $G(XY, Y) \in \overline{K}[X, Y]$. On pose

$$G^{(x)} := G(X, XY)/X^m \in \overline{K}[X, Y]$$

que l'on appelle transformé stricte de G de coordonnée exceptionnelle x. De la même façon, on pose

$$G^{(y)} := G(XY, Y)/Y^m \in \overline{K}[X, Y]$$

que l'on appelle transformé stricte de G de coordonnée exceptionnelle y. Le lemme qui suit est facile à montrer.

LEMME 2.2.1 *Soient $\{ x, y \}$ un ensemble de coordonnées de $\overline{F}/\overline{K}$ et $C(X, Y) \in \overline{K}[X, Y]$ le polynôme de définition de $\{ x, y \}$. Alors $C^{(x)}$ (resp. $C^{(y)}$) est le un polynôme de définition du transformé monoïdale de $\{ x, y \}$ de coordonnée exceptionnelle x (resp. y).*

Supposons que $P_0 = (\ 0, 0\ ;\ x, y\ )$ soit un point du corps de fonctions $\overline{F}/\overline{K}$ et soit $\mathfrak{P}$ une place dominant le point P.

1. Si $y_1 := y/x \in \mathcal{O}_{\mathfrak{P}}$, d'après la Proposition 2.1.14 et le Corollaire 2.1.16,

$$Q = (\ 0, y_1(\mathfrak{P})\ ;\ x, y_1\ )$$

   est un point de $\overline{F}/\overline{K}$ tel que $\mathfrak{P}|Q$ et $Q|P$.

2. De même, si $x_1 := x/y \in \mathcal{O}_{\mathfrak{P}}$, alors

$$Q' = (\ x_1(\mathfrak{P}), 0\ ;\ x_1, y\ )$$

   est un point de $\overline{F}/\overline{K}$ tel que $\mathfrak{P}|Q'$ et $Q'|P$.

On vérifie aisément que si à la fois $x_1 \in \mathcal{O}_{\mathfrak{P}}$ et $y_1 \in \mathcal{O}_{\mathfrak{P}}$, alors Q et Q' se domine mutuellement d'où $Q' \equiv Q$.

DÉFINITION 2.2.2 *Soient $P = (\ a, b\ ;\ x, y\ )$ un point de $\overline{F}/\overline{K}$ et $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ une place dominant le point P. Posons $x_0 := x - a$ et $y_0 := y - b$.*

1. *Si $y_1 := y_0/x_0 \in \mathcal{O}_{\mathfrak{P}}$, on pose*

$$P^{\mathfrak{P}} := (\ 0, \beta\ ;\ x_0, y_1\ )$$

   où $\beta := y_1(\mathfrak{P})$ et on appelle x_0 la coordonnée exceptionnelle *du point $P^{\mathfrak{P}}$.*

2. *Sinon on a $x_1 := x_0/y_0 \in \mathfrak{P}$. Dans ce cas, on pose*

$$P^{\mathfrak{P}} := (\ 0, 0\ ;\ x_1, y_0\ )$$

et on appelle y_0 la coordonnée exceptionnelle *du point $P^{\mathfrak{P}}$.*

On pose $P^{\mathfrak{P}^{(0)}} := P$ et pour $n \geq 1$, $P^{\mathfrak{P}^{(n)}} := \left(P^{\mathfrak{P}^{(n-1)}}\right)^{\mathfrak{P}}$. Le point $P^{\mathfrak{P}^{(n)}}$ est appelé le point infiniment voisin d'ordre *n de P* vers la place *$\mathfrak{P}$. On appelle* éclatement du point *P l'ensemble*

$$\mathcal{E}cl(P) = \left\{\ P^{\mathfrak{P}}\ \mid\ \mathfrak{P} \in \mathbb{P}_{\overline{F}} \text{ tel que } \mathfrak{P}|P\ \right\}.$$

On notera que l'éclatement d'un point est un ensemble fini en vertu du Corollaire 2.1.15.

Remarque 2.2.3 Soient $P := (\ a, b\ ;\ x, y\ )$ un point de $\overline{F}/\overline{K}$ et $\mathfrak{P}$ une place telle que $\mathfrak{P}|P$. Observons que si on applique la définition précédente au point $P_0 := (\ 0, 0\ ;\ x - a, y - b\ ) \equiv P$, on trouve $P_0^{\mathfrak{P}} = P^{\mathfrak{P}}$.

On veut déterminer les coordonnées des points de $\mathcal{E}cl(P)$ en fonction des coordonnées de P. Pour ce faire, supposons que $P = (\ 0, 0\ ;\ x, y\ )$ et soit $C(X, Y) \in \overline{K}[X, Y]$ un polynôme de définition de l'ensemble de coordonnées $\{\ x, y\ \}$. Soit $\operatorname{Init}(C)$ la forme initiale de C qui est de degré $m := m_P > 0$ et considérons sa factorisation (voir Remarque 2.1.1)

$$\operatorname{Init}(C) = \prod_{i=1}^{l} (\alpha_i X + \beta_i Y)^{e_i}$$

où les facteurs $(\alpha_i X + \beta_i Y)$ pour $i = 1, 2, \ldots, l$ sont deux à deux distincts. Soit $\{\ x, y_1\ \}$ (resp. $\{\ x_1, y\ \}$) le transformé monoïdale de $\{\ x, y\ \}$ de coordonnée exceptionnelle x (resp. y) qui admet $C^{(x)}$ (resp. $C^{(y)}$) comme polynôme de définition. Soit $H = C - \operatorname{Init}(C)$. Alors $r := \deg \operatorname{Init}(H) > m$ et on peut écrire

$$C^{(x)} = \prod_{i=1}^{r} (\alpha_i + \beta_i Y)^{e_i} + X^{(r-m)} H^{(x)}$$

de même que

$$C^{(y)} = \prod_{i=1}^{r} (\alpha_i X + \beta_i)^{e_i} + Y^{(r-m)} H^{(y)}.$$

Maintenant, soient $Q \in \mathcal{E}cl(P)$ et $\mathfrak{P}$ la place telle que $Q = P^{\mathfrak{P}}$.

1. Si $y_1 = y/x \in \mathcal{O}_{\mathfrak{P}}$, alors

$$0 = 0(\mathfrak{P}) = C^{(x)}(x, y_1)(\mathfrak{P}) = \prod_{i=1}^{r} (\alpha_i + \beta_i y_1(\mathfrak{P}))^{e_i} = \operatorname{Init}(C)(1, y_1(\mathfrak{P})). \quad (2.2)$$

Il existe donc i tel que $\beta_i \neq 0$ et $y_1(\mathfrak{P}) = -\alpha_i/\beta_i$. Cet entier i est unique et, par définition de Q, on a

$$Q = (\ 0, -\alpha_i/\beta_i\ ;\ x, y_1\ ) .$$

2. Si $y_1 \notin \mathcal{O}_{\mathfrak{P}}$, c'est-à-dire que $x_1 = x/y \in \mathfrak{P}$, alors $x_1(\mathfrak{P}) = 0$. Dans ce cas

$$0 = C^{(y)}(x_1, y)(\mathfrak{P}) = \prod_{i=1}^{r} (\alpha_i x_1(\mathfrak{P}) + \beta_i)^{e_i} = \prod_{i=1}^{r} \beta_i^{e_i} \tag{2.3}$$

d'où il existe i tel que $\beta_i = 0$. Cet entier i est unique et, par définition de Q, on a

$$Q = (\ 0, 0\ ;\ x_1, y\ ) .$$

On remarquera que les valeurs de $-\alpha_i/\beta_i$, pour lesquelles évidemment $\beta_i \neq 0$, sont exactement celles des racines distinctes du polynôme $\mathrm{Init}(C)(1, Y)$, de même qu'il existe j tel que $\beta_j = 0$ si et seulement si $\mathrm{Init}(C)(0, 1) = 0$. Plus précisément, on a

$$\mathcal{E}cl(P) := \left\{\ (\ 0, \gamma\ ;\ x, y_1\ )\ \mid\ \gamma \in \overline{K}, \mathrm{Init}(C)(1, \gamma) = 0\ \right\} \cup \mathcal{E}cl_\infty(P)$$

où

$$\mathcal{E}cl_\infty(P) = \begin{cases} \{\ (\ 0, 0\ ;\ x_1, y\ )\ \} & \text{si } \mathrm{Init}(C)(0, 1) = 0, \\ \emptyset & \text{sinon.} \end{cases}$$

Remarque 2.2.4 Soient $P := (\ 0, 0\ ;\ x, y\ )$ et $\mathcal{C}_\Gamma$ la courbe affine plane associée à l'ensemble de coordonnées $\Gamma := \{\ x, y\ \}$. On observera que les points de $\mathcal{E}cl(P)$ sont en correspondance biunivoque avec les facteurs linéaires distincts de $\mathrm{Init}(C)$ et donc avec les tangentes à la courbe au point P (voir Remarque 2.1.1). Plus précisément, $Q := (\ 0, \gamma\ ;\ x, y_1\ ) \in \mathcal{E}cl(P)$ si et seulement si la droite $\{\ \gamma X - Y = 0\ \}$ est tangente à la courbe en P. De même, $Q' := (\ 0, 0\ ;\ x_1, y\ ) \in \mathcal{E}cl(P)$ si et seulement si la droite $\{\ X = 0\ \}$ est tangente à la courbe en P.

Définition 2.2.5 *Soit P un point de $\overline{F}/\overline{K}$. On dit que $\{\ x, y\ \}$ est un* ensemble de coordonnées exceptionnelles de l'éclatement $\mathcal{E}cl(P)$ *si*

1. $P \equiv (\ 0, 0\ ;\ x, y\ )$,

2. $x/y \in \mathcal{O}_{\mathfrak{P}}$ *et* $y/x \in \mathcal{O}_{\mathfrak{P}}$ *quelle que soit la place* $\mathfrak{P}|P$.

Lemme 2.2.6 *Tout éclatement de point possède un ensemble de coordonnées exceptionnelles.*

Démonstration : Soient $P := (\, a, b\, ;\, x, y\,)$ un point de $\overline{F}/\overline{K}$. Posons $x' := x - a$ et $y' := y - b$ et soit C le polynôme de définition de $\{\, x', y'\, \}$. Posons $x_0 := x' + \alpha y'$ et $y_0 := x' + \beta y'$ où $\alpha, \beta \in \overline{K} \setminus \{\, 0\, \}$. Il est clair que si $\alpha \neq \beta$, alors $\Gamma_0 := \{\, x_0, y_0\, \}$ est un ensemble de coordonnées de $\overline{F}/\overline{K}$ et que $P \equiv (\, 0, 0\, ;\, x_0, y_0\,)$. Prenons α et β tels que $X + \alpha Y$ et $X + \beta Y$ ne divisent pas la forme initiale $\mathrm{Init}(C)$. En considérant les équations (2.2) et (2.3), on vérifie aisément que $y_0/x_0 \in \mathcal{O}_{\mathfrak{P}}$ et $x_0/y_0 \in \mathcal{O}_{\mathfrak{P}}$ pour toute place $\mathfrak{P}|P$ d'où $\{\, x_0, y_0\, \}$ est un ensemble de coordonnées exceptionnelles de $\mathcal{E}cl(P)$. □

Lemme 2.2.7 *Supposons que $P := (\, 0, 0\, ;\, x, y\,)$ soit un point de $\overline{F}/\overline{K}$ et soit $\mathfrak{P}$ une place dominant le point P. Si x est une coordonnée exceptionnelle de $P^{\mathfrak{P}}$ alors*

1. $\nu_{\mathfrak{P}}(x) = \min \{\, \nu_{\mathfrak{P}}(z) \mid z \in \mathcal{M}_P\, \}$,
2. $z/x \in \mathcal{O}_{P^{\mathfrak{P}}}$ *pour tout* $z \in \mathcal{M}_P$.

Démonstration : L'assertion (1) est équivalente au Lemme 2.1.12 car $\nu_{\mathfrak{P}}(x) \leq \nu_{\mathfrak{P}}(y)$. La démonstration de (2) est similaire à celle du Lemme 2.1.12 en remplaçant $\mathcal{O}_{\mathfrak{P}}$ par $\mathcal{O}_{P^{\mathfrak{P}}}$. □

La définition d'un point infiniment voisin vers une place dépend des coordonnées du point. Par contre, la proposition suivante montre que l'anneau local d'un point infiniment voisin d'un point P vers une place $\mathfrak{P}$ dépend uniquement de l'anneau local du point P et de la place $\mathfrak{P}$.

Proposition 2.2.8 *Soient P et R deux points équivalents de $\overline{F}/\overline{K}$ et $\mathfrak{P}$ une place de $\overline{F}/\overline{K}$ qui les domine. Pour tout $n \in \mathbb{N}$, on a*

$$P^{\mathfrak{P}^{(n)}} \equiv R^{\mathfrak{P}^{(n)}}.$$

Démonstration : Il est suffisant de montrer la proposition pour un point infiniment voisin d'ordre 1. Soit $\mathfrak{P}$ une place dominant les points P et R. Supposons sans perte de généralité que $P := (\, 0, 0\, ;\, x, y\,)$ et $R := (\, 0, 0\, ;\, u, v\,)$. Quitte à intervertir les rôles de x et y et les rôles de u et v, supposons que $\nu_{\mathfrak{P}}(x) \leq \nu_{\mathfrak{P}}(y)$ et $\nu_{\mathfrak{P}}(u) \leq \nu_{\mathfrak{P}}(v)$. Puisque $\mathcal{M}_P = \mathcal{M}_R$, on a $\nu_{\mathfrak{P}}(x) = \nu_{\mathfrak{P}}(u)$ d'après le Lemme 2.1.12. En vertu du lemme précédent, on a donc $x/u, y/u \in \mathcal{O}_{R^{\mathfrak{P}}}$. En particulier, x/u est inversible dans $\mathcal{O}_{R^{\mathfrak{P}}}$ et donc $y/x = (y/u)(u/x) \in \mathcal{O}_{R^{\mathfrak{P}}}$. L'anneau $\mathcal{O}_{R^{\mathfrak{P}}}$ contient alors l'ensemble de coordonnées $\{\, x, y/x\, \}$ ce qui est équivalent à $R^{\mathfrak{P}}|P^{\mathfrak{P}}$ d'après la Proposition 2.1.14. On montre de la même façon que $P^{\mathfrak{P}}|R^{\mathfrak{P}}$ d'où l'équivalence. □

Proposition 2.2.9 *Soit $P = (\,0,0\,;\,x,y\,)$ un point de $\overline{F}/\overline{K}$ et supposons que $y/x \in \mathcal{O}_{\mathfrak{P}}$ pour toute place $\mathfrak{P}$ dominant le point P. Alors*

$$x^{m_P - 1}\left(\bigcap_{Q \in \mathcal{E}cl(P)} \mathcal{O}_Q\right) \subseteq \mathcal{O}_P.$$

Démonstration : Perrin [38, Ch. IX, Lemme 4.7]

2.3 Diviseurs exceptionnels

Dans cette section on définit le diviseur exceptionnel d'un point. Ce diviseur joue un rôle essentiel pour le calcul d'une base de l'espace vectoriel $\mathcal{L}(D)$ où D est un diviseur du corps de fonctions $\overline{F}/\overline{K}$. Au Chapitre 3, Section 3.7, on déduira aussi de la définition du diviseur exceptionnel et de ses propriétés une méthode pour calculer les diviseurs principaux de fonctions.

Définition 2.3.1 *Soient P un point de $\overline{F}/\overline{K}$ et $u \in \overline{F} \setminus \{\,0\,\}$. On note $(u)_P$ le* diviseur local *de u au point P qui est défini par*

$$(u)_P := \sum_{\mathfrak{P}|P} \nu_{\mathfrak{P}}(u)\mathfrak{P}.$$

On vérifie que si $u, v \in \overline{F} \setminus \{\,0\,\}$, alors $(uv)_P = (u)_P + (v)_P$ pour tout point P de $\overline{F}/\overline{K}$.

Définition 2.3.2 *Soit P un point de $\overline{F}/\overline{K}$. Le* diviseur exceptionnel *du point P, noté E_P, est défini par*

$$E_P := \sum_{\mathfrak{P}|P} \mathrm{m}_{\mathfrak{P}}\mathfrak{P}$$

où pour toute place $\mathfrak{P}$ dominant le point P, l'entier $\mathrm{m}_{\mathfrak{P}}$ est tel que

$$\mathrm{m}_{\mathfrak{P}} := \min\{\,\nu_{\mathfrak{P}}(z) \;\mid\; z \in \mathcal{M}_P\,\}.$$

Lemme 2.3.3 *Soit $\{\,x,y\,\}$ un ensemble de coordonnées exceptionnelles de $\mathcal{E}cl(P)$. Alors*

$$(x)_P = (y)_P = E_P.$$

Démonstration : C'est clair par définition de E_P et grâce au Lemme 2.2.7. □

Remarque 2.3.4 Si P est un point simple, alors $E_P = \mathfrak{P}$ où $\mathfrak{P}$ est l'unique place telle que $\mathfrak{P} \equiv P$. La réciproque est vraie comme nous le verrons à la Proposition 2.4.8.

Supposons que $P := (\ 0, 0\ ;\ x, y\ )$ soit un point singulier de $\overline{F}/\overline{K}$ et soit $g \in \overline{F}$. Puisque toute place dominant P domine un seul point de $\mathcal{E}cl(P)$, on a

$$(g)_P = \sum_{Q \in \mathcal{E}cl(P)} (g)_Q.$$

Soit $G \in \overline{K}[X, Y]$ tel que $g = G(x, y)$. Notons l_Q la coordonnée exceptionnelle de $Q \in \mathcal{E}cl(P)$ et posons $x_1 := x/y$, $y_1 := y/x$ et

$$g^{(l_Q)} := \begin{cases} G^{(x)}(x, y_1) & \text{si } l_Q = x \\ G^{(y)}(x_1, y) & \text{si } l_Q = y. \end{cases}$$

On a

$$\begin{aligned} (g)_P &= \sum_{Q \in \mathcal{E}cl(P)} (l_Q^{\mathrm{m}_P(G)} g^{(l_Q)})_Q \\ &= \mathrm{m}_P(G) \sum_{Q \in \mathcal{E}cl(P)} (l_Q)_Q \ + \sum_{Q \in \mathcal{E}cl(P)} (g^{(l_Q)})_Q. \end{aligned}$$

Mais l_Q étant une coordonnée exceptionnelle du point $Q \in \mathcal{E}cl(P)$, on a

$$\nu_{\mathfrak{P}}(l_Q) = \min \{\, \nu_{\mathfrak{P}}(z) \mid z \in \mathcal{M}_P \,\}$$

pour toute place $\mathfrak{P}$ dominant le point Q d'après le Lemme 2.2.7. Par conséquent,

$$E_P = \sum_{Q \in \mathcal{E}cl(P)} (l_Q)_Q \tag{2.4}$$

d'où

$$(g)_P = \mathrm{m}_P(G) E_P + \sum_{Q \in \mathcal{E}cl(P)} (g^{(l_Q)})_Q. \tag{2.5}$$

Proposition 2.3.5 *Soient $P := (\ a, b\ ;\ x, y\ )$ un point de $\overline{F}/\overline{K}$ et $C \in \overline{F}/\overline{K}$ le polynôme de définition de $\{\, x, y \,\}$. Soient $g \in \overline{K}[x, y] \setminus \{\, 0 \,\}$ et $G \in \overline{K}[X, Y]$ tel que $g = G(x, y)$. Si la forme initiale de $G(X + a, Y + b)$ n'a pas de facteur commun avec la forme initiale de $C(X + a, Y + b)$ alors*

$$(g)_P = \mathrm{m}_P(G) E_P.$$

Démonstration : C'est clair en considérant l'équation (2.5) et la Remarque 2.2.4. □

2.4 Diviseurs d'intersection

On suppose maintenant que F/K et $\overline{F}/\overline{K}$ soient respectivement les corps de fonctions $K(\mathcal{C})$ et $\overline{K}(\mathcal{C})$ où $\mathcal{C} := \{ C = 0 \}$ est une courbe projective plane définie sur K.

Soient $S := \overline{K}[X_0, X_1, X_2]$ et $\overline{K}[\mathcal{C}] := S/\langle C \rangle$ l'anneau de coordonnées de la courbe. Notons respectivement par x_0, x_1 et x_2 les images résiduelles de X_0, X_1 et X_2 dans l'anneau $\overline{K}[\mathcal{C}]$ et appelons $\Gamma := \{ x_0, x_1, x_2 \}$ l'ensemble de coordonnées homogènes de $\mathcal{C}$. Les ensembles de coordonnées standards de la courbe $\Gamma_2 := \{ x_0/x_2, x_1/x_2 \}$, $\Gamma_1 := \{ x_0/x_1, x_2/x_1 \}$ et $\Gamma_0 := \{ x_1/x_0, x_2/x_0 \}$ sont des ensembles de coordonnées de $\overline{F}/\overline{K}$ définis sur K (cf. Annexe B.5.6). Ils ont respectivement $C(X, Y, 1)$, $C(X, 1, Y)$ et $C(1, X, Y)$ pour polynômes de définition.

Soit $P = (a_0 : a_1 : a_2) \in \mathcal{C}$. Par définition, au moins une des coordonnées de P est non nulle. Supposons que $a_2 \neq 0$. Alors $P_{*2} := (\ a_0/a_2, a_1/a_2\ ;\ x_0/x_2, x_1/x_2\ )$ est un point de $\overline{F}/\overline{K}$. De plus, on vérifie aisément que $\mathcal{O}_{P_{*2}} = \mathcal{O}_P(\mathcal{C})$. Si par exemple on a aussi $a_1 \neq 0$, alors $P_{*1} := (\ a_0/a_1, a_2/a_1\ ;\ x_0/x_1, x_2/x_1\ )$ est aussi un point de $\overline{F}/\overline{K}$ et $P_{*2} \equiv P_{*1}$. On peut ainsi identifier tout point de $\mathcal{C}$ à un point de $\overline{F}/\overline{K}$. Bien que l'anneau local $\mathcal{O}_{P_{*i}}$ soit le même quel que soit le choix de i tel que $a_i \neq 0$, certains calculs liés au point P dépendent de ce choix. On adopte donc la définition suivante :

Définition 2.4.1 *Soit* $\mathcal{C} := \{ C = 0 \}$ *une courbe projective plane et considérons* $\Gamma := \{ x_0, x_1, x_2 \}$ *l'ensemble de coordonnées homogènes correspondant. À tout point* $P := (a_0 : a_1 : a_2) \in \mathcal{C}$ *est associé un point* P_* *de* $\overline{K}(\mathcal{C})$ *défini comme suit :*

$$P_* := \begin{cases} (\ a_0/a_2, a_1/a_2\ ;\ x_0/x_2, x_1/x_2\ ) & \text{si } a_2 \neq 0 \\ (\ a_0/a_1, 0\ ;\ x_0/x_1, x_2/x_1\ ) & \text{si } a_2 = 0 \text{ et } a_1 \neq 0 \\ (\ 0, 0\ ;\ x_1/x_0, x_2/x_0\ ) & \text{si } P = (1 : 0 : 0). \end{cases}$$

De plus, pour un polynôme homogène $G \in S$*, on pose*

$$\overline{G}^P := \begin{cases} G(x_0, x_1, x_2)/x_2^{\deg G} & \text{si } a_2 \neq 0 \\ G(x_0, x_1, x_2)/x_1^{\deg G} & \text{si } a_2 = 0 \text{ et } a_1 \neq 0 \\ G(x_0, x_1, x_2)/x_0^{\deg G} & \text{si } P = (1 : 0 : 0). \end{cases}$$

Observons que $\overline{G}^P \in \overline{K}(\mathcal{C})$ quels que soient $P \in \mathcal{C}$ et un polynôme homogène $G \in S$. De plus, si $u = G(x_0, x_1, x_2)/H(x_0, x_1, x_2) \in \overline{K}(\mathcal{C})$, alors $u = \overline{G}^P/\overline{H}^P$ pour tout $P \in \mathcal{C}$.

Contrairement aux courbes affines planes, une place d'un corps de fonctions d'une courbe projective plane domine toujours un point de la courbe.

PROPOSITION 2.4.2 *Soit $\mathcal{C}$ une courbe projective plane.*

1. *Si $\mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C})}$ alors il existe un unique point $P \in \mathcal{C}$ tel que $\mathfrak{P}|P_*$.*
2. *Réciproquement, si $P \in \mathcal{C}$, alors $\left\{ \mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C})} \mid \mathfrak{P}|P_* \right\}$ est un ensemble fini et non vide.*

Démonstration : Au moins un des trois ensembles de coordonnées standards Γ_i, $i = 0, 1, 2$, est contenu dans l'anneau de valuation de la place $\mathfrak{P}$. La première assertion est donc une conséquence du Corollaire 2.1.16. La deuxième assertion est équivalente au Corollaire 2.1.15. □

DÉFINITION 2.4.3 *Soient $\mathcal{C}$ une courbe projective plane, $u \in \overline{K}(\mathcal{C})$ et $P \in \mathcal{C}$. On appelle le diviseur $(u)_P := (u)_{P_*}$ le* diviseur local *de u au point P.*

LEMME 2.4.4 *Soient $\mathcal{C}$ une courbe projective plane et $u \in \overline{K}(\mathcal{C})$. Alors*

$$(u) = \sum_{P \in \mathcal{C}} (u)_P.$$

Démonstration : C'est une conséquence de la Proposition 2.4.2. □

DÉFINITION 2.4.5 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $P \in \mathcal{C}$. Soit $G \in S \setminus \{ 0 \}$ tel que C ne divise pas G. Le* diviseur local d'intersection *de G au point P est le diviseur*

$$(G)_P := (\overline{G}^P)_P.$$

Le diviseur

$$(G) = \sum_{P \in \mathcal{C}} (G)_P.$$

est appelé le diviseur d'intersection *de G et $\mathcal{C}$.*

Le diviseur (G) est bien défini car $(G)_P = 0$ si et seulement si $G(P) \neq 0$ et d'après le Théorème de Bézout (cf. Annexe B.7), il n'existe qu'un nombre fini de point $P \in \mathcal{C}$ tel que $G(P) = 0$. De plus, il est clair que $(G)_P$ ne dépend pas de la définition de $\overline{G}^P$ (voir Définition 2.4.1).

La proposition suivante montre qu'on peut écrire le diviseur principal d'une fonction comme une différence de diviseurs d'intersection. On en déduira que deux polynômes homogènes de même degré admettent des diviseurs d'intersection de même degré.

Proposition 2.4.6 *Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et considérons $\Gamma := \{ x_0, x_1, x_2 \}$ l'ensemble de coordonnées homogènes correspondant. Soient $z \in \overline{K}(\mathcal{C}) \setminus \{ 0 \}$ et $G, H \in \overline{K}[X_0, X_1, X_2]$ des polynômes homogènes non divisibles par C tels que* $\deg G = \deg H$ *et*

$$z = \frac{G(x_0, x_1, x_2)}{H(x_0, x_1, x_2)}.$$

Alors

$$(z) = (G) - (H).$$

Démonstration : Soit $\mathfrak{P}$ une place quelconque de $\mathbb{P}_{\overline{K}(\mathcal{C})}$. Rappelons que $\frac{G(x_0,x_1,x_2)}{H(x_0,x_1,x_2)} = \overline{G}^P / \overline{H}^P$ pour tout $P \in \mathcal{C}$. On a donc

$$\begin{aligned} \nu_{\mathfrak{P}}(z) &= \nu_{\mathfrak{P}}(G(x_0, x_1, x_2)/H(x_0, x_1, x_2)) \\ &= \nu_{\mathfrak{P}}\left(\overline{G}^P / \overline{H}^P\right) \\ &= \nu_{\mathfrak{P}}\left(\overline{G}^P\right) - \nu_{\mathfrak{P}}\left(\overline{H}^P\right), \end{aligned}$$

d'où

$$\sum_{\mathfrak{P}|P} \nu_{\mathfrak{P}}(z)\mathfrak{P} = (G)_P - (H)_P.$$

La proposition est alors une conséquence du fait que d'après la Proposition 2.4.2 une place domine un unique point de $\mathcal{C}$. □

La proposition suivante est une variante du Théorème de Bézout.

Proposition 2.4.7 *Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et G un polynôme homogène non divisible par C. Alors*

$$\deg\,(G) = m \times n$$

où m et n sont respectivement les degrés de G et C.

Démonstration : On suppose d'abord sans perte de généralité que $C \neq X_2$ et $C \neq X_0$ de sorte que

$$\mathcal{C}_\infty := \mathcal{C} \cap \left\{ (a_0 : a_1 : a_2) \in \mathbb{P}^2 \;\middle|\; a_2 = 0 \right\}$$

soit un ensemble fini. D'après la Proposition 1.3.2, le degré d'un diviseur principal est 0. Alors, si H et H' sont deux polynômes homogènes de même degré et aucun d'eux n'est un multiple de C, le diviseur $(H) - (H')$ est un diviseur principal d'où $\deg(H) = \deg(H')$. De plus, pour tout polynôme homogène G', on a $(G'H') = (G') + (H')$. Il suffit donc de montrer la proposition avec $G := X_0$. On peut choisir un changement de coordonnées projectives (cf. Annexe B.6.1) de sorte que

$$\mathcal{V}(X_0 \cap C) \subset \mathcal{C} \setminus \mathcal{C}_\infty. \tag{2.6}$$

Soit $x := x_0/x_2$. Alors
$$(x) = (X_0) - (X_2)$$
et $\mathrm{supp}(X_0) \cap \mathrm{supp}(X_2) = \emptyset$ car par hypothèse on a $\mathcal{V}(X_0 \cap C \cap X_2) = \emptyset$. Par conséquent, $(x)_0 = (X_0)$ et donc
$$\deg(X_0) = \deg((x)_0) = [\overline{K}(\mathcal{C}) : \overline{K}(x)]$$
d'après la Proposition 1.3.2. Posons $y := x_1/x_2$. Alors $\{ x, y \}$ est un ensemble de coordonnées de $\overline{K}(\mathcal{C})$ qui admet $C_*(X,Y) := C(X,Y,1)$ comme polynôme de définition. Par conséquent, $p(Y) := C_*(x,Y) \in \overline{K}(x)[Y]$ est le polynôme minimal de y sur $\overline{K}(x)$. Pour finir il suffit de montrer que $\deg p(Y) = n$ car $\deg p(Y) = [\overline{K}(\mathcal{C}) : \overline{K}(x)]$. Or si ce n'est pas le cas, tous les monômes de $C(X_0, X_1, X_2)$ ont un degré en la variable X_1 strictement inférieur à n, et alors $C(0,1,0) = 0$, ce qui est contraire à l'hypothèse $\mathcal{V}(X_0 \cap C) \subset \mathcal{C} \setminus \mathcal{C}_\infty$. □

La proposition qui suit est importante : on en déduira que tout point infiniment voisin d'ordre suffisamment grand est un point simple.

PROPOSITION 2.4.8 *Soient $\overline{F}/\overline{K}$ un corps de fonctions et E_P le diviseur exceptionnel d'un point P de $\overline{F}/\overline{K}$. On a*
$$\deg E_P = \mathrm{m}_P.$$

Démonstration : Soit p la caractéristique de $\overline{K}$ et montrons la proposition pour le cas $p > 0$ (le cas $p = 0$ est traité à la remarque suivante). On peut supposer sans perte de généralité que P est un point d'une courbe projective plane $\mathcal{C} := \{ C = 0 \}$ (pas nécessairement définie sur K) telle que $\overline{K}(\mathcal{C}) \cong \overline{F}$. Si P est simple, alors $E_P = \mathfrak{P}$ où $\mathfrak{P} \equiv P$ et on a bien $\deg E_P = \mathrm{m}_P$. Supposons donc P singulier. D'après la Proposition 2.3.5, si G et C sont transverses en P (cf. Définition B.7.1), alors $(G)_P = \mathrm{m}_P(G) E_P$. Posons $V := \mathcal{V}(G \cap C)$ et supposons pour l'instant qu'il existe un polynôme homogène $G \in S$ tel que $G(P) = 0$ et tel que pour tout $P' \in V' := V \setminus \{ P \}$,

1. P' est un point simple de $\mathcal{C}$,

2. G et C sont transverses au point P'.

Dans ce cas, pour tout $P' \in V'$, on a $\deg E_{P'} = 1$ et
$$\deg(G)_{P'} = \mathrm{m}_{P'}(G) \times \deg E_{P'} = \mathrm{m}_{P'}(G) = I_{P'}(G, C) \tag{2.7}$$

où la dernière égalité est une conséquence des propriétés de l'indice d'intersection $I_{P'}(G,C)$ (voir Annexe B.7.2(5)). Posons $m := \deg G$ et $n := \deg C$. D'une part, on a, d'après la Proposition 2.4.7,

$$m \times n = \deg(G) = \deg(G)_P + \sum_{P' \in V'} \deg(G)_{P'} = \mathrm{m}_P(G) \times \deg E_P + \sum_{P' \in V'} \deg(G)_{P'}. \tag{2.8}$$

D'autre part, on a, d'après le Théorème de Bézout,

$$m \times n = I_P(G,C) + \sum_{P' \in V'} I_{P'}(G,C) = \mathrm{m}_P(G) \times \mathrm{m}_P(C) + \sum_{P' \in V'} I_{P'}(G,C). \tag{2.9}$$

En comparant (2.8) et (2.9) avec (2.7), on trouve

$$\mathrm{m}_P(G) \times \deg E_P = \mathrm{m}_P(G) \times \mathrm{m}_P(C),$$

d'où $\deg E_P = \mathrm{m}_P(C) = \mathrm{m}_P$. Pour terminer, montrons qu'il existe un polynôme G satisfaisant aux propriétés voulues. Quitte à appliquer un changement de coordonnées projectives, on peut supposer que

1. $P = (0:0:1)$,
2. $C(0,1,0) \neq 0$,
3. $C'_X \neq 0$ où C'_X est la dérivée[3] usuelle par rapport à X de $C'(X,Y) := C(X,Y,1)$,
4. Y ne divise pas $\mathrm{Init}(C')$.

Soit le polynôme homogène

$$G_\alpha := \alpha {X_0}^p + X_1 X_2^{p-1}$$

où $\alpha \in \overline{K}$. Quel que soit $0 \neq \alpha \in \overline{K}$, le point $P = (0:1:0)$ est le seul point à l'infini tel que $G_\alpha(P) = 0$. Pour tout $\alpha \neq 0$, on a donc $\mathcal{V}(G_\alpha \cap C) \subset \mathcal{C} \setminus \mathcal{C}_\infty$ car $C(0,1,0) \neq 0$. Posons

$$G'_\alpha(X,Y) := G_\alpha(X,Y,1) = Y + \alpha X^p.$$

Puisque Y ne divise pas $\mathrm{Init}(C')$, G et C sont transverses en $P = (0:0:1)$ pour tout $\alpha \neq 0$. Si $Q = (a:b:1) \in \mathcal{C} \setminus \mathcal{C}_\infty$ est un point simple, alors

$$\mathrm{Init}(C'(X+a, Y+b)) = C'_X(a,b)X + C'_Y(a,b)Y \neq 0.$$

3. on ne peut avoir $C'_X = C'_Y = 0$ car dans ce cas tous les points affines seraient singuliers!

D'autre part, quel que soit $Q = (a : b : 1)$ tel que $G_\alpha(Q) = 0$, on a

$$\mathrm{Init}(G'_\alpha(X+a, Y+b)) = \mathrm{Init}(((Y+b) + \alpha(X+a)^p)) = \mathrm{Init}((Y + \alpha X^p)) = Y.$$

On en déduit donc que si $Q = (a : b : 1) \in V$ est un point simple de $\mathcal{C}$, alors G et C sont transverses en Q si et seulement si $C'_X(a, b) \neq 0$. Puisque $C'_X \neq 0$ et que C' ne divise pas C'_X, l'ensemble

$$W := \{\, Q = (a : b : 1) \mid C'_X)(a, b) = 0 \,\} \cup \{\, Q \in \mathcal{C} \setminus \mathcal{C}_\infty \mid Q \text{ est singulier} \,\}$$

a au plus un nombre fini d'éléments. Il suffit donc de choisir $0 \neq \alpha \in \overline{K}$ tel que $G_\alpha(Q) \neq 0$ pour tout $Q \in W \setminus \{\, P \,\}$, ce qui est toujours possible. De cette façon, quel que soit $Q \in \mathcal{V}(G_\alpha \cap C) \setminus \{\, P \,\}$, le point Q est un point simple de $\mathcal{C}$, et G et C sont transverses en Q. □

Remarque 2.4.9 Dans le cas $p = 0$, on peut prendre $G = X + \alpha Y$ avec α tel que G et C aient exactement $\deg C - \mathrm{m}_P$ points d'intersection deux à deux distincts (voir Fulton [10, Problème 5.26, page 118]). En vertu du Théorème de Bézout, tous les points de $\mathcal{V}(G \cap C)$ sont des points simples de $\mathcal{C}$, et G et C sont transverses en tout point de $\mathcal{V}(G \cap C)$. Dans le cas $p > 0$, il peut exister un point terrible, c'est-à-dire un point P tel qu'il existe une infinité de droites passant par P qui coupent $\mathcal{C} := \{\, C = 0 \,\}$ en strictement moins de $\deg C - \mathrm{m}_P$ points. Par exemple, soient $\overline{K} := \overline{\mathbb{F}}_2$ et $C(X_0, X_1, X_2) = X_0^3 X_2^2 + X_1^5$. Alors la droite $\{\, \alpha X_0 + \beta X_1 = 0 \,\}$ a seulement deux points d'intersection P_1 et P_2 avec la courbe $\mathcal{C} := \{\, C = 0 \,\}$: si $\alpha = 0$, alors $P_1 := (0 : 0 : 1)$ et $P_2 := (1 : 0 : 0)$, sinon $P_2 := (\beta\gamma/\alpha : \gamma : 1)$, où γ est tel que $\gamma^2 = \beta^3/\alpha^3$. Or $\mathrm{m}_{P_1} = 3$, d'où le point est terrible.

2.5 Arbres de désingularisation

À un point P de $\overline{F}/\overline{K}$, on associe un arbre $\mathcal{T}_P$, appelé arbre de désingularisation de P, dont P est la racine et où chacun des noeuds de $\mathcal{T}_P$ est un point infiniment voisin de P. Il sera utile d'associer à tout noeud de l'arbre le diviseur exceptionnel du point correspondant. Plus précisément, l'arbre $\mathcal{T}_P$ admet la définition récursive suivante :

1. si P est simple, alors P correspond à une place $\mathfrak{P}$ et

$$\mathcal{T}_P = [P, E_P]$$

   où $E_P := \mathfrak{P}$,

2. si P est singulier, alors

$$\mathcal{T}_P = \{\,[P, E_P], \{\,\mathcal{T}_Q \mid Q \in \mathcal{E}cl(P)\,\}\,\}$$

où E_P est le diviseur exceptionnel du point P.

La Proposition 2.5.1 et le Théorème 2.5.2 montrent que l'arbre de désingularisation d'un point est fini. On en déduira que l'ensemble des places dominant le point P est en correspondance biunivoque avec l'ensemble des feuilles de $\mathcal{T}_P$.

PROPOSITION 2.5.1 *Soient P un point de $\overline{F}/\overline{K}$ et $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ une place dominant le point P. Alors quel que soit $u \in \mathcal{O}_{\mathfrak{P}}$, il existe $N_u \in \mathbb{N}$ tel que $u \in \mathcal{O}_{P^{\mathfrak{P}(n)}}$ pour tout $n \geq N_u$.*

Démonstration : Posons $P_0 := P$ et pour $i \in \mathbb{N}^*$ posons $P_i := P^{\mathfrak{P}^{(i)}}$. Pour chacun des points P_i, soit $\Gamma_i := \{\,x_i, y_i\,\}$ un ensemble de coordonnés de $\overline{F}$ tel que $P_i \equiv (\,0, 0\,;\,x_i, y_i\,)$ et, quitte à intervertir les rôles de x_i et y_i, supposons que $\nu_{\mathfrak{P}}(x_i) \leq \nu_{\mathfrak{P}}(y_i)$. D'après le Lemme 2.2.7, on a donç pour tout $i \in \mathbb{N}$,

$$z/x_i \in \mathcal{O}_{P_{i+1}} \text{ pour tout } z \in \mathcal{M}_{P_i}. \tag{2.10}$$

Soit $u \in \mathcal{O}_{\mathfrak{P}}$. Le corps $\overline{F}$ étant égal au corps des fractions de tout anneau local d'un point de $\overline{F}/\overline{K}$, on peut choisir $f, g \in \mathcal{O}_{P_0}$ tels que $u = f/g$. Si $g \notin \mathcal{M}_{P_0}$, alors $u \in \mathcal{O}_{P_0}$ et la démonstration est finie. Sinon $g \in \mathcal{M}_{P_0}$ et alors $g/x_0 \in \mathcal{O}_{P_1}$. Il existe donc un plus grand entier n tel que

$$g_n := g/(x_0 x_1 \cdots x_n) \in \mathcal{O}_{P_{n+1}}$$

car $\nu_{\mathfrak{P}}(x_i) > 0$ et $\mathcal{O}_{P_i} \subseteq \mathcal{O}_{\mathfrak{P}}$ pour tout $i \in \mathbb{N}^*$. Observons que $\nu_{\mathfrak{P}}(g_n) = 0$, car sinon $g_n \in \mathfrak{P} \cap \mathcal{O}_{P_{n+1}} = \mathcal{M}_{P_{n+1}}$ et alors $g_n/x_{n+1} \in \mathcal{O}_{P_{n+2}}$, contredisant ainsi le choix de n. Par conséquent, $g_n \in \mathcal{O}_{P_{n+1}} \setminus \mathcal{M}_{P_{n+1}}$ et g_n est donc inversible dans $\mathcal{O}_{P_{n+1}}$. Posons $f_n := f/(x_0 x_1 \cdots x_n)$. Puisque $\nu_{\mathfrak{P}}(f) \geq \nu_{\mathfrak{P}}(g)$ et $g_n \in \mathcal{O}_{P_{n+1}}$, on doit avoir $f_n \in \mathcal{O}_{P_{n+1}}$. Par conséquent $u = f_n g_n^{-1} \in \mathcal{O}_{P_{n+1}}$. □

THÉORÈME 2.5.2 *Soient P un point de $\overline{F}/\overline{K}$ et $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ une place dominant le point P. Alors il existe $N \in \mathbb{N}$ tel que $P^{\mathfrak{P}^{(n)}} \equiv \mathfrak{P}$ pour tout $n \geq N$.*

Démonstration : Pour $i \in \mathbb{N}^*$ posons $P_i := P^{\mathfrak{P}^{(i)}}$. D'après le Corollaire 1.5.5, il existe $u \in \mathfrak{P}$ tel que $\mathfrak{P}$ est l'unique zéro de u. En vertu de la proposition précédente, il existe l tel que $u \in \mathcal{O}_{P_l}$. En particulier, $u \in \mathfrak{P} \cap \mathcal{O}_{P_l} = \mathcal{M}_{P_l}$ d'où $\mathfrak{P}$ est l'unique place dominant P_l. Soit maintenant t un paramètre local de $\mathfrak{P}$. Il existe $n \geq l$ tel que $t \in \mathcal{O}_{P_n}$ et dans ce cas on a $E_{P_n} = \mathfrak{P}$ par définition des diviseurs exceptionnels. Par conséquent, P_n est un point simple car $\mathrm{m}_{P_n} = \deg E_{P_n} = 1$ d'après la Proposition 2.4.8. □

REMARQUE 2.5.3 Le théorème précédent, bien que formulé autrement, est un résultat classique de la théorie des éclatements de points (voir par exemple [38, Prop. 5.8]).

PROPOSITION 2.5.4 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $\mathcal{S}$ l'ensemble des points singuliers de $\mathcal{C}$. Soient $\mathfrak{P}$ une place de $\overline{K}(\mathcal{C})$ et $P \in \mathcal{C}$ l'unique point dominé par $\mathfrak{P}$. Alors*

1. *$P \equiv \mathfrak{P}$ si P est simple,*

2. *sinon il existe une unique feuille Q de $\mathcal{T}_P$ telle que $Q \equiv \mathfrak{P}$.*

En particulier, l'ensemble

$$(\mathcal{C} \setminus \mathcal{S}) \cup \{ Q \mid Q \text{ est une feuille de } \mathcal{T}_P, P \in \mathcal{S} \}$$

est en correspondance biunivoque avec $\mathbb{P}_{\overline{K}(\mathcal{C})}$.

Démonstration : C'est une conséquence triviale du théorème précédent et de la Proposition 2.4.2. □

2.5.1 Formule du genre pour une courbe projective plane

Le théorème qui suit est bien connu.

THÉORÈME 2.5.5 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $\mathcal{S}$ l'ensemble de tous les points singuliers de $\mathcal{C}$. Pour tout $P \in \mathcal{S}$, soit $\mathcal{I}_P$ l'ensemble de tous les noeuds de l'arbre $\mathcal{T}_P$ (incluant le point P). Soient g le genre de $\overline{K}(\mathcal{C})$ et $n := \deg C$. Alors*

$$g = \frac{(n-1)(n-2)}{2} - \frac{1}{2} \sum_{P \in \mathcal{S}} \sum_{Q \in \mathcal{I}_P} \mathrm{m}_Q(\mathrm{m}_Q - 1).$$

Démonstration : Hironaka [22]. Voir aussi Shafarevich [40, Section 4.1]. On trouvera aussi une démonstration de cette formule dans Fulton [10] dans le cas où les points singuliers de $\mathcal{C}$ sont ordinaires.[4]

4. Un point singulier est ordinaire s'il y a exactement m_P tangentes à la courbe au point P deux à deux distinctes. Dans ce cas, un éclatement suffit à désingulariser le point.

2.6 Diviseurs d'adjonction

La notion de diviseur d'adjonction joue un rôle très important pour l'étude des courbes planes. Il permet entre autre de caractériser la classe des diviseurs canoniques du corps des fonctions d'une courbe projective plane. C'est aussi des propriétés du diviseur d'adjonction que sera déduit, à la Section 2.7, un algorithme pour calculer une base de l'espace vectoriel associé à un diviseur.

DÉFINITION 2.6.1 *Soient P un point de $\overline{F}/\overline{K}$ et $\mathcal{T}_P$ son arbre de désingularisation. Soit $\mathcal{I}_P$ l'ensemble de tous les noeuds de l'arbre $\mathcal{T}_P$ (incluant le point P). On appelle* diviseur d'adjonction *du point P le diviseur*

$$\mathcal{A}_P := \sum_{Q \in \mathcal{I}_P} (\mathrm{m}_Q - 1) E_Q$$

où m_Q et E_Q sont respectivement la multiplicité et le diviseur exceptionnel du point Q.

DÉFINITION 2.6.2 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $P \in \mathcal{C}$. Le* diviseur d'adjonction *du point P est le diviseur*

$$\mathcal{A}_P := \mathcal{A}_{P_*}.$$

Le diviseur d'adjonction *de la courbe $\mathcal{C}$ est le diviseur*

$$\mathcal{A}(\mathcal{C}) := \sum_{P \in \mathcal{S}} \mathcal{A}_P$$

où $\mathcal{S}$ est l'ensemble de tous les points singuliers de $\mathcal{C}$.

Observons que pour tout $P \in \mathcal{C}$, on a $\deg \mathcal{A}_P \geq 0$ et que $\deg \mathcal{A}_P = 0$ si et seulement si P est simple.

La proposition suivante donne une condition suffisante pour qu'un élément de $\overline{F}/\overline{K}$ appartienne à l'anneau local d'un point.

PROPOSITION 2.6.3 *Soient P un point de $\overline{F}/\overline{K}$ et $u \in \overline{F}$. On a*

$$(u)_P \geq \mathcal{A}_P \Longrightarrow u \in \mathcal{O}_P.$$

Démonstration : Montrons la proposition par récurrence sur $N := \deg \mathcal{A}_P$. Si $N = 0$, alors P est simple et dans ce cas $(u)_P = \nu_{\mathfrak{P}}(u)\mathfrak{P}$ où $\mathfrak{P} \equiv P$. On a donc par hypothèse $\nu_{\mathfrak{P}}(u) \geq 0$ d'où $u \in \mathcal{O}_{\mathfrak{P}} = \mathcal{O}_P$. Supposons donc P singulier et que la proposition est vraie pour $n < N$. Supposons sans perte de généralité que $P \equiv (\,0, 0\,;\, x, y\,)$ et que $\{ x, y \}$ est un ensemble de coordonnées exceptionnelles de $\mathcal{E}cl(P)$. D'après la Remarque 2.3.4, on a

$$E_P = (x)_P = \sum_{Q \in \mathcal{E}cl(P)} (x)_Q$$

et plus particulièrement,

$$\begin{aligned} (u)_P &= \sum_{Q\in\mathcal{E}cl(P)}(u)_Q \\ &\geq \mathcal{A}_P \\ &= (\mathrm{m}_P - 1)E_P + \sum_{Q\in\mathcal{E}cl(P)} \mathcal{A}_Q \\ &= \sum_{Q\in\mathcal{E}cl(P)} \left((\mathrm{m}_P - 1)(x)_Q + \mathcal{A}_Q\right). \end{aligned}$$

Puisqu'une somme de diviseurs locaux en chacun des points de $\mathcal{E}cl(P)$ est une somme de diviseurs dont les supports sont deux à deux disjoints, on a

$$(u)_Q \geq (\mathrm{m}_P - 1)(x)_Q + \mathcal{A}_Q \text{ pour tout } Q \in \mathcal{E}cl(P)$$

qui est équivalent à

$$\left(\frac{u}{x^{\mathrm{m}_P - 1}}\right)_Q \geq \mathcal{A}_Q \text{ pour tout } Q \in \mathcal{E}cl(P).$$

Or, pour tout $Q \in \mathcal{E}cl(P)$, on a $\deg \mathcal{A}_Q < \deg \mathcal{A}_P = N$ et, en appliquant l'hypothèse de récurrence, on a

$$\frac{u}{x^{\mathrm{m}_P - 1}} \in \bigcap_{Q\in\mathcal{E}cl(P)} \mathcal{O}_Q.$$

La proposition est alors une conséquence de la Proposition 2.2.9 car

$$u \in x^{\mathrm{m}_P - 1}\left(\bigcap_{Q\in\mathcal{E}cl(P)} \mathcal{O}_Q\right) \subseteq \mathcal{O}_P.$$

□

PROPOSITION 2.6.4 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $\mathcal{A}$ son diviseur d'adjonction. Alors*

$$\deg \mathcal{A} = (n-1)(n-2) - 2g$$

où g est le genre de la courbe $\mathcal{C}$ et $n := \deg C$.

Démonstration : C'est une conséquence de la Proposition 2.4.8 et du Théorème 2.5.5.

□

REMARQUE 2.6.5 Cette formule pour le degré du diviseur d'adjonction en fonction du genre d'une courbe projective plane est bien connue. Dans [16], cette formule est définie en fonction du **conducteur** de l'anneau local $\mathcal{O}_P$ dans sa clôture intégrale $\mathcal{O}'_P$ prise dans le corps $\overline{K}(\mathcal{C})$; le conducteur est l'idéal de $\mathcal{O}_P$ donné par

$$C_P := \{\, z \in \mathcal{O}_P \mid z \cdot \mathcal{O}'_P \subseteq \mathcal{O}_P \,\}$$

qui est aussi un idéal de $\mathcal{O}'_P$. Si

$$\mathcal{A}_P = \sum_{i=1}^{r} n_i \mathfrak{P}_i,$$

on peut alors montrer que

$$C_P = \bigcap_{i=1}^{r} (\mathfrak{P}_i^{n_i} \cap \mathcal{O}_P)\,.$$

En particulier,

$$C_P = \{\, z \in \mathcal{O}_P \mid (z)_P \geq \mathcal{A}_P \,\}\,.$$

PROPOSITION 2.6.6 *Soient $\mathcal{C} := \{\, C = 0 \,\}$ une courbe projective plane et $\mathcal{A}$ le diviseur d'adjonction de $\mathcal{C}$. Si G est un polynôme homogène tel que* $\deg G = \deg C - 3$ *et $(G) \geq \mathcal{A}$, alors*

$$\mathcal{K} := (G) - \mathcal{A}$$

est un diviseur canonique du corps de fonctions $\overline{K}(\mathcal{C})$.

Démonstration : Gorenstein [16, Th. 9].

2.6.1 Théorème fondamental de Max Noether

DÉFINITION 2.6.7 *Soit $\mathcal{C} := \{\, C = 0 \,\}$ une courbe projective plane. Soient $G, H \in S$ deux polynômes homogènes et supposons que C ne divise pas G. On dit que le couple (H, G)* **satisfait la condition de Noether** *au point $P \in \mathcal{C}$ si*

$$\overline{H}^P / \overline{G}^P \in \mathcal{O}_P(\mathcal{C}).$$

THÉORÈME 2.6.8 (THÉORÈME FONDAMENTAL DE MAX NOETHER) *Soient $\mathcal{C} := \{C = 0\}$ une courbe projective plane et $G, H \in S$ deux polynômes homogènes où G n'est pas divisible par C. Les deux propositions suivantes sont équivalentes :*

1. *Il existe deux polynôme homogènes $A, B \in S$ tels que* $\deg A + \deg G = \deg B + \deg C = \deg H$ *et*

$$H = AG + BC.$$

2. *Le couple (H, G) satisfait la condition de Noether en tout point de $\mathcal{C}$.*

Démonstration : Gorenstein [16, Th. 7]. Voir aussi Fulton [10, page 120].

THÉORÈME 2.6.9 *Soient* $\mathcal{C} := \{ C = 0 \}$ *une courbe projective plane et* $\mathcal{A}$ *son diviseur d'adjonction. Soient* $G, H \in S$ *deux polynômes homogènes non divisibles par* C. *Si*

$$(H) \geq \mathcal{A} + (G),$$

alors il existe deux polynômes homogènes $A, B \in S$ *tels que* $\deg A + \deg G = \deg B + \deg C = \deg H$ *et*

$$H = AG + BC.$$

Démonstration : Si $(H) \geq \mathcal{A} + (G)$, alors $(H)_P \geq \mathcal{A}_P + (G)_P$ pour tout $P \in \mathcal{C}$. Le théorème est alors une conséquence de la Proposition 2.6.3 et du Théorème 2.6.8. □

2.6.2 Théorème des résidus

THÉORÈME 2.6.10 (THÉORÈME DES RÉSIDUS) *Soient* $\mathcal{C} := \{ C = 0 \}$ *une courbe projective plane et* $\mathcal{A}$ *son diviseur d'adjonction. Soient* D *et* D' *deux diviseurs de* $\overline{K}(\mathcal{C})$ *tels que* $D \equiv D'$ *et supposons que* D' *soit effectif* ($D' \geq 0$). *Si* $G \in S$ *est un polynôme homogène tel que*

$$(G) = D + \mathcal{A} + R$$

pour un certain diviseur $R \geq 0$, *alors il existe un polynôme homogène* $G' \in S$ *tel que* $\deg G' = \deg G$ *et*

$$(G') = D' + \mathcal{A} + R.$$

Démonstration : Puisque $D \equiv D'$, il existe $z \in \overline{K}(\mathcal{C})$ tel que

$$D = (z) + D'.$$

Soient $H, H' \in S$ deux polynômes homogènes tels que $(z) = (H) - (H')$. On a

$$\begin{aligned}(H'G) &= (H') + D + \mathcal{A} + R \\ &= (H') + (z) + D' + \mathcal{A} + R \\ &= (H) + D' + \mathcal{A} + R.\end{aligned}$$

Les diviseurs (H), D', $\mathcal{A}$ et R étant tous effectifs, on a

$$(H'G) \geq \mathcal{A} + (H).$$

Il existe donc, d'après le Théorème 2.6.9, deux polynômes homogènes $G', B \in S$ tels que $\deg G' + \deg H = \deg B + \deg C = \deg H'G$ et

$$H'G = G'H + BC.$$

On a donc $(H'G) = (G'H)$ et par suite $(G') = (H'G) - (H) = D' + \mathcal{A} + R$. □

2.7 Algorithme de Brill-Noether

Le théorème qui suit est une conséquence du Théorème 2.6.10. On en déduira un algorithme qui calcule une base de l'espace vectoriel associé à un diviseur.

THÉORÈME 2.7.1 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane, $\mathcal{A}$ son diviseur d'adjonction et D un diviseur de $\overline{K}(\mathcal{C})$. Soit $G_0 \in S_d$ ($d \in \mathbb{N}^*$) un polynôme homogène non divisible par C tel que*

$$(G_0) \geq D + \mathcal{A}.$$

Alors

$$\mathcal{L}(D) = \left\{ \overline{G}/\overline{G}_0 \;\middle|\; G \in S_d \text{ est non divisible par } C \text{ et } (G) \geq (G_0) - D \right\} \cup \{ 0 \}.$$

où $\overline{G}$ et $\overline{G}_0$ sont respectivement les images résiduelles de G et G_0 dans $\overline{K}[\mathcal{C}]$ et $S_d \subset S$ est l'ensemble des polynômes homogènes de degré d.

Démonstration : Soit $G \in S$ un polynôme homogène de même degré que G_0 non divisible par C tel que $(G) \geq (G_0) - D$ et posons $z := \overline{G}/\overline{G}_0$. On a

$$(z) + D = (G) - (G_0) + D \geq 0$$

d'où $z \in \mathcal{L}(D)$. Réciproquement, soit $z \in \mathcal{L}(D) \setminus \{ 0 \}$. Alors $D' := D + (z) \geq 0$ par définition de $\mathcal{L}(D)$. Puisque $D' \equiv D$ et $(G_0) \geq D + \mathcal{A}$, on peut appliquer le Théorème 2.6.10 à $R := (G_0) - (D + \mathcal{A}) \geq 0$ pour trouver $G' \in S$ tel que $\deg G' = \deg G_0$ et

$$(G') = D' + \mathcal{A} + R.$$

On a donc

$$(G') - (G_0) = D' - D = (z).$$

Soit $z' := \overline{G}'/\overline{G}_0$. Alors $(z/z') = 0$. Or, d'après la Proposition 1.2.19, seuls les constantes n'ont ni zéro ni pôle. Par conséquent, $\alpha := z/z' \in \overline{K}$ et

$$z = \alpha z' = \alpha \overline{G}'/\overline{G}_0.$$

□

Notons que le théorème précédent s'applique aux diviseurs non effectifs. Si D est un diviseur non effectif, il est clair que

$$(G_0) \geq \mathcal{A} + D \iff (G_0) \geq (\mathcal{A} + D)_+.$$

Il est donc suffisant de ne considérer que le diviseur $(\mathcal{A}+D)_+ \geq 0$ pour déterminer un polynôme homogène $G_0 \in S$ tels que $(G_0) \geq \mathcal{A}+D$.

L'algorithme qui suit, souvent appelé Algorithme de Brill-Noether, utilise le théorème précédent pour calculer une base de l'espace vectoriel associé à un diviseur.

Algorithme 2.7.2 **Brill-Noether**(D)

▷ **Entrée :** Un diviseur D du corps de fonctions $\overline{K}(\mathcal{C})$ où $\mathcal{C}$ est une courbe projective plane.

▷ **Sortie :** Un base de l'espace vectoriel $\mathcal{L}(D)$.

1 : Poser $B := D + \mathcal{A}$ où $\mathcal{A}$ est le diviseur d'adjonction de la courbe $\mathcal{C}$.

2 : Soit $d \in \mathbb{N}$ assez grand pour qu'il existe un polynôme homogène $G \in S_d$ non divisible par C tel que $(G) \geq B_+$ où B_+ est la partie positive de B.

3 : Calculer une base du $\overline{K}$-espace vectoriel

$$V := \{\, G \in S_d \;|\; C \text{ divise } G \text{ ou } (G) \geq B_+ \,\} \cup \{\, 0 \,\}\,.$$

4 : Soit $\{\, G_1, G_2, \ldots, G_s \,\}$ la base calculée à l'étape précédente. Si $d \geq \deg C$, alors il faut réduire la base $\{\, G_1, G_2, \ldots, G_s \,\}$ modulo l'espace vectoriel

$$W := \{\, A \in S_d \;|\; C \text{ divise } A \,\}\,.$$

Pour ce faire, il suffit de choisir une base $\{\, A_1, A_2, \ldots, A_k \,\}$ de W avec $A_i \in S_d$ pour $i = 1, 2, \ldots, k$ et de compléter cette base en une base

$$\{\, A_1, A_2, \ldots, A_k, G'_1, G'_2, \ldots, G'_{s'} \,\}$$

de l'espace vectoriel V. Dans ce cas, l'espace vectoriel $V' \subset S_d \cup \{\, 0 \,\}$ engendré par les éléments de $\{\, G'_1, G'_2, \ldots, G'_{s'} \,\}$ est tel que $V' \setminus \{\, 0 \,\}$ est exactement l'ensemble de tous les polynômes G homogènes de degré d non divisibles par C tels que $(G) \geq B_+$.

5 : Choisir $G_0 \in V'$ et calculer le diviseur d'intersection (G_0).

6 : De la même façon qu'aux étapes précédentes, déterminer une base $\{\, G_1, G_2, \ldots, G_k \,\}$ de l'espace vectoriel $V'' \subset S_d \cup \{\, 0 \,\}$ tel que $V'' \setminus \{\, 0 \,\}$ est l'ensemble de tous les polynômes homogènes $G \in S_d$ non divisibles par C tels que $(G) \geq (G_0) - D$.

7 : Poser $g_i := G_i + \langle C \rangle \in K[\mathcal{C}]$ pour $i := 0, 1, 2, \ldots, k$ et retourner

$$\{\, g_i / g_0 \;|\; i = 1, 2, \ldots, k \,\}$$

qui est une base de $\mathcal{L}(D)$.

En résumé, pour appliquer l'algorithme de Brill-Noether il faut savoir :

1. Calculer le diviseur d'adjonction d'une courbe projective plane $\mathcal{C} := \{\, C = 0 \,\}$.

2. Pour un diviseur B donné et un entier d, calculer une base du sous-espace vectoriel de $S_d \cup \{ 0 \}$

$$V := \{ G \in S_d \mid C \text{ divise } G \text{ ou } (G) \geq B \} \cup \{ 0 \} .$$

3. Pour tout polynôme homogène $G \in S \setminus \{ 0 \}$, calculer le diviseur d'intersection de G avec $\mathcal{C}$.

On verra au Chapitre 3, Section 3.7, comment calculer le diviseur d'adjonction d'une courbe et les diviseurs d'intersection de polynômes homogènes avec une courbe. On termine cette section en donnant une solution au problème du calcul d'une base de l'espace vectoriel V.

2.7.1 Polynômes d'interpolation

DÉFINITION 2.7.3 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et B un diviseur de $\overline{K}(\mathcal{C})$. Un* polynôme d'interpolation *du diviseur B est un polynôme homogène $G \in S$ vérifiant l'une ou l'autre des deux propriétés suivantes :*

1. C divise G.

2. $(G) \geq B$ si C ne divise pas G.

Pour calculer les polynômes d'interpolation de degré $d \in \mathbb{N}^*$ d'un diviseur B, on utilisera les séries $\mathfrak{P}$-adiques de fonctions de $\overline{K}(\mathcal{C})$ (cf. Annexe C). En accord avec la Définition 2.4.1, on a la définition suivante :

DÉFINITION 2.7.4 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane, $\mathfrak{P}$ une place de $\overline{K}(\mathcal{C})$ et $t \in \mathfrak{P}$ un paramètre local de $\mathfrak{P}$. Soient $P = (a : b : c) \in \mathcal{C}$ l'unique point dominé par $\mathfrak{P}$ et $\Gamma := \{ x, y \}$ l'ensemble de coordonnées tel que $P_* \in \mathcal{Z}(\Gamma)$. Soient respectivement $x(t)$ et $y(t)$ les séries $\mathfrak{P}$-adiques de x et y en fonction de t. À la place $\mathfrak{P}$ est associée sa* paramétrisation locale*, noté $[\mathfrak{P}]$, définie comme suit :*

$$[\mathfrak{P}] := \begin{cases} [x(t), y(t), 1] & \textit{si } c \neq 0 \\ [x(t), 1, y(t)] & \textit{si } c = 0 \textit{ et } b \neq 0 \\ [1, x(t), y(t)] & \textit{sinon.} \end{cases}$$

Si $G \in S$ est un polynôme homogène, on lui associe sa paramétrisation locale *en $\mathfrak{P}$ qui est définie par*

$$G[\mathfrak{P}] := G(s_0, s_1, s_2)$$

où $[\mathfrak{P}] = [s_0, s_1, s_2]$ est la paramétrisation locale de $\mathfrak{P}$.

Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $\{ x_0, x_1, x_2 \} \subset \overline{K}(\mathcal{C})$ l'ensemble de coordonnées homogènes correspondant. Fixons une place $\mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C})}$ et t un paramètre local de $\mathfrak{P}$. Soit $P = (a : b : c) \in \mathcal{C}$ l'unique point dominé par $\mathfrak{P}$ et supposons que $c \neq 0$. Soit $[\mathfrak{P}] = [s_0, s_1, s_2]$ la paramétrisation locale de $\mathfrak{P}$. Alors par définition, s_0, s_1 et s_2 sont respectivement les séries $\mathfrak{P}$-adiques de x_0/x_2, x_1/x_2 et $x_2/x_2 = 1$ en fonction de t. Soient $G \in S \setminus \{ 0 \}$ un polynôme homogène, $g := \overline{G}^P$ et $g(t) \in \overline{K}((t))$ la série $\mathfrak{P}$-adique de g en fonction de t. On a

$$g(t) = \frac{G(x_0, x_1, x_2)}{x_2^{\deg G}}(t) = G(x_0/x_2, x_1/x_2, 1)(t) = G(s_0, s_1, s_2) = G[\mathfrak{P}].$$

On a aussi

$$\nu_{\mathfrak{P}}(g) = \operatorname{ord}(G[\mathfrak{P}]).$$

Puisque $g \in \mathcal{O}_{\mathfrak{P}}$, on a $\nu_{\mathfrak{P}}(g) \geq 0$ et on peut alors écrire

$$G[\mathfrak{P}] = \sum_{i=0}^{\infty} c_i t^i \in \overline{K}((t)).$$

Pour $n \in \mathbb{N}$, posons

$$G[\mathfrak{P}]^{(n)} := (c_0, c_1, \ldots, c_{n-1}) \in \overline{K}^n.$$

L'application

$$\begin{array}{rccc} \psi_{n\mathfrak{P}} : & S_d \cup \{ 0 \} & \longrightarrow & \overline{K}^n \\ & G & \mapsto & G[\mathfrak{P}]^{(n)} \end{array}$$

est une application $\overline{K}$-linéaire de noyau

$$\begin{array}{rcl} \ker \psi_{n\mathfrak{P}} & = & \{ G \in S_d \mid \operatorname{ord}(G[\mathfrak{P}]) \geq n \} \cup \{ 0 \} \\ & = & \left\{ G \in S_d \mid \nu_{\mathfrak{P}}\left(\overline{G}^P\right) \geq n \right\} \cup \{ 0 \}. \end{array}$$

Fixons $\{ H_1, H_2, \ldots, H_l \}$ une base[5] de l'espace vectoriel $S_d \cup \{ 0 \}$. Soient

$$\psi_{n\mathfrak{P}}\left(H_j[\mathfrak{P}]^{(n)}\right) = (c_{j,0}, c_{j,1}, \ldots, c_{j,(n-1)}), \quad j = 1, 2, \ldots, l,$$

et considérons la matrice

$$M[n\mathfrak{P}]^{(d)} := \begin{bmatrix} c_{1,0} & c_{1,1} & \cdots & c_{1,(n-1)} \\ c_{2,0} & c_{2,1} & \cdots & c_{2,(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{l,0} & c_{l,1} & \cdots & c_{l,(n-1)} \end{bmatrix}.$$

5. On peut prendre l'ensemble de tous les monômes de degré d et il y en a exactement $l := (d+1)(d+2)/2$.

Alors

$$\nu_{\mathfrak{P}}\left(\sum_{i=1}^{l}\alpha_i\overline{H}_i^{\,P}\right)\geq n \iff [\alpha_1 \ \ \alpha_2 \ \ \cdots \ \ \alpha_l]M[n\mathfrak{P}]^{(d)}=0.$$

Ainsi, pour trouver une base de l'espace vectoriel des polynômes d'interpolation de degré d d'un diviseur effectif

$$B:=n_1\mathfrak{P}_1+n_2\mathfrak{P}_2+\cdots+n_k\mathfrak{P}_k$$

il suffit de calculer le noyau à gauche de la matrice

$$M[B]^{(d)}=[M[n_1\mathfrak{P}_1]^{(d)} \ \mid \ M[n_2\mathfrak{P}_2]^{(d)} \ \mid \ \cdots \ \mid \ M[n_k\mathfrak{P}_k]^{(d)}] \tag{2.11}$$

car dans ce cas

$$\left(\sum_{i=1}^{l}\alpha_i H_i\right)\geq B \text{ ou } C \text{ divise } \sum_{i=1}^{l}\alpha_i H_i \iff [\alpha_1 \ \ \alpha_2 \ \ \cdots \ \ \alpha_l]M[B]^{(d)}=0. \tag{2.12}$$

Pour qu'il existe un polynôme d'interpolation G du diviseur B tel que C ne divise pas G, il est clair que le degré de G doit être suffisamment grand.

Proposition 2.7.5 *Soient $\mathcal{C}:=\{\,C=0\,\}$ une courbe projective plane, $B\geq 0$ un diviseur de $\overline{K}(\mathcal{C})$ et $n:=\deg C$.*

1. *Si $n(n+1)/2>\deg B$ alors il existe $G\in S_{n-1}$ tel que $(G)\geq B$.*
2. *Soit $d\in\mathbb{N}$, $d\geq n$. Pour qu'il existe $G\in S_d$ tel que C ne divise pas G et $(G)\geq B$, il suffit que*
$$d>\frac{n}{2}+\frac{\deg B}{n}-\frac{3}{2}.$$

Démonstration : Avant de montrer la proposition, considérons ce qui suit. Soient $d\in\mathbb{N}$ et $\{\,H_1,H_2,\ldots,H_l\,\}$ une base de l'espace vectoriel $S_d\cup\{\,0\,\}$ qui est de dimension $l:=(d+1)(d+2)/2$. Soit la matrice $M[B]^{(d)}$ comme en (2.11) et considérons l'espace vectoriel

$$V_d:=\left\{\sum_{i=1}^{l}\alpha_i H_i \ \mid \ (\alpha_1,\alpha_2,\ldots,\alpha_l)M[B]^{(d)}=0\right\}.$$

Vu (2.12), si $G\in S_d$, alors C divise G ou $(G)\geq B$ si et seulement si $G\in V_d$. De plus, il est clair que

$$\dim_{\overline{K}}V_d=\dim_{\overline{K}}\ker_g M[B]^{(d)}$$

où $\ker_g M[B]^{(d)}$ est le noyau à gauche de la matrice $M[B]^{(d)}$. La matrice $M[B]^{(d)}$ est de dimension $l\times\deg B$ et il est facile de montrer par des arguments simples d'algèbre linéaire que

$$\dim_{\overline{K}}V_d\geq l-\deg B. \tag{2.13}$$

(1). Supposons que $n(n+1)/2 > \deg B$ et que $d = n-1$. Alors

$$\dim_{\overline{K}} V_d \geq l - \deg B = \frac{n(n+1)}{2} - \deg B > 0$$

et par conséquent $V_d \neq \{ 0 \}$. En particulier, pour tout $G \in V_d \setminus \{ 0 \}$ on a $(G) \geq B$ et il est clair que C ne divise pas G car $d < n$.

(2). Supposons que $d \geq n$ et considérons l'espace vectoriel des multiples de C :

$$M := \{ JC \mid J \in S_{d-n} \} \cup \{ 0 \} .$$

Il est clair que $M \subset V_d$ et

$$\dim_{\overline{K}} M = \dim_{\overline{K}}(S_{d-n} \cup \{ 0 \}) = \frac{((d-n)+1)((d-n)+2)}{2}.$$

Pour qu'il existe $G \in V_d \setminus \{ 0 \}$ tel que C ne divise pas G et $(G) \geq B$, il faut et il suffit que

$$\dim_{\overline{K}} V_d - \dim_{\overline{K}} M > 0.$$

Vu (2.13), l'inégalité précédente est satisfaite si

$$l - \deg B - \frac{((d-n)+1)((d-n)+2)}{2} > 0,$$

et cette dernière est équivalente à

$$d > \frac{n}{2} + \frac{\deg B}{n} - \frac{3}{2}.$$

□

Corollaire 2.7.6 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane et $B \geq 0$ un diviseur de $\overline{K}(\mathcal{C})$. Si $d \in \mathbb{N}$ est tel que*

$$d > \max \left\{ n-1, \frac{n}{2} + \frac{\deg B}{n} - \frac{3}{2} \right\}$$

où $n := \deg C$, alors il existe $G \in S_d$ tel que C ne divise pas G et $(G) \geq B$.

Démonstration : C'est une conséquence triviale de la proposition précédente. □

Remarque 2.7.7 La borne du corollaire précédent est la meilleur possible en général. En effet, il existe des cas tels que si $d \leq \max \{ n-1, \frac{n}{2} + \frac{\deg B}{n} - \frac{1}{2} \}$, alors il n'existe pas de polynôme d'interpolation de degré d du diviseur B (voir Chapitre 3, Remarque 3.9.9, page 121).

2.8 Algorithme de Brill-Noether sur un corps fini

Dans toute cette section on fixe $K := \mathbb{F}_q$.

Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K et soient les corps de fonctions $F := K(\mathcal{C})$ et $\overline{F} := \overline{K}(\mathcal{C})$. Dans cette section, on montre comment appliquer l'algorithme de Brill-Noether pour calculer une base de $\mathcal{L}(D)$ où D est un diviseur de F. Pour cela, on étudie d'abord les propriétés de l'extension de corps $K(\mathcal{C}) \subset \overline{K}(\mathcal{C})$.

2.8.1 Extensions algébriques de corps de fonctions

Soient F/K un corps de fonctions, Φ une clôture algébrique de F et $\overline{K} \subset \Phi$ la clôture algébrique de K. Si K' est un corps tel que $K \subseteq K' \subseteq \overline{K}$, on note $K'F$ le compositum de K' et F .

Définition 2.8.1 *Un corps de fonctions F'/K' est une* extension algébrique *(resp.* finie*) d'un corps de fonctions F/K si $\Phi \supseteq F' \supseteq F$, $K' \supseteq K$, et F' est une extension algébrique (resp. finie) de F. Si $F' = K'F$, on dit alors que F'/K' est* obtenue par extension du corps des constantes. *Une place $\mathfrak{P}' \in \mathbb{P}_{F'}$* domine *une place $\mathfrak{P} \in \mathbb{P}_F$ si $\mathfrak{P}' \supseteq \mathfrak{P}$ et dans ce cas on écrit $\mathfrak{P}'|\mathfrak{P}$. On dira aussi que $\mathfrak{P}'|\mathfrak{P}$ est une* extension de places.

Proposition 2.8.2 *Soit F'/K' une extension algébrique de F/K. Les énoncés suivants sont équivalents :*

1. $\mathfrak{P}'|\mathfrak{P}$.

2. $\mathcal{O}_{\mathfrak{P}'} \supseteq \mathcal{O}_{\mathfrak{P}}$.

3. *Il existe un entier $e \geq 1$ tel que $\nu_{\mathfrak{P}'}(x) = e\, \nu_{\mathfrak{P}}(x)$ pour tout $x \in F$.*

Démonstration : Stichtenoth [43, Proposition III.1.4].

La proposition précédente montre que si $\mathfrak{P}'|\mathfrak{P}$, alors il existe une injection canonique des corps résiduels $F_{\mathfrak{P}} \hookrightarrow F'_{\mathfrak{P}'}$.

Définition 2.8.3 *Soient F'/K' une extension algébrique de F/K et $\mathfrak{P}'|\mathfrak{P}$ une extension de places. L'entier $e \geq 1$ défini à la Proposition 2.8.2.(3) s'appelle* l'indice de ramification *de $\mathfrak{P}'|\mathfrak{P}$ et est noté $e(\mathfrak{P}'|\mathfrak{P})$. Le degré de l'extension $F'_{\mathfrak{P}'} \supseteq F_{\mathfrak{P}}$ s'appelle le* degré résiduel *de $\mathfrak{P}'|\mathfrak{P}$ et est noté $f(\mathfrak{P}'|\mathfrak{P})$ (il se peut que $f(\mathfrak{P}'|\mathfrak{P}) = \infty$). Si $e(\mathfrak{P}'|\mathfrak{P}) > 1$ (resp. $e(\mathfrak{P}'|\mathfrak{P}) = 1$), on dit que $\mathfrak{P}'|\mathfrak{P}$ est* ramifiée *(resp.* non ramifiée*).*

PROPOSITION 2.8.4 *Soit F'/K' une extension algébrique de F/K. Toute place $\mathfrak{P} \in \mathbb{P}_F$ est dominée par au moins une et au plus un nombre fini de places de F'/K'. Réciproquement, pour toute place $\mathfrak{P}' \in \mathbb{P}_{F'}$, $\mathfrak{P} := \mathfrak{P}' \cap F$ est une place de F/K et par conséquent l'unique place dominée par $\mathfrak{P}'$.*

Démonstration : Stichtenoth [43, Proposition III.1.7].

L'indice de ramification et le degré résiduel d'une extension de places sont liés au degré de l'extension de corps de fonctions.

THÉORÈME 2.8.5 *Soit F'/K' une extension finie de F/K. Pour toute place $\mathfrak{P} \in \mathbb{P}_F$, on a*

$$\sum_{\mathfrak{P}'|\mathfrak{P}} e(\mathfrak{P}'|\mathfrak{P}) f(\mathfrak{P}'|\mathfrak{P}) = [F' : F].$$

Démonstration : Stichtenoth [43, Théorème III.1.11].

DÉFINITION 2.8.6 *Soit F'/K' une extension algébrique de F/K. La* conorme *d'une place $\mathfrak{P}$ de F/K dans l'extension F'/K' est le diviseur de F'/K' défini par*

$$\mathrm{Con}_{F'/F}(\mathfrak{P}) := \sum_{\mathfrak{P}'|\mathfrak{P}} e(\mathfrak{P}'|\mathfrak{P})\mathfrak{P}'.$$

La conorme *d'un diviseur $D := \sum_{\mathfrak{P}\in\mathbb{P}_F} n_{\mathfrak{P}}\mathfrak{P}$ de F/K est le diviseur de F'/K' défini par*

$$\mathrm{Con}_{F'/F}(D) := \sum_{\mathfrak{P}\in\mathbb{P}_F} n_{\mathfrak{P}} \mathrm{Con}_{F'/F}(\mathfrak{P}).$$

2.8.2 Extension du corps des constantes

On s'intéresse ici aux extensions de corps de fonctions obtenues par extension du corps des constantes. Le théorème suivant regroupe les propriétés les plus remarquables de telles extensions.

THÉORÈME 2.8.7 *Soient F/K un corps de fonctions, $K' \subset \Phi$ une extension algébrique de K et $F' = FK'$.*

1. *K' est le corps des constantes de F'/K'.*

2. *L'extension F'/F est non ramifiée, c'est-à-dire que pour toute extension de places $\mathfrak{P}'|\mathfrak{P}$, on a $e(\mathfrak{P}'|\mathfrak{P}) = 1$.*

3. *Le genre de F'/K' est égal à celui de F/K.*

4. *Soit $W \in \mathcal{D}_F$. Alors W est un diviseur canonique si et seulement si* $\mathrm{Con}_{F'/F}(W)$ *est un diviseur canonique de F'/K'.*

5. *Soit $D \in \mathcal{D}_F$ et posons $D' := \mathrm{Con}_{F'/F}(D)$. Alors*

$$\deg D' = \deg D$$

et

$$\ell\,(D') = \ell\,(D)\,.$$

En particulier,

(a) *une base du K-espace vectoriel $\mathcal{L}(D)$ est une base du K'-espace vectoriel $\mathcal{L}(D')$ et,*

(b) *une base du K'-espace vectoriel $\mathcal{L}(D')$ formée d'éléments de F est une base du K-espace vectoriel $\mathcal{L}(D)$.*

Démonstration : Stichtenoth [43, Prop. III.6.1 et Th. III.6.3].

Ainsi, pour calculer une base de l'espace vectoriel $\mathcal{L}(D)$ où D est un diviseur de F, on appliquera l'algorithme de Brill-Noether au diviseur $D' := \mathrm{Con}_{\overline{F}/F}(D)$ en faisant en sorte que la base obtenue soit formée d'éléments de $K(\mathcal{C})$. À cette fin, lorsque $K = \mathbb{F}_q$, on considère l'application de Frobénius

$$\begin{array}{rccc} \varphi : & \overline{K} & \longrightarrow & \overline{K} \\ & \alpha & \mapsto & \alpha^q. \end{array}$$

Soient $g \in \overline{K}[\mathcal{C}]$ une forme et $G \in S$ un polynôme homogène tel que $g = G + \langle C \rangle$. Posons

$$g^\varphi := G^\varphi + \langle C \rangle$$

où G^φ est défini en faisant agir φ sur les coefficients de G. Puisque C a tous ses coefficients dans K, il est bien évident que $g^\varphi = 0$ si et seulement si $g = 0$. On peut donc prolonger φ au corps $\overline{F}$ comme suit :

$$\begin{array}{rccc} \sigma : & \overline{F} & \longrightarrow & \overline{F} \\ & g/h & \mapsto & g^\varphi/h^\varphi. \end{array}$$

On montrera sans difficulté que

$$(u \in \overline{F}) \quad u \in F \iff \sigma(u) = u,$$

c'est-à-dire que σ est un automorphisme qui laisse fixe le corps F.

Nous allons plus loin étendre σ à l'ensemble des points, des places et des diviseurs. La définition qui suit est classique.

DÉFINITION 2.8.8 *Soit E un ensemble sur lequel l'application σ est étendue. On dit que $a \in E$ est σ-*conjugué *à $b \in E$ s'il existe $i \in \mathbb{N}$ tel que $\sigma^i(a) = b$. On appelle l'ensemble*

$$\mathrm{Orb}_\sigma a := \left\{ \sigma^i(a) \mid i \in \mathbb{N} \right\}$$

*la σ-*orbite *de a.*

Par exemple, la proposition suivante montre qu'on peut étendre σ à l'ensemble des places de F/K.

PROPOSITION 2.8.9 *Soit $\mathfrak{Q}$ un place de $\overline{F}/\overline{K}$.*

1. *$\nu_{\mathfrak{Q}} \circ \sigma$ est une valuation discrète de $\overline{F}/\overline{K}$.*

2. *$\mathfrak{Q}^\sigma := \sigma(\mathfrak{Q})$ est une place de $\overline{F}/\overline{K}$, $\sigma(\mathcal{O}_{\mathfrak{Q}}) = \mathcal{O}_{\mathfrak{Q}^\sigma}$ et $\nu_{\mathfrak{Q}^\sigma} \circ \sigma = \nu_{\mathfrak{Q}}$.*

3. *Soient $\mathfrak{P} := \mathfrak{Q} \cap F$ et $r := \deg \mathfrak{P}$. Alors $\mathfrak{Q}^{\sigma^r} = \mathfrak{Q}$ et*

$$\mathrm{Con}_{\overline{F}/F}\mathfrak{P} = \sum_{\mathfrak{Q}' \in \mathrm{Orb}_\sigma \mathfrak{Q}} \mathfrak{Q}'.$$

Démonstration : Les assertions (1) et (2) sont évidentes du fait que σ est un automorphisme du corps $\overline{F}$ tel que $\sigma(\alpha) \in \overline{K}$ pour tout $\alpha \in \overline{K}$.

(3). D'après le Théorème 2.8.7, on a $\deg \mathfrak{P} = \deg \mathrm{Con}_{\overline{F}/F}\mathfrak{P}$. D'autre part, puisque σ laisse fixe le corps F, on a $\mathfrak{Q}^{\sigma^i}|\mathfrak{P}$ quel que soit $i \in \mathbb{N}$. Il suffit donc de montrer que les places $\mathfrak{Q}^{\sigma^i}$ sont deux à deux distinctes pour $i = 0, 1, \ldots, r-1$. Soient $u \in \mathcal{O}_{\mathfrak{P}}^*$ et $p \in K[T]$ un polynôme irréductible de degré r tels que $p(u) \in \mathfrak{P}$ (de tels u et p existent car $r = [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : K]$). En posant $\alpha := u(\mathfrak{Q})$, on a $p(\alpha) = p(u(\mathfrak{Q})) = p(u)(\mathfrak{Q}) = 0$ d'où $u - \alpha \in \mathfrak{Q}$. Puisque $u \in F$, on a $\sigma(u) = u$ et donc $u - \sigma^i(\alpha) \in \mathfrak{Q}^{\sigma^i}$ quel que soit $i \in \mathbb{N}$. Soient i, j tels que $0 \leq i \leq j \leq r-1$ et $\mathfrak{Q}^{\sigma^i} = \mathfrak{Q}^{\sigma^j}$. On a $u - \sigma^i(\alpha) - u + \sigma^j(\alpha) = \sigma^j(\alpha) - \sigma^i(\alpha) \in \mathfrak{Q}^{\sigma^i}$ d'où $\sigma^j(\alpha) - \sigma^i(\alpha) = 0$ d'après la Proposition 1.2.3. On doit donc avoir $i = j$ car les éléments $\sigma^i(\alpha)$ pour $i = 1, 2, \ldots, r-1$ sont exactement les r racines deux à deux distinctes du polynôme p. $\square$

REMARQUE 2.8.10 D'après la proposition précédente, il est donc suffisant de ne considérer qu'une seule place du support de $\mathrm{Con}_{\overline{F}/F}\mathfrak{P}$ puisqu'on retrouve les autres par l'action de σ. Le même raisonnement s'applique à un diviseur $D := n_1\mathfrak{P}_1 + n_2\mathfrak{P}_2 + \cdots + n_r\mathfrak{P}_r$ du corps de fonctions F/K ; dans ce cas il suffit pour représenter le diviseur $\mathrm{Con}_{\overline{F}/F}(D)$ de ne considérer pour chacune des places $\mathfrak{P}_i \in \mathrm{supp}D$ qu'une place de $\mathrm{suppCon}_{\overline{F}/F}\mathfrak{P}_i$.

Rappelons que l'algorithme de Brill-Noether fait intervenir le diviseur d'adjonction de la courbe $\mathcal{C}$ et les diviseurs d'intersection de polynômes homogènes avec la courbe. La question suivante se pose : ces diviseurs sont-ils les conormes de diviseurs du corps de fonctions F/K ? Afin de mieux formuler cette question et d'y répondre, on a la définition suivante :

DÉFINITION 2.8.11 *Soit σ l'application de Frobénius prolongée au corps $\overline{F}$.*

1. *Soit $D := \sum n_{\mathfrak{Q}}\mathfrak{Q}$ un diviseur de $\overline{F}/\overline{K}$. On appelle le diviseur*

$$D^\sigma := \sum n_{\mathfrak{Q}}\mathfrak{Q}^\sigma$$

le diviseur conjugué *à D par σ. Si D est tel que $D^\sigma = D$, on dit alors que D est* rationnel *sur K.*

2. *Soit $P := (\ a, b\ ;\ x, y\ )$ un point de $\overline{F}/\overline{K}$. On appelle*

$$P^\sigma := (\ \sigma(a), \sigma(b)\ ;\ \sigma(x), \sigma y\ )$$

le point conjugué *à P par σ.*

3. *Soit $\mathcal{T}_P$ l'arbre de désingularisation du point P. L'*arbre conjugué *à $\mathcal{T}_P$ par σ est l'arbre défini récursivement par*

   (a) $\mathcal{T}_P^\sigma := [P^\sigma, E_P^\sigma]$, si P est une feuille,

   (b) $\mathcal{T}_P^\sigma := \big\{\, [P^\sigma, E_P^\sigma], \big\{\, \mathcal{T}_Q^\sigma \ \mid\ Q \in \mathcal{E}cl(P) \,\big\}\, \big\}$, sinon.

Le lemme qui suit est une conséquence de la Proposition 2.8.9.

LEMME 2.8.12 *Soit D un diviseur de $\overline{F}/\overline{K}$. Il existe un diviseur A de F/K tel que $\mathrm{Con}_{\overline{F}/F}A = D$ si et seulement si D est rationnel sur K.*

On démontre alors sans peine le lemme suivant et son corollaire.

LEMME 2.8.13 *Soit P un point de $\overline{F}/\overline{K}$.*

1. *P^σ est un point de $\overline{F}/\overline{K}$.*

2. *Soit $\mathfrak{Q}$ une place de $\overline{K}/\overline{F}$. On a $\mathfrak{Q}|P$ si et seulement si $\mathfrak{Q}^\sigma$ domine P^σ.*

3. *$\mathcal{T}_P^\sigma = \mathcal{T}_{P^\sigma}$.*

4. *Pour tout $u \in \overline{F}$, on a $(u)_P^\sigma = (\sigma(u))_{P^\sigma}$.*

COROLLAIRE 2.8.14 *Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K.*

1. *$P := (a_0 : a_1 : a_2) \in \mathcal{C}$ si et seulement si $P^\sigma := (\sigma(a_0) : \sigma(a_1) : \sigma(a_2)) \in \mathcal{C}$. En particulier, pour tout $P \in \mathcal{C}$, on a $\sigma(\mathcal{O}_P) = \mathcal{O}_{P^\sigma}$; en conséquence, P est singulier si et seulement si P^σ est singulier.*

2. *Le diviseur d'adjonction de la courbe $\mathcal{C}$ est rationnel sur K.*

3. *Le diviseur d'intersection de la courbe $\mathcal{C}$ et d'un polynôme homogène à coefficients dans K est rationnel sur K.*

Les deux corollaires suivants sont des conséquences de la Proposition 2.8.9 et ne seront utilisés qu'au Chapitre 3.

COROLLAIRE 2.8.15 *Soit $P := (\, a, b \,;\, x, y \,)$ un point de $\overline{F}/\overline{K}$ où $\{ x, y \}$ est défini sur K. Soit $\mathfrak{Q}$ une place de $\overline{F}/\overline{K}$ dominant P et posons $\mathfrak{P} := \mathfrak{Q} \cap F$. Alors $[K(a,b) : K]$ divise* $\deg \mathfrak{P}$.

COROLLAIRE 2.8.16 *Soit F/K un corps de fonctions où $K = \mathbb{F}_q$. Soit K' une extension finie de degré r de K et considérons le corps de fonctions F'/K' où $F' := K'F$. Soient de plus $\mathfrak{Q} \in \mathbb{P}_{F'}$ et $\mathfrak{P} := \mathfrak{Q} \cap F$. Si $r := [K' : K]$ divise* $\deg \mathfrak{P}$ *alors* $\deg \mathfrak{P} = r \times \deg \mathfrak{Q}$.

2.8.3 Calcul d'une base de $\mathcal{L}(D)$

Soient $\mathcal{C} := \{ C = 0 \}$, F et $\overline{F}$ comme à la section précédente. Dans cette section, on applique l'algorithme de Brill-Noether pour calculer une base de $\mathcal{L}(D)$ où D est un diviseur de F. Suite à la Remarque 2.8.10, on convient de fixer un ensemble de places $\mathfrak{D} \subset \mathbb{P}_{\overline{F}}$ défini comme suit :

1. pour toute place $\mathfrak{P} \in \mathbb{P}_F$, on choisit une unique place $Q \in \mathrm{suppCon}_{\overline{F}/F}\mathfrak{P}$. Cette place est appelée la place distinguée de $\mathfrak{P}$ et est notée $\overline{\mathfrak{P}} := \mathfrak{Q}$.

2. On fixe une fois pour toute l'ensemble $\mathfrak{D} := \left\{ \overline{\mathfrak{P}} \mid \mathfrak{P} \in \mathbb{P}_F \right\}$.

Observons que l'ensemble $\mathfrak{D}$ est en correspondance biunivoque avec l'ensemble des places de F/K. À tout diviseur $D := \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \mathfrak{P}$ de F/K est associé le diviseur

$$\overline{D} := \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \overline{\mathfrak{P}}$$

qu'on appelle le **diviseur distingué** de D. Si $E := \sum_{\mathfrak{Q}\in\mathbb{P}_{\overline{F}}} n_{\mathfrak{Q}}\mathfrak{Q}$ est un diviseur de $\overline{F}/\overline{K}$ rationnel sur K on lui associe le diviseur

$$\overline{E} := \sum_{\mathfrak{Q}\in\mathfrak{D}} n_{\mathfrak{Q}}\mathfrak{Q}.$$

qu'on appelle le **diviseur distingué** de E. D'après le Lemme 2.8.12, le diviseur $\overline{E}$ est le diviseur distingué d'un diviseur de F/K.

Soient D un diviseur de F/K, $D' := \mathrm{Con}_{\overline{F}/F}(D)$ et $\mathcal{A}$ le diviseur d'adjonction de la courbe $\mathcal{C}$. Pour calculer une base de $\mathcal{L}(D')$, les seules diviseurs utilisés par l'algorithme de Brill-Noether sont les diviseurs $D+\mathcal{A}$, (G_0) et $(G_0)-D$ où G_0 est un polymôme homogène tel que $(G_0)\geq D+\mathcal{A}$. D'après le Lemme 2.8.12, le diviseur D' est rationnel sur K. Il en est de même du diviseur $D+\mathcal{A}$ car $\mathcal{A}$ est rationnel sur K d'après le Corollaire 2.8.14. On peut choisir le polynôme G_0 avec tous ses coefficients dans K et, dans ce cas, le diviseur (G_0) est rationnel sur K. Il suffit alors de ne considérer que les diviseurs distingués et de faire agir l'application de Frobénius seulement lorsque nécessaire. C'est ce que fait l'algorithme suivant qui, en fonction des diviseurs distingués, est une version adaptée de l'algorithme de Brill-Noether donné à la Section 2.7 (Algorithme 2.7.2).

ALGORITHME 2.8.17 **Brill-Noether**($\overline{D}$)

▷ **Entrée :** Le diviseur distingué d'un diviseur D du corps de fonctions $K(\mathcal{C})$ où $\mathcal{C}$ est une courbe projective plane définie sur K.

▷ **Sortie :** Un base de l'espace vectoriel $\mathcal{L}(D)$.

1 : Soit $\overline{\mathcal{A}}$ le diviseur d'adjonction distingué de la courbe $\mathcal{C}$. Posons $B := \overline{D}+\overline{\mathcal{A}}$ et

$$B_+ = n_1\mathfrak{Q}_1 + n_2\mathfrak{Q}_2 + \cdots n_r\mathfrak{Q}_r$$

la partie effective de B où $\mathfrak{Q}_i \in \mathfrak{D}$ et $\mathfrak{Q}_i \neq \mathfrak{Q}_j$ si $i \neq j$.

2 : Soit $d \in \mathbb{N}$ assez grand pour qu'il existe un polynôme[6] homogène $G \in S_d(K)$ non divisible par C tel que $\overline{(G)} \geq B$.

3 : Fixons $\{H_1, H_2, \ldots, H_l\}$ une base de l'espace vectoriel $S_d(K) \cup \{0\}$.

4 : En fonction de la base fixée à l'étape précédente, et pour chacune des places $\mathfrak{Q}_i \in \mathrm{supp}B_+$, déterminer la matrice $M_i := M[n_i\mathfrak{Q}_i]^{(d)}$ (cf. Section 2.7).

5 : Pour chacune des matrices M_i de l'étape précédente, construire la matrice M_i' à l'aide de l'algorithme suivant :

$M_i' := M_i$

Soient $c_1, c_2, \ldots, c_r$ les r colonnes de la matrice M_i'.

6. Observons que si G à tous ses coefficients dans K et que $\overline{(G)} \geq B$, alors $(G) \geq D+\mathcal{A}$. De plus, on peut utiliser le Lemme 2.7.5 pour déterminer l'entier d : il faut prendre garde cependant à l'appliquer au diviseur $D+\mathcal{A}$ et non au diviseur $B = \overline{D}+\overline{\mathcal{A}}$.

Pour $j = 1, 2, \dots, r$ faire

$c := c_j$

Tant que $c_j \neq c^\sigma$ répéter

ajouter la colonne c^σ à la matrice M'_i,

poser $c := c^\sigma$.

Retourner la matrice M'_i.

L'espace vectoriel engendré par les colonnes de la matrice M'_i est laissé invariant par l'action de σ. Note : si $s \in \mathbb{N}^*$ est tel que $\mathfrak{Q}_i^{\sigma^r} = \mathfrak{Q}_i$, alors l'ajout des colonnes correspond à l'ajout des conditions linéaires imposées par les places $\mathfrak{Q}_i^{\sigma^k}$ pour $k = 2, 3, \dots, r-1$.

6 : Calculer $M_i^{(e)}$, la forme colonne-échelonnée de chacune des matrice M'_i. Toutes les matrices $M_i^{(e)}$ sont alors à coefficients dans K.

7 : Calculer un base $\{ b_1, b_2, \dots, b_s \}$ (dans le corps K) du noyau à gauche de la matrice

$$[M_1^{(e)} \mid M_2^{(e)} \mid \cdots \mid M_r^{(e)}].$$

On a

$$b_i = (\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,l}) \in K^l$$

où $l = \dim_K(S_d(K) \cup \{ 0 \}) = (d+1)(d+2)/2$. Soient

$$G_i := \sum_{j=1}^{l} \alpha_{i,j} H_j, \quad i = 1, 2, \dots, s.$$

8 : Si $d \geq \deg C$, alors il faut réduire la base $\{ G_1, G_2, \dots, G_s \}$ modulo l'espace vectoriel

$$V := \{ A \in S_d \mid C \text{ divise } A \}.$$

Pour ce faire, il suffit de choisir une base $\{ A_1, A_2, \dots, A_k \}$ de V avec $A_i \in S_d(K)$ pour $i = 1, 2, \dots, k$ et de compléter cette base en une base

$$\{ A_1, A_2, \dots, A_k, G'_1, G'_2, \dots, G'_{s'} \}$$

de l'espace vectoriel engendré par $\{ G_1, G_2, \dots, G_s \}$. Dans ce cas, l'espace vectoriel $V' \subset S_d(K) \cup \{ 0 \}$ engendré par $\{ G'_1, G'_2, \dots, G'_{s'} \}$ est tel que $V' \setminus \{ 0 \}$ est exactement l'ensemble de tous les polynômes G homogènes de degré d non divisibles par C tels que $\overline{(G)} \geq B_+$.

9 : Choisir $G_0 \in V'$ et calculer le diviseur distingué $\overline{(G_0)}$.

10 : De la même façon qu'aux étapes précédentes, déterminer une base $\{ G_1, G_2, \dots, G_k \}$ de l'espace vectoriel V'' tel que $V'' \setminus \{ 0 \}$ est l'ensemble de tous les polynômes homogènes $G \in S_d$ non divisibles par C tels que $\overline{(G)} \geq \overline{(G_0)} - \overline{D}$.

11 : Poser $g_i := G_i + \langle C \rangle \in K[\mathcal{C}]$ pour $i := 0, 1, 2, \dots, k$ et retourner

$$\{ g_i/g_0 \mid i = 1, 2, \dots, k \}$$

qui est une base de $\mathcal{L}(D)$.

Remarque 2.8.18 Ce qui suit est très important. Considérons les matrices M_i comme définies à l'étape 4 de l'algorithme précédent et pour chacune d'elles, soit K_i la plus petite extension de K contenant tous les coefficients de M_i. À priori, tous les calculs liés aux matrices M_i se font dans la plus petite extension K' de K telle que $K' \supseteq K_i$ pour tout i. Le degré de l'extension K' peut être très grand car on doit avoir $[K' : K] = \text{ppcm}([K_i : K])$. Par contre, les calculs liés à la matrice M_i se font indépendamment de ceux liés à la matrice M_j si $i \neq j$ (voir étapes 5 et 6). Il sera judicieux de tenir compte de ce fait pour l'implantation de l'algorithme, c'est-à-dire de faire en sorte que les calculs liés à la matrices M_i soient faits dans le corps K_i.

Chapitre 3

Algorithmes et implantation en Axiom

Pour tout ce chapitre on fixe $K := \mathbb{F}_q$.

Ce chapitre est consacré au logiciel qui implante l'algorithme de Brill-Noether. J'ai réalisé ce logiciel dans le système de calcul Axiom et je suppose que lecteur connaît ce système, sinon il se reportera à l'Annexe D.

L'algorithme de Brill-Noether nécessite en théorie un corps algébriquement clos, ou du moins une extension suffisamment grande du corps de base. Or, comme on l'a indiqué à la Remarque 2.8.18, on veut être en mesure de considérer à la fois plusieurs extensions distinctes du corps de base. Pour ce faire, on utilise les *extensions dynamiques de corps*. Celles-ci seront définies à la Section 3.1 qui se termine par une description détaillée de l'implantation réalisant les extensions dynamiques de corps. En utilisant les propriétés propres à l'implantation des extensions dynamiques, je développerai, aux Sections 3.2 à 3.5, toutes les procédures sous-jacentes à l'algorithme de Brill-Noether. On trouvera à la Section 3.9 des exemples de constructions de codes géométriques obtenus en utilisant mon logiciel.

En général, pour réaliser l'implantation d'un algorithme dans un système de calcul formel quelconque, on définit d'abord les objets qui seront utilisés et ensuite on implante les algorithmes. En Axiom, une classe d'objets est définie par une *catégorie* et un objet particulier est construit par un *domaine*. Les algorithmes sont, selon leur nature, implantés dans un domaine ou dans un *paquetage*. Logiquement, dans ce chapitre je devrais d'abord présenter les catégories et les domaines que j'ai construits et ensuite présenter les algorithmes. Or, la représentation d'un objet est souvent justifiée par les algorithmes qui l'utiliseront. Pour cette raison, et dans le but de ne pas briser le fil conducteur de l'exposé, j'ai placé à la fin du chapitre (Section 3.8) la présentation de la plupart des catégories et des domaines que j'utiliserai.

3.1 Extensions dynamiques de corps

Soit $\mathcal{C}$ une courbe projective plane définie sur K. Pour appliquer l'algorithme de Brill-Noether comme défini à la Section 2.8.3, deux problèmes se posent :

1. il faut choisir un ensemble de places distinguées du corps de fonctions $\overline{K}(\mathcal{C})$,
2. il faut faire en sorte que les calculs se fassent toujours dans une extension de K aussi petite que possible (cf. Remarque 2.8.18).

La solution à ces deux problèmes repose essentiellement sur la façon dont est construit le corps $\overline{K}$ et cette section est consacrée à une construction particulière de $\overline{K}$, ou plutôt, un simulacre de $\overline{K}$.

Une technique simple de construction d'une clôture algébrique consiste à construire au fur et à mesure des calculs des extensions successives de K. Par exemple, on peut supposer à un instant donné qu'une extension K_1 de K est construite. Par la suite, s'il est nécessaire pour poursuivre les calculs d'avoir une racine d'un polynôme irréductible $p \in K_1[Z]$, on pose

$$\begin{cases} K_2 & := & K_1[Z]/\langle p\rangle \\ \alpha & := & Z + \langle p\rangle. \end{cases}$$

L'élément α est alors une racine de p. Le corps K_2 est une extension de K_1 de degré $\deg p$ et donc une extension de K degré $m := [K_2 : K_1][K_1 : K] = \deg p \times [K_1 : K]$ et on identifie à K_2 l'extension de K de degré m contenue dans $\overline{K}$. Malheureusement, cette construction ne permet pas de mettre à profit la Remarque 2.8.18. En effet, supposons que certains calculs se fassent dans une extension de K de degré 2 indépendamment d'autres dans une extension de degré 3. Soient p_2 et p_3 des polynômes irréductibles de $K[Z]$ de degré 2 et 3 respectivement. En utilisant la construction décrite ci-haut, il faudra alors construire l'extension

$$K_6 := K_2[Z]/\langle p_3\rangle$$

où $K_2 := K[Z]/\langle p_2\rangle$. Par conséquent, tout calcul qui se fait dans une extension de degré 3 de K se fait en réalité dans le corps K_6 et donc de complexité plus élevée que s'il avait été fait dans le corps $K[Z]/\langle p_3\rangle$. Pour remédier à ce problème, il faudra être en mesure de considérer à la fois le corps $K[Z]/\langle p_2\rangle$ et le corps $K[Z]/\langle p_3\rangle$. Pour cela j'utiliserai une version très simplifiée de la clôture algébrique dynamique d'un corps définie par D. Duval [8].

DÉFINITION 3.1.1 *(cf. [8]) Un* objet dynamique *E est un graphe orienté dont les sommets sont des ensembles et les flèches des applications entre ces ensembles et qui* *vérifie les propriétés suivantes :*

1. *Pour tout sommet C, il y a une unique flèche de C dans C, et c'est l'identité de C.*

2. *S'il y a une flèche $f : C \to C'$ et une flèche $f' : C' \to C''$, alors la composée $g = f' \circ f$ est une flèche $g : C \to C''$ de E.*

3. *Étant donnés deux sommets C et C', il y a au plus une flèche de C vers C'.*

4. *La relation notée $\leq$ sur les sommets de E, définie par*

$$C \leq C' \iff \text{il existe une flèche de } C \text{ vers } C'$$

est une relation d'ordre admettant un plus petit élément.

Les sommets maximaux pour l'ordre $\leq$ sont appelés les modèles *de E.*

Définition 3.1.2 *Soit K un corps. Une* extension dynamique *de K est un objet dynamique pour lequel K est l'unique élément minimal pour l'ordre $\leq$ et dont tous les sommets sont des extensions finies de K et les flèches des homomorphismes de corps.*

Remarque 3.1.3 La définition d'extension dynamique est apparentée à la définition de la *clôture algébrique dynamique* d'un corps (cf. [8]) qui est un objet dynamique où seuls les modèles sont des extensions de K et tout autre sommet est une K-algèbre. Cette définition plus générale est nécessaire du fait que la clôture algébrique dynamique d'un corps permet de résoudre des problèmes pouvant avoir plusieurs réponses dépendant par exemple des racines d'un polynôme $p(Z) \in K[Z]$ pas nécessairement irréductible. Or nous n'aurons pas à résoudre ce genre de problème pour nos applications et la Définition 3.1.2 suffira.

Définition 3.1.4 *Une* tour d'extension *T d'un corps K (ou simplement* tour*) de* longueur *n, noté $l(T)$, est une suite finie de n extensions algébriques du corps K*

$$T := \langle K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \rangle$$

où $K_0 := K$ et pour $i = 1, 2, \ldots, n$,

$$\begin{cases} K_i & := & K_{i-1}[Z]/\langle p_i \rangle \\ p_i & \in & K_{i-1}[Z] \text{ est irréductible et } \deg p_i > 1. \end{cases}$$

On note K_T la plus grande extension de la tour T.

Soit T une tour d'extension de K. On appelle

$$\deg_K T := [K_T : K] = \prod_{i=1}^{n} \deg p_i$$

le **degré d'extension** de la tour T. Soit $p \in K_T[Z]$ un polynôme irréductible. On définit une tour $T(P)$ en posant $T(p) := T$ si $\deg p = 1$, sinon

$$T(p) := \langle K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset K_{n+1} := K_n[Z]/\langle p \rangle \rangle.$$

On désigne par $T^{(i)}$ la **sous-tour** de longueur i :

$$T^{(i)} := \langle K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_i \rangle.$$

On définit un ordre partiel sur l'ensemble des tours d'extension de K par

$$T_1 \leq T_2 \iff l(T_1) \leq l(T_2) \text{ et } T_1 = T_2^{(l(T_1))}.$$

On écrira $T_1 \prec T_2$ s'il existe un polynôme irréductible $p \in K_{T_1}$ de degré $\deg p > 1$ tel que $T_2 = T_1(p)$. L'ensemble de toutes les tours possède un plus petit élément, soit la tour d'extension triviale $T^{(0)} := \langle K \rangle$. On note $\mathfrak{T}_K$ l'ensemble de toutes les tours d'extension de K. On a le lemme suivant.

Lemme 3.1.5 *Le graphe orienté tel que*

1. *les sommets sont des extensions K_T où $T \in \mathfrak{T}_K$,*
2. *les flèches sont les homomorphismes d'inclusions $K_{T_1} \hookrightarrow K_{T_2}$ existant seulement que pour les tours T_1 et T_2 telles que $T_1 \prec T_2$,*

est une extension dynamique de K.

Soit T une tour d'extension. Pour des considérations relatives à l'implantation des extensions dynamiques, on veut, pour tout élément $a \in K_T$, être en mesure d'identifier la plus petite sous-tour $T' \leq T$ telle que $a \in K_{T'}$. Pour cela, on considère l'ensemble

$$K^D := \{ (a, T) \mid T \in \mathfrak{T}_K, a \in K_T \text{ et } a \notin K_{T^{(i)}} \text{ si } i < l(T) \}. \tag{3.1}$$

Ainsi, $(a, T) \in K^D$ si $a \in K_T$, et a n'appartient à aucun sous-corps propre de K_T donné par les sous-tours de T. Par exemple, si $T := \langle K \subset K_1 \rangle$ où

$$\begin{cases} K_1 & := K[Z]/\langle p_1 \rangle \\ p_1 & \in K[Z] \text{ est irréductible et } \deg p_1 > 1 \end{cases}$$

et $\alpha := Z + \langle p_1 \rangle \in K_1$, alors $(\alpha, T) \in K^D$. Par contre, $(a, T) \notin K^D$ pour tout $a \in K$. À tout élément $\alpha := (a, T) \in K^D$ est associé sa **tour de définition** $T(\alpha) := T$.

Deux éléments $\alpha := (a, T_1), \beta := (b, T_2) \in K^D$ sont dits **liés** si $T_1 \leq T_2$ ou $T_1 \geq T_2$ et on le note $\alpha \sim \beta$. Dans ce cas, on définit une addition et une multiplication :

$$\begin{array}{rcll} \alpha + \beta & := & (a + b\ ,\ T), & \text{où } T := \min\{\, T' \leq \max\{\, T_1, T_2 \,\} \mid a + b \in K_{T'} \,\}, \\ \alpha \times \beta & := & (a \times b\ ,\ T), & \text{où } T := \min\{\, T' \leq \max\{\, T_1, T_2 \,\} \mid a \times b \in K_{T'} \,\}. \end{array}$$

Notons que le corps K se plonge dans K^D par l'application

$$\begin{array}{rcl} K & \longrightarrow & K^D \\ a & \mapsto & (a, T^{(0)}). \end{array}$$

Soit T une tour d'extension et considérons l'ensemble

$$K_T^D := \left\{\, (a, T') \in K^D \;\mid\; T' \leq T \,\right\}.$$

On a l'application bijective

$$\begin{array}{rrcl} \psi_T : & K_T & \longrightarrow & K_T^D \\ & a & \mapsto & (a, T') \end{array}$$

où $T' := \min\{\, T'' \leq T \mid a \in K_{T''} \,\}$. Si $a, b \in K_T$, alors

$$\begin{array}{rcl} \psi_T(a + b) & = & \psi_T(a) + \psi_T(b) \\ \psi_T(a \times b) & = & \psi_T(a) \times \psi_T(b). \end{array}$$

En fait, K_T^D muni des opérations d'addition et de multiplication de K^D est un corps isomorphe à K_T. En particulier, tout sous-corps de $\overline{K}$, voire même $\overline{K}$, s'identifie à une partie de K^D.

Remarque 3.1.6 À cause de la Remarque 2.8.18, il est clair qu'on ne veut pas identifier un élément de $\overline{K}$ à un unique élément de K^D : on veut plutôt identifier un élément de $\overline{K}$ à un élément de K_T^D en fonction d'une tour d'extension T de notre choix. Pour ce faire, il faut pour toute tour T fixer un K-homomorphisme

$$\varphi_T : K_T^D \longrightarrow \overline{K}.$$

De la sorte, on identifiera $a \in \varphi_T(K_T^D) \subset \overline{K}$ à l'élément α tel que $\varphi_T(\alpha) = a$. De plus, on exigera que cette identification soit cohérente avec la relation d'ordre partiel sur les tours : si T_1 et T_2 sont deux tours telles que $T_1 \leq T_2$ il faut que

$$\varphi_{T_2}|_{K_{T_1}} = \varphi_{T_1}.$$

Dans ce cas, si $a, b \in \overline{K}$ s'identifient respectivement à $\alpha, \beta \in K^D$ et si $\alpha \sim \beta$, on a alors

$$\varphi_T(\alpha + \beta) = \varphi_T(\alpha) + \varphi_T(\beta) = a + b$$

pour toute tour T telle que $T \geq \max\{\, T(\alpha), T(\beta) \,\}$.

3.1.1 Racines distinguées

Dans tout le reste du chapitre, on suppose fixé, pour toute tour d'extension T, un K-homomorphisme

$$\varphi_T : K_T^D \longrightarrow \overline{K}$$

comme à la Remarque 3.1.6. De plus, on identifie le corps K_T à $\varphi_T(K_T^D)$. Bien que deux tours T_1 et T_2 telles que $\deg_K T_1 = \deg_K T_2$ identifient le même sous-corps[1] de $\overline{K}$, on admettra implicitement que les calculs effectifs se font dans le corps $K_{T_i}^D$ lorsque la tour T_i est considérée.

J'introduis ici la notion *d'éléments distingués* de K^D qui sera suffisante pour déterminer un ensemble de places distinguées d'un corps de fonctions.

DÉFINITION 3.1.7 *Soit T une tour d'extension. On dit qu'un élément $\alpha := (a, T') \in K^D$ est T-*distingué *si l'une des deux propriétés suivantes est respecté.*

1. $T' \leq T$.

2. $T' := T(p)$ où $p \in K_T[Z]$ est irréductible, $\deg p > 1$ et $a := Z + \langle p \rangle$.

*Si $T = T^{(0)}$, on dira aussi que α est K-*distingué*. Les* racines T-distinguées *d'un polynôme $q \in K_T[Z]$ sont tous les éléments T-distingués $\alpha \in K^D$ tels que $q(\alpha) = 0$.*

Ainsi, à un élément T-distingué $\alpha := (a, T_\alpha) \in K^D$ correspond un unique polynôme irréductible $p \in K_T[Z]$:

1. si $T_\alpha \leq T$, alors à α correspond le polynôme irréductible $Z - a$,

2. sinon $T_\alpha > T$, et dans ce cas, à α correspond le polynôme irréductible $p \in K_T[Z]$ tel que $T(p) = T_\alpha$.

La proposition suivante est alors évidente.

PROPOSITION 3.1.8 *Soit T une tour d'extension et posons $r := \deg_K T$. L'ensemble des éléments T-distingués de K^D est en correspondance biunivoque avec l'ensemble des σ^r-orbites $\left\{ \mathrm{Orb}_{\sigma^r} a \mid a \in \overline{K} \right\}$. Si $\alpha \in K^D$ est T-distingué, cette correspondance est donnée par*

$$\alpha \mapsto \mathrm{Orb}_{\sigma^r}\left(\varphi_{T_\alpha}(\alpha)\right)$$

où T_α est la tour de définition de α .

1. C'est une conséquence du fait que toute extension d'un corps fini est normale et séparable.

On utilisera l'algorithme suivant pour déterminer les racines T-distinguées d'un polynôme $q \in K_T[Z]$.

ALGORITHME 3.1.9 **RacinesDistinguées**(q, T)

▷ **Entrée :** Un polynôme $q \in K_T[Z]$ où T est une tour d'extension de K.

▷ **Sortie :** Les racines T-distinguées de q.

1 : Factoriser q dans l'anneau $K_T[Z]$;

$$q := \prod_{i=1}^{l} p_i^{d_i}.$$

2 : **retourner** pour $i = 1, 2, \ldots, l$,

$$\alpha_i := \begin{cases} (a, T) & \text{si } p_i = Z - a \\ (Z + \langle p_i \rangle \ , \ T(p_i)) & \text{sinon.} \end{cases}$$

REMARQUE 3.1.10 Pour factoriser un polynôme $p \in K_T[Z]$, on peut utiliser l'algorithme de factorisation probabiliste dû à Cantor-Zassenhauss (cf. [32, 4]. Voir aussi [3]). Il suffit pour cet algorithme de connaître le nombre d'éléments du corps K_T et de pouvoir choisir aléatoirement des éléments de K_T.

3.1.2 Implantation

Soient T une tour d'extension et $\alpha = (a, T) \in K^D$. Si $T = T^{(a)}$, alors α s'identifie à un élément de K. Sinon, soient $T' \prec T$ et $p \in K_{T'}[Z]$ tel que $T'(p) = T$. Posons $b := Z + \langle p \rangle \in K_T = K_{T'}[Z]/\langle p \rangle$. Puisque $a \in K_T$, il existe $\gamma_0, \gamma_1, \ldots, \gamma_{r-1} \in K_{T'}$, où $r := \deg p$, tels que

$$a = \sum_{i=0}^{r-1} \gamma_i b^i.$$

Par conséquent, l'élément a s'identifie à un polynôme de $K_{T'}$. Or $K_{T'}$ est isomorphe à $K^D_{T'} \subset K^D$ et donc a s'identifie à un élément de "l'anneau" de polynôme $K^D[Z]$. D'autre part, le polynôme p suffit à identifier la tour T. Or, tout comme a, le polynôme p s'identifie à un élément de $K^D[Z]$. Par conséquent, tout élément de K^D peut être représenter par un élément de l'ensemble

$$\mathcal{E} := K \cup \left(K^D[Z] \times K^D[Z]\right).$$

En fait, K^D a une structure récursive : il se sert de lui-même pour se définir !

CODE AXIOM 3.1.11 *Le domaine qui implante K^D appartient à la catégorie*

```
PseudoAlgebraicClosureOfFiniteFieldCategory:Category  == Exports where
```

```
  SUP ==> SparseUnivariatePolynomial
  Exports == FiniteFieldCategory with
    distinguishedRootsOf: (SparseUnivariatePolynomial $,$) -> List $
    newElement: (SUP($), $, Symbol) -> $
    setTower_!: $ -> Void
    related_? : ($,$) -> Boolean
    extDegree: $ -> PositiveInteger
    maxTower: List $ -> $
```

Code Axiom 3.1.12 *Le domaine d'Axiom réalisant K^D utilisera l'ensemble $\mathcal{E}$ pour représenter ses éléments.*

```
)abbreviation  domain  PACOFF  PseudoAlgebraicClosureOfFiniteField
PseudoAlgebraicClosureOfFiniteField(K):Exports == Implementation where
  K:FiniteFieldCategory
  SUP ==> SparseUnivariatePolynomial
  recRep ==> Record(recEl:SUP($),_
                    recTower:SUP($),_
                    recDeg:PositiveInteger,_
                    recPrevTower:$,_
                    recName:Symbol)
  Exports == Join(PseudoAlgebraicClosureOfFiniteFieldCategory,_
                  ExtensionField(K))
  Implementation == add
    Rep := Union(recRep,K)
    ...
```

Le "Record" "recRep" réalise l'ensemble $\mathcal{R} := K^D[Z] \times K^D[Z]$. Les *sélecteurs* "recTower" et "recEl" réfèrent respectivement à une tour d'extension T et à un élément $a \in K_T$. Les trois autres sélecteurs sont secondaires : "recDeg" correspond au degré de la tour T, "recPrevTower" correspond à la tour d'extension précédente $T' \prec T$ et le sélecteur "recName" n'est utilisée que pour l'affichage à l'écran des éléments du domaine.

Lorsque l'on implante un domaine algébrique, la première fonction qu'il faut coder est le test d'égalité :

Code Axiom 3.1.13 *Test d'égalité du domaine* PACOFF.

```
    b:$ = a:$ : Boolean ==
      -- Si les tours d'extension respectives associées aux éléments
      -- a et b ne sont pas de même degré alors a n'est pas égal à b.
      not( extDegree(b) = extDegree(a) ) => false
      -- si b est un élément de K (et donc a aussi),
      -- on appelle le test d'égalité du corps K.
      (b case K)  =>  a =$K b
```

```
-- Si les tours d'extension sont différentes,
-- alors a n'est pas égal à b.
-- Notons que le test d'égalité de deux polynômes
-- appartenant à SUP($) se fait sur les coefficients.
-- Par conséquent, le test d'égalité =$SUP($)
-- appellera récursivement le test d'egalité
-- sur les éléments de PACOFF.
not (a.recTower =$SUP($) b.recTower) => false
-- À ce stade, a et b sont définis par la même
-- tour d'extension. On teste donc l'égalité
-- des sélecteurs recEl respectifs.
rdb.recEl =$SUP($) rda.recEl
```

Il est facile de coder l'addition et la multiplication des éléments du domaine "`PACOFF`" :

Code Axiom 3.1.14 *Addition du domaine* `PACOFF`.

```
a:$ + b:$ ==
  ---------------------------------------
  -- ATTENTION: On suppose a et b liés !!
  ---------------------------------------
  -- si a et b sont des éléments de K
  -- on additionne dans K.
  (a case K) and (b case K) => a +$K b
  -- si b est dans un sous-corps propre  du corps
  -- contenant a, on commute l'addition.
  extDegree(b) < extDegree(a)  => b + a
  extDegree(a) = extDegree(b) =>
    -- Ici a et b sont dans la même extension.
    -- On additionne donc les sélecteurs recEl en les
    -- considérant comme des polynômes non
    -- constant.
    tmp:=   b.recEl +$SUP($) a.recEl
    -- on prend une copie du Record de b
    -- (sinon gare aux effets de bord!)
    -- et on assigne tmp au sélecteur
    -- recEl de b.
    bb:= copy b
    bb.recEl := tmp
    -- on retourne le résultat au plus bas niveau
    down bb
  -- Ici, a est dans un sous-corps propre de l'extension
  -- de corps contenant b. On considère donc
  -- a.recEl  comme un polynôme constant par rapport
  -- au polynôme b.recEl.
```

```
aMono:=  monomial(a,0)$SUP($)
tmp:=  b.recEl +$SUP($) aMono
bb:= copy b
bb.recEl := tmp
down  bb
```

Le code de la multiplication est similaire à celui de l'addition à la différence qu'il faut calculer modulo le polynôme qui définit la tour d'extension :

Code Axiom 3.1.15 *Multiplication du domaine* `PACOFF`.

```
a:$ * b:$ ==
  -- ATTENTION: a et b sont supposés liés !!
  (a case K) and (b case K) => a *$K b
  extDegree(a) > extDegree(b) => b * a
  extDegree(a) = extDegree(b) =>
    tmp:= b.recEl *$SUP($) a.recEl rem b.recTower
    bb := copy b
    bb.recEl:=tmp
    down bb
  aMono:=  monomial(a,0)$SUP($)
  tmp := b.recEl *$SUP($) aMono
  bb:= copy b
  bb.recEl
  down bb
```

Rappelons que l'addition et la multiplication d'éléments de K^D sont définies par

$$\begin{aligned}\alpha + \beta \;&:=\; (a+b\,,\,T), \quad \text{où } T := \min\{\,T' \le \max\{\,T_1, T_2\,\} \;\mid\; a+b \in K_{T'}\,\},\\ \alpha \times \beta \;&:=\; (a\times b\,,\,T), \quad \text{où } T := \min\{\,T' \le \max\{\,T_1, T_2\,\} \;\mid\; a\times b \in K_{T'}\,\}.\end{aligned}$$

Le code donné plus haut pour l'addition et la multiplication est correct dans la mesure où la tour T associée au résultat est correctement déterminée et c'est le rôle de la fonction "`down`" de faire en sorte qu'il en soit ainsi. Cette fonction permet de ramener au plus bas niveau la représentation récursive des éléments de "`PACOFF`" :

Code Axiom 3.1.16

```
down(a:$) ==
  -- si a est déjà au niveau de K on retourne a.
  a case K => a
  -- on teste si a.recEl n'est pas une constante
  -- en tant que polynôme de SUP($).
  -- Si c'est le cas on retourne a.
  ^ground?(a.recEl) => a
  -- Sinon, on retire la constante du polynôme
```

```
    -- a.recEl que l'on considère alors
    -- comme un élément du domaine et
    -- non plus comme un polynôme et on appelle récursivement down
    -- sur cette constante.
    gel:$:=ground(a.recEl)
    down(gel)
```

On définit maintenant le calcul de l'inverse des éléments de "`PACOFF`". Soit $\alpha := (a, T) \neq 0$ tel que $T > T^{(0)}$. Soient de plus la tour $T_0 \prec T$, le polynôme $q \in K_{T_0}[Z]$ tel que $T = T_0(q)$ et le polynôme $p \in K_{T_0}[Z]$ tel que $a = p + \langle q \rangle$. Pour calculer l'inverse de α, il suffit d'appliquer l'algorithme d'Euclide étendu aux polynômes p et q. Il est clair que $\mathrm{pgcd}(p, q) = 1$ par définition de α. L'algorithme d'Euclide étendu retourne alors deux polynômes $s \in K_{T_0}[Z]$ et $t \in K_{T_0}[Z]$ tels que

$$1 = sp + tq.$$

Il est clair que $a^{-1} \in K_T \setminus K_{T_0}$ car par définition de α on a $a \in K_T \setminus K_{T_0}$. Par conséquent, $\alpha^{-1} = (b, T)$ où $b := s + \langle q \rangle$. Le code suivant utilise la fonction "`extendedEuclidean`" déja fourni avec Axiom.

Code Axiom 3.1.17 *Calcul de l'inverse des éléments de* `PACOFF`*.*

```
inv(a)==
  a case K => inv(a)$K
  aRecEl:= a.recEl
  aDefPoly:= a.recTower
  aInv := extendedEuclidean( aRecEl , aDefPoly, 1 )
  aInv  case "failed" => error "PACOFF : division by zero"
  -- On doit retourner un Record représentant l'inverse de a.
  -- Ce Record est exactement le même que celui de a sauf
  -- qu'il faut remplacer le polynôme du selecteur recEl
  -- par le polynôme représentant l'inverse de a :
  -- C'est ce que fait la fonction replaceRecEl.
  replaceRecEl( a , aInv.coef1 )
```

Voici le code de la la fonction "`newElement`" qui crée une racine T-distinguée d'un polynôme irréductible $p \in K_T[Z]$:

Code Axiom 3.1.18

```
newElement(p:SUP($),grdFld:$,inName:Symbol): $ ==
  -- p est un polynôme irréductible à coefficients
  -- dans le corps défini par la tour d'extension T
  -- associée à l'élément grdFld. La variable inName
  -- ne sera utilisée que pour l'affichage.
```

```
  -- Si p est une constante, on ne peut pas créer un nouvel élément.
  ground?(p) => error "Cannot create a new element with a constant"
  dp:=degree p
  one?(dp) =>
    -- ici, p est de la forme aZ+b.
    -- on retourne 0 si b = 0, sinon on retourne -b/a.
    listCoef:=coefficients(p)
    one?(#listCoef) => 0
    - last(listCoef) / first(listCoef)
  -- on calcule le degré de l'extension dans laquelle le nouvel
  -- élément est défini.
  d:= dp  * extDegree(grdFld)
  -- on retourne le représentant de l'élément distingué (Z + <p>, T(p)).
  [monomial(1,1),p,d,grdFld,inName]
```

Pour calculer les racines d'un polynôme quelconque $q \in K_T[Z]$, il faut être en mesure de factoriser dans l'anneau $K_T[Z]$. Pour cela, on utilisera l'algorithme de Cantor-Zassenhauss et il faut alors engendrer aléatoirement des éléments du domaines "`PACOFF`" qui représentent des éléments du corps K_T. De plus, tout paquetage implantant l'algorithme de Cantor-Zassenhauss doit connaître le nombre d'éléments du corps sur lequel il doit factoriser, et fera alors appelle à la fonction "`size`" qui est exportée par la catégorie "`FiniteFieldCategory`". Il faut donc implanter cette fonction et faire en sorte que l'on puisse contrôler à volonté son résultat :

Code Axiom 3.1.19

```
-- variables locales au domaine PACOFF
localTower :$   := 1$K
localSize  :NNI := size()$K

setTower!(a) ==
  -- on assigne a localTower sa nouvelle valeur.
  -- De la sorte, le domaine PACOFF représentera
  -- le corps K_T où T est la tour d'extension
  -- associée à l'élément a
  localTower:=a
  -- on calcule le nombre d'éléments de K_T
  localSize:=(size()$K)**extDegree(a)
  -- et on retourne ... rien.
  void()

size ==
  -- on retourne le nombre d'éléments
  -- du corps K_T spécifié par le dernier
```

```
  -- appel de setTower!
  localSize
```

Pour choisir aléatoirement un élément du corps K_T spécifié par le dernier appel de la fonction "`setTower!`", on a le code suivant :

Code Axiom 3.1.20

```
localRandom(a) ==
  -- Cette fonction est locale au domaine PACOFF.
  -- Elle retourne un élément choisi aléatoirement
  -- dans le corps K_T où T est la tour d'extension
  -- associée à l'élément a.
  -- Si a appartient à K alors on appelle la fonction random de K.
  a case K => random()$K
  -- Sinon, on construit un polynôme de K_T'[Z] où
  -- T' est la tour précédente à T et qui est
  -- donné par le sélecteur recPrevTower de a.
  -- Ce polynôme représentera un élément de K_T. Les coefficients
  -- du polynmôme sont choisis aléatoirement par un appel
  -- récursif de localRandom avec a.recPrevTower.
  subTower:=a.recPrevTower
  d:=degree(a.recTower)-1
  polAlea:=reduce("+",[monomial(localRandom(subTower),i)$SUP($)
                     for i in 0..d])
  aa:= copy a
  aa.recEl := polAlea
  down aa

random ==
  -- On retourne un élément aléatoire
  -- du corps K_T spécifié par le dernier
  -- appel de setTower!
  localRandom localTower
```

Pour calculer les racines T-distinguées d'un polynôme quelconque $q \in K_T[Z]$, on a :

Code Axiom 3.1.21

```
distinguishedRootsOf(q,T) ==
    setTower!(T)
    zero?(q) =>
      -- il ne faut tout de même pas retourner
      -- tous les éléments de PACOFF !!!
      error "to lazy to give you all the roots of 0 !!!"
    -- on factorise le polynôme q sur le corps K_T
```

```
    -- spécifié par setTower!(T)
    factorq := factor(q)$FFFACTOR($,SUP($))
    -- on retire tous les facteurs irréductibles
    -- deux à deux distincts de la factorisation.
    listFact:List SUP $ := [pol.fctr for pol in factorList(factorq)]
    -- pour chacun des facteurs irréductibles, on crée un
    -- nouvel élément.
    listOfZeros:List($):=empty()
    for p in listFact repeat
      root:=newElement( p, T, new(D::Symbol)$Symbol )
      listOfZeros:=cons( root , listOfZeros)
    -- on retourne la liste des racines T-distinguées
    -- créées par la fonction newElement.
    listOfZeros
```

Le paquetage “`FFFACTOR`” (abréviation de “`FiniteFieldFactorization`”) implante l’algorithme de Cantor-Zassenhauss et a été réalisé par C. Quitté et P. Naudin. On utilisera la fonction “`distinguishedRootsOf`” par l’intermédiaire d’un paquetage :

Code Axiom 3.1.22

```
RootsFindingPackage(K):Exports == Implementation where
  K:Field
  SUP ==> SparseUnivariatePolynomial
  -- Le selecteur extDegree du Record REC indiquera le degré
  -- de l'extension de K qui contient toutes les racines du
  -- polynôme si le domaine K n'appartient pas à la catégorie
  -- PseudoAlgebraicClosureOfFiniteFieldCategory.
  REC ==> Record(zeros:List(K),extDegree:INT)
  Exports == with
    distinguishedRootsOf: (SUP(K),K) -> REC
  Implementation == add
    distinguishedRootsOf(p, T) ==
      K has PseudoAlgebraicClosureOfFiniteFieldCategory =>
        zero?(p) =>
          -- le message d'erreur qui devrait apparaitre ici
          -- sera plutôt retourné par le paquetage appelant
          -- cette fonction.
          [empty(),0]
        listOfZeros:List(K):=distinguishedRootsOf(p,T)$K
        [listOfZeros,1]
      -- Si K n'appartient pas à la catégorie
      -- PseudoAlgebraicClosureOfFiniteFieldCategory,
      -- on retourne toutes les racines du polynôme p.
      ...
```

3.2 Ensembles algébriques

Revenons maintenant au problème de déterminer un ensemble des places distinguées du corps de fonctions $\overline{K}(\mathcal{C})$. On sait qu'une place de $\overline{K}(\mathcal{C})$ domine un et un seul point de $\mathcal{C}$. De plus, si $\mathfrak{D}$ est un ensemble de places distinguées de $\overline{K}(\mathcal{C})$, il est clair que

$$\mathcal{C}_{\mathfrak{d}} := \{\, P \in \mathcal{C} \mid \text{ il existe } \mathfrak{P} \in \mathfrak{D} \text{ tel que } \mathfrak{Q}|P \,\}$$

est en correspondance biunivoque avec les σ-orbites des points de $\mathcal{C}$. En particulier, si $\mathcal{C}$ est lisse, alors $\mathcal{C}_{\mathfrak{d}}$ est biunivoque à $\mathfrak{D}$. Sinon, pour obtenir un ensembles de places distinguées, il suffira d'éclater les points singuliers de $\mathcal{C}_{\mathfrak{d}}$ et de choisir convenablement les feuilles des arbres de désingularisation correspondants.

Bien que K^D ne soit pas un corps, il sera utile de considérer le *plan affine* sur K^D.

DÉFINITION 3.2.1 *L'ensemble*

$$\mathbb{A}^2(K^D) := \{\, (\alpha, \beta) \mid \alpha, \beta \in K^D, \alpha \sim \beta \,\}$$

est appelé plan affine *sur K^D. À tout point $P := (\alpha, \beta)$ est associé sa* tour de définition *$T_P := \max\{\, T(\alpha), T(\beta) \,\}$ et son* degré *$\deg P := \deg_K T_P$.*

Observons que l'application

$$\begin{array}{rccc} \varphi : & \mathbb{A}^2(K^D) & \longrightarrow & \mathbb{A}^2 \\ & P := (\alpha, \beta) & \mapsto & (\, \varphi_{T_P}(\alpha), \varphi_{T_P}(\beta)) \end{array} \tag{3.2}$$

est bien définie, surjective mais pas injective. En appliquant la notion d'éléments T-distingués de K^D à $\mathbb{A}^2(K^D)$, je vais établir une correspondance biunivoque entre les σ-orbites de points de $\mathbb{A}^2$ et une partie de $\mathbb{A}^2(K^D)$.

DÉFINITION 3.2.2 *Soit T une tour d'extension. Un point $P := (\alpha, \beta) \in \mathbb{A}^2(K^D)$ est dit* T-distingué *si*

$$\alpha := (a, T_1) \text{ est } T\text{-distingué et } \beta \text{ est } T_1\text{-distingué.}$$

Si $T = T^{(0)}$ et P est T-distingué, on dira aussi que P est K-distingué. L'ensemble des points K-distingués de $\mathbb{A}^2(K^D)$ est noté $\mathbb{A}^2_{\mathfrak{d}}(K^D)$.

PROPOSITION 3.2.3 *L'ensemble des points K-distingués $\mathbb{A}^2_{\mathfrak{d}}(K^D)$ est en correspondance biunivoque avec l'ensemble des orbites de points $\{\, \mathrm{Orb}_\sigma R \mid R \in \mathbb{A}^2 \,\}$. Si $R \in \mathbb{A}^2_{\mathfrak{d}}(K^D)$, cette correspondance est donnée par*

$$P \mapsto \mathrm{Orb}_\sigma \varphi(P)$$

où φ est l'application définie en (3.2).

Démonstration : C'est une conséquence de la Proposition 3.1.8. □

DÉFINITION 3.2.4 *L'ensemble* $\mathbb{A}^2_{\mathfrak{d}} := \varphi(\mathbb{A}^2_{\mathfrak{d}})$ *est appelé le* plan affine distingué.

De façon similaire au plan affine, on définit :

DÉFINITION 3.2.5 *L'ensemble*

$$\mathbb{P}^2(K^D) := \{\, (\alpha_0 : \alpha_1 : \alpha_2) \mid \alpha_i \in K^D, \alpha_i \sim \alpha_j, \text{ il existe } i \text{ tel que } \alpha_i \neq 0 \,\}.$$

est appelé le plan projectif *sur* K^D.

On définit les points T-distingués de $\mathbb{P}^2(K^D)$ comme suit.

DÉFINITION 3.2.6 *Soient T une tour d'extension. Les points T-distingués $\mathbb{P}^2(K^D)$ sont exactement les points :*

1. $P = (1 : 0 : 0)$.
2. $P = (\alpha : 1 : 0)$ *où α est T-distingué.*
3. $P = (\alpha : \beta : 1)$ *où $(\alpha, \beta) \in \mathbb{A}^2(K^D)$ est T-distingué.*

Respectivement aux trois cas précédents, la tour $T^{(0)}$, $T(\alpha)$ ou $\max\{\, T(\alpha), T(\beta) \,\}$ s'appelle la tour de définition *de P et on la note T_P. Si $T = T^{(0)}$ et P est T-distingué on dira aussi que P est K-distingué. L'ensemble des point K-distingués de $\mathbb{P}^2(K^D)$ est noté $\mathbb{P}^2_{\mathfrak{d}}(K^D)$.*

Il est évident que l'application

$$\begin{array}{rccc} \varphi : & \mathbb{P}^2_{\mathfrak{d}} & \longrightarrow & \mathbb{P}^2 \\ & P := (\alpha_0 : \alpha_1 : \alpha_2) & \mapsto & (\varphi_{T_P}(\alpha_0) : \varphi_{T_P}(\alpha_1) : \varphi_{T_P}(\alpha_2)) \end{array} \tag{3.3}$$

est bien définie.

PROPOSITION 3.2.7 *L'ensemble des points K-distingués $\mathbb{P}^2_{\mathfrak{d}}(K^D)$ est en correspondance biunivoque avec l'ensemble des orbites de points $\{\, \mathrm{Orb}_\sigma P \mid P \in \mathbb{P}^2 \,\}$. Si $P \in \mathbb{P}^2_{\mathfrak{d}}(K^D)$, cette correspondance est donnée par*

$$P \mapsto \mathrm{Orb}_\sigma \varphi(P)$$

où φ est l'application définie en (3.3).

Démonstration : C'est une conséquence de la Proposition 3.2.3. □

DÉFINITION 3.2.8 *L'ensemble* $\mathbb{P}^2_{\mathfrak{d}} := \varphi(\mathbb{P}^2_{\mathfrak{d}}(K^D))$ *est appelé* le plan projectif distingué.

DÉFINITION 3.2.9 *Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K. On appelle*

$$\mathcal{C}_{\mathfrak{d}} := \mathcal{C} \cap \mathbb{P}^2_{\mathfrak{d}}$$

*la courbe K-*distinguée *de $\mathcal{C}$.*

Le corollaire suivant est évident. Il fournit un ensemble de places distinguées de $\overline{K}(\mathcal{C})$ dans le cas où $\mathcal{C}$ est une courbe projective plane lisse.

COROLLAIRE 3.2.10 *Soit $\mathcal{C}$ une courbe projective plane lisse et $\mathfrak{D}$ un ensemble de places distinguées de $\overline{K}(\mathcal{C})$. Alors $\mathcal{C}_{\mathfrak{d}}$ est en correspondance biunivoque avec $\mathfrak{D}$.*

DÉFINITION 3.2.11 *Soit $I \in \overline{K}[X, Y]$ un idéal défini sur K. On appelle l'ensemble*

$$\mathcal{V}^D(I) := \left\{ P \in \mathbb{A}^2(K^D) \mid P \text{ est } K\text{-distingué et } G(P) = 0 \text{ pour tout } G \in I \right\}$$

*l'*ensemble algébrique distingué *de I. De même, soit $J \subset S$ un idéal engendré par des polynômes homogènes de $S(K) := K[X_0, X_1, X_2]$. On appelle l'ensemble*

$$\mathcal{V}^D(J) := \left\{ P \in \mathbb{P}^2(K^D) \mid P \text{ est } K\text{-distingué et } G(P) = 0 \text{ pour tout } G \in J \right\}$$

*l'*ensemble algébrique distingué *de J.*

Il est bien évident qu'il suffit de savoir déterminer les ensembles algébriques distingués de $\mathbb{A}^2(K^D)$ pour déduire ceux de $\mathbb{P}^2(K^D)$. De plus, seuls les ensembles algébriques finis seront considérés. Soit donc $I \subset \overline{K}[X, Y]$ un idéal défini sur K dont l'ensemble algébrique $\mathcal{V}(I)$ est fini. Considérons l'ensemble

$$\mathcal{V}_X(I) := \left\{ a \in \overline{K} \mid \text{ il existe } b \in \overline{K} \text{ tel que } (a, b) \in \mathcal{V}(I) \right\}.$$

et posons

$$p(Z) := \prod_{a \in \mathcal{V}_X(I)} (Z - a).$$

D'après le Théorème des zéros de Hilbert, il existe $n \in \mathbb{N}$ assez grand tel que $q := p^n \in I$. D'autre part, puisque $\mathcal{V}(I)$ est laissé invariant par l'action de σ, il en est de même de $\mathcal{V}_X(I)$ et donc $\sigma(p) = p$ d'où $p \in K[Z]$ et $q \in K[Z]$. On a donc

$$a \in \overline{K} \text{ est une racine de } q \iff \text{ il existe } b \in \overline{K} \text{ tel que } (a, b) \in \mathcal{V}(I)$$

ce qui est équivalent à

$$\alpha \in K^D \text{ est } K\text{-distingué et } q(\alpha) = 0 \iff \text{ il existe } \beta \in K^D \text{ tel que } (\alpha, \beta) \in \mathcal{V}^D(I).$$

Pour calculer $\mathcal{V}^D(I)$, on a l'algorithme suivant :

ALGORITHME 3.2.12 **EnsAlg**($\{ G_1, G_2, \ldots, G_r \}$)

▷ **Entrée :** Un ensemble de générateurs $\{ G_1, G_2, \ldots, G_r \} \subset K[X, Y]$ d'un idéal I.

▹ **Sortie :** L'ensemble $\mathcal{V}^D(I)$ s'il est fini. Dans le cas contraire, on quitte l'algorithme avec un message d'erreur.

1 : $V := \emptyset$.

2 : Si $1 \in I$ alors retourner $\emptyset$.

3 : Soit $A := K[X] \cap I$. Si $A = \{ 0 \}$ alors $\mathcal{V}(I)$ n'est pas fini. Dans ce cas, retourner un message d'erreur.

4 : Choisir $q \in A$ et déterminer l'ensemble

$$\{ \alpha_1, \alpha_2, \ldots, \alpha_l \} := \texttt{distinguishedRootsOf}(q, 1) \subset K^D.$$

5 : Pour $i = 1, 2, \ldots, l$ faire

6 : Poser $H_j := G_j(\alpha_i, Y)$ pour $j = 1, 2, \ldots, r$. Si $H_j = 0$ pour tout j, alors $\mathcal{V}(I)$ n'est pas fini. Dans ce cas, retourner un message d'erreur.

7 : $q_i(Y) := \mathrm{pgcd}(\{ H_j \mid j = 1, 2, \ldots, r \})$

8 : $V := V \cup \{ (\alpha_i, \beta) \mid \beta \in \texttt{distinguishedRootsOf}(q_i, \alpha_i) \}$.

9 : **retourner** V.

Remarque 3.2.13 Soit I l'idéal considéré à l'algorithme précédent. Pour déterminer si $1 \in I$ et ensuite $A := K[X] \cap I$ (étapes 2 et 3), il suffit de calculer une base de Groebner B de l'idéal I avec l'ordre lexicographique $X < Y$. De la sorte,

1. $1 \in B$ si et seulement si $1 \in I$,
2. si q est le générateur de l'idéal principal $A := K[X] \cap I$, alors $\{ q \} = B \cap K[X]$.

Pour calculer les ensembles algébriques projectifs distingués, on a :

Algorithme 3.2.14 **EnsAlgProj**$(G_1, G_2, \ldots, G_r)$

▹ **Entrée :** Des générateurs homogènes $G_1, G_2, \ldots, G_r \in S(K)$ d'un idéal J.

▹ **Sortie :** L'ensemble algébrique distingué $\mathcal{V}^D(J) \subset \mathbb{P}^2(K^D)$.

▹ *On calcule les points de la forme $P = (a : b : 1)$*

1 : $V := \{ (a : b : 1) \mid (a, b) \in \textbf{EnsAlg}(G_1(X, Y, 1), G_2(X, Y, 1), \ldots, G_r(X, Y, 1)) \}$.

▹ *On calcule les points de la forme $P = (a : 1 : 0)$*

2 : Poser $g_i := G_i(X, 1, 0)$ pour $i = 1, 2, \ldots, r$. Si $g_1 = g_2 = \cdots = g_r = 0$, alors $\mathcal{V}^D(J)$ possède une infinité de points. Dans ce cas, retourner un message d'erreur.

3 : $p := \mathrm{pgcd}(\{ g_1, g_2, \ldots, g_r \})$.

4 : $V := V \cup \{ (a : 1 : 0) \mid a \in \texttt{distinguishedRootsOf}(p, 1) \}$.

▹ *On vérifie si $P = (1 : 0 : 0) \in \mathcal{V}^D(J)$.*

5 : **si** $0 = G_1(1, 0, 0) = G_2(1, 0, 0) = \cdots = G_r(1 : 0 : 0)$, **alors retourner**

$$V \cup \{ (1 : 0 : 0) \}$$

6 : **sinon retourner** V.

On peut utiliser l'algorithme précédent pour calculer les points singuliers K-distingués d'une courbe projective plane $\mathcal{C} := \{ C = 0 \}$; il suffit de l'appliquer aux polynômes $C_{X_0} := \partial C/\partial X_0$, $C_{X_1} := \partial C/\partial X_1$ et $C_{X_2} := \partial C/\partial X_2$. Or pour déterminer les points singuliers de la forme $(a : b : 1)$, il n'est pas nécessaire de considérer le polynôme C_{X_2} de même qu'il n'est pas nécessaire de considérer le polynôme C_{X_1} pour déterminer les points de la forme $(a : 1 : 0)$. On utilisera donc avantageusement l'algorithme suivant :

Algorithme 3.2.15 **PointsSinguliers**(C)

▷ **Entrée :** Un polynôme homogène $C \in K[X_0, X_1, X_2]$ irréductible (l'absolue irréductibilité n'est pas nécessaire pour cet algorithme).

▷ **Sortie :** L'ensemble des points singuliers K-distingués de la courbe $\mathcal{C} := \{ C = 0 \}$.

$C_{X_0} := \partial C/\partial X_0$, $C_{X_1} := \partial C/\partial X_1$, $C_{X_2} := \partial C/\partial X_2$.

▷ *On calcule les points singuliers de la forme* $P = (a : b : 1)$

$V := \{ (a : b : 1) \mid (a, b) \in \mathbf{EnsAlg}(\{ C(X, Y, 1), C_{X_0}(X, Y, 1), C_{X_1}(X, Y, 1) \}) \}$

▷ *On calcule les points singuliers de la forme* $P = (a : 1 : 0)$

si $C(X, 1, 0) = C_{X_0}(X, 1, 0) = C_{X_2}(X, 1, 0) = 0$, retourner un message d'erreur car dans ce cas il y a une infinité de points singuliers.

$p := \mathrm{pgcd}(\{ C(X, 1, 0), C_{X_0}(X, 1, 0), C_{X_2}(X, 1, 0) \})$

$V := V \cup \{ (a : 1 : 0) \mid a \in$ `distinguishedRootsOf`$(p, 1) \}$.

▷ *On vérifie si* $P = (1 : 0 : 0)$ *est un point singulier*

si $0 = C(1, 0, 0) = C_{X_1}(1, 0, 0) = C_{X_2}(1, 0, 0)$, **alors retourner**

$$V \cup \{ (1 : 0 : 0) \}$$

sinon retourner V.

Il est aussi facile de calculer tous les points d'une courbe qui sont de degré $r \in \mathbb{N}^*$:

Algorithme 3.2.16 **PointsDeDegré**(C, r)

▷ **Entrée :** Un polynôme homogène $C \in K[X_0, X_1, X_2]$ irréductible (l'absolue irréductibilité n'est pas nécessaire pour cet algorithme) et un entier $r \in \mathbb{N}^*$.

▷ **Sortie :** L'ensemble des points K-distingués de la courbe $\mathcal{C} := \{ C = 0 \}$ de degré r, c'est-à-dire

$$\{ P \in \mathcal{C}_{\mathfrak{d}} \mid \deg_K T_P = r \} .$$

$q := \#K$.

$p_X := X^{q^r} - X$.

$p_Y := Y^{q^r} - Y$.

▷ *On calcule les points de la forme* $P = (a : b : 1)$

$V := \{ (a : b : 1) \mid (a, b) \in \mathbf{EnsAlg}(\{ C(X, Y, 1), p_X, p_Y \}) \}$

▷ *On calcule les points de la forme $P = (a : 1 : 0)$*

5 : $p := \mathrm{pgcd}(\{\, C(X,1,0), p_X \,\})$

6 : $V := V \cup \{\, (a : 1 : 0) \mid a \in \texttt{distinguishedRootsOf}(p, 1) \,\}$.

▷ *On vérifie si $P = (1 : 0 : 0) \in \mathcal{C}$.*

7 : **si** $0 = C(1,0,0)$, alors $V := V \cup \{\, (1 : 0 : 0) \,\}$.

8 : **retourner** $\{\, P \in V \mid r = \deg_K T_P \,\}$.

Le paquetage qui réalise les algorithmes précédents est le suivant :

Code Axiom 3.2.17

```
ProjectiveAlgebraicSetPackage(K,S,R,P,...):Exports == Implementation where
  K   : Field        -- un corps quelconque
  S   : List Symbol  -- la liste des variables utilisées ;
                     -- par exemple [X0,X1,X2]
  R   : PolynomialCategory(K,...)
  P   : ProjectivePointCategory(K)
  ...
  Exports ==>  with
    algebraicSet   : List R             -> List P
    singularPoints : R                  -> List P
    pointsOfDegree :(R,PositiveInteger) -> List P
```

3.3 Éclatement de points

Pour les points d'un corps de fonctions, on a une définition similaire à celle des points T-distingués de $\mathbb{A}^2(K^D)$.

Définition 3.3.1 *Soit $P := (\ \alpha, \beta\ ;\ x, y\ )$ un point de $\overline{F}/\overline{K}$. On dit que le point P est T-distingué si $\{\, x, y \,\}$ est défini sur K_T et (α, β) est T-distingué. Si $T = T^{(0)}$ et P est T-distingué, on dit aussi que P est K-distingué.*

Soient $P := (\alpha : \beta : 1)$ un point K-distingué d'une courbe projective plane $\mathcal{C}/K$, T_P sa tour de définition et supposons que $r := [K_{T_P} : K] > 1$. Considérons le point[2] $P_* = (\ \alpha, \beta\ ;\ x, y\ )$ qui est K-distingué et soit $C \in K[X,Y]$ le polynôme de définitions de $\{\, x, y \,\}$. Pour éclater le point P_*, on pose d'abord $P' := (\ 0, 0\ ;\ x_0, y_0\ )$ où $x_0 := x - \alpha$ et $y_0 := y - \beta$ et alors $\{\, x_0, y_0 \,\}$ admet $C_0(X + \alpha, Y + \beta)$ comme polynôme de définition. Il est clair que $C_0 \in K_{T_P}[X,Y]$, mais supposons néanmoins que $C_0 \in K[X,Y]$ (cela est possible, voir Remarque 2.1.6). Soit $\mathfrak{Q}$ une place dominant le point P et supposons la telle que $y_1 := y_0/x_0 \in \mathcal{O}_{\mathfrak{Q}}$ et $\beta_0 := y_1(\mathfrak{Q}) \notin K$. Puisque

2. Voir Définition 2.4.1.

β_0 est une racine du polynôme $\mathrm{Init}(C_0)(1, Y) \in K[Y]$, il en est de même de tous ses conjugués $\beta_i := \sigma^i(\beta_0)$ car $C_0 \in K[X, Y]$. Par conséquent,

$$Q_i := (\ 0, \beta_i\ ;\ x_0, y_1\ ) \in \mathcal{E}cl(P).$$

Soit $s \neq 0$ le plus petit entier tel que $\beta_0 = \beta_s$. Alors

$$q(Y) := \prod_{i=0}^{s-1}(Y - \beta_i) \in K[X, Y] \text{ et } q(Y) \text{ divise } \mathrm{Init}(C_0)(1, Y).$$

En supposant que β_0 soit la racine K-distinguée de q, il suffirait alors d'identifier l'ensemble de points infiniment voisins $O = \{\, Q_i \mid i = 0, 1, \ldots, s-1 \,\}$ au point Q_0. Or, tout point de O n'est pas conjugué par σ à un autre point de O ; en effet, puisque $[K_{T_P} : K] > 1$, on a $P^\sigma \neq P$ et donc $\mathcal{E}cl(P) \cap \mathcal{E}cl(P^\sigma) = \emptyset$. Par conséquent, pour tout $Q_i \in \mathcal{E}cl(P)$, on a $Q_i^\sigma \notin \mathcal{E}cl(P)$. Par contre, les points de O sont deux à deux conjugués sous l'action de $\sigma_r := \sigma^r$ car $P^{\sigma_r} = P$. Il faudra donc non pas considérer la racine K-distinguée du polynôme q, mais plutôt les racines T_P-distinguées pour identifier les orbites des points de O.

Pour calculer les points infiniment voisins de $P := (\ \alpha, \beta\ ;\ x, y\ )$, il n'est pas nécessaire de considérer l'ensemble de coordonnées $\{\, x, y \,\}$; seuls (α, β), C et T_P suffisent. On représentera donc le point P par la donnée $[(\alpha, \beta), C, T_P]$ et on écrira

$$P \simeq [(\alpha, \beta), C, T_P]. \tag{3.4}$$

Ces considérations devraient aider à justifier l'algorithme suivant :

Algorithme 3.3.2 **Éclatement**$([(\alpha, \beta), C, T_P])$

▷ **Entrée :** Le représentant d'un point $P := (\ \alpha, \beta\ ;\ x, y\ )$ de $\overline{F}/\overline{K}$.

▷ **Sortie :** Le couple $[\mathrm{m}_P, \mathcal{E}]$ où m_P est la multiplicité du point P et $\mathcal{E} = \emptyset$ si $\mathrm{m}_P = 1$, sinon

$$\mathcal{E} := \{\, [(\alpha_1, \beta_1), C_Q, T_Q] \simeq Q \mid Q \in \mathcal{E}cl(P) \text{ et } (\alpha_1, \beta_1) \text{ est } T_P\text{-distingué} \,\}$$

où, si $Q = (\ \alpha_1, \beta_1\ ;\ x_1, y_1\ ) \in \mathcal{E}cl(P)$, C_Q est le polynôme de définition de $\{\, x_1, y_1 \,\}$ et $T_Q := \max\{\, T_P, T(\alpha_1), T(\beta_1) \,\}$

▷ *Note: tous les calculs se font dans le corps K_{T_P}.*

▷ *On ramène le point à l'origine.*

1 : $C_0(X, Y) := C(X + \alpha, Y + \beta)$

▷ *Le polynôme C_0 est le polynôme de définition de $\{x_0, y_0\}$ où $x_0 := x - \alpha$ et $y_0 := y - \beta$.*

2 : $m := \deg \mathrm{Init}(C_0)$.

3 : **si** $m = 1$, **retourner** $[1, \emptyset]$, *4 :* **sinon**

▷ *On détermine d'abord les points infiniment voisins de coordonnée exceptionnelle x_0.*

5 : Soit $q := \mathrm{Init}(C')(1, Z) \in K_{T_P}[Z]$. Calculer

$$V := \texttt{distinguishedRootsOf}(q, T_P)$$

et poser

$$\mathcal{E} := \left\{ [(0, \beta'), C_0{}^{(x_0)}, \max \{ T_P, T(\beta') \}] \mid \beta' \in V \right\}.$$

▷ *On vérifie s'il y a un point infiniment voisin de coordonnée exceptionnelle y_0.*

6 : **si** $\mathrm{Init}(C)(0,1) = 0$, **alors** $\mathcal{E} := \mathcal{E} \cup \left\{ [(0,0), C_0{}^{(y_0)}, T_P] \right\}$

7 : **retourner** $[m, \mathcal{E}]$.

Définition 3.3.3 *On appelle* éclatement distingué *de $P \simeq [(\alpha, \beta), C, T_P]$ le résultat retourné par* **Éclatement**$((\alpha, \beta), C, T_P)$ *et on le note $\mathcal{E}cl_{\mathfrak{d}}(P)$.*

La proposition suivante se passe de démonstration.

Proposition 3.3.4 *Soit P un point T-distingué de $\overline{F}/\overline{K}$. Tout point de $\mathcal{E}cl_{\mathfrak{d}}(P)$ est T_P-distingué.*

Le paquetage qui implante l'algorithme **Éclatement** s'appelle "`DesingTree-Package`". On y reviendra à la Section 3.7. Disons seulement que la fonction qui réalise l'algorithme **Éclatement** a pour signature :

Code Axiom 3.3.5

```
blowUp : InfinitlyClosePoint(...) -> List InfinitlyClosePoint(...)
```

3.4 Arbres de désingularisation

Il est facile de construire l'arbre de désingularisation en utilisant la fonction "`blowUp`".

Code Axiom 3.4.1

```
desingTreeAtPointLocal: InfinitlyClosePoint ->
                        DesingTree InfinitlyClosePoint
desingTreeAtPointLocal(P) ==
  -- on éclate le point.
  -- Note: la fonction blowUp calcule la multiplicité
  -- du point P et modifie par effet de bord
  -- la représentation du point P pour lui assigner sa  multiplicité.
  -- Si le point P est simple alors blowUp retourne le point P
```

```
-- sinon la liste des points infiniment voisins d'ordre 1 du point P.
ecl := blowUp P
-- La fonction multV est implantée dans le domaine InfinitlyClosePoint
-- et retourne la valeur du sélecteur correspondant à la
-- multiplicité du point P.
multP := multV P
one? multP =>
  -- Si le point est simple alors on retourne
  -- l'arbre constitué du seul sommet P.
  tree( P )$DesingTree(InfinitlyClosePoint)
-- Sinon le point est singulier et on applique alors
-- récursivement la fonction desingTreeAtPointLocal
-- à chacun des points infiniment voisins de P.
tree( P , [ desingTreeAtPointLocal( Q )  for Q in ecl ] )
```

Pour calculer les arbres de désingularisation de tous les points singuliers d'une courbe projective plane $\mathcal{C} := \{ C = 0 \}$, on a la fonction suivante :

Code Axiom 3.4.2

```
desingTree: PolyRing -> List DesingTree(InfinitlyClosePoint)
desingTree(C)==
  -- on calcule les points singuliers de la courbe
  -- définie par le polynôme C.
  sing:=singularPoints(C)
  -- La fonction createInfClsPt(P,C) crée le point
  -- infiniment voisin correspondant au point P_*.
  singInf:= [ createInfClsPt(P,C) for P in sing]
  -- on retourne les arbres de désingularisation
  -- de chacun des points singuliers.
  [ desingTreeAtPointLocal(Pinf) for Pinf in singInf ]
```

Soient $P \in \mathcal{C}$ un point singulier et $\mathcal{T}_P$ l'arbre de désingularisation de P calculé par "`desingTree(C)`". Soient Q une feuille de $\mathcal{T}_P$ et $\mathfrak{Q}$ la place représentée par Q. Posons $\mathfrak{P} := \mathfrak{Q} \cap K(\mathcal{C})$. Le lemme suivant sera utilisé pour montrer que le degré de la place $\mathfrak{P}$ est donné par le degré de la tour de définition du point Q.

Lemme 3.4.3 *Soient P un point simple T-distingué de $\overline{F}/\overline{K}$ et $\mathfrak{Q}$ la place de $\overline{F}/\overline{K}$ telle que $\mathfrak{Q} \equiv P$. Posons $\mathfrak{P} := \mathfrak{Q} \cap F_T$ où $F_T := K_T F$. Alors*

$$\deg \mathfrak{P} = \frac{\deg_K T_P}{\deg_K T}.$$

Démonstration : Soient $s := \deg \mathfrak{P}$, $r := [K_T, K]$ et $P = (\ \alpha, \beta\ ;\ x, y\ )$. Par définition, l'ensemble de coordonnées $\{ x, y \}$ est défini sur K_T. Sous l'action de σ^r, le point

P admet donc exactement $s := \frac{\deg_K T_P}{\deg_K T}$ points conjugués car σ^r fixe le corps F_T. Par conséquent, s est le plus petit entier tel que $\sigma^{r^s}(P) = P$ et, en vertu de la Proposition 2.8.9, on a bien $s = \deg \mathfrak{P}$. □

Proposition 3.4.4 *Soient P un point T-distingué de $\overline{F}/\overline{K}$ et $\mathcal{T}_P$ l'arbre de désingularisation de P calculé par* `desingTreeAtPointLocal`*. Soient Q une feuille de $\mathcal{T}_P$ et $\mathfrak{Q}$ la place représentée par Q. Posons $\mathfrak{P} := \mathfrak{Q} \cap K_T(\mathcal{C})$. Alors*

$$\deg \mathfrak{P} := \frac{\deg_K T_Q}{\deg_K T}$$

où T_Q est la tour de définition du point Q.

Démonstration : Soit n le nombre d'éclatements nécessaires pour obtenir le représentant du point Q et montrons la proposition par récurrence sur n. Soit le point (unique!) $P_1 \in \mathcal{E}cl_{\mathfrak{d}}(P)$ dominé par $\mathfrak{Q}$. D'après le Proposition 3.3.4, le point P_1 est T_P-distingué. Posons $\mathfrak{P}_1 := \mathfrak{Q} \cap F_1$ où $F_1 := K_{T_P}F$. Si $n = 1$, alors P_1 est un point simple, c'est-à-dire $Q = P_1$. En appliquant le lemme précédent, on a

$$\deg \mathfrak{P}_1 = \frac{\deg_K T_Q}{\deg_K T_P}. \tag{3.5}$$

D'autre part, on déduit du Corollaire 2.8.15 que $[K_{T_P} : K_T]$ divise $\deg \mathfrak{P}$. D'après le Corollaire 2.8.16, on a donc

$$\deg \mathfrak{P} = [K_{T_P} : K_T] \times \deg \mathfrak{P}_1 = \frac{\deg_K T_P}{\deg_K T} \times \frac{\deg_K T_Q}{\deg_K T_P} = \frac{\deg_K T_Q}{\deg_K T}. \tag{3.6}$$

Montrons maintenant la proposition pour $n > 1$ en supposant qu'elle est vraie pour $n - 1$. Dans ce cas, l'égalité (3.5) est vérifiée par hypothèse de récurrence et on termine la démonstration en utilisant le même argument que celui utilisé en (3.6). □

Proposition 3.4.5 *Soient $P \in \mathcal{C} := \{ C = 0 \}$ un point singulier K-distingué et $\mathcal{T}_P$ l'arbre de désingularisation de P calculé par* `desingTree(C)`*. Soient Q une feuille de $\mathcal{T}_P$ et $\mathfrak{Q}$ la place représentée par Q. Posons $\mathfrak{P} := \mathfrak{Q} \cap K(\mathcal{C})$. Alors*

$$\deg \mathfrak{P} := \deg_K T_Q$$

où T_Q est la tour de définition du point Q.

Démonstration : C'est une conséquence évidente de la Proposition 3.4.4. □

La proposition suivante donne une réponse au problème posé au début de la Section 3.1, soit celui de déterminer un ensemble de places distinguées de $\overline{K}(\mathcal{C})$.

Proposition 3.4.6 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K et $\mathcal{C}_{\mathfrak{d}}$ sa courbe K-distinguée. Soit*

$$\mathcal{S}_{\mathfrak{d}} := \{ P \in \mathcal{C}_{\mathfrak{d}} \mid P \text{ est singulier} \}$$

l'ensemble des points singuliers de $\mathcal{C}_{\mathfrak{d}}$. Soit $\mathcal{F}$ l'ensemble des toutes les feuilles de tous les arbres de désingularisation calculés par `desingTree(C)`. *Alors*

$$\mathfrak{D} := \left\{ \mathfrak{Q} \in \mathbb{P}_{\overline{K}(\mathcal{C})} \mid \mathfrak{Q} \equiv Q \in (\mathcal{C}_{\mathfrak{d}} \setminus \mathcal{S}_{\mathfrak{d}}) \cup \mathcal{F} \right\}$$

est un ensemble de places distinguées de $\overline{K}(\mathcal{C})$.

Démonstration : Soit $\mathfrak{Q}_1 \in \mathfrak{D}$ et posons $\mathfrak{P} := \mathfrak{Q}_1 \cap K(\mathcal{C})$. On veut montrer que $\mathfrak{Q}_1$ est l'unique place de $\mathfrak{D}$ qui domine $\mathfrak{P}$: ceci est clair si $\mathfrak{Q}_1$ domine un point simple de $\mathcal{C}_{\mathfrak{d}}$. Supposons donc que $\mathfrak{Q}_1$ domine un point singulier $P \in \mathcal{S}_{\mathfrak{d}}$ et soit $\mathfrak{Q}_2 \in \mathfrak{D}$ tel que $\mathfrak{Q}_2$ domine $\mathfrak{P}$. La place $\mathfrak{Q}_1$ est σ-conjuguée à $\mathfrak{Q}_2$ d'après la Proposition 2.8.9. Soit Q_i la feuille telle que $Q_i \equiv \mathfrak{Q}_i$ $(i = 1, 2)$. Par définition de $\mathfrak{D}$, la place $\mathfrak{Q}_2$ doit aussi dominer le point P. Soit l'unique point $R_i \in \mathcal{E}cl_{\mathfrak{d}}(P)$ dominé par Q_i $(i = 1, 2)$. Par définition de l'algorithme **Éclatement**, on a donc $T_{Q_i} \geq T_P$ pour $i = 1, 2$. On en déduit que R_1 est σ^r-conjugué à R_2 où $r := \deg_K T_P$. Par conséquent, si $R_1 := (\, 0, b\, ;\, x, y\,)$, alors $R_1^{\sigma^r} = (\, 0, \sigma^r(b)\, ;\, x, y\,)$ car les points R_i étant T_P-distingués (Proposition 3.3.4), l'ensemble de coordonnées $\{ x, y \}$ est défini sur K_{T_P} et donc laissé fixe par σ^r. Par conséquent, b et $\sigma^r(b)$ sont les racines d'un même polynôme irréductible $q \in K_{T_P}[Z]$, d'où $b = \sigma^r(b)$ puisque b et $\sigma^r(b)$ sont par définition T_P-distingués. On a donc $R_1 = R_2$. Le même raisonnement s'applique au point R_1 pour montrer que Q_1 et Q_2 dominent le même point de $\mathcal{E}cl_{\mathfrak{d}}(R_1)$ et ainsi de suite. Puisque Q_1 et Q_2 ont été obtenus après un nombre fini d'éclatements, il est clair alors que $Q_1 = Q_2$, c'est-à-dire $\mathfrak{Q}_1 = \mathfrak{Q}_2$. $\square$

Remarque 3.4.7 Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K et $\mathcal{S}_{\mathfrak{d}}$ l'ensemble de tous les points singuliers K-distingués. Soit $\mathcal{I}$ l'ensemble de tous les points qui sont des noeuds de tous les arbres de désingularisation calculés par `desingTree(C)`. Alors en utilisant le Théorème 2.5.5 et des arguments similaires à ceux utilisés à la démonstration de la Proposition 3.4.4, on montre aisément que le genre de $K(\mathcal{C})$ est égal à

$$\frac{(n-1)(n-2)}{2} - \frac{1}{2} \sum_{Q \in \mathcal{I}} (\mathrm{m}_Q - 1)\mathrm{m}_Q \deg_K T_Q.$$

3.5 Séries $\mathfrak{P}$-adiques

Cette section traite du calcul d'une paramétrisation locale $[\mathfrak{P}]$ (voir Définition 2.7.4) où $\mathfrak{P}$ est une place du corps de fonctions $\overline{F}/\overline{K}$. Supposons que $P := (\ 0,0\ ;\ x,y\ )$ soit un point représentant la place $\mathfrak{P}$ et supposons de plus que $t := x$ soit un paramètre local de la place $\mathfrak{P}$. On veut calculer la série $\mathfrak{P}$-adique de y en fonction de t. Cependant, il n'est pas plus difficile de calculer la série $\mathfrak{P}$-adique d'une fonction $g \in \overline{K}[x,y]$. Pour calculer $g(t)$, on détermine d'abord dans un premier temps $e := \nu_{\mathfrak{P}}(g)$ et la fonction g_1 tel que $g = t^e g_1$. C'est ce que fait l'algorithme suivant et l'idée est d'éclater le point simple P.

Remarque 3.5.1 L'algorithme qui suit ne nécessite aucun calcul de racines de polynômes. Il ne sera donc pas nécessaire de considérer les tours d'extension.

Algorithme 3.5.2 **ValuationEtPlus**(G, C)

▷ **Entrée :**

1. Un polynôme de définition $C \in \overline{K}[X,Y]$ d'un ensemble de coordonnées $\{\ x,y\ \}$ pour lequel
   (a) $P = (\ 0,0\ ;\ x,y\ )$ est un point simple de $\overline{F}/\overline{K}$,
   (b) $t := x$ est un paramètre local de $\mathfrak{P} \equiv P$.
2. Un polynôme $G \in \overline{K}[X,Y]$ représentant la fonction $g = G(x,y) \neq 0$. Important : puisqu'on suppose $g \neq 0$, il faut que C ne divise pas G car sinon cet algorithme boucle à l'infini.

▷ **Sortie :** Un quadruplet $[e, a, C_1, G_1]$ où

1. $e = \nu_{\mathfrak{P}}(g)$,
2. $a \in \overline{K}$ tel que $\nu_{\mathfrak{P}}(g - at^e) > e$,
3. C_1 est le polynôme de définition d'un ensemble de coordonnées $\{\ x, y_1\ \}$ tel que $P_1 := (0,0,x,y_1) \equiv P$,
4. G_1 est un polynôme tel que

$$g = x^e G_1(x, y_1).$$

1 : $a := G(0,0)$.

2 : **si** $a \neq 0$, **retourner**

$$[0, a, C, G].$$

3 : **sinon**

▷ *On éclate le point simple !!*

4 : $C' := C^{(x)}$

5 : $C' := G^{(x)}$

6 : $b := C'(0,0)$ (on remarquera qu'ici $b = (y/x)(\mathfrak{P})$),

$\triangleright$ *On ramène le tout à l'origine.*

7 : $C_0 := C'(X, Y+b)$.

8 : $G_0 := G'(X, Y+b)$.

9 : $[e_1, a_1, C_1, G_1] :=$ **ValuationEtPlus**(G_0, C_0).

10 : **retourner**

$$[\mathrm{m}_P(G) + e_1, a_1, C_1, G_1].$$

Preuve de l'algorithme : Montrons le par récurrence sur $n := \nu_{\mathfrak{P}}(G(x,y))$. Soit $a := G(0,0)$. Si $n = 0$, alors on a nécessairement $a \neq 0$ et l'algorithme retourne bien le bon quadruplet. Supposons que $\nu_{\mathfrak{P}}(G(x,y)) = n > 0$. Soit G_0 comme à l'étape 8 de l'algorithme. Posons $e := \mathrm{m}_P(G)$ et $y_0 := y/x - b$. On a

$$G(x,y) \;=\; x^e G^{(x)}(x, y/x) = x^e G(x, y_0) \tag{3.7}$$

et donc $\nu_{\mathfrak{P}}(G(x,y)) = e + \nu_{\mathfrak{P}}(G_0(x,y_0))$ car $\nu_{\mathfrak{P}}(x) = 1$. On a $\nu_{\mathfrak{P}}(G_0(x,y_0)) < n$ car $a = G(0,0) = 0$ entraîne $e > 0$. D'autre part, C_0 est le polynôme de définition de $\{x, y_0\}$. On peut donc appliquer l'hypothèse de récurrence au quadruplet

$$[e_1, a_1, C_1, G_1] := \textbf{ValuationEtPlus}(G_0, C_0)$$

pour en déduire que

$$\left\{ \begin{array}{rcl} e_1 & = & \nu_{\mathfrak{P}}(G_0(x,y_0)), \\ \nu_{\mathfrak{P}}(G_0(x,y_0) - a_1 x^{e_1}) & > & e_1, \\ G_0(x,y_0) & = & x^{e_1} G_1(x,y_1), \end{array} \right.$$

où y_1 est tel que $\{x, y_1\}$ est l'ensemble de coordonnées correspondant au polynôme C_1. En utilisant l'équation (3.7) et ce qui précède, on trouve $\nu_{\mathfrak{P}}(G(x,y)) = e + e_1$,

$$G(x,y) = G_0(x,y_0)x^e = x^{e+e_1} G_1(x,y_1)$$

et

$$\nu_{\mathfrak{P}}\left(g - a_1 x^{e+e_1}\right) = \nu_{\mathfrak{P}}(x^e(G_0(x,y_0) - a_1 x^{e_1})) = e + \nu_{\mathfrak{P}}(G_0(x,y_0) - a_1 x^{e_1}) > e + e_1$$

montrant ainsi que l'algorithme retourne le bon résultat, c'est-à-dire $[e+e_1, a_1, C_1, G_1]$.

$\square$

Code Axiom 3.5.3 *La fonction qui implante* **ValuationEtPlus** *a pour signature :*

```
KX  ==> SparseUnivariatePolynomial( K )
```

```
KXY ==> SparseUnivariatePolynomial( KX )
valuationAndMore: ( KXY, KXY ) -> Record(ord:INT,_
                                         value:K,_
                                         crv:KXY,_
                                         fnc:KXY)
```

Le domaine "SparseUnivariatePolynomial" réalise les anneaux de polynômes en une indéterminée sans nommer l'indéterminée. Ici, "KX" réalise l'anneau de polynômes $K[X]$, et "KXY" réalise $K[X][Y]$. Le choix de représenter l'anneau de polynômes $K[X,Y]$ par $K[X][Y]$ n'est pas sans fondement : on remarquera que dans l'algorithme **ValuationEtPlus**, seule la variable Y subit une transformation de la forme $Y \to Y + b$. On a donc avantage à utiliser une représentation de $K[X,Y]$ qui regroupe les termes en Y comme le fait le domaine "KXY".

En supposant que le langage de calcul formel utilisé pour mettre en oeuvre les algorithmes permette les évaluations paresseuses, on peut considérer l'algorithme suivant qui retourne la série $\mathfrak{P}$-adique de g. Il applique exactement la construction des séries $\mathfrak{P}$-adiques comme décrite à l'Annexe C, Remarque C.4.

ALGORITHME 3.5.4 **ParamOrigine**(G, C, e)

▷ **Entrée :**

1. Un polynôme de définition $C \in \overline{K}[X,Y]$ d'un ensemble de coordonnées $\{\, x, y \,\}$ pour lequel
   (a) $P = (\, 0, 0 \;;\; x, y \,)$ est un point simple de $\overline{F}/\overline{K}$,
   (b) $t := x$ est un paramètre local de $\mathfrak{P} \equiv P$.
2. Un polynôme $G \in \overline{K}[X,Y]$ représentant la fonction $g = G(x,y) \neq 0$.
3. $e \in \mathbb{Z}$.

▷ **Sortie :** La série $\mathfrak{P}$-adique de $x^e g$ en fonction du paramètre local t.

Évaluer de façon paresseuse :
  si C divise G, **retourner** 0.
  $[e_1, a_1, C_1, G_1] :=$ **ValuationEtPlus**(G, C),
  $e_2 := e + e_1$
  $G_2 := G_1 - a_1$
  retourner

$$a_1 t^{e_2} + \textbf{ParamOrigine}(G_2, C_1, e_2).$$

Il est facile d'implanter un tel algorithme en Axiom. Pour cela on utilise le domaine "Stream" fourni avec Axiom. Ce domaine prend en paramètre un domaine

"`D`" quelconque et réalise les suites infinies d'éléments de "`D`".

Code Axiom 3.5.5 *La catégorie et le domaine qui réalisent les séries $\mathfrak{P}$-adiques s'appellent respectivement*

```
LocalPowerSeriesCategory
NeitherSparseOrDensePowerSeries
```

Le domaine "`NeitherSparseOrDensePowerSeries`" utilise le domaine "`Stream`" et est calqué sur le domaine "`UnivariateLaurentSeries`" (voir Section 3.8.2). Voici le code qui implante l'algorithme **ParamOrigine** :

Code Axiom 3.5.6

```
PCS ==> NeitherSparseOrDensePowerSeries(K)
paramAtOrigin: ( KXY, KXY , Integer) -> PCS
paramAtOrigin(G:KXY,C:KXY,e:Integer) == delay
  zero?(G) => 0
  -- sinon on teste si G est divisible par C
  tt:=G exquo C
  ^(tt case "failed") => 0
  firstTerm:=valuationAndMore(G,C)
  e1:=firstTerm.ord
  a1:=firstTerm.value
  G2:=firstTerm.fnc - a1
  C1:=firstTerm.crv
  e2:= e1 + e
  -- La fonction createSeries est exportée par PCS.
  -- Elle construit l'élément de PCS correspondant :
  -- par exemple, createSeries( a, e , s ) construit
  -- la série a*t^e + s .
  createSeries( a1 , e2 , paramAtOrigin( G2, C1, e2 ) )
```

La définition de la fonction "`paramAtOrigin`" débute avec "`delay`" : c'est une fonction qui prend en argument le code de "`paramAtOrigin`" et sa fonction est d'en retarder son exécution. Le code sera exécuté seulement si nécessaire : par exemple, on peut imaginer que les n premiers termes d'une séries aient été calculés. Si pour un certain calcul, le m-ième terme est nécessaire, alors aucun calcul ne sera fait si $m \leq n$, sinon, la fonction "`paramAtOrigin`" bouclera jusqu'à ce que le m-ième terme soit obtenu.

3.6 Places et paramétrisations locales

Dans mon logiciel, j'accorde plus d'importance à la paramétrisation locale $[\mathfrak{P}]$ (voir Définition 2.7.4) d'une place $\mathfrak{P}$ qu'à la place $\mathfrak{P}$ elle-même. Si $\mathfrak{P}$ est équivalente à un point simple P, je crée la place $\mathfrak{P}$ en rattachant à P la paramétrisation locale $[\mathfrak{P}]$. Si $\mathfrak{P}$ est équivalente à une feuille d'un arbre de désingularisation, je crée la place $\mathfrak{P}$ en lui assignant un symbole (engendré automatiquement par Axiom) auquel est rattaché $[\mathfrak{P}]$.

Afin de déterminer la paramétrisation locale d'une place $\mathfrak{P}$, on utilisera les deux algorithmes suivants. Le premier concerne les points simples et choisit lui-même le paramètre local. Le deuxième concerne les points singuliers : dans ce cas l'algorithme utilise l'arbre de désingularisation du point.

Algorithme 3.6.1 **ParamPtSimple**$((a,b),C)$

▷ **Entrée :** Un point $(a,b) \in \mathbb{A}^2$ et un polynôme C représentant un point simple $(\ a,b\ ;\ x,y\ )$ où C est le polynôme de définition de $\{\,x,y\,\}$.

▷ **Sortie :** La paramétrisation locale $[x(t),y(t)]$ où t est un paramètre local de $\mathfrak{P} \equiv P$ (choisi par l'algorithme).

▷ *On ramène le point à l'origine.*

1 : Soit $C_1 := C(X+a, Y+b)$.

▷ *On teste si $x-a$ est un paramètre local, et si c'est le cas, on prend $t := x-a$ pour paramètre local de $\mathfrak{P}$.*

2 : Si X ne divise pas $\mathrm{Init}(C_1)$ **alors**

$$\begin{aligned} x(t) &:= a+t \\ y(t) &:= b+\mathbf{ParamOrigine}(Y, C_1, 0) \end{aligned}$$

3 : **sinon**

▷ *$t := y-b$ est un paramètre local et il faut intervertir X et Y pour appliquer l'algorithme* **ParamOrigine**.

4 : $C_2 := C'(Y,X)$,

$$\begin{aligned} x(t) &:= a+\mathbf{ParamOrigine}(Y, C'', 0) \\ y(t) &:= b+t \end{aligned}$$

5 : **retourner** $[x(t),y(t)]$.

Ainsi, si P est un point simple d'une courbe projective plane et $\mathfrak{P} \equiv P$, il suffit pour déterminer $[\mathfrak{P}]$ d'appliquer l'algorithme précédent avec P_* et le polynôme de définition correspondant et ensuite de déterminer $[\mathfrak{P}]$ selon la Définition 2.7.4 :

Algorithme 3.6.2 **ParamétrisationLocalePointSimple**(P,C)

▷ **Entrée :** Un point simple $P := (a_0 : a_1 : a_2)$ d'une courbe projective plane $\mathcal{C} := \{\,C=0\,\}$.

▷ **Sortie :** La place $\mathfrak{P} \equiv P$ à laquelle est rattachée la paramétrisation locale $[\mathfrak{P}]$.

Selon la Définition 2.7.4, déterminer $P_* := (\ a, b\ ;\ x, y\ )$ et $C \in \overline{K}[X,Y]$ le polynôme de définition de $\{\, x, y \,\}$.

Calculer $[x(t), y(t)] :=$ **ParamPtSimple**$((a,b), C)$.

retourner la place $\mathfrak{P}$ représentée par $(a_0 : a_1 : a_2)$ et à laquelle est rattachée la paramétrisation locale

$$[\mathfrak{P}] := \begin{cases} [x(t), y(t), 1] & \text{si } a_2 \neq 0, \\ [x(t), 1, y(t)] & \text{si } a_2 = 0 \text{ et } a_1 \neq 0, \\ [1, x(t), y(t)] & \text{sinon.} \end{cases}$$

Dans le cas où $\mathfrak{P}$ domine un point singulier P, la place $\mathfrak{P}$ est équivalente à un point $Q := (\ a, b\ ;\ x, y\ )$ correspondant à une feuille de l'arbre $\mathcal{T}_P$. Soient $x(t)$ et $y(t)$ les séries $\mathfrak{P}$-adiques calculées par l'algorithme précédent appliqué au point Q. Supposons que $P = (0 : 0 : 1)$ et que $P_* = (\ 0, 0\ ;\ x_0, y_0\ )$. L'algorithme suivant permettra entre autre de déterminer pour une fonction $g \in \overline{K}[x_0, y_0]$, un polynôme $G(X,Y)$ tel que $g = G(x,y)$. Par conséquent, si $H_{x_0}(X,Y)$ et $H_{y_0}(X,Y)$ sont tels que $x_0 = H_{x_0}(x,y)$ et $y_0 = H_{y_0}(x,y)$, alors

$$[\mathfrak{P}] = [H_{x_0}\left(x(t), y(t)\right), H_{y_0}\left((x(t), y(t)\right), 1].$$

Dans ce cas, on crée la place $\mathfrak{P}$ en lui assignant un symbole auquel est rattaché $[\mathfrak{P}]$. Il sera aussi pratique d'attacher à la feuille Q le couple de séries $(x(t), y(t))$. On utilise avantageusement la structure récursive de $\mathcal{T}_P$ pour déterminer $[\mathfrak{P}]$ pour chacune des places $\mathfrak{P}|P$:

Algorithme 3.6.3 **ParamétrisationLocalFeuille**$(\mathcal{T}_Q, G_1, G_2, P)$

▷ **Entrée :**

1. L'arbre de désingularisation $\mathcal{T}_Q$ d'un point $Q = (\ a, b\ ;\ x, y\ )$ dominant un point singulier $P := (a_0 : a_1 : a_2)$ d'une courbe projective plane.
2. Deux polynômes $G_1, G_2 \in \overline{K}[X,Y]$ représentant $g_1 := G_1(x,y)$ et $g_2 := G_2(x,y)$.

▷ **Sortie :** Aucune ! L'algorithme agit par effet de bord. À la fin, une place sera créée pour chacune des feuilles de $\mathcal{T}_Q$ en lui assignant sa paramétrisation locale. De plus, à chacune des feuilles de $\mathcal{T}_Q$ sera rattachée une paramétrisation de la feuille.

si $Q \simeq [(\alpha, \beta), C, \mathcal{T}_Q]$ est un point simple, alors

calculer $[x(t), y(t)] :=$ **ParamPtSimple**(Q, C).

Rattacher à la feuille Q la paramétrisation $[x(t), y(t)]$.

Calculer

$$\begin{cases} x_0(t) & := & G_1(\, x(t), y(t)\,) \\ y_0(t) & := & G_2(\, x(t), y(t)\,). \end{cases}$$

En fonction du point $P = (a_0 : a_1 : a_2)$, créer la place $\mathfrak{Q}$ correspondant à la feuille Q en lui assignant la paramétrisation locale

$$[\mathfrak{Q}] := \begin{cases} [x_0(t), y_0(t), 1] & \text{si } a_2 \neq 0, \\ [x_0(t), 1, y_0(t)] & \text{si } a_2 = 0 \text{ et } a_1 \neq 0, \\ [1, x_0(t), y_0(t)] & \text{sinon.} \end{cases}$$

sinon on a

$$\mathcal{T}_Q = \{ [(\alpha, \beta), C, T_Q], \{ \mathcal{T}_R \mid R \in \mathcal{E}cl_{\mathfrak{d}}(Q) \} \},$$

où $Q \simeq [(\alpha, \beta), C, T_Q]$ est la racine de $\mathcal{T}_Q$.

▷ *Il faut ramener le tout à l'origine avant de faire subir à G_1 et G_2 les transformés monoïdales donnant les points de $\mathcal{E}cl_{\mathfrak{d}}(Q)$*

$G'_1 := G_1(X + \alpha, Y + \beta)$

$G'_2 := G_2(X + \alpha, Y + \beta)$

$S := \emptyset$

Pour chaque $R \in \mathcal{E}cl_{\mathfrak{d}}(P)$ faire

soit l_R la coordonnée exceptionnelle de R.

si $l_R = x$, **alors**

▷ *on applique la transformation $\{ x, y \} \mapsto \{ x, y/x \}$*

$$\begin{aligned} G''_1 &:= G'_1(X, XY) \\ G''_2 &:= G'_2(X, XY) \end{aligned}$$

sinon

▷ *on applique la transformation $\{ x, y \} \mapsto \{ x/y, y \}$*

$$\begin{aligned} G''_1 &:= G'_1(XY, Y) \\ G''_2 &:= G'_2(XY, Y) \end{aligned}$$

▷ *On applique récursivement l'algorithme*

ParamétrisationLocaleArbre$(\mathcal{T}_R, G''_1, G''_2, P)$

retourner NIL.

Il suffit de faire

$$\textbf{ParamétrisationLocaleArbre}(\mathcal{T}_{P_*}, X, Y, P)$$

pour déterminer les paramétrisations locales de toutes les places dominant un point singulier P d'une courbe projective plane $\mathcal{C}$.

3.7 Diviseurs

Dans cette section, je m'intéresse aux calculs des diviseurs suivants :

1. les diviseurs exceptionnels de points infiniment voisins,
2. le diviseur d'adjonction d'une courbe projective plane,
3. les diviseurs d'intersection de polynômes homogènes avec une courbe projective plane.

Pour calculer ces diviseurs, j'utiliserai les calculs déjà faits pour les paramétrisations locales de places. La méthode que je propose utilisera les paramétrisations locales de places pour les places correspondant aux points simples de la courbe. Par contre, si une place correspond à une feuille d'un arbre de désingularisation, j'utiliserai la paramétrisation associée à la feuille plutôt que la paramétrisation locale de la place. Néanmoins, afin de justifier ma méthode, voyons comment on pourrait utiliser les paramétrisations locales des places correspondant à des feuilles. Prenons pour exemple le cas particulier du calcul du diviseur exceptionnel d'un point du corps de fonctions $\overline{K}(\mathcal{C})$ où $\mathcal{C}$ est une courbe projective plane. Supposons que $P := (0 : 0 : 1)$ soit un point singulier de $\mathcal{C}$. Alors $P_* := (\ 0, 0\ ;\ x, y\ )$, où $\{\, x, y\,\}$ est l'ensemble de coordonnées standard adéquat (voir Annexe B.5.6). Soient $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_r$ les places dominant le point P. Alors les paramétrisations locales des places $\mathfrak{Q}_i$ sont toutes de la forme

$$[\mathfrak{Q}_i] = [x(t_i), y(t_i), 1]$$

où t_i est un paramètre local de la place $\mathfrak{Q}_i$. Posons, pour $i = 1, 2, \ldots, r$,

$$m_i := \min \{\, \mathrm{ord}\,(x(t_i))\,, \mathrm{ord}\,(y(t_i))\,\}\,.$$

Il est clair que

$$m_i = \min \{\, \nu_{\mathfrak{Q}_i}(x), \nu_{\mathfrak{Q}_i}(y)\,\}\,.$$

D'après la définition des diviseurs exceptionnels (voir Définition 2.3.2), on a donc

$$E_{P_*} = \sum_{i=1}^{r} m_i \mathfrak{Q}_i.$$

On veut maintenant calculer le diviseur exceptionnel d'un point $R \in \mathcal{E}cl(P_*)$. Supposons sans perte de généralité que $R = (\ 0, b\ ;\ x, y/x\ )$ et posons $y_1 := y/x - b = (y - bx)/x$. Pour calculer E_R, il faut calculer $\nu_{\mathfrak{Q}_i}(y_1)$ pour chacune des places $\mathfrak{Q}_i$ dominant le point R. Il suffit pour cela de calculer $\mathrm{ord}\,(y(t_i) - bx(t_i)) - \mathrm{ord}\,(x(t_i))$. Or, si $b \neq 0$, alors $\nu_{\mathfrak{Q}_i}(y) = \nu_{\mathfrak{Q}_i}(x)$, et dans ce cas, pour calculer $\mathrm{ord}\,(y(t_i) - bx(t_i))$, il faut calculer au moins les seconds termes de $y(t_i)$ et $x(t_i)$. Ce calcul devra être fait aussi pour chacune des places dominant le point R. Cette dernière considération justifie ma méthode car elle a pour particularité :

1. de ne pas calculer inutilement trop de termes des séries, voire même de n'en calculer aucun,

2. d'éviter de considérer une par une les places dominant un point P.

Soit $\overline{F}/\overline{K}$ un corps de fonctions et $P := (\ a, b\ ;\ x, y\ )$ un point singulier de $\overline{F}/\overline{K}$. Je vais montrer comment calculer les diviseurs locaux au point P de fonctions $g \in \overline{K}[x, y]$. Supposons que $P = (\ 0, 0\ ;\ x, y\ )$ et soit $G \in \overline{K}[X, Y]$ tel que $g = G(x, y)$. Dans ce cas, on peut écrire

$$(g)_P = \mathrm{m}_P(G)E_P + \sum_{Q \in \mathcal{E}cl(P)} (g^{(l_Q)})_Q \tag{3.8}$$

comme à l'équation (2.5) de la Section 2.3 (page 27). L'algorithme qui calculera $(g)_P$ applique exactement cette équation. On supposera par contre que P est un point distingué pour une certaine tour et on ne considérera que l'éclatement distingué $\mathcal{E}cl_{\mathfrak{d}}(P)$. On supposera aussi que les paramétrisations des feuilles de l'arbre $\mathcal{T}_P$ ont été calculées.

L'algorithme suivant applique l'équation (3.8) pour calculer le diviseur $(g)_P$. Soulignons que la Remarque 3.5.1 s'applique aussi à cet algorithme.

Algorithme 3.7.1 **DiviseurLocal**$(G, \mathcal{T}_P)$

▷ **Entrée :** Un polynôme $G \in \overline{K}[X, Y]$ et $\mathcal{T}_P$ l'arbre de désingularisation d'un point $P = (\ a, b\ ;\ x, y\ )$.

▷ **Sortie :** Le diviseur $(g)_P$ où $g = G(x, y)$.

1 : **si** $G(a, b) \neq 0$, **retourner** le diviseur 0.

2 : **si** P est une feuille, alors calculer

$$n := \mathrm{ord}\,(G(x(t), y(t)))$$

où $[x(t), y(t)]$ est la paramétrisation associée à la feuille P.

3 : **retourner** le diviseur $n\mathfrak{P}$ où $\mathfrak{P}$ est la place correspondant au point P,

4 : **sinon retourner**

$$\mathrm{m}_P(G)E_P + \sum_{Q \in \mathcal{E}cl_{\mathfrak{d}}(P)} \mathbf{DiviseurLocal}(G_Q, \mathcal{T}_Q)$$

où $G_Q := G(X + a, Y + b)^{(l_Q)}$, l_Q étant la coordonnée exceptionnelle du point Q.

Évidemment, il faut calculer les diviseurs exceptionnels de chacun des noeuds de l'arbre de désingularisation avant d'appliquer l'algorithme précédent. Pour ce faire, il suffit d'utiliser l'algorithme suivant qui utilise l'équation

$$E_P = \sum_{Q \in \mathcal{E}cl(P)} (l_Q)_Q$$

(voir l'équation (2.4) de la Section 2.3, page 27).

Algorithme 3.7.2 **ArbreDivExcp**($\mathcal{T}_P$)

▷ **Entrée :** Un arbre $\mathcal{T}_P$.

▷ **Sortie :** Aucune ! L'algorithme agit par effet de bord en rattachant à chaque noeud de l'arbre $\mathcal{T}_P$ le diviseur exceptionnel correspondant.

1 : **si** P est une feuille, alors rattacher le diviseur $E_P = \mathfrak{P}$ où $\mathfrak{P}$ est la place correspondant au point P,

2 : **sinon** , pour chaque $Q \in \mathcal{E}cl_{\mathfrak{d}}(P)$, faire

$$\textbf{ArbreDivExcp}(\mathcal{T}_Q).$$

▷ *À présent, les diviseurs exceptionnels de tous les noeuds de $\mathcal{T}_P$ sont calculés, sauf pour P.*

3 : Calculer le diviseur E_P :

$$E_P := \sum_{Q \in \mathcal{E}cl_{\mathfrak{d}}(P)} \textbf{DiviseurLocal}(L_Q, \mathcal{T}_Q)$$

où $L_Q = X$ si x est la coordonnée exceptionnelle du point Q, sinon $L_Q = Y$.

4 : rattacher le diviseur E_P au noeud de P.

On peut ensuite calculer le diviseur d'adjonction distingué d'un point :

Algorithme 3.7.3 **DivAdj**($\mathcal{T}_P$)

▷ **Entrée :** L'arbre de désingularisation d'un point.

▷ **Sortie :** Le diviseur d'adjonction distingué $\overline{\mathcal{A}}_P$.

1 : retourner

$$(\mathrm{m}_P - 1)E_P + \sum_{Q \in \mathcal{E}cl_{\mathfrak{d}}(P)} \textbf{DivAdj}(\mathcal{T}_Q).$$

Il est alors très facile de calculer le diviseur d'intersection distingué d'un polynôme homogène G avec une courbe projective plane $\mathcal{C}$.

Algorithme 3.7.4 **DivInter**(G, C)

▷ *Note : On suppose calculés tous les arbres de désingularisation de tous les points singuliers de la courbe $\mathcal{C} := \{ C = 0 \}$.*

▷ **Entrée :** Deux polynômes homogènes $G, C \in K[X_0, X_1, X_2]$ où C est absolument irréductible et ne divise pas G.

▷ **Sortie :** Le diviseur d'intersection distingué de G avec la courbe projective plane $\mathcal{C} := \{ C = 0 \}$.

$\overline{(G)} := 0$

Pour chacun des points $P \in \mathbf{EnsAlgProj}(G, C)$, répéter

Si P est simple, alors

Si ce n'est déjà fait, créer la place $\mathfrak{P} \equiv P$ en lui assignant la paramétrisation locale $[\mathfrak{P}]$ (calculé avec l'algorithme 3.6.2).

calculer $n := \nu_{\mathfrak{P}}\left(\overline{G}^P\right) = \mathrm{ord}\,(G[\mathfrak{P}])$.

$\overline{(G)} := \overline{(G)} + n\mathfrak{P}$

Sinon

$$\overline{(G)} := \overline{(G)} + \mathbf{DiviseurLocal}(G^P, \mathcal{T}_P)$$

où $\mathcal{T}_P$ est l'arbre de désingularisation de P et où G^P défini en fonction de $P = (a_0 : a_1 : a_2)$ est donné par

$$G^P(X,Y) := \begin{cases} G(X,Y,1) & \text{si } a_2 \neq 0, \text{ sinon} \\ G(X,1,Y) & \text{si } a_2 = 0 \text{ et } a_1 \neq 0, \\ G(1,X,Y) & \text{sinon.} \end{cases}$$

retourner $\overline{(G)}$.

Le théorème qui suit montre que le degré des tours d'extension utilisées par l'algorithme de Brill-Noether est borné par une unique valeur définie en fonction du degré de la courbe et du degré du diviseur D pour lequel on veut calculer une base de $\mathcal{L}(D)$.

THÉORÈME 3.7.5 *Soient $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K et D un diviseur de $K(\mathcal{C})$. En utilisant l'algorithme de Brill-Noether pour calculer une base $\mathcal{L}(D)$ avec les extensions dynamiques, on peut faire en sorte que toute tour d'extension T construite par l'algorithme soit telle que*

$$\deg_K T \leq N := \max\left\{ \deg D_+,\ \ n^2,\ \ \deg D_+ + \frac{3n^2 - 7n}{2} - 2g + 2 \right\}$$

où D_+ est la partie positive de D, $n := \deg C$ et g est le genre de $K(\mathcal{C})$.

Démonstration : Il suffit de montrer qu'on peut faire en sorte que toute place $\mathfrak{P}$ intervenant dans les calculs soit telle que $\deg \mathfrak{P} < N$: en effet, une telle place $\mathfrak{P}$ est équivalente à un point P de $K(\mathcal{C})$ et $\deg_K \mathcal{T}_P = \deg \mathfrak{P}$ d'après la Proposition 3.4.4. D'autre part, il est clair que $\mathfrak{P}$ est soit une place du support de D, soit une place du diviseur d'adjonction ou soit une place du support d'un diviseur d'intersection (G) d'un polynôme homogène $G \in S(K)$ avec la courbe $\mathcal{C}$. Puisqu'on suppose implicitement que $\deg D \geq 0$ (car sinon $\mathcal{L}(D) = \{ 0 \}$), si $\mathfrak{P} \in \mathrm{supp} D$, alors $\deg \mathfrak{P} \leq \deg D_+ \leq N$. Pour finir, il suffit donc de montrer que $\deg(G) \leq N$ pour tout diviseur intervenant dans les calculs. Soit $\mathcal{A}$ le diviseur d'adjonction de $\mathcal{C}$ et posons

$$B := D_+ + \mathcal{A}.$$

Les seuls diviseurs d'intersection utilisés sont ceux des polynômes d'interpolation qui sont tous de degré $d := \deg G_0$ où $G_0 \in S(K)$ est tel que

$$(G_0) \geq B.$$

D'après le Corollaire 2.7.6, un tel diviseur G_0 existe si

$$\deg G_0 = d > \max\left\{ n-1, \frac{n}{2} + \frac{\deg B}{n} - \frac{3}{2} \right\}.$$

On peut donc prendre d tel que

$$d \leq \max\left\{ n, \frac{n}{2} + \frac{\deg B}{n} - \frac{1}{2} \right\}.$$

Si $d = n$, alors $\deg(G_0) = n^2$ d'après la Proposition 2.4.7, et par conséquent, $\deg(G_0) \leq N$. Sinon

$$\deg(G_0) = n \times d \leq n \times \left(\frac{n}{2} + \frac{\deg B}{n} - \frac{1}{2} \right) = \frac{n^2 - n}{2} + \deg B.$$

D'après la Proposition 2.6.4, on a $\deg \mathcal{A} = n^2 - 3n - 2g + 2$. Par conséquent, puisque $D_+ \geq 0$ et $\mathcal{A} \geq 0$, on a $\deg B = \deg D_+ + n^2 - 3n - 2g + 2$ et donc

$$\deg(G_0) \leq \deg D_+ + \frac{3n^2 - 7n}{2} - 2g + 2 \leq N.$$

□

Remarque 3.7.6 Le théorème précédent prendrait toute sa valeur si l'on savait formuler de façon précise la complexité de l'algorithme de Brill-Noether en fonction de n et $\deg D$. Essentiellement, cette complexité repose sur celle du calcul des arbres de désingularisation qui est de complexité polynomial (voir [45, Prop. 2.5.33]). On trouvera dans [21] (voir aussi [33]) une bonne étude de cette complexité dans le cas où le corps de base est de caractéristique 0. On y montre que le nombre d'opérations sur le corps de base pour désingulariser une courbe plane est d'ordre $O(n^8)$ (cette complexité est déduite des propriétés des développements de Puiseux). Soulignons aussi que cette complexité est calculée pour un algorithme d'éclatement de points utilisant le principe d'évaluation paresseuse : l'idée est de ne prendre compte que des monômes qui suffiront à déterminer la forme initiale du transformé strict obtenu après un éclatement. De la sorte, les monômes considérés sont de degré beaucoup plus petit que le degré du polynôme définissant la courbe.

3.8 Implantation des catégories et domaines

Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane définie sur K et considérons le corps de fonctions $F := K(\mathcal{C})$. Voici la liste de tous les objets qu'il faut considérer pour implanter l'algorithme de Brill-Noether :

1. le corps K,
2. l'anneau de polynômes $K[X_0, X_1, X_2]$,
3. le plan projectif $\mathbb{P}^2$,
4. l'ensemble des places du corps de fonctions F/K,
5. l'ensemble des diviseurs de F/K,
6. l'ensemble des points infiniment voisins d'un point singulier de $\mathcal{C}$,
7. l'ensemble des arbres de désingularisation des points singuliers.

L'ordre dans lequel sont présentés les objets n'est pas aléatoire : si l'implantation d'un objet dépend d'un autre objet, ce dernier doit le précéder dans la liste. Par exemple, les points infiniment voisins utiliseront les points projectifs. On observera par contre que les places précèdent les points infiniment voisins bien qu'une place soit déterminée après avoir calculé les points infiniment voisins qu'elle domine. La raison à cela est toute simple : à tout point infiniment voisin est associé son diviseur exceptionnel qui est défini en fonction des places.

Pour l'anneau de polynômes $K[X_0, X_1, X_2]$, on utilisera l'un des domaines suivants livrés avec Axiom :

```
DistributedMultivariatePolynomial
HomogeneousDistributedMultivariatePolynomial
GeneralDistributedMultivariatePolynomial
```

Tous les autres objets sont respectivement traités aux Sections 3.8.1 à 3.8.5. Notons qu'il n'est pas question ici de donner la liste exhaustive des fonctions exportées par les catégories et les domaines : seules les fonctions importantes seront considérées.

3.8.1 Le plan projectif

La construction du plan projectif est simple. Elle est réalisée en représentant les points de $\mathbb{P}^2$ par une liste d'éléments de K. Il suffit de s'assurer que cette liste a toujours 3 éléments. De plus, en accord avec la Définition 2.4.1, on fera toujours en sorte que le dernier élément non nul de la liste soit égal à 1. Par exemple, si $K = \mathbb{Q}$, alors le point $(1 : 2 : 0)$ sera représenté par la liste "`[1/2, 1, 0]`". La catégorie et le domaine qui réalisent le plan projectif sont :

```
ProjectiveSpaceCategory(K:Field):Category == SetCategory with
  coerce: List K -> %
  ...
ProjectivePlane(K):Exports == Implementation where
  K:Field
  Exports ==> ProjectiveSpaceCategory(K)
  Implementation ==> List(K) add
    Rep:= List K
    ...
```

3.8.2 Les places

La catégorie définissant les places des corps de fonctions s'appelle

```
PlacesCategory
```

Pour les calculs qui nous intéressent, il est suffisant de connaître le degré de $\mathfrak{P}$ et sa paramétrisation locale $[\mathfrak{P}]$ (voir Définition 2.7.4). Il est clair qu'on ne veut pas calculer $\deg \mathfrak{P}$ à chaque fois que $\deg \mathfrak{P}$ sera utilisée. Il sera donc commode d'associer à $\mathfrak{P}$ son degré. Le même raisonnement s'applique à la paramétrisation locale $[\mathfrak{P}]$. On devra donc utiliser un domaine réalisant le corps des séries de Laurent. Le domaine

```
UnivariateLaurentSeries
```

fourni avec Axiom réalise le corps des séries de Laurent. Cependant, pour des raisons non pas algorithmiques mais plutôt techniques, son implantation laisse à désirer. J'ai donc construit une catégorie et un domaine pour les séries de Laurent :

```
LocalPowerSeriesCategory(K:Field)
NeitherSparseOrDensePowerSeries(K:Field)
```

La catégorie "`LocalPowerSeriesCategory`" appartient à la catégorie "`Field`" fournie avec Axiom et exporte des opérations qui seront utilisées pour calculer les matrices définies à la Section 2.7.1 pour le calcul des polynômes d'interpolation.

L'implantation de "NeitherSparseOrDensePowerSeries" est calquée sur celle de "UnivariateLaurentSeries". Par contre, comme son nom l'indique, la représentation des séries n'est ni dense ni creuse ce qui facilite l'implantation. Il s'en suit par contre que les éléments de $K((t))$ n'ont pas de représentation canonique. Cela ne posera aucun problème car le test d'égalité de séries est à toute fin pratique irréalisable (à moins bien sûr que les séries soient finies).

Pour des considérations relatives à la mise au point de mon logiciel, je n'ai pas voulu fixer une fois pour toutes le domaine réalisant le corps des séries de Laurent. Par conséquent, la catégorie et le domaine réalisant les places auront pour paramètres le corps de base K et un domaine appartenant à la catégorie "LocalPowerSeriesCategory(K)" :

```
PlacesCategory(K:Field,_
              PCS:LocalPowerSeriesCategory(K)):Category_
              == SetCategoryWithDegree with
  ...
Places(K,PCS):Exports == Implementation where
  K   : FIELD
  PCS : LocalPowerSeriesCategory(K)
  Exports ==> PlacesCategory(K,PCS)
  Implementation ==>  add
    Rep :=  Record(theName : Union( List(K), Symbol ),_
                   locPar  : List PCS,_
                   deg     : PositiveInteger,_
                   isALeaf : Boolean,_
                   inName  : Symbol )
    ...
```

Les places sont donc représentées par un "Record". Le sélecteur "theName" est utilisé pour l'affichage à l'écran et n'a aucune valeur algorithmique. Les sélecteur "locPar" et "deg" donnent respectivement la paramétrisation locale et le degré d'une place. Le sélecteur "isALeaf" indique par un booléen si la place est équivalente à un point simple d'une courbe ou à une feuille d'un arbre de désingularisation d'un point singulier d'une courbe. Le sélecteur "inName" est seulement utilisé localement par le domaine pour le test d'égalité.

On notera que la catégorie "PlacesCategory" appartient à la catégorie

```
SetCategoryWithDegree
```

Celle-ci est exactement la catégorie "SetCategory" avec en plus la fonction exportée

```
degree : % -> PositiveInteger
```

qui retournera le degré d'une place. L'utilité de cette catégorie sera claire lorsque seront définis les constructeurs pour les diviseurs de corps de fonctions.

3.8.3 Les diviseurs

Le domaine réalisant les diviseurs s'appelle "`Divisor`". Rappelons que les diviseurs d'un corps de fonctions sont par définition des éléments d'un groupe abélien libre sur l'ensemble des places d'un corps de fonctions. Or, il sera suffisant que "`Divisor`" réalise le groupe abélien libre[3] sur un ensemble quelconque. On veut néanmoins exporter l'opération qui retournera le degré d'un diviseur. Puisque le degré d'un diviseur est défini en fonction du degré des places, le domaine qui sera donné en paramètre à "`Divisor`" devra exporter l'opération "`degree : % ->PositiveInteger`" : ceci justifie la catégorie "`SetCategoryWithDegree`". La catégorie à laquelle appartiendra le domaine "`Divisor`" est construite essentiellement avec des catégories déjà existantes en Axiom :

```
DivisorCategory(S:SetCategory):Category ==_
  Join(AbelianGroup,_
       Module Integer,_
       FreeAbelianMonoidCategory(S, Integer)) with
    degree: % -> INT
Divisor(S:SetCategoryWithDegree):Exports == Implementation where
  PT   ==>  Record(gen:S,exp: Integer)
  Exports == DivisorCategory(S)
  Implementation == List PT add
    Rep := List PT
    ...
```

3.8.4 Les points infiniment voisins

Les seuls points de $\overline{F}/\overline{K}$ considérés pour les calculs sont

1. les points infiniment voisins des points singuliers,
2. les points P_* si P est un point singulier de la courbe projective plane (voir Définition 2.4.1).

Pour l'implantation, si P est un point singulier de la courbe, on considère le point P_* comme un point infiniment voisin. Le domaine qui réalise les points de $\overline{F}/\overline{K}$ est

3. Il aurait suffit d'utiliser le domaine "`FreeAbelianGroup`" fourni avec Axiom. Or, dans sa première version, ce domaine avait un "bug" assez gênant : il n'était pas abélien !

donc celui qui réalisera les points infiniment voisins en utilisant la représentation donnée à la Section 3.3. On voudra par contre ajouter un peu plus d'information à la représentation d'un point infiniment voisin, à savoir :

1. la multiplicité,
2. la coordonnée exceptionnelle du point,
3. le diviseur exceptionnel,
4. la paramétrisation locale du point si le point est une feuille,
5. le point de la courbe dominé par le point,
6. un symbole qui sera utilisé pour l'affichage à l'écran.

Le domaine qui réalise la représentation des points infiniment voisins appartient à la catégorie "`InfinitlyClosePointCategory`". Les seules fonctions exportées par cette catégorie sont des fonctions qui permettent de créer, de lire ou de modifier la représentation d'un point infiniment voisin (afin de ne pas alourdir le texte, on omet d'en donner la liste).

```
)abbrev domain   INFCLSPT InfinitlyClosePoint
InfinitlyClosePoint(K,...):Exports == Implementation where
  -- Chacun des objets utilisé pour la représentation
  -- d'un point infiniment voisin appartient
  -- à l'un des domaines suivants :
  K:Field
  PolyRing: Ring
  PCS: LocalPowerSeriesCategory(K)
  ProjPt:ProjectivePointCategory(K)
  Plc: PlacesCategory(K,PCS)
  DIVISOR: DivisorCategory(Plc)
  -- Les domaines qui précedent sont exactement ceux
  -- donnés en arguments au domaine InfinitlyClosePoint.

  Exports == InfinitlyClosePointCategory(K,PolyRing,ProjPt,PCS,Plc,DIVISOR)
  Implementation ==  add
    Rep :=   Record(localPoint:ProjPt,
                    curve:PolyRing,
                    definingTower:K,
                    mult:NNI,
                    chart:LIST(INT),
                    excpDiv:DIVISOR,
                    localParam:List(PCS),
```

```
                    dominate:ProjPt,
                    symbName:Symbol)
    ...
```

3.8.5 Les arbres de désingularisation

Le domaine “`DesingTree`” réalise les arbres de désingularisation. Il est essentiellement le même que le domaine “`Tree`” fourni avec Axiom qui exporte entre autres la fonction “`tree: S ->$`” : celle-ci crée un arbre formé d’un seul sommet appartenant au domaine “`S`”. Or cette fonction est exportée au niveau du domaine “`Tree`” et non par une catégorie à laquelle le domaine “`Tree`” appartient. Par conséquent, tout domaine ou paquetage prenant en argument le domaine “`Tree`” n’aura pas accès à cette fonction. Il a donc été nécessaire de créer une catégorie exportant cette fonction :

```
DesingTreeCategory(S: SetCategory):Category == RecursiveAggregate(S) with
     tree: (S,List $) -> $
       ++ tree(nd,la) crée un arbre ayant pour racine le sommet
       ++ ``nd'' et pour sous-arbres liés à ce sommet les arbres
       ++ contenus dans la liste ``la''.
     tree: S -> $
       ++ tree(nd) crée l'arbre constitué du seul sommet nd.
```

Le domaine “`DesingTree`” a pour code :

```
DesingTree(S: SetCategory): Exports ==Implementation where
  Exports == DesingTreeCategory(S)
  Implementation == add
    Rep ==> Record(value: S, args: List $)
    tree(s,ls) == [s,ls]
    tree(s:S) == [s,empty()$List($)]
```

3.9 Exemples

Dans cette section, je donne trois exemples d’utilisation de mon logiciel. Le premier montre comment construire un code géométrique $C_{\mathcal{L}}(F, \mathcal{P}, D)$ en utilisant toutes les places de degré 1 pour le diviseur $\mathcal{P}$. Le deuxième traite de l’utilisation du paquetage “`PAFFFF`” qui regroupe tous les paquetages que j’ai réalisés en Axiom. Je montre comment l’utiliser en reprenant une partie des calculs expérimentaux avec lesquels j’ai déduit une méthode de construction effective des codes définis sur des extensions du type d’Artin-Schreier dont il est question au Chapitre 4. Pour le dernier exemple, je construit un code *quasi auto-dual*.

3.9.1 Un $[33, 5, 27]_{2^4}$-code

Dans ce premier exemple, je fais tous les calculs, étape par étape, pour calculer une base de l'espace vectoriel associé à un diviseur afin de construire un code géométrique. Comme dans [28], je construis un code à partir de la courbe $\mathcal{C} := \{ C = 0 \}$ définie sur $K := \mathbb{F}_2$ où

$$C = X^5 + Y^2 Z^3 + Y Z^4 \in K[X, Y, Z]$$

est absolument irréductible. Cette courbe n'a qu'un point singulier $P := (0 : 1 : 0)$ dominé par une unique place $\mathfrak{P}$ qui est de degré 1. Sur $K' := \mathbb{F}_{2^4}$, la courbe $\mathcal{C}$ possède 33 points[4] rationnels. Le corps $F' := K'(\mathcal{C})$ a donc 33 places rationnelles sur K', c'est-à-dire de degré 1. Soit un code géométrique $C_{\mathcal{L}}(F', \mathcal{P}, D')$ où D' et $\mathcal{P}$ sont des diviseurs de F' tels que $\mathrm{supp} D' \cap \mathrm{supp} \mathcal{P} = \emptyset$ et $\mathcal{P}$ est formé d'une somme de n places de degré 1, deux à deux distinctes. Habituellement, pour le diviseur $\mathcal{P}$, on utilise toutes les places de degré 1 sauf une qui est utilisée pour le diviseur D'. Or rien n'empêche d'utiliser un diviseur D' formé de places de degré supérieur à 1. Pour cet exemple, le diviseur D' que j'utiliserai sera formé d'une place de degré 3. De la sorte, le code $C_{\mathcal{L}}(F', \mathcal{P}, D')$ sera de longueur 33, soit de longueur égale au nombre de places de degré 1 du corps de fonctions F'.

Pour faire des calculs en Axiom, il faut d'abord définir les domaines qui seront utilisés. Dans un premier temps, on définit le corps de base et l'anneau de polynômes. Pour plus de clarté, les variables X_0, X_1, X_2 seront dorénavant respectivement notées X, Y et Z.

```
Kbase     := PF 2
K         := PACOFF Kbase
symb      := [X,Y,Z]
PolyRing  := DMP(symb,K)
```

On définit ensuite le plan projectif, le corps des séries de Laurent, les places et les diviseurs.

```
ProjPt    := PlaneProjectivePoint(K)
PCS       := NeitherSparseOrDensePowerSeries(K)
Plc       := Places(K,PCS)
Div       := Divisor(Plc)
```

Après sont définis les points infiniment voisins et les arbres de désingularisation.

```
ICP       := InfinitlyClosePoint(K,PolyRing,ProjPt,PCS,Plc,Div)
DesTree   := DesingTree(ICP)
```

4. D'après la borne de Weil, sur $\mathbb{F}_{2^4}$, cette courbe a le maximum de points rationnels possibles.

Une fois les domaines déclarés, on fait de même pour les paquetages qui seront utilisés. Les trois paquetages suivants implantent des opérations liées aux polynômes et aux points projectifs.

```
PackPoly   := PackageForPoly(K,symb,PolyRing,E)
Pack1      := PolynomialPackageForCurve1(K,symb,PolyRing,E,ProjPt)
Pack2      := PolynomialPackageForCurve2(K,symb,PolyRing,E,ProjPt)
RSP        := RationalAndSingularPointsPackage(K,symb,PolyRing,E,ProjPt)
```

Les deux paquetages suivants réalisent tous les algorithmes liés aux calculs des séries $\mathfrak{P}$-adiques.

```
ParamSplPt := LocalParametrizationOfSimplePointPackage(K,symb,PolyRing,E,
                                                 ProjPt,PCS,Plc)
ParamPack  := ParametrizationPackage(K,symb,PolyRing,E,ProjPt,PCS,Plc)
```

Viennent ensuite les paquetages concernant les calculs liés aux diviseurs.

```
IntDivPack := IntersectionDivisorPackage(K,symb,PolyRing,E,
                                  ProjPt,PCS,Plc,Div,ICP,DesTree)
IntFrmPack := InterpolateFormsPackage(K,symb,PolyRing,E,ProjPt,PCS,Plc,Div)
```

Finalement, on a le paquetage qui gère tous les calculs liés aux arbres de désingularisation.

```
DesTrPack  := DesingTreePackage(K,symb,PolyRing,E,ProjPt,PCS,Plc,Div,ICP,DesTree)
```

On peut maintenant commencer les calculs. On définit le polynôme de définition de la courbe.

```
(1) -> C:PolyRing:= X**5 Y**2 * Z**3 + Y * Z**4

          5    2 3      4
         X  + Y Z  + Y Z
```

On calcule les points singuliers et on assigne l'unique point singulier à la variable "pt".

```
(2) -> singularPoints(C)$RSP

                 1
         [(0:1:0) ]

(3) -> pt:=%.1

                1
         (0:1:0)
```

L'exposant accolé au point indique le degré du point.

Pour éclater le point "`pt`", il faut d'abord créer un point infiniment voisin (d'ordre 0) lui correspondant.

```
(4) -> create(pt,C)$ICP

                                  5    2 3      4                      1
   [name= %P0, mult= 0, defCurve= X  + Y Z  + Y Z , localPoint= (0:1:0) ,
    chart= [0,0,2], expD= 0]
```

Ensuite, on applique la fonction "`blowUp`" :

```
(5) -> blowUp(ipt0)$DesTrPack

                                      2      4    3                      1
    [ [name= %I1, mult= 0, defCurve= X  + X Z  + Z , localPoint= (0:1:0) ,
       chart= [1,3,2], expD= 0] ]
```

La fonction "`blowUp`" retourne une liste de points infiniment voisins. Ici, il n'y en a qu'un. La liste d'entiers "`[1,3,2]`" est utilisée pour repérer la coordonnée exceptionelle du point et le voisinage affine standard utilisé : le premier entier indique la position de la variable dans la liste "`[X,Y,Z]`" correspondant à la coordonnée exceptionelle. Le dernier entier donne la position de la dernière coordonnée non nulle du point de la courbe dominé par le point infiniment voisin (évidemment, le second entier est redondant car il se déduit des deux autres, mais il est commode de l'avoir sous la main). Un point infiniment voisin représentant un point de la courbe a toujours un "`chart`" de la forme $[0, 0, n]$. Notons que la multiplicité du point n'est pas calculée : elle ne le sera que si l'on éclate le point (cf. plus loin).

On peut éclater maintenant l'unique point infiniment voisin : on constate que celui-ci ne possède qu'un seul point infiniment voisin et ce dernier sera éclaté à son tour.

```
(6) -> ipt1:=first %;

(7) -> blowUp(ipt1)$DesTrPack

                                      2      3                         1
     [[name= %I2, mult= 0, defCurve= X  + X Z  + Z, localPoint= (0:1:0) ,
       chart= [3,1,2], expD= 0]]

(8) -> ipt2:=first %;

(9) -> blowUp(ipt2)$DesTrPack

         []
```

Une liste vide est retournée lorsqu'on éclate un point simple. Observons que les multiplicités de chacun des points ont été calculées et assignées par effet de bord.

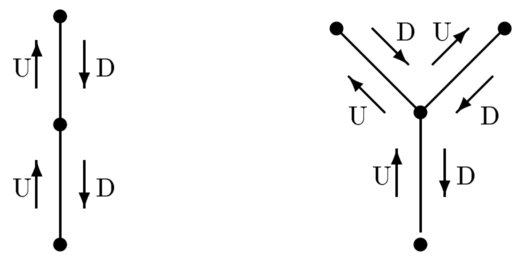

Fig. 3.1 – *Les arbres ci-dessus sont respectivement ceux donnés par "UUDD" et "UUDUDD".*

(10) -> `ipt0`

```
                                  5    2 3      4                       1
   [name= %P0, mult= 3, defCurve= X  + Y Z  + Y Z , localPoint= (0:1:0) ,
    chart= [0,0,2], expD= 0]
```

(11) -> `ipt1`

```
                                   2      4    3                       1
    [name= %I2, mult= 2, defCurve= X  + X Z  + Z , localPoint= (0:1:0) ,
     chart= [1,3,2], expD= 0]
```

(12) -> `ipt2`

```
                                   2      3                          1
    [name= %I2, mult= 1, defCurve= X  + X Z  + Z, localPoint= (0:1:0) ,
     chart= [3,1,2], expD= 0]
```

On vient de calculer l'arbre de désingularisation. Il est clair qu'il est en général fastidieux de le faire ainsi, c'est-à-dire "à la main". On utilisera plutôt :

(13) -> `desTree:=desingTreeAtPoint(C,pt,[0,0,2],pt)$DesTrPack`

```
       "UUDD"
```

Il s'agit bien ici d'un arbre de désingularisation mais sous forme "encodé". On se reportera à la Figure 3.1 pour l'interprétation de "`UUDD`".

Pour afficher l'arbre de désingularisation au complet, on appelle la fonction suivante :

(14) -> `fullOutput(true)$DesTree`

(15) -> **desTree**

```
                                  5    2 3      4                    1
   [name= %RI0, mult= 3, defCurve= X  + Y Z  + Y Z , localPoint= (0:1:0) ,
    chart= [0,0,2], expD= 0]
                                    2      4    3                    1
      [name= %I0, mult= 2, defCurve= X  + X Z  + Z , localPoint= (0:1:0) ,
       chart= [1,3,2], expD= 0]
                                       2      3                        1
         [name= %I1, mult= 1, defCurve= X  + X Z  + Z, localPoint= (0:1:0) ,
          chart= [3,1,2], expD= 0]
```

Les diviseurs exceptionnels ne sont toujours pas calculés. Pour les obtenir, il faut d'abord calculer les paramétrisations locales des places dominant le point P.

(16) -> **initializeParamOfPlaces(desTree)$DesTrPack**

(17) -> **desTree**

```
                                  5    2 3      4                    1
   [name= %RI0, mult= 3, defCurve= X  + Y Z  + Y Z , localPoint= (0:1:0) ,
    chart= [0,0,2], expD= 0]
                                    2      4    3                    1
      [name= %I0, mult= 2, defCurve= X  + X Z  + Z , localPoint= (0:1:0) ,
       chart= [1,3,2], expD= 0]
                                       2      3                        1
         [name= %I1, mult= 1, defCurve= X  + X Z  + Z, localPoint= (0:1:0) ,
                                 1
          chart= [3,1,2], expD= %I1 ]
```

Observons que seul le diviseur exceptionnel de la feuille de l'arbre est calculé : en fait, il n'y a pas de calcul à faire car une feuille est un point simple. Par contre, une place a été créée pour cette feuille qui est représentée par le symbole "`%I1`" et l'exposant qui lui est associé est son degré. De plus, la paramétrisation associée à la feuille et la paramétrisation locale de la place ont été calculées.

La séquence "`first leaves desTree`" extrait la première feuille de la liste des feuilles de l'arbre "`desTree`". La fonction "`localParamV`" retourne la paramétrisation associée à un point infiniment voisin (si le point n'est pas une feuille alors une liste vide est retournée).

(18) -> **localParamV first leaves desTree**

```
                2    7     12     22     27     42     47
         [t,  1,  t  + t  + t   + t   + t   + t   + t  + ... ]
```

On peut extraire la paramétrisation locale de la place correspondant à l'unique feuille de l'arbre comme suit :

(19) -> `localParam first supp excpDivV first leaves desTree`

```
     3     8     13     23     28     43     48     53     83     88
   [ t  + t  + t   + t   + t   + t   + t   + t   + t   + t   + ...,

    1,

     5     15     25     45
    t  + t   + t   + t   + ... ]
```

On peut maintenant calculer les diviseurs exceptionnels de chacun des points infiniment voisins de l'arbre et calculer le diviseur d'adjonction $\mathcal{A}_P$ du point singulier $P = (0:1:0)$: observons que $\mathcal{A}_P$ est aussi le diviseur d'adjonction de la courbe car P est l'unique point singulier de la courbe.

(20) -> `blowUpWithExcpDiv(desTree)$DesTrPack`

(21) -> `desTree`

```
                                    5    2 3      4                      1
   [name= %RI0, mult= 3, defCurve= X  + Y Z  + Y Z , localPoint= (0:1:0) ,
                                1
    chart= [0,0,2], expD= 3 %I1 ]
                                      2      4    3                      1
      [name= %I0, mult= 2, defCurve= X  + X Z  + Z , localPoint= (0:1:0) ,
                                   1
       chart= [1,3,2], expD= 2 %I1 ]
                                         2      3                          1
         [name= %I1, mult= 1, defCurve= X  + X Z  + Z, localPoint= (0:1:0) ,
                                     1
          chart= [3,1,2], expD= %I1 ]
```

(22) -> `A:=adjunctionDivisor(desTree)$DesTrPack`

```
           1
        8 %I1
```

Ainsi, le diviseur d'adjonction $\mathcal{A}$ de la courbe $\mathcal{C}$ est de degré 8. D'après la Proposition 2.6.4, le corps de fonctions $K(\mathcal{C})$ a pour genre

$$g = \frac{(5-1)(5-2)}{2} - \frac{1}{2}\deg \mathcal{A} = 6 - 4 = 2.$$

On construit maintenant une place de degré 3. Si une telle place existe, elle doit correspondre à un point simple de la courbe et ce point sera aussi de degré 3. La fonction suivante retourne tous les points de la courbe rationnels sur une extension de degré 3 de K, soit le corps $\mathbb{F}_{2^3}$.

(23) -> **rationalPoints(C,3)$RSP**

```
           1         1            2        3             2    3         1
[(0:1:1) ,(0:0:1) ,(%D14:%D14  + 1:1) ,(%D14:%D14 :1) ,(0:1:0) ]
```

(24) -> **Q:=%.3**

```
           2        3
(%D14:%D14  + 1:1)
```

Comme on le voit, il y a 3 points de degré 1 et deux de degré 3. Pour construire la place de degré 3, on utilisera le point assigné à la variable "`Q`". Le symbole "`%D14`" représente un élément de "`PACOFF`" et est une racine distinguée d'un certain polynôme irréductible. La fonction "`previousTower`" permet de déduire sur quelle tour l'élément est distingué (note : "`Q.1`" réfère à la première coordonnée de "`Q`").

(25) -> **previousTower Q.1**

```
1
```

La fonction ayant retourné un élément du corps de base K, on en déduit que "`%D14`" est une racine K-distinguée du polynôme :

(26) -> **definingPolynomial Q.1**

```
  3     2
 ?  + ?  + 1
```

Pour créer la place représentée par le point simple Q, on procède comme suit :

(27) -> **Qplace := pointToPlace(Q,C)$ParamSplPt**

```
           2        3
[%D14,%D14  + 1,1]
```

La place est représentée par les coordonnés du point Q (on remarquera aussi qu'une place est affichée en utilisant des crochets "`[...]`" plutôt que des parenthèses). On notera que la fonction "`pointToPlace`" s'occupe de calculer la paramétrisation locale de la place qui est retournée par la fonction "`localParam`" (cette fonction ne fait aucun calcul, elle ne fait que retourner la paramétrisation locale déja calculée).

(28) -> `localParam Qplace`

```
[ %D14 + t,

        2           2                     2       2        4    5
   %D14  + 1 + (%D14  + %D14 + 1)t + %D14 t  + (%D14  + %D14)t  + t

 +
              8    10        2      16    20        2         32
   (%D14 + 1)t  + t   + (%D14  + 1)t   + t   + (%D14  + %D14)t   + ... ,

  1 ]
```

Notons $\mathfrak{Q}$ la place "`Qplace`" et posons $D := 2\mathfrak{Q}$. Je vais maintenant calculer une base de $\mathcal{L}(D)$ en appliquant l'algorithme de Brill-Noether. Il faut d'abord construire le diviseur D :

(29) -> `D:= 2 * (Qplace :: Div)`

```
                  2         3
     2 [ %D14, %D14  + 1, 1 ]
```

Je reprends maintenant, étape par étape, l'Algorithme 2.8.17. À l'étape 1, on pose

(30) -> `B:=D + A`

```
                   2         3        1
      2 [ %D14, %D14  + 1, 1 ]  + 8 %I1
```

Ensuite, il faut déterminer $d \in \mathbb{N}$ assez grand pour qu'il existe un polynôme $G \in K[X,Y,Z]$ homogène de degré d, non divisible par C et tel que $(G) \geq B$. D'après le Lemme 2.7.5, il suffit de prendre $d = 10$. On fixe une base de l'espace vectoriel $S_d(K) \cup \{0\}$:

(31) -> `Hpol:=listAllMono(10)$PackPoly`

```
  10     9   2 8          10
[Z  , Y Z , Y Z , ... , X  ]
```

Les étapes 4 à 8 sont prises en charge par la fonction "`interpolateForms`" et on choisit un polynôme d'interpolation à l'étape 9. On prend ici le premier retourné par la fonction "`interpolateForms`".

(32) -> `G0:= first interpolateForms(D+A,10,C,Hpol)$IntFrmPack`

```
 8 2    10
X Y  + Z
```

Le polynôme "`G0`" sera le dénominateur commun à tous les éléments de la base de $\mathcal{L}(D)$. On calcule ensuite le diviseur d'intersection (G_0).

(33) -> **divG0:=intersectionDivisor(G0,C,[desTree],[pt])$IntDivPack**

```
        1              2      3              9      10
24 %I1  + 2 [%D14,%D14  + 1,1]  + 2 [%D21,%D21  + 1,1]
```

(34) -> **degree divG0**

```
50
```

Le diviseur (G_0) est de degré 50 comme le prédit le Théorème de Bézout. Observons aussi qu'il y a une place de degré 10 et une place de degré 3 dans le support de (G_0). Si le domaine "`PACOFF`" n'était pas utilisé, une extension de degré 30 du corps K aurait été nécessaire. Pour finir, on calcule une base de l'espace vectoriel des polynômes d'interpolation du diviseur $(G_0) - D$:

(35) -> **lBaseNumer:=interpolateForms(divG0 - D,10,C,Hpol)$IntFrmPack**

La variable "`lBaseNumer`" contient les cinq polynômes suivants :

$$\begin{aligned}
G_1 &:= X^8Y^2 + Z^{10},\\
G_2 &:= X^9Y + X^8Z^2 + X^7Y^2Z + X^7YZ^2 + X^6Y^2Z^2 +\\
&\quad X^5Y^5 + X^5Y^4Z + X^5Y^3Z^2 + X^4Y^3Z^3 + X^4Z^6 + Y^7Z^3,\\
G_3 &:= X^{10} + X^9Y + X^8Y^2 + X^7Y^3 + X^6Y^2Z^2 +\\
&\quad X^6Z^4 + X^2Y^5Z^3 + XZ^9,\\
G_4 &:= X^9Z + X^8Y^2 + X^8YZ + X^7Y^2Z + X^6Y^4 +\\
&\quad X^6Y^3Z + X^5Y^2Z^3 + X^5Z^5 + XY^6Z^3,\\
G_5 &:= X^{10} + X^9Y + X^8Y^2 + X^7Y^3 + X^7Y^2Z +\\
&\quad X^7Z^3 + X^6YZ^3 + X^6Z^4 + X^5Y^3Z^2 +\\
&\quad X^5Y^2Z^3 + X^3Y^4Z^3 + X^2Y^5Z^3 + X^2Z^8
\end{aligned}$$

Ainsi, $\mathcal{L}(D)$ a pour base

$$B := \left\{ \overline{G}_i/\overline{G}_0 \;\middle|\; i = 1, 2, \ldots, 5 \right\}$$

et $\ell(D) = 5$ comme prévu par le Théorème de Riemann-Roch car $6 = \deg D \geq 2g - 1 = 5$ entraîne

$$\ell(D) = \deg D - g + 1 = 6 - 2 + 1 = 5.$$

On construit maintenant un code sur $K' := \mathbb{F}_{2^4}$. Soient donc $F' := K'(\mathcal{C})$ et $\mathfrak{Q}'$ une place de F'/K' dominant la place $\mathfrak{Q}$. En utilisant la Proposition 2.8.9, on peut montrer que $\mathfrak{Q}'$ est l'unique place de F'/K' dominant la place $\mathfrak{Q}$. Par conséquent

$$D' := \mathrm{Con}_{F'/F} D = 2\mathfrak{Q}'$$

et $\mathcal{L}(D')$ admet B pour base. Pour construire le code $C_{\mathcal{L}}(F', \mathcal{P}, D')$ où $\mathcal{P}$ est la somme des 33 places de F'/K', il faut faire les calculs sur le corps $\mathbb{F}_{2^4}$. On doit donc redéfinir tous les polynômes considérés, les domaines et les paquetages en fonction du corps K'.

```
K'            := FiniteFieldCyclicGroup(2,4)
PolyRing'     := DMP(symb,K')
ProjPt'       := PlaneProjectivePoint(K')
PCS'          := NeitherSparseOrDensePowerSeries(K')
Plc'          := Places(K')
RSP'          := RationalAndSingularPointsPackage(K',...)
ParamSplPt'   := LocalParametrizationOfSimplePointPackage(K',...)
ParamPack'    := ParametrizationPackage(K',...)
C':PolyRing'  := X**5  Y**2 * Z**3  + Y * Z**4
G0':PolyRing':= G0 :: PolyRing'
lBaseNumer'   := lBaseNumer :: List PolyRing'
```

On calcule tous les points simples de $\mathcal{C}$ rationnels sur K' :

(36) `-> setDifference(rationalPoints(C',1)$RSP',singularPoints(C')$RSP')`

```
        1         1        10   1             5   1     1   4   1     1   1   1
[(0:1:1) , (0:0:1) , (1:%A   :1) , ..., (1:%A :1) , (%A :%A :1) , (%A :%A :1) ]
```

Ensuite, on crée pour chacun des points simples la place correspondante :

(37) `-> plc':=setUnion( [pointToPlace(p,C')$ParamSplPt' for p in splPt'], supp A)`

```
        1         1        10   1             5   1     1   4   1     1   1   1
[[0,1,1] , [0,0,1] , [1,%A   ,1] , ..., [1,%A ,1] , [%A ,%A ,1] , [%A ,%A ,1] ]
```

Pour chaque polynôme G' de "`lBaseNumer'`" et pour chaque place $\mathfrak{w}$ de "`plc'`", on calcule la série $\mathfrak{w}$-adique

$$G'[\mathfrak{w}]/G'_0[\mathfrak{w}] \in K'((t)).$$

(38) `-> [[parametrize(G',G0',pl)$ParamPack' for pl in plc'] for G' in lBaseNumer'];`

Le terme constant de la série $G'[\mathfrak{w}]/G'_0[\mathfrak{w}]$ est exactement l'évaluation de $\overline{G}'/\overline{G}'_0$ à la place $\mathfrak{w}$.

(39) `-> matrix [[findCoef(s,0) for s in l] for l in %];`

On fait de même pour la place correspondant à la place "`%I1`". Observons par contre que la place "`%I1`" a été calculée par les paquetages définis sur K et non sur K'. Il faut donc utiliser les paquetages déclarés pour K.

(40) `-> [parametrize(G,G0,first supp A)$ParamPack for for G in lBaseNumer];`

```
(41) -> [findCoef(s,0) for s in %]

    [1,0,1,1,0]
```

En transposant ce qui précède et en l'ajoutant à la matrice du calcul (39), on obtient une matrice génératrice du code $C_{\mathcal{L}}(F', \mathcal{P}, D)$:

$$\left[\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots \\ 1 & 0 & \alpha^{10} & \alpha^{5} & \alpha^{9} & \alpha^{14} & \alpha^{3} & \alpha^{13} & \alpha^{9} & \alpha^{13} & \alpha^{11} & \alpha^{6} & \alpha^{12} & \alpha^{3} & \alpha^{11} & \alpha^{3} & \cdots \\ 0 & 0 & \alpha^{5} & \alpha^{10} & \alpha^{6} & 0 & \alpha^{12} & 0 & \alpha^{14} & \alpha^{7} & 0 & \alpha^{9} & \alpha^{13} & \alpha^{7} & \alpha^{14} & \alpha^{13} & \cdots \\ 0 & 0 & \alpha^{10} & \alpha^{5} & \alpha^{10} & 1 & \alpha^{5} & 1 & \alpha^{12} & \alpha^{1} & 1 & \alpha^{10} & \alpha^{2} & \alpha^{8} & \alpha^{2} & \alpha^{9} & \cdots \\ 0 & 0 & 1 & 1 & \alpha^{8} & \alpha^{1} & \alpha^{1} & \alpha^{2} & \alpha^{8} & \alpha^{2} & \alpha^{4} & \alpha^{2} & \alpha^{4} & \alpha^{1} & \alpha^{4} & \alpha^{1} & \cdots \end{matrix}\right.$$

$$\left.\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha^{14} & \alpha^{10} & \alpha^{7} & \alpha^{12} & \alpha^{14} & \alpha^{12} & \alpha^{6} & \alpha^{9} & \alpha^{5} & \alpha^{7} & \alpha^{6} & \alpha^{7} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^{5} & 0 \\ \alpha^{5} & 1 & 0 & \alpha^{3} & \alpha^{11} & \alpha^{7} & \alpha^{14} & \alpha^{11} & 1 & \alpha^{10} & \alpha^{11} & \alpha^{13} & 1 & \alpha^{5} & \alpha^{10} & 1 & 1 \\ \alpha^{6} & \alpha^{2} & 1 & \alpha^{5} & \alpha^{8} & \alpha^{6} & \alpha^{1} & \alpha^{4} & \alpha^{1} & \alpha^{3} & \alpha^{3} & \alpha^{4} & \alpha^{8} & \alpha^{9} & \alpha^{12} & \alpha^{4} & 1 \\ \alpha^{1} & 1 & \alpha^{8} & \alpha^{4} & \alpha^{1} & \alpha^{4} & \alpha^{2} & \alpha^{8} & 1 & \alpha^{8} & \alpha^{2} & \alpha^{8} & 1 & \alpha^{4} & \alpha^{2} & 1 & 0 \end{matrix}\right]$$

D'après la Proposition 1.6.2, le code $C_{\mathcal{L}}(F', \mathcal{P}, D)$ est un $[n, k, d]_{2^4}$-code où

$$\left\{\begin{array}{lcl} n & = & 33 \\ k & = & 5 \\ d & \geq & n - \deg D = 27. \end{array}\right.$$

On remarquera que la troisième ligne de la matrice génératrice est de poids 27. Par conséquent, $C_{\mathcal{L}}(F', \mathcal{P}, D)$ est un $[33, 5, 27]_{2^4}$-code.

3.9.2 Le paquetage `PAFFFF`

Afin de faciliter l'utilisation de mon logiciel, j'ai regroupé en un seul paquetage tous les paquetages que j'ai implantés. Il s'appelle

`PackageForAlgebaicFunctionFieldOverFiniteField`

et a pour abréviation "`PAFFFF`". Il prend pour seuls arguments un corps fini et une liste de trois symboles identifiant les variables de l'anneau de polynômes S. Il exporte entre autres les fonctions suivantes :

```
setCurve: PolyRing -> PolyRing
genus: () -> NNI
desingTree: () -> LIST DesTree
rationalPoints: () -> LIST(ProjPt)
```

```
singularPoints: () -> LIST(ProjPt)
parametrize: (PolyRing,Plc) -> PCS
lBasis: Div -> Record(num:List PolyRing, den: PolyRing)
interpolateForms: (Div,NNI) -> LIST(PolyRing)
eval: (PolyRing,PolyRing,Plc) -> K
intersectionDivisor: PolyRing -> Div
adjunctionDivisor: () -> Div
goppaCode: (Div,Div) -> Matrix K
```

Voici un exemple de son utilisation. On considère le corps $K := \mathbb{F}_{2^2}$ et le corps de fonctions $F := K(x_1, x_2, x_3)$ où les x_i vérifient :

$$\left\{ \begin{array}{lcrcl} C_1 & := & x_2^2 x_1 + x_2 + x_1^2 & = & 0 \\ C_2 & := & x_3^2 x_2 + x_3 + x_2^2 & = & 0 \end{array} \right.$$

Le corps F est une extension du type d'Artin-Schreier du corps rationnel $K(x_1)$ et K est son corps des constantes. C'est en faisant des calculs expérimentaux sur ce corps que j'ai déduit la méthode de construction effective dont il est question au Chapitre 4. Ces calculs consistaient à déterminer les séries $\mathfrak{P}$-adiques des fonctions x_i où $\mathfrak{P}$ est un zéro ou un pôle de x_i. Je montre ici comment ou peut le faire à l'aide de mon logiciel.

Il faut un modèle plan du corps de fonctions F/K. En calculant une base de Groebner B de l'idéal engendré par les polynômes C_1 et C_2 avec l'ordre lexicographique $x_2 > x_1 > x_3$, on trouve deux relations données par deux polynômes de B :

$$0 = x_2 x_3^3 + x_2 + x_1^3 x_3^2 + x_1^2 x_3^6 + x_1^2 + x_1 x_3^4 + x_1 x_3 + x_3^5 \tag{3.9}$$

$$0 = x_1^4 + x_1^3\, x_3^4 + x_1 x_3^3 + x_3 \tag{3.10}$$

De la première on déduit :

$$x_2 = \frac{x_1^3 x_3^2 + x_1^2 x_3^6 + x_1^2 + x_1 x_3^4 + x_1 x_3 + x_3^5}{x_3^3 + 1}$$

d'où $x_2 \in K(x_1, x_3)$ et donc

$$F := K(x_1, x_3).$$

On peut montrer que $[F : K(x_1)] = 4$ (voir Chapitre 4, Théorème 4.1.3). Par conséquent, d'après l'équation (3.10), le polynôme

$$X_1^4 + X_1^3 X_3^4 + X_1 X_3^3 + X_3$$

est le polynôme de définition de l'ensemble de coordonnées $\{x_1, x_3\}$. Le corps de fonctions F/K est donc le corps des fonctions de la courbe projective plane $\mathcal{C} := \{C = 0\}$ définie sur K où

$$C := X_1^4 Z^3 + X_1^3 X_3^4 + X_1 X_3^3 Z^3 + X_3 Z^6.$$

On peut maintenant faire les calculs en Axiom.

```
K    := FFCG(2,2)
symb := [X1, X3, Z]
P    := PAFFFF(K,symb)
```

L'anneau de polynômes utilisé par "PAFFFF" est "DistributedMultivariate-Polynomial" qui est fourni avec Axiom :

```
R    := DMP(symb,K)
```

Un fois le paquetage "PAFFFF" déclaré avec les bons paramètres, on lui fournit le polynôme de la courbe.

```
(1) -> setCurve( X1**4 * Z**3 + X1**3 * X3**4 + X1 * X3**3 * Z**3 + X3 * Z**6 )$P

         4 3     3  4         3 3       6
       X1 Z  + X1 X3  + X1 X3 Z  + X3 Z
```

On peut demander alors les points singuliers, les arbres de désingularisation correspondants, le diviseur d'adjonction et le genre.

```
(2) -> singularPoints()$P

                 1        1        1    1   1   1    2   2   1
         [(1:0:0) ,(0:1:0) ,(1:1:1) ,(%A :%A :1) ,(%A :%A :1) ]
```

Le symbole "%A" représente un élément primitif $\alpha \in K$ qui vérifie $\alpha^2 + \alpha + 1 = 0$.

```
(3) -> desingTree()$P

       [".U","..U.UU",".U.U",".U.U",".U.U"]

(4) -> adjunctionDivisor()$P

              1        1        1       1       1       1       1       1       1
         6 %I0  + 3 %I2  + 5 %I3  + %I4  + %I5  + %I6  + %I7  + %I8  + %I9

(5) -> genus()$P

        5
```

Pour calculer les séries $\mathfrak{P}$-adiques de x_1, x_2 et x_3, il faut d'abord les exprimer comme quotient de formes de même degré dans l'anneau de coordonnées de la courbe projective $\mathcal{C}$:

$$\begin{aligned} x_1 &\equiv X_1/Z, \\ x_2 &\equiv H_1/H_2, \\ x_3 &\equiv X_3/Z, \end{aligned}$$

où

$$\begin{aligned} H_1 &= X_1^3X_3^2Z^3 + X_1^2X_3^6 + X_1^2Z^6 + X_1X_3^4Z^3 + X_1X_3Z^6 + X_3^5Z^3, \\ H_2 &= X_3^3Z^5 + Z^8 \end{aligned}$$

Ainsi, pour calculer la série $\mathfrak{P}$-adique de x_2 en fonction du paramètre local de la paramétrisation locale $[\mathfrak{P}]$, il suffit de calculer $H_1[\mathfrak{P}]/H_2[\mathfrak{P}]$. Prenons par exemple l'unique place $\mathfrak{P}$ de F/K qui est un pôle commun de x_1, x_2 et x_3 (cf. Chapitre 4, Corollaire 4.4.10). On obtient cette place en calculant le diviseur principal $(x_1) = (X_1) - (Z)$ car dans ce cas $(x_1)_\infty = \mathfrak{P}$.

```
(6) -> divx1:= intersectionDivisor(X1)$P - intersectionDivisor(Z)$P

             1          1        1        1
   [0,0,1]   + 2 %I2   + %I3 - 4 %I0
```

La place $\mathfrak{P}$ est représentée par "%I0" et $\deg \mathfrak{P} = 1$. On assigne à la variable "Pplace" la place "%I0",

```
(7) -> Pplace:= first suppOfPole divx1

       1
   %I0
```

et on calcule $x_2(t) = H_1[\mathfrak{P}]/H_2[\mathfrak{P}]$ où t est le paramètre local utilisé pour $[\mathfrak{P}]$. On définit d'abord les polynômes,

```
(8) -> H1 :R := X1**3 * X3**2 * Z**3 + ... + X3**5 *Z**3

     3   2 3      2  6      2 6         4 3           6      5 3
   X1  X3  Z  + X1  X3  + X1  Z  + X1 X3  Z  + X1 X3 Z  + X3  Z


(9) -> H2 :R := X3**3 * Z**5 + Z**8

     3 5    8
   X3  Z  + Z
```

et par la suite, on calcule $x_2(t) = H_1[\mathfrak{P}]/H_2[\mathfrak{P}]$:

```
(10) -> parametrize(H1,Pplace)$P / parametrize(H2,Pplace)$P

    - 2        4    10    22    46    94
   t    + t + t  + t   + t   + t   + t   + ...
```

3.9.3 Construction effective de codes géométriques auto-duaux

Le premier critère sur les codes géométriques auto-duaux a été donné par Y. Driencourt et J.F. Michon [6] pour des codes construits à partir de courbes elliptiques. En considérant les codes *quasi auto-duaux*, H Stichtenoth [42] a donné un critère généralisé à toute courbe quelqu'en soit le genre. Un critère équivalent est donné par W. Scharlau [39] mais il est exprimé en terme du groupe des classes d'un corps de fonctions. Tous ces critères sont suffisants pour qu'un code géométrique soit quasi auto-dual. En revanche, Y. Driencourt et H. Stichtenoth [7] de même que C. Munuera et R. Pellikaan [36], montrent que ces critères sont nécessaires sous certaines conditions.

Soient $K := \mathbb{F}_q$ et deux codes linéaires, C_1 et C_2, définis sur K de longueur n. Considérons le produit terme à terme de deux vecteurs $a = (a_1, a_2, \dots, a_n) \in K^n$ et $b = (b_1, b_2, \dots, b_n) \in K^n$ défini par

$$a * b = (a_1 b_1, a_2 b_2, \dots, a_n b_n) \in K^n.$$

On dit que C_1 est **quasi égal** à C_2 s'il existe $a = (a_1, a_2, \dots, a_n) \in K^n$ tel que $a_i \neq 0$ pour $i = 1, 2, \dots, n$ et

$$C_1 = a * C_2 = \{\, a * b \;|\; b \in C_2 \,\}.$$

On dira qu'un code C est **quasi auto-dual** si C est quasi égal à son dual, c'est-à-dire s'il existe $a = (a_1, a_2, \dots, a_n) \in K^n$ tel que $a_i \neq 0$ pour $i = 1, 2, \dots, n$ et

$$a * C = C^{\perp}.$$

Remarque 3.9.1 Soient C un code quasi auto-dual et $a \in K^n$ tel que $a * C = C^{\perp}$. Supposons qu'il existe $b \in K^n$ tel que $b * b = a$. Alors $b * C = (b * C)^{\perp}$ d'où le code $b * C$ est auto-dual. Observons qu'un tel b existe si K est de caractéristique 2.

Le théorème suivant donne une caractérisation des codes géométriques quasi auto-duaux.

Théorème 3.9.2 *Soit F/K un corps de fonctions de genre g. Soient $k \in \mathbb{N}^*$, $n := 2k$ et le diviseur*

$$\mathcal{P} = \mathfrak{P}_1 + \mathfrak{P}_2 + \cdots + \mathfrak{P}_n$$

où les places $\mathfrak{P}_i$ sont deux à deux distinctes et $\deg \mathfrak{P}_i = 1$ pour $i = 1, 2, \dots, n$. Soit D un diviseur tel que $\mathrm{supp} D \cap \mathcal{P} = \emptyset$.

1. *Si $2D - \mathcal{P}$ est un diviseur canonique de F/K, alors le code $C_{\mathcal{L}}(F, \mathcal{P}, D)$ est quasi auto-dual.*

2. *Si $n > 2g+2$ et $C_{\mathcal{L}}(F, \mathcal{P}, D)$ est quasi auto-dual, alors $2D - \mathcal{P}$ est un diviseur canonique de F/K.*

Démonstration : (1) [45, Th. 3.1.46]. (2) [35, Th. 5.5].

Théorème 3.9.3 *Avec les mêmes notations qu'au théorème précédent, s'il existe un diviseur A tel que $2A \equiv \mathcal{P}$, alors il existe un diviseur D tel que $C_{\mathcal{L}}(F, \mathcal{P}, D)$ est quasi auto-dual.*

Démonstration : Scharlau [39, 6, Satz 1].

Remarque 3.9.4 On peut montrer [5] que l'existence d'un diviseur A tel que $2A \equiv \mathcal{P}$ est équivalente à l'existence d'un diviseur D tel que $2D - \mathcal{P}$ est un diviseur canonique. Le Théorème 3.9.3 est donc équivalent à la première assertion du Théorème 3.9.2.

La construction des codes géométriques quasi auto-duaux que je propose est basée sur le *groupe des classes* d'un corps de fonctions F/K : soient $\mathcal{D}_F$ le groupe des diviseurs de F/K, le sous-groupe des diviseurs principaux

$$\mathrm{Pr}_F := \{ (u) \mid u \in F \}$$

et considérons le groupe quotient

$$Cl_F := \mathcal{D}_F / \mathrm{Pr}_F.$$

On note $[A]$ la classe de $A \in \mathcal{D}_F$ dans Cl_F. Si deux diviseurs $A, B \in \mathcal{D}_F$ sont tels que $[A] = [B]$, alors il est clair que $\deg A = \deg B$. Par conséquent, l'ensemble

$$Cl_F^0 := \{ [A] \in Cl_F \mid A \in \mathcal{D}_F, \ \deg A = 0 \}$$

est un sous-groupe de Cl_F. Le sous-groupe Cl_F^0 est appelé le **groupe des classes** de F/K.

Théorème 3.9.5 *Soit F/K un corps de fonctions. Si K est un corps fini, alors le groupe des classes Cl_F^0 est fini. On appelle l'ordre du groupe Cl_F^0 le* **nombre de classes** *et on le note h_F.*

Démonstration : Stichtenoth [43, Prop. V.1.3].

La construction effective des codes géométriques quasi auto-duaux repose sur la proposition suivante :

5. Il existe une preuve élémentaire dans le cas où le corps de base est de caractéristique 2 (voir [45, Prop. 2.3.21]).

PROPOSITION 3.9.6 *Soit F/K un corps de fonctions de genre g. Soient $k \in \mathbb{N}^*$, $n := 2k$ et le diviseur*

$$\mathcal{P} = \mathfrak{P}_1 + \mathfrak{P}_2 + \cdots + \mathfrak{P}_n$$

où les places $\mathfrak{P}_i$ sont deux à deux distinctes et $\deg \mathfrak{P}_i = 1$ pour $i = 1, 2, \ldots, n$. Supposons que

1. *le groupe des classes Cl_F^0 soit monogène d'ordre $h > 1$ non divisible par 2,*
2. *il existe un diviseur A tel que $[A] \in Cl_F^0$ soit un générateur du groupe Cl_F^0 et tel que $\mathrm{supp} A \cap \mathrm{supp} \mathcal{P} = \emptyset$,*
3. *il existe un diviseur B tel que $\deg B = 1$ et $\mathrm{supp} B \cap \mathrm{supp} \mathcal{P} = \emptyset$.*

Alors il existe un entier $m \in \{0, 1, \ldots, (h-1)\}$ tel que, si on pose

$$D := (k + g - 1)B + mA,$$

le code géométrique $C_{\mathcal{L}}(F, \mathcal{P}, D)$ est quasi auto-dual.

Démonstration : Puisque 2 ne divise pas h, $[2A]$ est aussi un générateur du groupe Cl_F^0. Il existe donc un entier m_1 tel que

$$\mathcal{P} \equiv nB + 2m_1 A = 2kB + 2m_1 A.$$

Soit maintenant W un diviseur canonique de F/K. D'après le Corollaire 1.5.2, on a $\deg W = 2g - 2$. Il existe donc un entier m_2 tel que

$$W \equiv (2g - 2)B + 2m_2 A.$$

Soit $m \in \{0, 1, \ldots, (h-1)\}$ tel que $m = m_1 + m_2 \pmod{h}$ et posons

$$D := (k + g - 1)B + 2mA.$$

Alors

$$\begin{aligned} 2D - \mathcal{P} &\equiv 2(k + g - 1)B + 2mA - 2kB - 2m_1 A \\ &\equiv (2g - 2)B + 2m_2 A \\ &\equiv W. \end{aligned}$$

Le diviseur $2D - \mathcal{P}$ est donc un diviseur canonique d'après le Corollaire 1.5.3. La proposition est alors une conséquence du Théorème 3.9.2. □

Le calcul du nombre de classes d'un corps de fonctions F/K fait appel à la fonction *Zéta* du corps de fonctions (pour plus de détails sur ce qui suit on se reportera à [43, Sec. V.1]). Soit

$$A_n := \#\{ A \in \mathcal{D}_F \mid A \geq 0, \deg A = n \},$$

c'est-à-dire le nombre de diviseurs effectifs de degré n du corps de fonctions F/K. La fonction Zéta de F/K est la série

$$Z(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}((t)).$$

Cette série est convergente si $|t| < q^{-1}$. On peut montrer que

$$L(t) := (1-t)(1-qt)Z(t)$$

est un polynôme. Il s'appelle le L-polynôme de F/K. Pour $r \in \mathbb{N}^*$, posons $K_r := \mathbb{F}_{q^r}$ et $F_r := K_r F$. Posons de plus

$$N_r := \#\{\,\mathfrak{P} \in \mathbb{P}_{F_r} \mid \deg \mathfrak{P} = 1\,\}$$

et

$$S_r := N_r - (q^r + 1).$$

L'entier N_r est le nombre de places de degré 1 du corps de fonctions F_r/K_r. Le théorème qui suit permet de calculer le nombre de classes de F/K.

THÉORÈME 3.9.7 *Le L-polynôme d'un corps de fonctions F/K de genre g et de nombre de classes h satisfont aux propriétés suivantes :*

1. $L(t) \in \mathbb{Z}[t]$ *et* $\deg L(t) = 2g$,

2. $L(1) = h$,

3. $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$ *où* $a_0 = 1$ *et pour* $i = 0, 1, \ldots g$ *on a*

$$a_{2g-i} = q^{g-i} a_i.$$

De plus, pour $i = 1, 2, \ldots, g$,

$$i a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}.$$

Démonstration : Stichtenoth [43, Th. V.1.15 et Cor. V.1.17]

Ainsi, pour calculer $L(t)$ puis h, il suffit de connaître $N_1, N_2, \ldots, N_g$. Malheureusement, il n'existe pas en général de formule explicite pour N_r. Il faut donc déterminer de façon effective toutes les places de degrés $1, 2, \ldots, g$. Il est clair que si $\#K$ ou g sont grands, alors les calculs seront d'une trop grande complexité. Or, on aimerait tout de même appliquer la Proposition 3.9.6 pour construire des codes géométriques quasi auto-duaux sur des corps $\mathbb{F}_{q^r}$ où r peut être grand. Pour ce faire, on utilisera les propriétés des extensions de corps de fonctions obtenus par extension du corps des constantes.

PROPOSITION 3.9.8 *Soient F/K un corps de fonctions et F_r/K_r défini comme précédemment. Soient $n = 2k$ et le diviseur de F_r/K_r*

$$\mathcal{P} = \mathfrak{P}_1 + \mathfrak{P}_2 + \cdots + \mathfrak{P}_n$$

où les places $\mathfrak{P}_i$ sont deux à deux distinctes, $\deg \mathfrak{P}_i = 1$ pour $i = 1, 2, \ldots, n$ et supposons $\mathcal{P}$ rationnel sur K. Supposons de plus que

1. *le groupe des classes Cl_F^0 soit monogène et d'ordre $h > 1$ non divisible par 2,*
2. *il existe un diviseur A de F/K tel que $[A] \in Cl_F^0$ soit un générateur du groupe Cl_F^0 et tel que $\operatorname{suppCon}_{F_r/F}(A) \cap \operatorname{supp}\mathcal{P} = \emptyset$,*
3. *il existe un diviseur B de F/K tel que $\deg B = 1$ et $\operatorname{suppCon}_{F_r/F}(B) \cap \operatorname{supp}\mathcal{P} = \emptyset$.*

Alors il existe un entier $m \in \{0, 1, \ldots, (h-1)\}$ tel que, si on pose

$$D := \operatorname{Con}_{F_r/F}((k + g - 1)B + mA),$$

le code géométrique $C_{\mathcal{L}}(F_r, \mathcal{P}, D)$ sur K_r est quasi auto-dual.

Démonstration : Le diviseur $\mathcal{P}$ étant rationnel sur K, il existe un diviseur $\mathcal{P}_0$ de F/K tel que $\operatorname{Con}_{F_r/F}(\mathcal{P}_0) = \mathcal{P}$. De la même façon qu'à la démonstration de la Proposition 3.9.6, on montre qu'il existe un entier $m \in \{0, 1, \ldots, (h-1)\}$ tel que, si on pose

$$D_0 := (k + g - 1)B + 2mA,$$

le diviseur $2D_0 - \mathcal{P}_0$ est un diviseur canonique. Il en est de même du diviseur

$$\operatorname{Con}_{F_r/F}(2D_0 - \mathcal{P}_0) = 2\operatorname{Con}_{F_r/F}(D_0) - \mathcal{P} = 2D - \mathcal{P}$$

d'après le Théorème 2.8.7. La proposition est donc une conséquence du Théorème 3.9.2 □

Je vais maintenant appliquer la proposition précédente et construire un code quasi auto-dual à l'aide de mon logiciel. J'utilise la courbe projective plane $\mathcal{C} := \{C = 0\}$ définie sur $K := \mathbb{F}_2$ où

$$C := (Y^2 + XY + X^2)Z^3 + (Y^3 + XY^2)Z^2 + (X^2Y^2 + X^4)Z + X^2Y^3 + X^5$$

est absolument irréductible. Le corps de fonctions $F := K(\mathcal{C})$ est de genre $g = 4$. Posons $K' := \mathbb{F}_{2^6}$ et $F' := K'F$. Le corps de fonctions F'/K' possède 114 places[6] de degré 1. Comme on le verra, ces 114 places dominent exactement

1. 3 places $\mathfrak{P}_{1,1}, \mathfrak{P}_{1,2}, \mathfrak{P}_{1,3}$ de degré 1,
2. 3 places $\mathfrak{P}_{2,1}, \mathfrak{P}_{2,2}, \mathfrak{P}_{2,3}$ de degré 2,
3. 3 places $\mathfrak{P}_{3,1}, \mathfrak{P}_{3,2}, \mathfrak{P}_{3,3}$ de degré 3,
4. 16 places $\mathfrak{P}_{6,1}, \mathfrak{P}_{6,2}, \ldots, \mathfrak{P}_{6,16}$ de degré 6.

On utilise le paquetage "`P:=PAFFFF(PF 2,[X,Y,Z])`". On calcule le nombre de classes de F en utilisant la fonction "`classNumber`" qui utilise le Théorème 3.9.7 :

```
(1) -> classNumber()$P

   31
```

Le groupe des classes de F/K est donc monogène d'ordre non divisible par 2. Voici les trois places de degré 1 :

```
(2) -> placesOfDegree(1)$P

                1          1    1
       [[0,1,1] ,[1,1,0] ,%I0 ]
```

et notons les respectivement $\mathfrak{P}_{1,1}, \mathfrak{P}_{1,2}, \mathfrak{P}_{1,3}$. Les places $\mathfrak{P}_{1,1}, \mathfrak{P}_{1,2}$ correspondent à des points simples et $\mathfrak{P}_{1,3}$ correspond à une feuille d'un arbre de désingularisation (cf. plus loin). On a les places de degré 2 :

```
(3) -> placesOfDegree(2)$P

                   2            2    2
         [[1,%D15,1] ,[%D12,1,0] ,%I1 ]
```

que l'on note respectivement $\mathfrak{P}_{2,1}, \mathfrak{P}_{2,2}, \mathfrak{P}_{2,3}$. Les symboles "`%D15`" "`%D12`" représentent des racines K-distinguées de $z^2 + z + 1 \in K[z]$. Voici les arbres de désingularisation :

```
(4) -> desingTree()$P

     [ "UD" , "UD" ]
```

On en déduit que $\mathfrak{P}_{1,3}$ et $\mathfrak{P}_{2,3}$ sont les seules places correspondant à des feuilles. Par conséquent, tout autre place de F/K correspond à un point simple de $\mathcal{C}$.

6. La borne de Serre prédit un maximum de 129 places de degré 1 pour un corps de fonctions sur $\mathbb{F}_{2^6}$ de genre 4. Selon [34], on ne connaît toujours pas de corps de fonctions sur $\mathbb{F}_{2^6}$ de genre 4 ayant plus de 114 places de degré 1.

Notons respectivement $\mathfrak{P}_{3,1}, \mathfrak{P}_{3,2}, \mathfrak{P}_{3,3}$ les trois places de degré 3 :

(5) -> **placesOfDegree(3)$P**

```
                    3                    3           3
        [[%D21,1,1] ,[%D21,%D21 + 1,1] ,[%D21,0,1] ]
```

Ici "%D21" est une racine K-distinguée de $z^3 + z^2 + 1$.

Notons respectivement $\mathfrak{P}_{6,1}, \mathfrak{P}_{6,2}, \ldots, \mathfrak{P}_{6,16}$ les 16 places de degré 6 :

(6) -> **placesOfDegree(6)$P**

```
  [[%D32,%D60,1] , [%D34,%D34  + %D34  + %D34 ,1] , [%D34,%D34  + %D34 ,1] ,
             2   6              5       3        2           6
    [%D34,%D34 ,1] , [%D35,%D35  + %D35  + %D35  + %D35,1] ,
             5       4       3       2       6
    [%D36,%D36  + %D36  + %D36  + %D36  + 1,1] ,
             4       2           6              3       2           6
    [%D36,%D36  + %D36  + %D36,1] , [%D36,%D36  + %D36  + %D36,1] ,
             5       2   6              5       4       6
    [%D37,%D37  + %D37 ,1] , [%D38,%D38  + %D38  + 1,1] ,
             5       4       3       2       6
    [%D39,%D39  + %D39  + %D39  + %D39  + 1,1] ,
             5       3       2           6
    [%D40,%D40  + %D40  + %D40  + %D40,1] ,
             4       3       2       6               2           6
    [%D40,%D40  + %D40  + %D40  + 1,1] , [%D40,%D40  + %D40,1] ,
             4       3       2   6              4       3           6
    [%D41,%D41  + %D41  + %D41 ,1] , [%D41,%D41  + %D41  + %D41,1] ]
```

Il est inutile de donner la définition de chacun des éléments du domaine "PACOFF" utilisés pour les places de degré 6. Observons par contre que la première place de la liste précédente est définie en fonction de deux éléments de "PACOFF". Le premier, "%D32", est une racine K-distinguée de $p = z^2 + z + 1 \in K[z]$ tandis que "%D60" est une racine $T(p)$-distinguée de $q = z^3 + z + 1 \in K_{T(p)}[z]$.

Pour utiliser la Proposition 3.9.8, il suffit d'appliquer sa démonstration. J'ai choisi pour diviseurs :

$$\begin{array}{rcl} A & := & \mathfrak{P}_{1,1} - \mathfrak{P}_{1,2} \\ B & := & \mathfrak{P}_{1,2} \\ \mathcal{P}_0 & := & \mathfrak{P}_{1,3} + \sum_{j=1}^{3} \mathfrak{P}_{2,j} + \sum_{j=1}^{3} \mathfrak{P}_{3,j} + \sum_{j=1}^{16} \mathfrak{P}_{6,j} \\ \mathcal{P} & = & \mathrm{Con}_{F'/F} \mathcal{P}_0 \end{array}$$

Il faut d'abord s'assurer que A est bien tel que $[A] \in Cl_F^0$ soit un générateur du groupe des classes : il suffit de vérifier que A ne soit pas un diviseur principal ce qui est équivalent à vérifier que $\mathcal{L}(A) = \{ 0 \}$:

(7) -> `lBasis(A)$P`

```
[num= [0],den= X]
```

L'appel de "`lBasis(A)`" retourne une base de $\mathcal{L}(A)$ sous la forme d'un "`Record`" où les sélecteurs "`num`" et "`den`" correspondent respectivement à la liste des formes qui sont les numérateurs des éléments de la base et au dénominateur commun de tous ces éléments.

On a

$$\deg \mathcal{P} = \deg \mathcal{P}_0 = 1 + (3 \times 2) + (3 \times 3) + (16 \times 6) = 112.$$

De plus, on déduit de la Proposition 2.8.9 que $\deg \mathfrak{Q} = 1$ pour tout $\mathfrak{Q} \in \operatorname{supp}\mathcal{P}$. En appliquant la Proposition 3.9.8 avec le diviseur $\mathcal{P}$ de F'/K', on pourra donc construire un code géométrique quasi auto-dual, défini sur K', de longueur $n = 112$ et de dimension $k = 56$.

Il faut maintenant déterminer l'entier m tel que, si on pose

$$D := \operatorname{Con}_{F'/F}\left((k + g - 1)B + 2mA\right) = \operatorname{Con}_{F'/F}\left(59B + 2mA\right),$$

alors le code $C_{\mathcal{L}}(F', \mathcal{P}, D)$ est quasi auto-dual. Pour ce faire, on détermine d'abord un entier m_1 tel que

$$\mathcal{P}_0 \equiv 112B + 2m_1 A.$$

On pourrait par exemple calculer

$$\mathcal{L}(\mathcal{P}_0 - 112B - 2rA)$$

pour $r = 0, 1, 2, \ldots, (h-1) = 30$ en s'arrêtant à l'entier $m_1 = r$ tel que $\mathcal{L}(\mathcal{P}_0 - 112B - 2m_1A) \neq \{\, 0 \,\}$ qui est une condition nécessaire et suffisante pour que $\mathcal{P}_0 \equiv 112B + 2rA$. Étant donné le degré de $\mathcal{P}_0$, le calcul de $\mathcal{L}(D)$ est trop long (il est tout de même réalisable avec mon logiciel). On procède plutôt comme suit : soit $\mathfrak{P}$ une place de F/K. Puisque $\deg B = 1$, on a $\deg(\mathfrak{P} - (\deg \mathfrak{P})B) = 0$. Par conséquent, il existe un unique entier $m_{\mathfrak{P}} \in \{\, 0, 1, 2, \ldots, h-1 \,\}$ tel que

$$\mathfrak{P} \equiv (\deg \mathfrak{P})B + m_{\mathfrak{P}} A.$$

Posons

$$m_{\mathcal{P}} := \sum_{\mathfrak{P} \in \operatorname{supp}\mathcal{P}_0} m_{\mathfrak{P}}.$$

Alors

$$\mathcal{P}_0 \equiv 112B + m_{\mathcal{P}} A \equiv 112B + 2m_1 A$$

où m_1 est tel que $2m_1 = m_{\mathcal{P}}$ (mod 31). Afin de déterminer l'entier $m_{\mathfrak{P}}$ pour chacune des places $\mathfrak{P} \in \mathrm{supp}\mathcal{P}_0$, on calcule successivement, pour $r = 0, 1, 2, \ldots, 30$, une base de

$$\mathcal{L}(\mathfrak{P} - (\deg \mathfrak{P})B - r\,A)$$

et on s'arrête à l'entier $r = m_{\mathfrak{P}}$ tel que $\mathcal{L}(\mathfrak{P} - (\deg \mathfrak{P})B - r\,A) \neq \{\,0\,\}$. Voici le résultat de ces calculs :

1. pour les places $\mathfrak{P}_{1,3}$ et $\mathfrak{P}_{i,j}$ où $i = 2, 3$ et $j = 1, 2, 3$, on trouve respectivement pour $m_{\mathfrak{P}}$:
$$15, \quad 11, \quad 26, \quad 25, \quad 23, \quad 24, \quad 0.$$
2. Pour les 16 places de degré 6, on trouve pour $m_{\mathfrak{P}}$:
$$21, \quad 8, \quad 29, \quad 26, \quad 7, \quad 3, \quad 1, \quad 28, \quad 30, \quad 20, \quad 28, \quad 4, \quad 2, \quad 26, \quad 8, \quad 16.$$

On a donc

$$m_{\mathcal{P}} = 381 = 9 \text{ (mod 31)}.$$

En prenant $m_1 := 20$, et puisque $2 \times 20 = 9$ (mod 31), on a

$$\mathcal{P}_0 \equiv 112B + (2 \times m_1)A.$$

Il faut maintenant déterminer un entier m_2 tel que

$$W \equiv (2g - 2)B + 2m_2A = 4B + 2m_2A$$

où W est un diviseur canonique. D'après la Proposition 2.6.6, si $G \in S(K)$ est un polynôme homogène non divisible par C tel que $\deg G = \deg C - 3$ et $(G) \geq \mathcal{A}$, où $\mathcal{A}$ est le diviseur d'adjonction de $\mathcal{C}$, alors

$$W := (G) - \mathcal{A}$$

est un diviseur canonique de F/K. Calculons d'abord le diviseur d'adjonction :

```
(8) -> Adj:=adjunctionDivisor()$P

                1        2
          2 %I0   + %I1
```

On a donc

$$\mathcal{A} = 2\mathfrak{P}_{1,3} + \mathfrak{P}_{2,3}.$$

Calculons ensuite un polynôme d'interpolation de $\mathcal{A}$ de degré $\deg C - 3 = 5 - 3 = 2$:

(9) -> `interpolateForms( Adj , 2 )$P`

```
                        2
   [Y Z, X Z, X Y, X  ]
```

On choisit $G := X^2$ et on calcule son diviseur d'intersection :

(10) -> `intersectionDivisor( X**2 )$P`

```
          1        2            1
    4 %I0   + 2 %I1   + 2 [0,1,1]
```

d'où

$$(G) = 4\mathfrak{P}_{1,3} + 2\mathfrak{P}_{2,3} + 2\mathfrak{P}_{1,1}$$

et donc

$$W := (G) - \mathcal{A} = 2\mathfrak{P}_{1,3} + \mathfrak{P}_{2,3} + 2\mathfrak{P}_{1,1}$$

est un diviseur canonique de F/K (observons qu'on a bien $\deg W = 2g - 2 = 6$). Par des calculs similaires à ceux qui ont été utilisés pour déterminer l'entier m_1, on trouve $m_2 := 13$ tel que

$$W \equiv 6B + (2 \times m_2)A.$$

L'entier $m \in \{0, 1, 2, \ldots, h-1\}$ recherché est donc $m := 2 = m_1 + m_2 \pmod{31}$. On prend donc pour diviseur D_0 le diviseur

$$\begin{aligned} D_0 &= (k + g - 1)B + 2mA \\ &= 59B + 4A \\ &= 55\mathfrak{P}_{1,2} + 4\mathfrak{P}_{1,1}. \end{aligned}$$

Ainsi, en prenant le diviseur $D := \mathrm{Con}_{F'/F} D_0$, le code $C_{\mathcal{L}}(F', \mathcal{P}, \mathcal{D})$ est un code quasi auto-dual défini sur K'.

On calcule maitenant une base de $\mathcal{L}(D_0)$ qui sera aussi une base de $\mathcal{L}(D)$. Il faut déterminer un polynôme homogène $G_0 \in S(K)$ tel que C ne divise pas G_0 et

$$(G_0) \geq D_0 + \mathcal{A}.$$

D'après le Corollaire 2.7.6, un tel polynôme existe si

$$\begin{aligned} \deg G_0 &> \max\left\{ n, \tfrac{n}{2} + \tfrac{\deg(D_0 + \mathcal{A})}{n} - \tfrac{3}{2} \right\} \\ &= \max\left\{ 5, \tfrac{5}{2} + \tfrac{59+4}{5} - \tfrac{3}{2} \right\} \\ &= 13.6\ . \end{aligned}$$

Remarque 3.9.9 On peut se demander par contre s'il n'existe pas un polynôme d'interpolation de degré 13 pour le diviseur $D_0 + \mathcal{A}$:

```
(11) -> interpolateForms( D0 + adjunctionDivisor()$P, 13 )$P

         [0]
```

Il n'y a donc pas de polynôme d'interpolation de degré 13 et ceci confirme la Remarque 2.7.7.

On considère donc les polynômes d'interpolation de degré 14.

```
(12) -> interpolateForms( D0 + adjunctionDivisor()$P, 14 )$P
```

La fonction précédente retourne 4 polynômes mais je n'ai pas voulu en donner la liste car ils ont tous au moins 32 mônomes. Parmi ces quatre polynômes, on a le polynôme

$$\begin{aligned} G_0 \;:=\; & X^{14}+X^{13}Y+X^{13}Z+X^{12}Y^2+X^{12}YZ+X^{11}Y^2Z+ \\ & X^{11}YZ^2+X^{11}Z^3+X^{10}Y^3Z+X^{10}YZ^3+X^{10}Z^4+X^9Y^4Z+ \\ & X^9Y^3Z^2+X^9Z^5+X^8Y^6+X^8Y^5Z+X^8YZ^5+X^8Z^6+ \\ & X^7YZ^6+X^6Y^7Z+X^6Y^6Z^2+X^6YZ^7+X^5Y^8Z+X^5Y^7Z^2+ \\ & X^4Y^9Z+X^4Z^{10}+X^3Y^9Z^2+X^3YZ^{10}+X^3Z^{11}+X^2Y^{12}+ \\ & X^2Y^{10}Z^2+XY^{13}+XY^{12}Z \end{aligned}$$

qui sera le dénominateur commun des éléments de la base de $\mathcal{L}(D_0)$. Le polynôme G_0 a pour diviseur d'intersection avec la courbe $\mathcal{C}$:

```
(13) -> divGo0 := intersectionDivisor(G0)$P

               1        2                      3             1              1
        2 %I0   + 3 %I1   + [%D35,%D35 + 1,1]   + 4 [0,1,1]   + 55 [1,1,0]
```

c'est-à-dire

$$(G_0) = 2\mathfrak{P}_{1,3} + 3\mathfrak{P}_{2,3} + \mathfrak{P}_{3,2} + 4\mathfrak{P}_{1,1} + 55\mathfrak{P}_{1,2}.$$

On calcule ensuite une base de l'espace vectoriel des polynômes d'interpolation du diviseur $(G_0) - D_0$. On trouvera dans la Table 3.1 les polynômes retournés par :

```
(14) -> interpolateForms( divGo0 - D0 , 14 )$P
```

La fonction précédente retourne 56 polynômes $G_1, G_2, \ldots, G_{56}$. Soit g_i l'image résiduelle de G_i dans l'anneau de coordonnées $K[\mathcal{C}]$ ($i = 0, 1, \ldots, 56$). Alors $\mathcal{L}(D_0)$ et donc $\mathcal{L}(D)$ admet pour base

$$\mathcal{B} := \{\, g_i/g_0 \;\mid\; i = 1, 2, \ldots, 56 \,\}.$$

Ceci est en accord avec le Théorème de Riemann-Roch car, puisque $\deg D_0 > 2g-1$, on a

$$\ell\,(D_0) = \deg D_0 - g + 1 = 59 - 4 + 1 = 56.$$

D'après la Proposition 1.6.2, puisque $7 = 2g - 1 \leq \deg D < n = 112$, le code $C_{\mathcal{L}}(F', \mathcal{P}, D)$ est un $[112, 56, d]_{2^4}$-code où

$$d \geq n - \deg D = 112 - 59 = 53.$$

Je ne juge pas utile de donner ici la matrice génératrice du code $C_{\mathcal{L}}(F', \mathcal{P}, D)$. Je souligne seulement qu'il n'est pas nécessaire d'évaluer chacune des fonctions $u \in \mathcal{B}$ en chaque place $\mathfrak{Q} \in \mathrm{supp}\mathcal{P}$: en effet, il n'est pas nécessaire d'évaluer pour les places conjuguées à $\mathfrak{Q}$ par l'action de $\sigma : \alpha \mapsto \alpha^2$; il suffit simplement d'ajouter les colonnes conjuguées par l'action de σ. De la sorte, on n'évaluera les fonctions de $\mathcal{B}$ que pour $27 = \#\mathrm{supp}\mathcal{P}_0$ places. De plus, il suffit d'utiliser les séries $\mathfrak{Q}$-adiques seulement pour les places

$$\mathfrak{P} \in \mathrm{supp}(\mathrm{Con}_{F'/F}(G_0)) \cap \mathrm{supp}\mathcal{P}.$$

En effet, toute place $\mathfrak{Q} \in \mathrm{supp}\mathcal{P} \setminus \mathrm{supp}(\mathrm{Con}_{F'/F}(G_0))$ correspond à un point simple $Q := (a : b : c) \in \mathcal{C} \cap \mathbb{P}^2(K')$ tel que $\nu_{\mathfrak{Q}}(\overline{G}_0^Q) = 0$ et donc $\overline{G}_0^Q(\mathfrak{Q}) \neq 0$. Par conséquent, si par exemple $u = g_1/g_0$, alors $u(\mathfrak{Q}) = G_1(Q)/G_0(Q) = G_1(a, b, c)/G_0(a, b, c)$.

Après avoir calculé une matrice génératrice du code, on constate qu'il existe un mot de poids 53 d'où le code $C_{\mathcal{L}}(F', \mathcal{P}, D)$ est un $[112, 56, 53]_{2^6}$-code quasi auto-dual. Puisque que K' est de caractéristique 2, il existe $b \in K'^n$ tel que $b * C_{\mathcal{L}}(F', \mathcal{P}, D)$ est auto-dual (le vecteur b se trouve par de simples calculs d'algèbre linéaire).

$X^{13}Y + Y^{12}Z^2$	$X^{13}Y + X^6Y^8$
$X^{14} + X^{13}Y + X^{12}Y^2 + Y^{13}Z$	$X^{14} + X^7Z^7$
$X^{14} + XY^{11}Z^2$	$X^{14} + X^{12}Y^2 + X^7YZ^6$
$X^{14} + X^{12}Y^2 + XY^{12}Z$	$X^{13}Y + X^7Y^5Z^2$
$X^{13}Y + X^{12}Y^2 + XY^{13}$	$X^{14} + X^{13}Y + X^{12}Y^2 + X^7Y^6Z$
$X^{14} + X^2YZ^{11}$	$X^{14} + X^7Y^7$
$X^{13}Y + X^{12}Y^2 + X^2Y^{10}Z^2$	$X^{12}Y^2 + X^8Z^6$
$X^{12}Y^2 + X^2Y^{11}Z$	$X^{14} + X^{13}Y + X^8YZ^5$
$X^{14} + X^{13}Y + X^2Y^{12}$	$X^{14} + X^8Y^4Z^2$
$X^{13}Y + X^{12}Y^2 + X^3Z^{11}$	$X^{14} + X^{12}Y^2 + X^8Y^5Z$
$X^{12}Y^2 + X^3YZ^{10}$	$X^{13}Y + X^{12}Y^2 + X^8Y^6$
$X^{14} + X^{13}Y + X^3Y^9Z^2$	$X^{14} + X^{13}Y + X^{12}Y^2 + X^9Z^5$
$X^{13}Y + X^3Y^{10}Z$	$X^{14} + X^9YZ^4$
$X^{14} + X^{13}Y + X^{12}Y^2 + X^3Y^{11}$	$X^{13}Y + X^{12}Y^2 + X^9Y^3Z^2$
$X^{13}Y + X^4Z^{10}$	$X^{12}Y^2 + X^9Y^4Z$
$X^{14} + X^{13}Y + X^{12}Y^2 + X^4YZ^9$	$X^{14} + X^{13}Y + X^9Y^5$
$X^{14} + X^{13}Y + X^{12}Y^2 + X^4Y^8Z^2$	$X^{13}Y + X^{12}Y^2 + X^{10}Z^4$
$X^{14} + X^4Y^9Z$	$X^{12}Y^2 + X^{10}YZ^3$
$X^{14} + X^{12}Y^2 + X^4Y^{10}$	$X^{14} + X^{13}Y + X^{10}Y^2Z^2$
$X^{14} + X^{12}Y^2 + X^5Z^9$	$X^{13}Y + X^{10}Y^3Z$
$X^{13}Y + X^{12}Y^2 + X^5YZ^8$	$X^{14} + X^{13}Y + X^{12}Y^2 + X^{10}Y^4$
$X^{14} + X^{12}Y^2 + X^5Y^7Z^2$	$X^{13}Y + X^{11}Z^3$
$X^{13}Y + X^{12}Y^2 + X^5Y^8Z$	$X^{14} + X^{13}Y + X^{12}Y^2 + X^{11}YZ^2$
$X^{12}Y^2 + X^5Y^9$	$X^{14} + X^{11}Y^2Z$
$X^{14} + X^{13}Y + X^6Z^8$	$X^{14} + X^{12}Y^2 + X^{11}Y^3$
$X^{13}Y + X^6YZ^7$	$X^{14} + X^{12}Y^2 + X^{12}Z^2$
$X^{12}Y^2 + X^6Y^6Z^2$	$X^{13}Y + X^{12}Y^2 + X^{12}YZ$
$X^{14} + X^{13}Y + X^6Y^7Z$	$X^{14} + X^{13}Y + X^{13}Z$

TAB. 3.1 – *Base de l'espace vectoriel des polynômes d'interpolation de degré 14 du diviseur $(G_0) - D_0$ où $(G_0) \geq D_0 + \mathcal{A}$. Ce sont donc les numérateurs des éléments de la base de $\mathcal{L}(D_0)$.*

Chapitre 4

Codes sur des extensions du type d'Artin-Schreier

Dans tout ce chapitre on fixe $K = \mathbb{F}_{q^2}$.

En 1982, Tsfasman, Vlăduţ et Zink [44] ont donné la première construction d'une classe de codes correcteurs ayant des paramètres dépassant la borne de Varshamov-Gilbert. Ce sont des codes géométriques définis à partir de corps de fonctions de courbes modulaires. La théorie des courbes modulaire est, disons-le, peu accessible à la plupart des spécialistes des codes correcteurs. Depuis, plusieurs chercheurs ont tenté d'obtenir une construction plus simple d'une classe de codes ayant des paramètres dépassant la borne de Varshamov-Gilbert. Ce n'est que tout récemment (1995) que Garcia et Stichtenoth [11] ont donné une construction simple d'une tour de corps de fonctions sur $K := \mathbb{F}_{q^2}$

$$F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_n \subset \cdots$$

telle que

$$\lim_{n\to\infty} N_n/g_n = q - 1$$

où N_n est le nombre de places de degré 1, g_n est le genre de F_n/K et $g_n \to \infty$ lorsque $i \to \infty$. Dans le cas où $q \geq 3$, on peut, en théorie, construire à partir de ces corps de fonctions une classe de bons codes ([43, Prop. VII.2.5]) et, si $q \geq 7$, on peut construire une classe de codes dépassant la borne de Varshamov-Gilbert ([45, Th. 3.4.4]).

Dans ce chapitre, je propose une méthode de construction effective de codes géométriques définis à partir des corps de fonctions F_n/K donnés par Garcia et Stichtenoth et la première section est consacrée à un bref rappel des résultats qu'ils ont obtenus. À la Section 4.2, je montre qu'il est possible, pour certains diviseurs $D \in \mathcal{D}_{F_n}$, d'exprimer sous forme de polynômes à n variables tous les éléments d'une base de $\mathcal{L}(D)$. J'en déduirai une méthode pour calculer cette base à l'aide des séries $\mathfrak{P}$-adiques. À la Section 4.3, j'introduis la notion de *séquence de valuation* du corps de fonctions $\overline{F}_n/\overline{K}$ où $\overline{F}_n := F_n\overline{K}$. Ces séquences de valuation seront utilisées pour calculer les séries $\mathfrak{P}$-adiques de toutes les places intervenant dans le calcul de la base de $\mathcal{L}(D)$. Celles-ci seront caractérisées à la Section 4.4 en utilisant des propriétés liées aux séquences de valuation. Dès lors, on est en mesure d'appliquer ma méthode de calcul d'une base de $\mathcal{L}(D)$. Je donne un exemple à la Section 4.5.

4.1 Définition des corps de fonctions

Les corps de fonctions $F_n/\mathbb{F}_{q^2}$ utilisés dans [11] sont définis comme suit : on a $F_1 := K(x_1)$ et pour $n \geq 2$ on pose

$$F_n := K(x_1, x_2, \ldots, x_n)$$

où pour $i = 2, 3, \ldots, n$ les x_i vérifient

$$x_i^q x_{i-1}^{q-1} + x_i - x_{i-1}^q \quad = \quad 0. \tag{4.1}$$

Observons qu'en posant

$$z_n := x_n x_{n-1}$$

et en multipliant x_{n-1} par (4.1) avec $i = n$, on trouve

$$z_n^q + z_n = x_{n-1}^{q+1} \tag{4.2}$$

et il est clair alors que pour $n \geq 2$ on a

$$F_n = F_{n-1}(z_n).$$

C'est l'équation (4.2) qui caractérise le fait que les extensions F_n/F_{n-1} sont du type d'Artin-Schreier (cf. [43, Rema. III.7.9]).

Voici le résultat principal qu'ont obtenu A. Garcia et H. Stichtenoth.

THÉORÈME 4.1.1 *Pour $n \geq 1$, soient respectivement g_n et N_n, le genre et le nombre de places de degré 1 du corps de fonctions $F_n/\mathbb{F}_{q^2}$. On a*

1.
$$g_n = \begin{cases} q^n + q^{n-1} - \frac{1}{2}q^{n/2-1} - \frac{3}{2}q^{n/2} - q^{n/2-1} + 1 & \textit{si } n \textit{ est pair,} \\ q^n + q^{n-1} - q^{(n+1)/2} - 2q^{(n-1)/2} + 1 & \textit{si } n \textit{ est impair,} \end{cases}$$

2. *si $n \geq 3$, alors*
$$N_n \geq (q^2 - 1)q^{n-1} + 2q,$$

3. $\lim_{n\to\infty} N_n/g_n = q - 1$.

Remarque 4.1.2 La classe des corps de fonctions F_n a ceci de remarquable qu'elle atteint la borne de Drinfeld-Vlăduţ dont voici un bref rappel. Soit $l := p^m \in \mathbb{N}$ où p est premier et pour un entier $g \geq 0$ posons

$$N_l(g) := \max \{ N(F) \mid F \text{ est un corps de fonctions sur } \mathbb{F}_l \text{ de genre } g \}$$

où $N(F)$ est le nombre de places de degré 1 du corps de fonctions F. À l'entier l on associe un nombre $A(l) \in \mathbb{R}$ défini par

$$A(l) := \limsup_{g\to\infty} \frac{N_l(g)}{g}.$$

On a la *borne de Drinfeld-Vlăduţ* (cf. [45, Th. 2.3.22])

$$A(l) \leq \sqrt{l} - 1.$$

En prenant $q := p^m$, on déduit aisément du Théorème 4.1.1 que si $l = q^2 = p^{2m}$, c'est-à-dire que l est un carré, alors

$$A(l) = \sqrt{l} - 1.$$

En fait, ce résultat à d'abord été obtenu par Ihara [25] et simultanément par Tsfasman, Vlăduţ et Zink [44] dans le cas $l = p^2$ ou $l = p^4$. Néanmoins, la démonstration du Théorème 4.1.1 est de loin plus accessible que celles que l'on trouve dans [25] et [44] qui utilisent la théorie des courbe modulaire. Ceci dit, N. D. Elkies a montré[1] que les corps de fonctions obtenus par A. Garcia et H. Stichtenoth [11] sont ni plus ni moins que des corps de fonctions de courbes modulaires.

Voici le théorème sur lequel repose tous les résultats obtenus dans [11]. C'est aussi de ce théorème qu'est déduite en grande partie ma méthode de calcul d'une base de l'espace vectoriel associé à un diviseur du corps de fonctions F_n/K.

Théorème 4.1.3 *(cf. [11]) Soit le corps de fonctions F_n/K $(n \geq 1)$. Alors*

1. *K $(= \mathbb{F}_{q^2})$ est le corps des constantes de F_n,*
2. *il existe une place $\mathfrak{P} \in \mathbb{P}_{F_n}$ telle que $\nu_{\mathfrak{P}}(x_n) = -1$,*
3. *toute place $\mathfrak{P} \in \mathbb{P}_{F_n}$ telle que $\nu_{\mathfrak{P}}(x_n) = -1$ se ramifie totalement dans F_{n+1}, c'est-à-dire qu'il existe une unique place $\mathfrak{P}' \in \mathbb{P}_{F_{n+1}}$ dominant $\mathfrak{P}$ et elle est telle que $e(\mathfrak{P}'|\mathfrak{P}) = q$. De plus,* $\deg \mathfrak{P}' = \deg \mathfrak{P}$.

1. Conférence “Curves and Computations”, Édinbourg, Écosse, mars 1996.

4. $[F_{n+1} : F_n] = q$.

REMARQUE 4.1.4 Le théorème précédent reste vrai en remplaçant le corps de fonctions F_n/K par $\overline{F}_n/\overline{K}$ où $\overline{F}_n = \overline{K}F_n$.

4.2 Calcul d'une base de $\mathcal{L}(D)$

Le corps F_1/K est le corps rationnel et F_2/K est le corps hermitien (voir [43, Lemme VI.4.4]). Il est donc aisé de donner une formulation explicite de codes définis sur le corps F_n pour $n = 1, 2$. Pour $n = 3$, Høholdt et Voss [23] ont donné une formulation explicite de codes $C_{\mathcal{L}}(F_3, \mathcal{P}, D)$ pour des diviseurs particuliers D et $\mathcal{P}$ du corps de fonctions $F_3/\mathbb{F}_{q^2}$. Malheureusement, cette méthode ne se généralise pas à $n \geq 4$.

Le problème essentiel pour construire un code géométrique est de déterminer une base de l'espace vectoriel associé à un diviseur. Je propose une méthode pour calculer de façon effective une base de l'espace vectoriel $\mathcal{L}(D)$ où D est un diviseur du corps de fonctions F_n/K pour $n \geq 2$. On pourrait utiliser l'algorithme de Brill-Noether mais la complexité des calculs devient vite trop élevée car le degré du polynôme C_n définissant une courbe projective plane $\mathcal{C}_n := \{ C_n = 0 \}$ définie sur K telle que $K(\mathcal{C}_n) \cong F_n$ est d'ordre $O(q^{n/2})$: en effet, d'après le Théorème 4.1.1, le genre g_n de F_n est d'ordre $O(q^n)$. D'autre part, d'après le Théorème 2.5.5, on a $g_n \leq (d-1)(d-2)/2$ où $d := \deg C_n$. Par conséquent, $d^2 \simeq O(q^n)$ d'où $d \simeq O(q^{n/2})$ (voir aussi l'exemple donné au Chapitre 3, Section 3.9.2).

Soit D un diviseur de F_n $(n \geq 1)$. Le calcul d'une base de $\mathcal{L}(D)$ reposera sur le calcul des séries $\mathfrak{P}$-adiques. Celles-ci n'étant définies que pour des places de degré 1, il sera en général nécessaire de considérer une extension suffisamment grande de K. En fait, comme pour l'algorithme de Brill-Noether, on définit un algorithme calculant une base de $\mathcal{L}(D')$ où

$$D' := \mathrm{Con}_{\overline{F}_n/F_n} D.$$

Le fait de considérer un corps de base algébriquement clos ne posera pas de problème pour l'implantation de l'algorithme : il suffira d'utiliser les extensions dynamiques de corps (cf. Section 3.1).

Soit D un diviseur de $\overline{F}_n$. L'algorithme calculera une base de $\mathcal{L}(D)$ si D est tel que $\mathcal{L}(D) \subset \overline{K}[x_1, x_2, \ldots, x_n]$: de tels diviseurs existent et comme on le verra, ce fait est une conséquence de la proposition suivante et de son corollaire.

Avant de poursuivre, et dans le but d'alléger le texte, pour $n \geq 1$ posons

$$R_n := \overline{K}[\underline{x}] := \overline{K}[x_1, x_2, \ldots, x_n]$$

et si $G \in \overline{K}[\underline{X}]$, on pose

$$G(\underline{x}) := G(x_1, x_2, \ldots, x_n).$$

Proposition 4.2.1 *Soit $n \geq 2$ et pour $i = 2, 3, \ldots, n$, posons*

$$G_i := X_i^q X_{i-1}^{q-1} + X_i - X_{i-1}^q \subset \overline{K}[\underline{X}].$$

L'idéal $I_n := \langle G_2, G_3, \ldots, G_n \rangle$ est un idéal premier.

Démonstration : Considérons les deux K-homomorphismes suivants :

$$\begin{array}{rccc} \psi_n : & \overline{K}[\underline{X}] & \longrightarrow & R_{n-1}[X_n] \\ & G & \mapsto & G(x_1, x_2, \ldots, x_{n-1}, X_n) \end{array}$$

et

$$\begin{array}{rccc} \varphi_n : & R_{n-1}[X_n] & \longrightarrow & R_n \\ & G(x_1, x_2, \ldots, x_{n-1}, X_n) & \mapsto & G(x_1, x_2, \ldots, x_n). \end{array}$$

L'anneau R_n étant intègre, le noyau $\ker(\varphi_n \circ \psi_n)$ est premier. Montrons que $I_n = \ker(\varphi_n \circ \psi_n)$ par récurrence sur n. Pour $n = 2$ on a $F_2 := \overline{K}(x_1, x_2)$ et il est clair que $G_2(x_1, x_2) = 0$. Or $\deg_{X_2} G_2 = q$ et d'après le Théorème 4.1.3, on a $q = [F_2 : F_1]$. On en déduit que G_2 est irréductible et que $I_2 = \ker(\varphi_2 \circ \psi_2)$. Observons que le même raisonnement s'applique pour montrer que $\ker \varphi_n = \langle g_n \rangle$ où $g_n = G_n(x_1, x_2, \ldots, x_{n-1}, X_n)$. Supposons maintenant que $I_{n-1} = \ker(\varphi_{n-1} \circ \psi_{n-1})$. Soit $G \in \overline{K}[\underline{X}]$ tel que $(\varphi_n \circ \psi_n)(G) = 0$. Alors $\psi_n(G) \in \ker \varphi_n$ d'où il existe $h \in R_{n-1}[X_n]$ tel que $\psi_n(G) = h g_n$. L'application ψ_n étant surjective il existe $H \in \overline{K}[\underline{X}]$ tel que $\psi_n(G) = \psi_n(HG_n)$ et donc $\psi(G - HG_n) \in \ker \varphi_n$. Or, il est clair que $\ker \varphi_n = \ker(\varphi_{n-1} \circ \psi_{n-1})$. Par hypothèse de récurrence on a donc $G - HG_n \in I_{n-1}$. Par conséquent, $G \in I_n$ d'où $\ker(\varphi_n \circ \psi_n) \subseteq I_n$; il est évident que $I_n \subseteq \ker(\varphi_n \circ \psi_n)$ d'où $I_n = \ker(\varphi_n \circ \psi_n)$. □

Corollaire 4.2.2 *Soit I_n défini comme à la proposition précédente et soit la variété affine*

$$\mathcal{C}_n := \{ P \in \mathbb{A}^n \mid H(P) = 0 \text{ pour tout } H \in I_n \}.$$

Alors

1. *$\overline{K}(\mathcal{C}_n)$ est $\overline{K}$-isomorphe à $\overline{F}_n$,*
2. $\mathrm{ht}\,(I_n) = n - 1$,
3. *$\mathcal{C}_n$ est une courbe affine lisse.*

Démonstration : (1). C'est une conséquence de la proposition précédente.

(2). C'est un conséquence du Théorème B.3.3.

(3). Puisque $\overline{K}(\mathcal{C}_n) \cong \overline{F}_n$, l'ensemble algébrique $\mathcal{C}_n$ est une courbe affine par définition. Pour montrer que $\mathcal{C}_n$ est lisse il suffit d'appliquer la Définition B.4.1. On a $\mathcal{I}(\mathcal{C}_n) = I_n = \langle G_2, G_3, \ldots, G_n \rangle$ et pour $i = 2, 3, \ldots, n-1$ et $j = 1, 2, \ldots, n$ on a

$$\frac{\partial G_i}{\partial X_j} = \begin{cases} 1 & \text{si } j = i \\ (q-1)X_i^q X_{i-1}^{q-2} & \text{si } j = i-1 \\ 0 & \text{sinon.} \end{cases}$$

Il est clair alors que tous les points de $\mathcal{C}_n$ sont simples. □

PROPOSITION 4.2.3 *Soit le corps de fonctions $\overline{F}_n/\overline{K}$ et posons*

$$\mathbb{P}_n^\infty := \left\{ \mathfrak{P} \in \mathbb{P}_{\overline{F}_n} \;\middle|\; \textit{il existe } i \in \{1, 2, \ldots, n\} \textit{ tel que } \nu_{\mathfrak{P}}(x_i) < 0 \right\}.$$

Soit D un diviseur de $\overline{F}_n$. Si $\mathrm{supp}D \subseteq \mathbb{P}_n^\infty$, *alors*

$$\mathcal{L}(D) \subset R_n.$$

Démonstration : Posons $\mathcal{Q} := \mathbb{P}_{\overline{F}_n} \setminus \mathbb{P}_n^\infty$. Il est clair que $\mathfrak{Q} \in \mathcal{Q}$ si et seulement si $R_n \subset \mathcal{O}_{\mathfrak{Q}}$. Soit $\mathfrak{Q} \in \mathcal{Q}$ et posons $a_i := x_i(\mathfrak{Q}) \in \overline{K}$ pour $i = 1, 2, \ldots, n$. Il est facile de montrer[2] que $Q = (a_1, a_2, \ldots, a_n) \in \mathcal{C}_n$ et $\mathcal{O}_Q(\mathcal{C}_n) \subseteq \mathcal{O}_{\mathfrak{Q}}$. D'après le corollaire précédent, le point Q est simple d'où $\mathcal{O}_Q(\mathcal{C}_n) = \mathcal{O}_{\mathfrak{Q}}$. D'autre part, il est clair aussi que tout point de $\mathcal{C}_n$ est dominé par une place de $\mathcal{Q}$. D'après la Proposition B.2.3, on a donc

$$R_n = \bigcap_{Q \in \mathcal{C}_n} \mathcal{O}_Q(\mathcal{C}_n) = \bigcap_{\mathfrak{Q} \in \mathcal{Q}} \mathcal{O}_{\mathfrak{Q}}.$$

Or, par définition de $\mathcal{L}(D)$, on a $\mathcal{L}(D) \subset \mathcal{O}_{\mathfrak{P}}$ pour toute place $\mathfrak{P} \notin \mathrm{supp}D$. Par conséquent, si $\mathrm{supp}D \subseteq \mathbb{P}_n^\infty$, alors

$$\mathcal{L}(D) \subset \bigcap_{\mathfrak{P} \notin \mathrm{supp}D} \mathcal{O}_{\mathfrak{P}} \subseteq \bigcap_{\mathfrak{P} \notin \mathbb{P}_n^\infty} \mathcal{O}_{\mathfrak{P}} = \bigcap_{\mathfrak{Q} \in \mathcal{Q}} \mathcal{O}_{\mathfrak{Q}} = R_n.$$

□

Ainsi, pour les diviseurs D tels que $\mathrm{supp}D \subset \mathbb{P}_n^\infty$, on peut trouver une base de $\mathcal{L}(D)$ formée de polynômes en $x_1, x_2, \ldots, x_n$ et non de fractions rationnelles en $x_1, x_2, \ldots, x_n$ comme c'est le cas en général.

2. La démonstration est similaire à celle de la Proposition 2.1.14.

Voici comment on peut calculer une base de $\mathcal{L}(D)$ pour les diviseurs D tels que $\mathrm{supp}D \subset \mathbb{P}_n^\infty$. Pour ce faire, on introduit d'abord quelques notations. Soient $\mathfrak{P}$ une place de $\overline{F}_n$ et $t_\mathfrak{P}$ un paramètre local de la place $\mathfrak{P}$. Pour $i = 1, 2, \ldots, n$, soit

$$s_i := x_i(t) \in \overline{K}((t_\mathfrak{P}))$$

la série $\mathfrak{P}$-adique de x_i en fonction de t. Pour un polynôme $G \in \overline{K}[\underline{X}]$ posons

$$G[\mathfrak{P}] := G(s_1, s_2, \ldots, s_n) \in \overline{K}((t_\mathfrak{P})).$$

Si

$$G[\mathfrak{P}] = \sum_{i=l}^{\infty} a_i t_\mathfrak{P}^i$$

on définit l'ordre de $G[\mathfrak{P}]$ par

$$\mathrm{ord}\,(G[\mathfrak{P}]) := \min\{\, i \mid a_i \neq 0 \,\}.$$

De plus, pour deux entiers m et n, on définit la série partielle

$$G[\mathfrak{P}]_m^n := \begin{cases} a_m t_\mathfrak{P}^m + a_{m+1} t_\mathfrak{P}^{m+1} + \cdots + a_{n-1} t_\mathfrak{P}^{n-1} & \text{si } l \leq m < n \\ 0 & \text{sinon.} \end{cases}$$

La Proposition 4.2.3 a pour corollaire :

Corollaire 4.2.4 *Avec les mêmes notations qu'à la proposition précédente, soit D un diviseur de $\overline{F}_n$ tel que $\mathrm{supp}D \subseteq \mathbb{P}_n^\infty$. Si, pour $i = 1, 2, \ldots, r$, $H_i \in \overline{K}[\underline{X}]$ et $\alpha_i \in \overline{K}$, alors*

$$\sum_{j=1}^{r} \alpha_j H_j(\underline{x}) \in \mathcal{L}(D) \iff \sum_{j=1}^{r} \alpha_j H_j[\mathfrak{P}]_{m_\mathfrak{P}}^{-n_\mathfrak{P}} = 0 \textit{ pour tout } \mathfrak{P} \in \mathbb{P}_{\overline{F}_n} \setminus \mathcal{Q}$$

où les entiers $n_\mathfrak{P}$ et $m_\mathfrak{P}$ sont définis par

$$\begin{cases} n_\mathfrak{P} & := & n_\mathfrak{P}(D), \\ m_\mathfrak{P} & := & \min\{\, \mathrm{ord}\,(H_j[\mathfrak{P}]) \mid j = 1, 2, \ldots, r \,\}. \end{cases}$$

Démonstration : Quels que soient $\alpha_1, \alpha_2, \ldots, \alpha_r \in \overline{K}$ et $\mathfrak{P} \in \mathbb{P}_n^\infty$, on a

$$m_\mathfrak{P} \leq \nu_\mathfrak{P}\left(\sum_{j=1}^{r} \alpha_j H_j(\underline{x})\right).$$

Par conséquent, pour tout $\mathfrak{P} \in \mathbb{P}_n^\infty$, on a

$$\nu_\mathfrak{P}\left(\sum_{j=1}^{r} \alpha_j H_j(\underline{x})\right) \geq -n_\mathfrak{P} \iff \sum_{j=1}^{r} \alpha_j H_j[\mathfrak{P}]_{m_\mathfrak{P}}^{-n_\mathfrak{P}} = 0.$$

Le corollaire est alors une conséquence de la définition de $\mathcal{L}(D)$ et de la Proposition 4.2.3. □

Soient $H_1, H_2, \ldots, H_r \in \overline{K}[\underline{X}]$. Considérons les espaces vectoriels

$$V := \left\{ \sum_{j=1}^{r} \alpha_j H_j \mid \alpha_j \in \overline{K}, j = 1, 2, \ldots, r \right\}$$

et

$$V_{\overline{F}_n} := \{ G(\underline{x}) \mid G \in V \} \subset \overline{F}_n.$$

Soit D un diviseur tel que $\mathrm{supp} D \subseteq \mathbb{P}_n^{\infty}$ et $V_{\overline{F}_n} \supseteq \mathcal{L}(D)$. En appliquant le Corollaire 4.2.4, on peut donc calculer un base de $\mathcal{L}(D)$ si l'on sait

1. calculer les séries $\mathfrak{P}$-adiques de $x_1, x_2, \ldots, x_n$ pour toutes places $\mathfrak{P} \in \mathbb{P}_n^{\infty}$,
2. déterminer un sous-espace vectoriel $V \subset \overline{K}[\underline{X}]$ tel que $V_{\overline{F}_n} \supseteq \mathcal{L}(D)$ (si possible tel que $\dim_{\overline{K}} V_{\overline{F}_n} - \ell(D)$ ne soit pas trop grand).

À la section suivante, on montre comment calculer les séries $\mathfrak{P}$-adiques et, à la Section 4.4, on déterminera l'ensemble de places $\mathbb{P}_n^{\infty}$.

4.3 Calcul des séries $\mathfrak{P}$-adiques

Soient $\mathfrak{P}$ une place de $\overline{F}_n$ et $S := (s_1, s_2, \ldots, s_n) \in \overline{K}((t_{\mathfrak{P}}))^n$ où $s_1, s_2, \ldots, s_n$ sont les séries $\mathfrak{P}$-adiques respectives de $x_1, x_2, \ldots, x_n$ en fonction d'un paramètre local $t_{\mathfrak{P}}$ de $\mathfrak{P}$. Pour $G \in \overline{K}[\underline{X}]$ posons

$$G[S] := G(s_1, s_2, \ldots, s_n) \in \overline{K}((t_{\mathfrak{P}})).$$

Il est clair que

$$\mathfrak{P} = \{ G[S]/H[S] \mid \mathrm{ord}\,(H[S]) < \infty \text{ et } \mathrm{ord}\,(G[S]) - \mathrm{ord}\,(G[S]) > 0 \}. \tag{4.3}$$

Cette égalité fournit le point de départ pour le calcul des séries $\mathfrak{P}$-adiques. En considérant le corps des séries de Laurent $\overline{K}((t))$, l'idée est de construire une séquence $S := (s_1, s_2, \ldots, s_n) \in \overline{K}((t))^n$ tel que S détermine une place comme en (4.3)[3]. Pour ce faire, on introduit ici la notion de *séquence de valuation* de $\overline{F}_n$.

DÉFINITION 4.3.1 *Soit $S = (s_1, s_2, \ldots, s_n)$ où $s_i \in \overline{K}((t))$, $i = 1, 2, \ldots, n$. On dira que S est une* séquence de valuation (s.d.v.) *de $\overline{F}_n$ si*

1. $s_i \notin \overline{K}$, $(i = 1, 2, \ldots, n)$,

3. Insistons sur le fait que $t \in \overline{K}((t))$ est ici une indéterminée et non un paramètre local d'une place de $\overline{F}_n$.

2. *pour $i = 2, 3, \ldots, n$, les s_i vérifient*

$$s_i^q s_{i-1}^{q-1} + s_i - s_{i-1}^q = 0,$$

3. *il existe $G, H \in \overline{K}[\underline{X}]$ tels que*

$$\mathrm{ord}\,(G[S]) - \mathrm{ord}\,(H[S]) = 1.$$

Proposition 4.3.2 *Soit $S = (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$. Alors*

1. *l'application*

$$\begin{array}{rccc} \varphi_S : & \overline{F}_n & \longrightarrow & \overline{K}((t)) \\ & G(\underline{x})/H(\underline{x}) & \mapsto & G[S]/H[S] \end{array} \tag{4.4}$$

est un homomorphisme de corps,

2. *l'application*

$$\begin{array}{rccc} \nu_S : & \overline{F}_n & \longrightarrow & \mathbb{Z} \cup \{\,\infty\,\} \\ & u & \mapsto & \mathrm{ord}\,(\varphi_S(u)) \end{array} \tag{4.5}$$

est une valuation discrète de $\overline{F}_n$ triviale sur $\overline{K}$.

Démonstration : (1). Considérons les $\overline{K}$-homomorphismes

$$\begin{array}{rccc} \varphi : & \overline{K}[\underline{X}] & \longrightarrow & R_n \\ & H(\underline{X}) & \mapsto & H(\underline{x}) \end{array}$$

et

$$\begin{array}{rccc} \psi : & \overline{K}[\underline{X}] & \longrightarrow & \overline{K}((t)) \\ & H(\underline{X}) & \mapsto & H[S]. \end{array}$$

D'après la Proposition 4.2.1 et la définition de S, on a $\ker\varphi \subseteq \ker\psi$. Par conséquent,

$$\begin{array}{rccc} \varphi' : & R_n & \longrightarrow & \overline{K}((t)) \\ & G(\underline{x}) & \mapsto & G[S] \end{array}$$

est l'unique homomorphisme tel que $\psi = \varphi' \circ \varphi$. Pour finir, il suffit de vérifier que φ' est injectif, car dans ce cas, on peut prolonger φ' à $\overline{F}_n$ qui est le corps des fractions de R_n et ainsi obtenir l'homomorphisme φ_S. Pour cela, il suffit (et il faut) que $\ker\varphi = \ker\psi$. Mais si ce n'est pas le cas, alors $\ker\varphi \subsetneq \ker\psi$. Par conséquent, $\mathrm{ht}\,(\ker\psi) > \mathrm{ht}\,(\ker\varphi) = n-1$ (cf. Corollaire 4.2.2). Puisque $\ker\psi \neq \overline{K}[\underline{X}]$ et que $\dim \overline{K}[\underline{X}] = n$, on en déduit que $\ker\psi$ est un idéal maximal. Mais alors on a $\psi(G) \in \overline{K}$ quel que soit $G \in \overline{K}[\underline{X}]$ ce qui est impossible car par définition de la s.d.v. $S = (s_1, s_2, \ldots, s_n)$ on doit avoir $s_i \notin \overline{K}$ pour $i = 1, 2, \ldots, n$.

(2). Par définition, il existe $G, H \in \overline{K}[\underline{X}]$ tels que $\mathrm{ord}\,(G[S]) - \mathrm{ord}\,((H[S]) = 1$. Il est clair alors que φ_S est une application surjective et qu'elle vérifie toutes les propriétés d'une valuation discrète triviale sur $\overline{K}$. $\square$

Si donc pour toute place $\mathfrak{P} \in \mathbb{P}_n^\infty$ on sait construire une séquence de valuation S telle que $\nu_S = \nu_{\mathfrak{P}}$, on sait calculer les séries $\mathfrak{P}$-adiques pour toutes fonctions de $\overline{F}_n$. Toutefois, il est possible que deux séquences de valuation distinctes S et S' soient telles que $\nu_S = \nu_{S'}$. Or, il est clair qu'on ne veut pas construire deux séquences distinctes pour une même place. Pour résoudre ce problème, on définit ce qui suit.

Définition 4.3.3 *On dira que deux s.d.v. S et S' de $\overline{F}_n$ sont* équivalentes *si et seulement si $\nu_S = \nu_{S'}$ et on le note $S \equiv S'$.*

Proposition 4.3.4 *Soient S et S' deux s.d.v. de $\overline{F}_n$. S'il existe $u \in \overline{F}_n$ tel que $\varphi_S(u) = \varphi_{S'}(u) = t$ alors*

$$S \equiv S' \iff S = S'.$$

Démonstration : L'implication $(\Leftarrow)$ est évidente. Pour montrer la réciproque, soient

$$S = (s_1, s_2, \ldots, s_n) \quad \text{et} \quad S' = (s'_1, s'_2, \ldots, s'_n)$$

et supposons que $S \neq S'$ avec par exemple $s_1 \neq s'_1$. Soit $u \in \overline{F}_n$ tel que $\varphi_S(u) = \varphi_{S'}(u) = t$. Supposons que $\mathrm{ord}\,(s_1) \leq \mathrm{ord}\,(s'_1)$ et soit $l := \mathrm{ord}\,(s_1 - s'_1)$. Alors $\mathrm{ord}\,(s_1) \leq l < \infty$. Écrivons

$$s_1 = \sum_{i=\mathrm{ord}(s_1)}^{\infty} a_i t^i$$

et posons

$$w := \sum_{i=\mathrm{ord}(s_1)}^{l} a_i t^i.$$

Posons de plus

$$v := \sum_{i=\mathrm{ord}(s_1)}^{l} a_i u^i.$$

Alors $\varphi_S(x_1 - v) = s_1 - w$ et $\varphi_{S'}(x_1 - v) = s'_1 - w$. En particulier, on a

$$\begin{aligned}
\nu_S(x_1 - v) &= \mathrm{ord}\,(s_1 - w) \\
&> l = \mathrm{ord}\,(s'_1 - s_1) \\
&= \mathrm{ord}\,((s'_1 - s_1) + (s_1 - w)) \\
&= \mathrm{ord}\,(s'_1 - w) \\
&= \nu_{S'}(x_1 - v)
\end{aligned}$$

d'où $S \not\equiv S'$ car $\nu_S \neq \nu_{S'}$. $\square$

La construction des séquences de valuation de $\overline{F}_n$ repose essentiellement sur la proposition suivante.

PROPOSITION 4.3.5 *Soient K un corps et $s \in K((t))$ tel que* $\mathrm{ord}\,(s) \geq 1$. *Alors l'application*

$$\begin{array}{rccc} \phi_s : & K((t)) & \longrightarrow & K((t)) \\ & \sum_{i=l}^{\infty} a_i t^i & \mapsto & \sum_{i=l}^{\infty} a_i s^i \end{array}$$

est un K-homomorphisme.

Démonstration : Zariski-Samuel [47, Vol. II page 135].

Soient $S = (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$. On veut à partir de S construire (si possible) une s.d.v. de $\overline{F}_{n+1}$. Soit $u \in \overline{K}((t))$. Il est clair que $S' := (s_1, s_2, \ldots, s_n, u)$ est une s.d.v. de $\overline{F}_{n+1}$ si et seulement si u est une racine du polynôme

$$p(U) := U^q s_n^{q-1} + U - s_n^q \in \overline{K}((t))[U].$$

Le corps $\overline{K}((t))$ n'étant pas algébriquement clos, un tel polynôme n'a pas toujours ses racines dans $\overline{K}((t))$. Le lemme suivant et son corollaire montrent qu'il suffit que s soit tel que $\mathrm{ord}\,(s) \geq 0$ pour que $p(U)$ ait toutes ses racines dans $\overline{K}((t))$.

LEMME 4.3.6 *Soit $s \in \overline{K}((t))$ tel que* $\mathrm{ord}\,(s) \geq 0$. *Alors le polynôme*

$$T^q + T - s \in \overline{K}((t))[T]$$

admet q racines deux à deux distinctes dans $\overline{K}((t))$.

Démonstration : Supposons tout d'abord que $s = \gamma + t$ où $\gamma \in \overline{K}$. Soient $\beta_1, \beta_2, \ldots, \beta_q \in \overline{K}$ les q racines deux à deux distinctes de $X^q + X - \gamma \in \overline{K}[X]$ et posons

$$v_j := \beta_j + \sum_{i=0}^{\infty} (-1)^i t^{q^i} = \beta_i + t - t^{q^2} + t^{q^3} - t^{q^4} + \cdots, \quad j = 1, 2, \ldots, q.$$

Alors

$$\begin{aligned} {v_j}^q + v_j &= {\beta_j}^q + \sum_{i=0}^{\infty} (-1)^i t^{q^{i+1}} + \beta_j + \sum_{i=0}^{\infty} (-1)^i t^{q^i} \\ &= ({\beta_j}^q + \beta_j) + \sum_{i=0}^{\infty} (-1)^i t^{q^{i+1}} + \left(t + \sum_{i=0}^{\infty} (-1)^{i+1} t^{q^{i+1}} \right) \\ &= \gamma + t. \end{aligned}$$

Par suite, $v_1, v_2, \ldots, v_q$ sont les q racines deux à deux distinctes de $T^q + T - (\gamma + t)$. De façon plus générale, si $s = \gamma + s_0$ où $\mathrm{ord}\,(s_0) \geq 1$, alors

$$\begin{aligned} \phi_{s_0}(v_j)^q + \phi_{s_0}(v_j) - s &= \phi_{s_0}(v_j)^q + \phi_{s_0}(v_j) - (\gamma + \phi_{s_0}(t)) \\ &= \phi_{s_0}(v_j)^q + \phi_{s_0}(v_j) - \phi_{s_0}(\gamma + t) \\ &= \phi_{s_0}({v_j}^q + v_j - (\gamma + t)) \\ &= 0. \end{aligned}$$

Par suite, pour $j = 1, 2 \ldots, q$, les $\phi_{s_0}(v_j)$ sont les q racines deux à deux distinctes de $T^q + T - s$. $\square$

Corollaire 4.3.7 *Soit $s \in \overline{K}((t))$ tel que* $\mathrm{ord}\,(s) \geq 0$. *Alors le polynôme*

$$U^q s^{q-1} + U - s^q \in \overline{K}((t))[U] \tag{4.6}$$

a toutes ses racines $u_1, u_2, \ldots, u_q$ dans $\overline{K}((t))$ et elles sont deux à deux distinctes. En particulier,

1. *si* $\mathrm{ord}\,(s) = 0$, *alors* $\mathrm{ord}\,(u_i) = 0$ *pour $i = 1, 2, \ldots, q$,*
2. *si* $\mathrm{ord}\,(s) > 0$, *alors en supposant que* $\mathrm{ord}\,(u_1) \geq \mathrm{ord}\,(u_i)$, $i = 2, 3, \ldots, q$ *(quitte à réordonner les indices), on a*

$$\begin{cases} \mathrm{ord}\,(u_1) = q\,\mathrm{ord}\,(s) \\ \mathrm{ord}\,(u_i) = -\mathrm{ord}\,(s) \quad (i = 2, 3, \ldots, q). \end{cases}$$

Démonstration : Soient $v_1, v_2, \ldots, v_q$ les q racines deux à deux distinctes du polynôme $T^q + T - s^{q+1}$. Alors les $u_i := s^{-1} v_i$ sont les q racines deux à deux distinctes du polynôme donné en (4.6). La dernière assertion est évidente en considérant le fait que toutes les racines de $T^q + T - s^{q+1}$ sont d'ordre 0 si $\mathrm{ord}\,(s) = 0$, et si $\mathrm{ord}\,(s) > 0$, les racines sont toutes d'ordre 0 sauf exactement une qui est d'ordre $(q+1)\mathrm{ord}\,(s)$. $\square$

Corollaire 4.3.8 *Soit $S := (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$ telle que $s_1 = t$ et* $\mathrm{ord}\,(s_n) \geq 0$. *Soient $u_1, u_2, \ldots, u_q$ les q racines distinctes du polynôme*

$$U^q s_n^{q-1} + U - s_n^{q+1} \in \overline{K}((t))[U].$$

Alors les séquences

$$S_i := (s_1, s_2, \ldots, s_n, u_i), \quad i = 1, 2, \ldots, q,$$

sont des s.d.v. de $\overline{F}_{n+1}$ deux à deux non équivalentes.

Démonstration : C'est une conséquence du corollaire précédent et de la Proposition 4.3.4. □

Soit $S := (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$ telle que $s_1 = t$. Si $\operatorname{ord}(s_n) > 0$, alors en appliquant le corollaire précédent on peut construire q s.d.v. de $\overline{F}_{n+1}$ à partir de S. On peut se demander par contre si, de façon similaire, on peut construire des s.d.v. de $\overline{F}_{n+1}$ dans le cas $\operatorname{ord}(s_n) < 0$. Pour répondre à cela, on donne une condition suffisante pour qu'un élément $\mu \in \overline{K}((t))$ tel que $\operatorname{ord}(\mu) < 0$ soit tel que le polynôme

$$U^q \mu^{q-1} + U - \mu^q \in \overline{K}((t))[U]$$

admet toutes ses racines dans $\overline{K}((t))$.

Soit $v, v' \in \overline{K}((t))$. On écrit

$$v = v' + \mathrm{O}(t^n)$$

pour signifier que $\operatorname{ord}(v - v') \geq n$.

Proposition 4.3.9 *Soit*

$$\vartheta = \alpha t^{-1} + \mathrm{O}(t^q)$$

où $\alpha \in \overline{K}$ est tel que $\alpha \neq 0$ et $\alpha^q + \alpha = 0$. Soit

$$\xi := \sum_{i=0}^{\infty} (-1)^i t^{(q+1)q^i - 1} = t^q - t^{q^2+q-1} + t^{q^3+q^2-1} - \cdots$$

et posons

$$\mu := \phi_\xi(\vartheta).$$

Alors le polynôme

$$U^q \mu^{q-1} + U - \mu^q \in \overline{K}((t))[U]$$

admet q racines $u_1, u_2, \ldots, u_q \in \overline{K}((t))$ deux à deux distinctes. De plus, chacune des racines u_i est telle que

$$u_i = \alpha^q t^{-1} + \mathrm{O}(t^q).$$

Démonstration : Il suffit de montrer que le polynôme $\varphi(T) = T^q + T - \mu^{q+1}$ admet ses q racines dans $\overline{K}((t))$: en effet, si $w_1, w_2, \ldots, w_q$ sont les racines de $\varphi(T)$, alors en posant $u_i = \mu^{-1} w_i$, on a $u_i{}^q \mu^{q-1} + u_i - \mu^q = 0$. Pour un certain $\beta \in \overline{K}$, on a

$$\vartheta^{q+1} = \alpha^{q+1} t^{-(q+1)} + \beta + \mathrm{O}(t^1).$$

Par conséquent,

$$\begin{aligned}
\mu^{q+1} &= \phi_\xi(\vartheta)^{q+1} \\
&= \phi_\xi(\vartheta^{q+1}) \\
&= \phi_\xi(\alpha^{q+1}t^{-(q+1)} + \beta + \mathrm{O}(t^1)) \\
&= \alpha^{q+1}\xi^{-(q+1)} + \beta + \mathrm{O}(t^q). \qquad (4.7)
\end{aligned}$$

Pour déterminer les racines de $\varphi(T)$, il faut calculer les premiers termes de $\xi^{-(q+1)}$. Observons que $\xi = t^{-1}v$ où

$$v = \sum_{i=0}^{\infty} (-1)^i t^{(q+1)q^i}$$

est une racine du polynôme $T^q + T - t^{q+1}$ (voir la démonstration du Lemme 4.3.6). On en déduit par des calculs simples que

$$\xi^{-(q+1)} = t^{-q(q+1)} + t^{-(q+1)} + \mathrm{O}(t^1). \qquad (4.8)$$

Après substitution dans l'équation (4.7) on trouve

$$\mu^{q+1} = \alpha^{q+1}t^{-q(q+1)} + \alpha^{q+1}t^{-(q+1)} + \beta + r$$

où $r \in \overline{K}((t))$ est tel que $\mathrm{ord}\,(r) > 0$. Soient $\lambda_1, \lambda_2, \ldots, \lambda_q \in \overline{K}$ les q racines deux à deux distinctes de $X^q + X - \beta$ et posons

$$w_i := \alpha^{q+1}t^{-(q+1)} + \lambda_i + \phi_r(v) \qquad (4.9)$$

où

$$v := t - t^q + t^{q^2} - t^{q^3} + \cdots.$$

Puisque $\alpha^q + \alpha = 0$, et qu'en particulier $\alpha^{q^2} = \alpha$, on a $(\alpha^{q+1})^q = \alpha^{q+1}$. De plus, $\phi_r(v)^q + \phi_r(v) = \phi_r(v^q + v) = \phi_r(t) = r$. On a donc pour $i = 1, 2, \ldots, q$,

$$\begin{aligned}
{w_i}^q + w_i &= \alpha^{q+1}t^{-q(q+1)} + \alpha^{q+1}t^{-(q+1)} + (\lambda_i^q + \lambda_i) + \phi_r(v)^q + \phi_r(v) \\
&= \alpha^{q+1}t^{-q(q+1)} + \alpha^{q+1}t^{-(q+1)} + \beta + r \\
&= \mu^{q+1}.
\end{aligned}$$

Ainsi, en posant

$$u_i := \mu^{-1}w_i$$

pour $i = 1, 2, \ldots, q$, on a

$${u_i}^q\mu^{q-1} + u_i - \mu^q = 0$$

et $u_i \neq u_j$ si $i \neq j$. Pour finir, on a

$$\mu^{-1} = \alpha^{-1}t^q + \mathrm{O}(t^{q^2+q-1})$$

et en multipliant ce qui précède par (4.9), on trouve

$$u_i = \mu^{-1} w_i = \alpha^q t^{-1} + \mathrm{O}(t^q), \quad i = 1, 2, \ldots, q.$$

□

Le lemme suivant donne une autre méthode pour obtenir une s.d.v. de $\overline{F}_{n+1}$ à partir d'une s.d.v. de $\overline{F}_n$. En l'utilisant avec le Corollaire 4.3.8 et la Proposition 4.3.9, on pourra construire pour toute place $\mathfrak{P} \in \mathbb{P}_n^\infty$ telle que $\nu_{\mathfrak{P}}(x_1) > 0$ une séquence de valuation S telle que $\nu_S = \nu_{\mathfrak{P}}$.

Lemme 4.3.10 *Soit $S = (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$ tel que $s_1 = t$. Soit ξ comme à la Proposition 4.3.9. Alors*

$$S_\xi := (t, \xi, \phi_\xi(s_2), \phi_\xi(s_3), \ldots, \phi_\xi(s_n))$$

est une s.d.v. de $\overline{F}_{n+1}$.

Démonstration : Rappelons que $\xi = t^{-1}v$ où v est une racine du polynôme $T^q + T - t^{q+1}$ (voir la démonstration de la Proposition 4.3.9). On a donc

$$\begin{aligned} \xi^q t^{q-1} + \xi - t^q &= (t^{-1}v)^q t^{q-1} + t^{-1}v - t^q \\ &= t^{-1}v^q + t^{-1}v - t^q \\ &= t^{-1}(v^q + v - t^{q+1}) \\ &= 0 \end{aligned}$$

d'où (t, ξ) est une s.d.v. de $\overline{F}_2$. De même, $(t, \xi, \phi_\xi(s_2))$ est une s.d.v. de $\overline{F}_3$ car $\xi = \phi_\xi(t) = \phi_\xi(s_1)$ et

$$\phi_\xi(s_2)^q \xi^{q-1} + \phi_\xi(s_2) - \xi^{q+1} = \phi_\xi(s_2^q s_1^{q-1} + s_2 - s_1^{q+1}) = 0.$$

Toujours de la même façon, pour $i = 3, 4, \ldots, n$,

$$\phi_\xi(s_i)^q \phi_\xi(s_{i-1})^{q-1} + \phi_\xi(s_i) - \phi_\xi(s_{i-1})^q = \phi_\xi\left(s_i^q s_{i-1}^{q-1} + s_i - s_{i-1}^q\right) = 0$$

d'où S_ξ est une s.d.v. de $\overline{F}_{n+1}$. □

Corollaire 4.3.11 *Soient n pair et $S := (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$. Si S est telle que*

$$\begin{cases} s_1 = t, \\ s_n = \alpha t^{-1} + \mathrm{O}(t^q), \end{cases}$$

alors il existe q s.d.v. $S' := (s'_1, s'_2 \ldots, s'_{n+2})$ de $\overline{F}_{n+2}$ deux à deux non équivalentes telles que

$$\begin{cases} s'_1 = t, \\ s'_{n+2} = \alpha^q t^{-1} + \mathrm{O}(t^q). \end{cases}$$

Démonstration : On peut appliquer la Proposition 4.3.9 à la séquence S pour obtenir la s.d.v. de $\overline{F}_{n+1}$

$$S_\xi := (t, \xi, \phi_\xi(s_2), \phi_\xi(s_3), \ldots, \phi_\xi(s_n)).$$

Par hypothèse, on peut appliquer la Proposition 4.3.9 aux éléments $\vartheta := s_n$ et $\mu := \phi_\xi(s_n)$ pour obtenir q racines $u_1, u_2, \ldots, u_q$ deux à deux distinctes du polynôme

$$U^q \phi_\xi(s_n)^{q-1} + U - \phi_\xi(s_n)^q$$

et qui sont telles que

$$u_i = \alpha^q t^{-1} + \mathrm{O}(t^q).$$

Mais il est clair alors que les q séquences

$$S'_i := (t, \xi, \phi_\xi(s_2), \phi_\xi(s_3), \ldots, \phi_\xi(s_n), u_i), \quad i = 1, 2, \ldots, q,$$

sont des s.d.v. de $\overline{F}_{n+2}$ deux à deux non équivalentes et qu'elles vérifient les propriétés voulues. □

Pour le cas n pair, le corollaire suivant montre qu'il existe au moins $(q-1)q^{n/2-1}$ places $\mathfrak{P} \in \mathbb{P}_n^\infty$ telles que $\nu_\mathfrak{P}(x_1) = 1$ et $\nu_\mathfrak{P}(x_n) = -1$.

Corollaire 4.3.12 *Soit le corps de fonctions $\overline{F}_n$ avec n pair. Alors il existe au moins $(q-1)q^{n/2-1}$ s.d.v. $S = (s_1, s_2, \ldots, s_n)$ deux à deux non équivalentes telles que*

$$\begin{cases} s_1 &= t, \\ s_n &= \alpha t^{-1} + \mathrm{O}(t^q) \end{cases} \tag{4.10}$$

où $\alpha \in \overline{K}$ est tel que $\alpha \neq 0$ et $\alpha^q + \alpha = 0$.

Démonstration : Montrons par récurrence sur n pair. Si $n = 2$, soient $\alpha_2, \alpha_3, \ldots, \alpha_q$ les $q-1$ racines non nulles de $X^q + X \in \overline{K}[X]$ et soit

$$v := \sum_{i=0}^{\infty} (-1)^i t^{(q+1)q^i} = t^{q+1} - t^{(q+1)q} + t^{(q+1)q^2} - \cdots$$

qui est l'unique racine de $T^q + T - t^{q+1}$ telle que $\mathrm{ord}\,(v) > 0$. Pour $i = 2, 3, \ldots, q$, posons

$$v_i := \alpha_i + v.$$

Alors

$$v_i{}^q + v_i - t^{q+1} = (\alpha_i^q + v^q) + (\alpha_i + v) - t^{q+1} = (\alpha_i^q + \alpha_i) + v^q + v - t^{q+1} = 0$$

d'où en posant $u_i := t^{-1}v_i$, on a $q-1$ s.d.v. (t, u_i) de $\overline{F}_2$. De plus, ces $q-1$ s.d.v. sont deux à deux non équivalentes car les racines α_i sont deux à deux distinctes. La proposition est donc vraie pour $n=2$ car

$$u_i = t^{-1}v_i = t^{-1}(\alpha_i + v) = \alpha_i t^{-1} + t^{-1}v = \alpha_i t^{-1} + \mathrm{O}(t^q)$$

avec $\alpha_i^q + \alpha_i = 0$ pour $i = 2, 3, \ldots, q$. Soit maintenant $n > 2$, n pair, et supposons le corollaire vrai pour $n-2$, c'est-à-dire qu'il existe $q^{(n-2)/2-1}(q-1) = q^{n/2-2}(q-1)$ s.d.v. de $\overline{F}_{n-2}$ vérifiant (4.10). On peut appliquer à chacune de ces $q^{n/2-2}(q-1)$ s.d.v. le Corollaire 4.3.11 pour obtenir q s.d.v. vérifiant (4.10). On a donc au total $q \times q^{(n/2-2)}(q-1) = q^{n/2-1}$ s.d.v. de $\overline{F}_n$ et il est clair qu'elles sont toutes deux à deux non équivalentes. $\square$

4.4 Caractérisation des places

Dans cette section, on montre comment construire une s.d.v. S de $\overline{F}_n$ telle que $\nu_S = \nu_{\mathfrak{Q}}$ pour chacune des places $\mathfrak{Q} \in \mathbb{P}_n^\infty$. Pour ce faire, on montre dans un premier temps qu'il existe une unique place $\mathfrak{P}$ de $\overline{F}_n$ telle que $\nu_{\mathfrak{P}}(x_i) > 0$ pour $i = 1, 2, \ldots, n$. Bien que $\mathfrak{P} \notin \mathbb{P}_n^\infty$, il faut considérer cette place car il existe exactement $q-1$ places de $\mathbb{P}_{n+1}^\infty$ dominant la place $\mathfrak{P}$ (cf. Proposition 4.4.2).

Lemme 4.4.1 *Soit $\mathfrak{P}$ une place de F_n. Alors pour tout $i \in \{1, 2, \ldots, n-1\}$ on a*

1. *si $\nu_{\mathfrak{P}}(x_i) \geq 0$, alors $\nu_{\mathfrak{P}}(x_{i+1}) = q \times \nu_{\mathfrak{P}}(x_i)$ ou $\nu_{\mathfrak{P}}(x_{i+1}) = -\nu_{\mathfrak{P}}(x_i)$,*
2. *si $\nu_{\mathfrak{P}}(x_i) < 0$, alors $q \times \nu_{\mathfrak{P}}(x_{i+1}) = \nu_{\mathfrak{P}}(x_i)$,*
3. *$\nu_{\mathfrak{P}}(x_i) = 0 \iff \nu_{\mathfrak{P}}(x_{i+1}) = 0$.*

Démonstration : Montrons seulement (1) (les énoncés (2) et (3) se démontrent de façon similaire). Posons $z_{i+1} = x_{i+1}x_i$. On a $z_{i+1}^q + z_{i+1} = x_i^{q+1}$ et

$$\nu_{\mathfrak{P}}\left(z_{i+1}^q + z_{i+1}\right) = (q+1)\nu_{\mathfrak{P}}(x_i).$$

Observons d'abord que

$$\nu_{\mathfrak{P}}(x_i) \geq 0 \iff \nu_{\mathfrak{P}}\left(z_{i+1}^q + z_{i+1}\right) \geq 0 \iff \nu_{\mathfrak{P}}(z_{i+1}) \geq 0.$$

Étant donné que $\nu_{\mathfrak{P}}(z_{i+1}) = \nu_{\mathfrak{P}}(x_{i+1}) + \nu_{\mathfrak{P}}(x_i)$, il est clair que $\nu_{\mathfrak{P}}(z_{i+1}) = 0$ entraîne $\nu_{\mathfrak{P}}(x_{i+1}) = -\nu_{\mathfrak{P}}(x_i)$. Sinon $\nu_{\mathfrak{P}}(z_{i+1}) > 0$ et alors

$$\nu_{\mathfrak{P}}(x_{i+1}) + \nu_{\mathfrak{P}}(x_i) = \nu_{\mathfrak{P}}(z_{i+1}) = \nu_{\mathfrak{P}}\left(z_{i+1}^q + z_{i+1}\right) = \nu_{\mathfrak{P}}\left(x_i^{q+1}\right) = (q+1)\nu_{\mathfrak{P}}(x_i)$$

et donc $q \times \nu_{\mathfrak{P}}(x_i) = \nu_{\mathfrak{P}}(x_{i+1})$. □

Proposition 4.4.2 *Soit le corps de fonction $\overline{F}_n$ et supposons qu'il existe une place $\mathfrak{P}$ telle que $\nu_{\mathfrak{P}}(x_1) = 1$ et $\nu_{\mathfrak{P}}(x_i) > 0$ pour $i = 2, 3, \ldots, n$. Alors*

1. *$\nu_{\mathfrak{P}}(x_i) = q^{i-1}$ pour $i = 1, 2, \ldots, n$,*
2. *il existe exactement q places $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_q$ de $\overline{F}_{n+1}$ dominant $\mathfrak{P}$. En particulier, pour $j = 1, 2, \ldots, q$, on a $e(\mathfrak{Q}_j|\mathfrak{P}) = 1$,*
3. *exactement une des q places dominant $\mathfrak{P}$, disons $\mathfrak{Q}_1$, est tel que $\nu_{\mathfrak{Q}}(x_{n+1}) > 0$. Plus précisément, on a*

$$\begin{cases} \nu_{\mathfrak{Q}_1}(x_{n+1}) &= q^n, \\ \nu_{\mathfrak{Q}_j}(x_{n+1}) &= -\nu_{\mathfrak{P}}(x_n) \text{ pour } j = 2, 3, \ldots, q. \end{cases}$$

Démonstration : (1). C'est une conséquence du Lemme 4.4.1.

(2). D'après le Théorème 4.1.3, on a $q = [\overline{F}_{n+1}, \overline{F}_n]$. Puisque $\nu_{\mathfrak{P}}(x_1) = 1$, $t := x_1$ est un paramètre local de $\mathfrak{P}$. Pour $i = 1, 2, \ldots, n$, soit $s_i := x_i(t)$ la série $\mathfrak{P}$-adique de x_i en fonction de t. Alors $S := (s_1, s_2, \ldots, s_n)$ est une s.d.v. de $\overline{F}_n$. Puisque $s_1 = t$, on peut appliquer le Corollaire 4.3.8 pour obtenir q s.d.v. de $\overline{F}_{n+1}$ deux à deux non équivalentes. Celles-ci correspondent à autant de places $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_q$ deux à deux distinctes et il est clair que chacune d'elles domine la place $\mathfrak{P}$. En vertu du Théorème 2.8.5, ces places sont les seules places qui dominent $\mathfrak{P}$ et $e(\mathfrak{Q}_i \mid \mathfrak{P}) = 1$ pour $i = 1, 2, \ldots, q$.

(3). C'est un conséquence du Corollaire 4.3.7. □

Proposition 4.4.3 *Il existe une unique place $\mathfrak{P}$ de $\overline{F}_n$ telle que $\nu_{\mathfrak{P}}(x_i) > 0$. En particulier, cette place est telle que $\nu_{\mathfrak{P}}(x_1) = 1$.*

Démonstration : Par récurrence sur n. Pour $n = 1$, il est clair qu'il existe une unique place $\mathfrak{P}$ de $\overline{F}_1 = \overline{K}(x_1)$ qui est un zéro de x_1 et qu'elle est telle que $\nu_{\mathfrak{P}}(x_1) = 1$ (voir Exemple 1.2.2). Supposons maintenant la proposition vraie pour n et montrons la pour $n+1$. Soit $\mathfrak{P} \in \mathbb{P}_{\overline{F}_n}$ l'unique place telle que $\nu_{\mathfrak{P}}(x_i) > 0$ pour $i = 1, 2, \ldots, n$. D'après la Proposition 4.4.2, la place $\mathfrak{P}$ est dominée par q places de $\overline{F}_{n+1}$ dont exactement une, disons $\mathfrak{Q}$, est telle que $\nu_{\mathfrak{Q}}(x_{n+1}) = q^n$. Par conséquent, $\mathfrak{Q}$ est telle que $\nu_{\mathfrak{Q}}(x_i) > 0$ pour $i = 1, 2, \ldots, n+1$. De plus, toujours d'après la Proposition 4.4.2, on a $e(\mathfrak{Q}|\mathfrak{P}) = 1$ d'où $\nu_{\mathfrak{Q}}(x_1) = \nu_{\mathfrak{P}}(x_1) = 1$. Pour terminer la démonstration, il faut montrer que $\mathfrak{Q}$ est l'unique place telle que $\nu_{\mathfrak{Q}}(x_i) > 0$ pour $i = 1, 2, \ldots, n+1$. Soit $\mathfrak{Q}' \in \mathbb{P}_{\overline{F}_{n+1}}$ telle que $\nu_{\mathfrak{Q}'}(x_i) > 0$ pour $i = 1, 2, \ldots, n+1$. Alors $\mathfrak{P}' = \mathfrak{Q}' \cap \overline{F}_n$ est telle que $\nu_{\mathfrak{P}'}(x_i) > 0$ pour $i = 1, 2, \dots, n$ d'où $\mathfrak{P}' = \mathfrak{P}$ par unicité de $\mathfrak{P}$. Mais dans ce cas, on a $\mathfrak{Q}'|\mathfrak{P}$ d'où $\mathfrak{Q}' = \mathfrak{Q}$ du fait que $\mathfrak{Q}$ est l'unique place dominant $\mathfrak{P}$ avec $\nu_{\mathfrak{Q}}(x_{n+1}) > 0$. $\square$

Soit n pair et considérons l'ensemble

$$V := \{\, \mathfrak{P} \in \mathbb{P}_n^{\infty} \;\mid\; \nu_{\mathfrak{P}}\,(x_1) = 1 \text{ et } \nu_{\mathfrak{P}}\,(x_n) = -1 \,\}\,.$$

On a vu au Corollaire 4.3.12 qu'on peut construire au moins $(q-1)q^{n/2-1}$ s.d.v. $S := (s_1, s_2, \dots, s_n)$ telles que $s_1 = t$ et $\operatorname{ord}(s_n) = -1$. Celles-ci correspondent à autant de places de $\mathbb{P}_n^{\infty}$ deux à deux distinctes. On en déduit donc que

$$(q-1)q^{n/2-1} \leq \#V.$$

Il est clair alors qu'il suffit de montrer $(q-1)q^{n/2-1} = \#V$ pour affirmer que l'on sait construire une s.d.v. pour chacune des places de V. D'une manière plus générale, on appliquera ce raisonnement à l'ensemble suivant :

$$V_r^n := \left\{\, \mathfrak{P} \in \mathbb{P}_{\overline{F}_n} \;\mid\; \nu_{\mathfrak{P}}\,(x_1) = 1, \nu_{\mathfrak{P}}\,(x_n) < 0 \text{ et } \nu_{\mathfrak{P}}\,(x_r) = -\nu_{\mathfrak{P}}\,(x_n) \,\right\}$$

où $n \geq 2$ et r est un entier tel et $1 \leq r < n$. Le lemme qui suit donne une borne supérieure sur le nombre d'éléments de V_r^n.

Lemme 4.4.4 *Soient $n \geq 2$ et r un entier tel et $1 \leq r < n$. Alors*

1. *$V_r^n = \emptyset$ si $n - r$ est pair,*

2. *$\#V_r^n \leq (q-1)q^{(n-r+1)/2-1}$ si $n - r$ est impair.*

Démonstration : (1). Montrons plutôt que $V_n^r \neq \emptyset$ entraîne $n-r$ impair. Soit $\mathfrak{Q} \in V_n^r$. Puisque $\nu_{\mathfrak{Q}}\,(x_1) > 0$ et $\nu_{\mathfrak{Q}}\,(x_n) < 0$, il existe l, $1 \leq l < n$, tel que $\nu_{\mathfrak{Q}}\,(x_l) = -\nu_{\mathfrak{Q}}\,(x_{l+1})$ (Lemme 4.4.1). On a forcément $r \leq l$ et $l + 1 \leq n$. De plus, on vérifie aisément que $q^{l-r}\nu_{\mathfrak{Q}}\,(x_r) = \nu_{\mathfrak{Q}}\,(x_l)$ et $q^{n-l+1}\nu_{\mathfrak{Q}}\,(x_n) = \nu_{\mathfrak{Q}}\,(x_{l+1})$. On en déduit que $n-l+1 = l-r$ d'où $n - r = 2l - 2r + 1$ est impair.

(2). Supposons $n - r$ impair et montrons la propriété par récurrence sur $n \geq 2$. Si $n = 2$, alors d'après la Proposition 4.4.2, V_1^2 est exactement l'ensemble des $q - 1$ places $\mathfrak{Q}$ de $\overline{F}_2$ telles que $\nu_{\mathfrak{P}}(x_2) = -1$ et $\mathfrak{Q}|\mathfrak{P}_0$ où $\mathfrak{P}_0 \in \mathbb{P}_{\overline{F}_1}$ est l'unique zéro de x_1. Supposons maintenant que l'assertion (2) est vraie pour $n - 1$. Si $V_r^n = \emptyset$, il n'y a rien à montrer. Supposons donc $V_r^n \neq \emptyset$. Soient $\mathfrak{Q} \in V_r^n$ et $\mathfrak{P} := \mathfrak{Q} \cap \overline{F}_{n-1}$. On a $e(\mathfrak{Q}|\mathfrak{P}) = 1$ car $1 = \nu_{\mathfrak{Q}}\,(x_1) = e(\mathfrak{Q}|\mathfrak{P})\nu_{\mathfrak{P}}(x_1)$. Par conséquent, $\nu_{\mathfrak{P}}\,(x_i) = \nu_{\mathfrak{Q}}\,(x_i)$ pour $i = 1, 2, \dots, n-1$ et on en déduit que $\mathfrak{P} \in V_{r+1}^{n-1}$. Donc toute place de V_r^n domine une place de V_{r+1}^{n-1}. Or au plus q places de $\overline{F}_n$ dominent une place de $\overline{F}_{n-1}$

car $[\overline{F}_n : \overline{F}_{n-1}] = q$. On a donc $\#V_r^n \leq q \times \#V_{r+1}^{n-1}$ d'où en utilisant l'hypothèse de récurrence

$$\#V_r^n \leq q(q-1)q^{((n-1)-(r+1)+1)/2-1} = (q-1)q^{(n-r+1)/2-1}.$$

$\square$

THÉORÈME 4.4.5 *Soient $n \geq 2$ et r un entier, $1 \leq r < n$, tel que $n-r$ soit impair. Alors*

$$\#V_r^n = (q-1)q^{(n-r+1)/2-1}.$$

Démonstration : Par récurrence sur $n \geq 2$ tel que $n-r$ soit impair. Vu le lemme précédent, il suffit de montrer que

$$\#V_r^n \geq (q-1)q^{(n-r+1)/2-1}.$$

Supposons que $r = n-1$ et soit $\mathfrak{P}$ l'unique place de $\overline{F}_{n-1}$ telle que $\nu_{\mathfrak{P}}(x_i) > 0$ pour $i = 1, 2, \dots, n-1$. D'après la Proposition 4.4.2, il existe $q-1$ places $\mathfrak{Q}_i \in \mathbb{P}_{\overline{F}_n}$ dominant la place $\mathfrak{P}$ et ces places sont telles que $\nu_{\mathfrak{Q}_i}(x_n) = -\nu_{\mathfrak{Q}_i}(x_{n-1})$. En particulier, $\mathfrak{Q}_i \in V_{n-1}^n$ d'où $\#V_{n-1}^n \geq (q-1)$. Le théorème est donc vrai si $r = n-1$ et en particulier si $n = 2$. Supposons donc $n > 2$, $1 \leq r < n-1$ et que le théorème est vrai pour $n-1$. Soit le corps de fonctions $\overline{F}_{n-r+1}$. Puisque $n-r+1$ est pair, d'après le Corollaire 4.3.12, il existe $l := (q-1)q^{(n-r+1)/2-1}$ s.d.v. de $\overline{F}_{n-r+1}$ correspondant à autant de places $\mathfrak{Q}_1, \mathfrak{Q}_2, \dots, \mathfrak{Q}_l$ deux à deux distinctes telles que $\nu_{\mathfrak{Q}_i}(x_1) = 1$ et $\nu_{\mathfrak{Q}_i}(x_{n-r+1}) = -1$. Par conséquent, $V_1^{n-r+1} \supseteq \{\, \mathfrak{Q}_1, \mathfrak{Q}_2, \dots, \mathfrak{Q}_l \,\}$ et

$$\#V_1^{n-r+1} \geq (q-1)q^{(n-r+1)/2-1}.$$

Chacune des places $\mathfrak{Q} \in V_1^{n-r+1}$ admet $t := x_1$ pour paramètre local. On a donc pour chacune des places $\mathfrak{Q} \in V_1^{n-r+1}$ une s.d.v. $S_{\mathfrak{Q}} := (s_1, s_2, \dots, s_{n-r+1})$ de $\overline{F}_{n-r+1}$ où $s_i := x_i(t)$ est la série $\mathfrak{Q}$-adique de x_i en fonction de t. En appliquant le Lemme 4.3.10 à chacune des s.d.v. $S_{\mathfrak{Q}}$, on obtient autant de s.d.v. de $\overline{F}_{n-r+2}$ deux à deux non équivalentes. Celles-ci à leur tour correspondent à autant de places de $\overline{F}_{n-r+2}$ deux à deux distinctes et il est aisé de montrer que toutes ces places sont dans l'ensemble V_2^{n-r+2}. On a donc

$$\#V_2^{n-r+2} \geq \#V_1^{n-r+1}.$$

De la même façon, on montre que $\#V_3^{n-r+3} \geq \#V_2^{n-r+2}$ et ainsi de suite pour obtenir

$$\#V_r^n \geq \#V_{r-1}^{n-1} \geq \cdots \geq \#V_1^{n-r+1} \geq (q-1)q^{(n-r+1)/2-1}.$$

$\square$

On vient donc de montrer qu'on peut construire une s.d.v. de $\overline{F}_n$ telle que $\nu_S = \nu_{\mathfrak{P}}$ pour toute place $\mathfrak{P} \in \mathbb{P}_n^\infty$ telle que $\nu_{\mathfrak{P}}(x_1) = 1$. Or on ne sait toujours pas construire une s.d.v. pour chacune des places de $\mathbb{P}_n^\infty$ car il existe au moins une place $\mathfrak{P} \in \mathbb{P}_n^\infty$ telle que $\nu_{\mathfrak{P}}(x_1) < 0$ (cf. Corollaire 1.2.17). C'est grâce à une propriété particulière des équations qui définissent les corps de fonctions $\overline{F}_n$ qu'on pourra calculer les s.d.v. correspondant aux pôles de x_1. En effet, comme le montre la proposition suivante, les s.d.v. de $\overline{F}_n$ sont en quelque sorte "réversibles".

Proposition 4.4.6 *Soit $S = (s_1, s_2, \ldots, s_n)$ une s.d.v. de $\overline{F}_n$. Alors*

$$S^{-1} := (s_n^{-1}, s_{n-1}^{-1}, \ldots, s_1^{-1})$$

est une s.d.v. de $\overline{F}_n$.

Démonstration : Montrons que les trois propriétés de la Définition 4.3.1 sont satisfaites par S^{-1}. Il est clair que $s_i^{-1} \notin \overline{K}$ car $s_i \notin \overline{K}$. Ensuite, pour $i = 1, 2, \ldots, n-1$ on a

$$(s_i^{-1})^q (s_{i+1}^{-1})^{q-1} + s_i^{-1} - (s_{i+1}^{-1})^q = s_{i+1}^{-q} s_i^{-q} \left(s_{i+1}^q s_i^q + s_{i+1} - s_i^q \right) = 0.$$

Maintenant, soient $G, H \in \overline{K}[\underline{X}]$ tels que

$$\mathrm{ord}\,(G[S]) - \mathrm{ord}\,(H[G]) = 1.$$

On peut choisir un entier N assez grand de sorte qu'il existe $G', H' \in \overline{K}[\underline{X}]$ tels que

$$\begin{aligned} G'[S^{-1}] &= (s_1 s_2 \cdots s_n)^{-N} G[S], \\ H'[S^{-1}] &= (s_1 s_2 \cdots s_n)^{-N} H[S] \end{aligned}$$

et donc

$$\mathrm{ord}\left(G'[S^{-1}]\right) - \mathrm{ord}\left(H'[S^{-1}]\right) = 1.$$

$\square$

Lemme 4.4.7 *Soient $S = (s_1, s_2, \ldots, s_n)$ et $S' = (s'_1, s'_2, \ldots, s'_n)$ deux s.d.v. de $\overline{F}_n$. Si $s_1 = s'_1 = t$, alors*

$$S \equiv S' \iff S^{-1} \equiv {S'}^{-1}.$$

Démonstration : L'implication ($\Rightarrow$) est évidente du fait que, d'après la Proposition 4.3.4, $s_1 = s'_1 = t$ entraîne $S \equiv S'$ si et seulement si $S = S'$. Réciproquement, supposons que $S \not\equiv S'$. Alors il existe $l > 1$ tel que $s_l \neq s'_l$ d'où $S^{-1} \neq S'^{-1}$. Mais $t = \varphi_{S^{-1}}(1/x_n) = \varphi_{S'^{-1}}(1/x_n)$ et donc $S^{-1} \not\equiv S'^{-1}$ en vertu de la Proposition 4.3.4.

$\square$

Étant donnée une s.d.v. $S := (s_1, s_2, \ldots, s_n)$ de $\overline{F}_n$ telle que $s_1 = t$, la s.d.v. S^{-1} correspond donc à une place de $\mathfrak{P} \in \mathbb{P}_n^\infty$ telle que $\nu_\mathfrak{P}(x_n) = -1$. On sait donc construire des s.d.v. dont les places $\mathfrak{P}$ correspondantes sont telles que $\nu_\mathfrak{P}(x_1) = 1$ ou $\nu_\mathfrak{P}(x_n) = -1$. En fait, les s.d.v. $S := (s_1, s_2, \ldots, s_n)$ de $\overline{F}_n$ telles que $s_1 = t$ et leurs réciproques S^{-1} suffiront pour construire une s.d.v. pour chacune des places de $\mathbb{P}_n^\infty$. Pour montrer ce fait, on a besoin du théorème suivant.

Théorème 4.4.8 *Soient $\mathfrak{P}$ une place de $\overline{F}_n$ telle que $\nu_\mathfrak{P}(x_1) = 1$ et $\mathfrak{Q}$ une place de $\overline{F}_{n+1}$ dominant la place $\mathfrak{P}$. Alors*

$$e(\mathfrak{Q}|\mathfrak{P}) = 1 \iff \nu_\mathfrak{P}(x_n) \neq -1.$$

Démonstration : On sait d'après le Théorème 4.1.3 que si $\nu_\mathfrak{P}(x_n) = -1$, alors il existe une unique place $\mathfrak{Q}$ de $\overline{F}_{n+1}$ dominant $\mathfrak{P}$ et elle est telle que $e(\mathfrak{Q}|\mathfrak{P}) = q$. Réciproquement, supposons que $\nu_\mathfrak{P}(x_n) \neq -1$. Si $\nu_\mathfrak{P}(x_n) \geq 0$, alors on déduit du Corollaire 4.3.8 qu'il existe q places de $\overline{F}_{n+1}$ dominant $\mathfrak{P}$ et donc $e(\mathfrak{Q}|\mathfrak{P}) = 1$. Supposons que $\nu_\mathfrak{P}(x_n) < -1$. Alors il existe $r > 1$ tel que $\nu_\mathfrak{P}(x_r) = -\nu_\mathfrak{P}(x_n)$ d'où $\mathfrak{P} \in V_r^n$. Par conséquent $n - r$ est impair et $V_{r-1}^{n+1} \neq \emptyset$ (Lemme 4.4.4 et Théorème 4.4.5). Soit donc $\mathfrak{Q}' \in V_{r-1}^{n+1}$. Alors $\mathfrak{P}' := \mathfrak{Q}' \cap \overline{F}_n \in V_r^n$. En particulier,

$$V_{r-1}^{n+1} \subseteq V := \left\{ \mathfrak{Q} \in \mathbb{P}_{\overline{F}_{n+1}} \;\middle|\; \mathfrak{Q}|\mathfrak{P}, \mathfrak{P} \in V_r^n \right\}.$$

Puisque qu'une place de $\overline{F}_n$ est dominée par au plus q places de $\overline{F}_{n+1}$, on a $q \times \#V_r^n \geq \#V$. D'après le Théorème 4.4.5, on a $q \times \#V_r^n = \#V_{r-1}^{n+1}$ d'où $\#V = \#V_{r-1}^{n+1}$ et par conséquent $V = V_{r-1}^{n+1}$. Ainsi, quelle que soit la place $\mathfrak{Q}$ dominant la place $\mathfrak{P}$, on a $\mathfrak{Q} \in V_{r-1}^{n+1}$ et en particulier $\nu_\mathfrak{Q}(x_1) = 1$. Or par hypothèse $\nu_\mathfrak{P}(x_1) = 1$ d'où

$$1 = \nu_\mathfrak{Q}(x_1) = e(\mathfrak{Q}|\mathfrak{P})\nu_\mathfrak{P}(x_1) = e(\mathfrak{Q}|\mathfrak{P}).$$

□

Corollaire 4.4.9 *Soit $\mathfrak{P}$ une place de $\overline{F}_n$ telle que $\nu_\mathfrak{P}(x_1) \neq 0$. Alors $\nu_\mathfrak{P}(x_1) = 1$ ou $\nu_\mathfrak{P}(x_n) = -1$.*

Démonstration : C'est évident pour $n = 1$. Supposons que le corollaire est vrai pour n et montrons le pour $n + 1$. Soit $\mathfrak{Q} \in \mathbb{P}_{\overline{F}_{n+1}}$ telle que $\nu_\mathfrak{Q}(x_1) \neq 0$ et supposons que $\nu_\mathfrak{Q}(x_{n+1}) \neq -1$. On veut montrer que $\nu_\mathfrak{Q}(x_1) = 1$. Soit la place $\mathfrak{P} := \mathfrak{Q} \cap \overline{F}_n$. Alors $\nu_\mathfrak{P}(x_n) \neq -1$ car sinon $e(\mathfrak{Q}|\mathfrak{P}) = q$ (Théorème 4.1.3) et alors, contrairement à l'hypothèse initiale, on aurait $\nu_\mathfrak{Q}(x_{n+1}) = -1$. D'après le théorème précédent, on a donc $e(\mathfrak{Q}|\mathfrak{P}) = 1$. De plus, il est clair aussi que $\nu_{\mathfrak{P}}(x_1) \neq 0$ d'où, par hypothèse de récurrence, on a $\nu_{\mathfrak{P}}(x_1) = 1$. Par conséquent,

$$\nu_{\mathfrak{Q}}(x_1) = e(\mathfrak{Q}|\mathfrak{P})\nu_{\mathfrak{P}}(x_1) = 1.$$

□

COROLLAIRE 4.4.10 *Les fonctions $x_1, x_2, \ldots, x_n$ de $\overline{F}_n$ ont un unique pôle en commun.*

Démonstration : Pour montrer l'existence, considérons $\mathfrak{P}_0$ l'unique zéro commun de x_i pour $i = 1, 2, \ldots, n$. Soit $S_0 = (s_1, s_2, \ldots, s_n)$ une s.d.v. telle que $\nu_{S_0} = \nu_{\mathfrak{P}_0}$ et $s_1 = t$. Alors S_0^{-1} est une s.d.v. telle que $\nu_{S_0^{-1}}(x_i) < 0$ pour $i = 1, 2, \ldots, n$. Par conséquent, la place $\mathfrak{P}_\infty$ telle que $\nu_{\mathfrak{P}_\infty} = \nu_{S_0^{-1}}$ est un pôle commun de $x_1, x_2, \ldots, x_n$. Pour montrer l'unicité, soit une place $\mathfrak{P}''$ telle que $\nu_{\mathfrak{P}''}(x_i) < 0$ pour $i = 1, 2, \ldots, n$. D'après le corollaire précédent, on doit avoir $\nu_{\mathfrak{P}''}(x_n) = -1$. Il existe donc une s.d.v. $S'' = (s''_1, s''_2, \ldots, s''_n)$ telle que $\nu_{S''} = \nu_{\mathfrak{P}''}$ et $s''_n = t^{-1}$. En particulier,

$$S''^{-1} = (t, s''^{-1}_{n-1}, \ldots, s''^{-1}_1)$$

est telle que $\nu_{S''^{-1}}(x_i) > 0$ pour $i = 1, 2, \ldots, n$. Par unicité de $\mathfrak{P}_0$, on doit avoir $S''^{-1} \equiv S_0$, d'où d'après le Lemme 4.4.7, on doit avoir $S'' \equiv S_0^{-1}$, montrant ainsi que $\mathfrak{P}'' = \mathfrak{P}_\infty$. □

Ainsi, dans $\overline{F}_n$, les fonctions $x_1, x_2, \ldots, x_n$ ont un unique pôle (resp. zéro, cf. Proposition 4.4.3) en commun. La proposition suivante est évidente.

PROPOSITION 4.4.11 *Soit $\mathfrak{P}_0 \in \mathbb{P}_{\overline{F}_n}$ (resp. $\mathfrak{P}_\infty \in \mathbb{P}_{\overline{F}_n}$) l'unique zéro (resp. pôle) commun de $x_1, x_2, \ldots, x_n$ et soit S une s.d.v. de $\overline{F}_n$. Alors*

$$\nu_S = \nu_{\mathfrak{P}_0} \iff \nu_{S^{-1}} = \nu_{\mathfrak{P}_\infty}.$$

On montre maintenant qu'on peut construire une s.d.v. de $\overline{F}_n$ pour chacune des places de $\mathbb{P}_n^\infty$ distinctes de $\mathfrak{P}_0$ et $\mathfrak{P}_\infty$. Soient $n \geq 2$ et r tel que $1 \leq r < n$ et $n - r$ impair. On sait construire chacune des s.d.v. de l'ensemble suivant :

$$\mathcal{S}_r^n := \{\, S = (s_1, s_2, \ldots, s_n) \mid s_1 = t \text{ et } \mathrm{ord}\,(s_r) = -\mathrm{ord}\,(s_n) \,\}.$$

On sait aussi construire toutes les s.d.v. de l'ensemble

$$\mathcal{IS}_r^n := \{\, S^{-1} \mid S \in \mathcal{S}_r^n \,\}.$$

COROLLAIRE 4.4.12 *Soit $\mathfrak{P}$ une place de $\overline{F}_n$ telle que $\nu_{\mathfrak{P}}(x_1) \neq 0$, distincte de l'unique zéro et de l'unique pôle commun à $x_1, x_2, \ldots, x_n$.*

1. *Si $\nu_{\mathfrak{P}}(x_1) = 1$, alors il existe $r < n$ et $S \in \mathcal{S}_r^n$ tel que $\nu_{\mathfrak{P}} = \nu_S$.*

2. Si $\nu_{\mathfrak{P}}(x_1) \neq 1$, alors il existe $r < n$ et $S \in \mathcal{IS}_r^n$ tel que $\nu_{\mathfrak{P}} = \nu_S$.

Démonstration : (1). C'est une conséquence du Théorème 4.4.5.

(2). Supposons que $\nu_{\mathfrak{P}}(x_1) \neq 1$. D'après le Corollaire 4.4.9, on a donc $\nu_{\mathfrak{P}}(x_n) = -1$ et on peut choisir $t := x_n^{-1}$ pour paramètre local de la place $\mathfrak{P}$. Pour $i = 1, 2, \ldots, n$, soit

$$s_i := x_i(t)$$

la série $\mathfrak{P}$-adique de x_i en fonction de t. Il est clair que $S = (s_1, s_2, \ldots, s_n)$ est une s.d.v. telle que $\nu_{\mathfrak{P}} = \nu_S$. De plus, $\mathrm{ord}\,(s_1) > 0$ car sinon on aurait $\mathfrak{P} = \mathfrak{P}_\infty$. On en déduit que

$$S^{-1} = (s_n^{-1}, s_{n-1}^{-1}, \ldots, s_1^{-1}) \in V_r^n$$

pour un certain $r < n$ et donc $S \in \mathcal{IS}_r^n$. □

On appliquera le corollaire qui suit pour calculer une base de l'espace vectoriel $\mathcal{L}(m\mathfrak{P}_\infty)$ où $\mathfrak{P}_\infty$ est le pôle commun des fonctions $x_1, x_2, \ldots, x_n$ de $\overline{F}_n$.

Corollaire 4.4.13 *On pose*

$$\mathcal{S} := \mathcal{S}_1^n \cup \bigcup_{i=1}^{[n/2]-1} \mathcal{S}_{2i+1}^n \cup \bigcup_{i=1}^{[n/2]-1} \mathcal{IS}_{2i+1}^n \qquad \textit{si } n \textit{ est pair}$$

et

$$\mathcal{S} := \bigcup_{i=1}^{[n/2]} \mathcal{S}_{2i}^n \cup \bigcup_{i=1}^{[n/2]} \mathcal{IS}_{2i}^n \qquad \textit{sinon.}$$

Soit $\mathfrak{P}_\infty$ l'unique pôle commun à $x_1, x_2, \ldots, x_n$ et soit S_∞ une s.d.v. telle que $\nu_{S_\infty} = \nu_{\mathfrak{P}_\infty}$. Soit $m \in \mathbb{N}$ et considérons l'espace vectoriel $\mathcal{L}(m\mathfrak{P}_\infty)$. Si $H_1, H_2, \ldots, H_l \in \overline{K}[\underline{X}]$ et $\alpha_1, \alpha_2, \ldots, \alpha_l \in \overline{K}$, alors

$$\sum_{i=1}^{l} \alpha_i H(\underline{x}) \in \mathcal{L}(m\mathfrak{P}_\infty) \iff \left\{ \begin{array}{rcl} \mathrm{ord}\left(\sum_{i=1}^{l} \alpha_i H_i[S_\infty]\right) & \geq & -m \textit{ et} \\ \mathrm{ord}\left(\sum_{i=1}^{l} \alpha_i H_i[S]\right) & \geq & 0, \textit{ pour tout } S \in \mathcal{S}. \end{array} \right.$$

Démonstration : C'est une conséquence de la Proposition 4.2.3 et du Corollaire 4.4.12. □

4.5 Exemple

On considère le cas $q = 4$ et $n = 4$. Posons $K := \mathbb{F}_{4^2}$ et $\overline{K} := \overline{\mathbb{F}}_{4^2}$. Alors $\overline{F}_4 := \overline{K}(x_1, x_2, x_3, x_4)$ où

$$\left\{ \begin{array}{rcl} x_2^4 x_1^3 + x_2 + x_1^4 & = & 0, \\ x_3^4 x_2^3 + x_3 + x_2^4 & = & 0, \\ x_4^4 x_3^3 + x_4 + x_3^4 & = & 0. \end{array} \right.$$

Le genre de $\overline{F}_4$ est $g = 261$. Soit $\mathfrak{P}_\infty$ l'unique pôle commun de x_1, x_2, x_3, x_4 et soit

$$\mathfrak{P}'_\infty := \mathfrak{P}_\infty \cap F_4.$$

On vérifiera aisément que $\deg \mathfrak{P}'_\infty = 1$ (c'est une conséquence du Théorème 4.1.3). Soit $\mathcal{Q}$ l'ensemble des places de degré 1 de F_4 ;

$$\mathcal{Q} := \{\, \mathfrak{P} \in \mathbb{P}_{F_4} \mid \deg \mathfrak{P} = 1 \,\}.$$

Soient les diviseurs

$$\mathcal{P} := \sum_{\mathfrak{P} \in \mathcal{Q} \setminus \{\, \mathfrak{P}'_\infty \,\}} \mathfrak{P}$$

et

$$D := 521 \mathfrak{P}'_\infty.$$

Dans cet exemple, on calcule une base[4] de $\mathcal{L}(D)$ et ensuite on explique comment calculer la matrice génératrice du code $C_{\mathcal{L}}(F_4, \mathcal{P}, D)$.

On a

$$\mathrm{Con}_{\overline{F}_4/F_4} \mathfrak{P}'_\infty = \mathfrak{P}_\infty.$$

D'après le Théorème 2.8.7, il existe donc une base du $\overline{K}$-espace vectoriel $\mathcal{L}(521\mathfrak{P}_\infty)$, formée d'éléments de F_4, qui est une base de $\mathcal{L}(521\mathfrak{P}'_\infty)$. Pour calculer une base de $\mathcal{L}(521\mathfrak{P}_\infty)$, on applique le Corollaire 4.4.13. On doit donc construire toutes les s.d.v. correspondant à toutes les places $\mathfrak{P} \in \mathbb{P}_{\overline{F}_4}$ telles que $\nu_{\mathfrak{P}}(x_1) \neq 0$, c'est-à-dire toutes les s.d.v. de l'ensemble

$$\mathcal{S} := \mathcal{S}_1^4 \cup \mathcal{S}_3^4 \cup \mathcal{IS}_3^4$$

et une s.d.v. S_∞ telle que $\nu_{S_\infty} = \nu_{\mathfrak{P}_\infty}$.

Pour construire la s.d.v. S_∞, on construit d'abord une s.d.v.

$$S_0 = (s_{0,1}, s_{0,2}, s_{0,3}, s_{0,4})$$

telle que $\nu_{S_0} = \nu_{\mathfrak{P}_0}$ où $\mathfrak{P}_0$ est l'unique zéro commun de x_1, x_2, x_3, x_4. On a $\nu_{\mathfrak{P}_0}(x_1) = 1$. Par conséquent, $t := x_1$ est un paramètre local de la place $\mathfrak{P}_0$. On peut prendre $s_{0,1} := t$. Soit

$$\xi := \sum_{i=0}^{\infty} (-1)^i t^{(q+1)q^i - 1} = t^q - t^{q^2+q-1} + t^{q^3+q^2-1} - \cdots$$

4. Si g est le genre d'un corps de fonctions F et D est un diviseur de degré $2g-1$ alors $\ell(D) = g$ (Théorème 1.5.4). En particulier, si $D = (2g-1)\mathfrak{P}$ où $\mathfrak{P}$ est une place de degré 1, on associe à la place $\mathfrak{P}$ les sauts de Weierstrass $i_1 < i_2 < \cdots < i_g \leq 2g-1$; un saut de Weierstrass en $\mathfrak{P}$ est un entier $i \geq 1$ tel qu'il n'existe aucune fonction $u \in F$ tel que $\nu_{\mathfrak{P}}(u) = -i$ et $\nu_{\mathfrak{Q}}(u) \geq 0$ pour toute place $\mathfrak{Q} \in \mathbb{P}_F \setminus \{\, \mathfrak{P} \,\}$. Toute place de degré 1 possède exactement g sauts de Weierstrass. Dans certains cas, la connaissance des sauts de Weierstrass est utile pour déterminer une meilleure borne pour la distance minimale des codes géométriques (voir [27]).

comme au Lemme 4.3.10. Posons $q = 4$ dans ξ et posons successivement $s_{0,2} := \xi$, $s_{0,3} := \phi_\xi(s_{0,2})$ et $s_{0,4} := \phi_\xi(s_{0,3})$. On trouve

$$\begin{aligned} s_{0,2} &= t^4 + t^{19} + t^{80} + t^{319} + t^{1279} + t^{5119} + t^{20479} + \cdots \\ s_{0,3} &= t^{16} + t^{91} + t^{106} + t^{121} + t^{151} + t^{181} + t^{226} + \cdots \\ s_{0,4} &= t^{64} + t^{304} + t^{364} + t^{379} + t^{394} + \cdots . \end{aligned}$$

D'après le Lemme 4.3.10, on a, pour $i = 1, 2, 3$,

$$s_{0,i+1}^4 s_{0,i}^3 + s_{0,i+1} + s_{0,i}^3 = 0$$

et donc S_0 est une s.d.v. telle que $\nu_{S_0} = \nu_{\mathfrak{P}_0}$. Soit maintenant $\mathfrak{P}_\infty$ l'unique pôle commun à x_i pour $i = 1, 2, 3, 4$. Alors

$$S_\infty := S_0^{-1} = (s_{0,4}^{-1}, s_{0,3}^{-1}, s_{0,2}^{-1}, s_{0,1}^{-1})$$

est une s.d.v. telle que $\nu_{S_\infty} = \nu_{\mathfrak{P}_\infty}$. On a

$$\begin{aligned} s_{0,4}^{-1} &= t^{-64} + t^{176} + t^{236} + t^{251} + \cdots \\ s_{0,3}^{-1} &= t^{-16} + t^{59} + t^{74} + t^{89} + \cdots \\ s_{0,2}^{-1} &= t^{-4} + t^{11} + t^{26} + t^{41} + t^{56} + t^{86} + \cdots \\ s_{0,1}^{-1} &= t^{-1} \end{aligned}$$

Construisons maintenant les s.d.v. de l'ensemble $\mathcal{S}_3^4$. Il est nécessaire d'abord de déterminer les s.d.v. de $\mathcal{S}_1^2$. D'après le Corollaire 4.3.12, il en existe exactement $q - 1 = 3$, disons S_1, S_2 et S_3, construites au début de la démonstration du Corollaire 4.3.12 ; on a $S_i = (t, s_i)$ où pour $i = 1, 2, 3$,

$$\begin{aligned} s_1 &= t^{-1} + t^4 + t^{19} + t^{79} + \cdots \\ s_2 &= \alpha^5 t^{-1} + t^4 + t^{19} + t^{79} + \cdots \\ s_3 &= \alpha^{10} t^{-1} + t^4 + t^{19} + t^{79} + \cdots , \end{aligned}$$

où $\alpha \in \overline{K}$ est tel que $\alpha^4 + \alpha + 1 = 0$. En appliquant le Lemme 4.3.10 à chacune des s.d.v. de $\mathcal{S}_1^2$, on trouve $\mathcal{S}_2^3 = \{ S_1', S_2', S_3' \}$ où pour $i = 1, 2, 3$,

$$S_i' = (t, \xi, \phi_\xi(s_i))$$

et

$$\begin{aligned} \phi_\xi(s_1) &= t^{-4} + t^{11} + t^{16} + t^{26} + \cdots \\ \phi_\xi(s_2) &= \alpha^5 t^{-4} + \alpha^5 t^{11} + t^{16} + \alpha^5 t^{26} + \cdots \\ \phi_\xi(s_3) &= \alpha^{10} t^{-4} + \alpha^{10} t^{11} + t^{16} + \alpha^{10} t^{26} + \cdots \end{aligned}$$

En appliquant le Lemme 4.3.10 aux s.d.v. de $\mathcal{S}_2^3$, on trouve $\mathcal{S}_3^4 = \{ S''_1, S''_2, S''_3 \}$ où

$$S''_i = (t, \xi, \phi_\xi(\xi), \phi_\xi(\phi_\xi(s_i))),$$

$$\phi_\xi(\xi) = t^{16} + t^{91} + t^{106} + t^{121} + t^{151} + t^{181} + t^{226} + \cdots$$

et

$$\begin{aligned}
\phi_\xi(\phi_\xi(s_1)) &= t^{-16} + t^{59} + t^{64} + t^{74} + \cdots, \\
\phi_\xi(\phi_\xi(s_2)) &= \alpha^5 t^{-16} + \alpha^5 t^{59} + t^{64} + \alpha^5 t^{74} + \cdots, \\
\phi_\xi(\phi_\xi(s_3)) &= \alpha^{10} t^{-16} + \alpha^{10} t^{59} + t^{64} + \alpha^{10} t^{74} + \cdots.
\end{aligned}$$

Les s.d.v. de $\mathcal{IS}_3^4$ sont exactement ${S''}_1^{-1}, {S''}_2^{-1}, {S''}_3^{-1}$. On a, pour $i = 1, 2, 3$,

$${S''}_i^{-1} := (\phi_\xi(\phi_\xi(s_i))^{-1}, \phi_\xi(\xi)^{-1}, \xi^{-1}, t^{-1})$$

où

$$\begin{aligned}
\phi_\xi(\phi_\xi(s_1))^{-1} &= t^{16} + t^{91} + t^{96} + t^{106} + t^{121} + \cdots, \\
\phi_\xi(\phi_\xi(s_2))^{-1} &= \alpha^{10} t^{16} + \alpha^{10} t^{91} + \alpha^5 t^{96} + \alpha^{10} t^{106} + \cdots, \\
\phi_\xi(\phi_\xi(s_3))^{-1} &= \alpha^5 t^{16} + \alpha^5 t^{91} + \alpha^{10} t^{96} + \alpha^5 t^{106} + \cdots
\end{aligned}$$

et

$$\begin{aligned}
\phi_\xi(\xi)^{-1} &= t^{-16} + t^{59} + t^{74} + t^{89} + t^{119} + \cdots, \\
\xi^{-1} &= t^{-4} + t^{11} + t^{26} + t^{41} + t^{56} + \cdots.
\end{aligned}$$

Les s.d.v. de $\mathcal{S}_1^4$ sont obtenues à partir des s.d.v. de $\mathcal{S}_2^3$ en appliquant la Proposition 4.3.9. Par exemple, la s.d.v. $S'_1 = (s'_1, s'_2, s'_3) \in \mathcal{S}_2^3$ permet de calculer 4 s.d.v. (s'_1, s'_2, s'_3, u_i) où

$$\begin{aligned}
u_1 &= t^{-1} + \alpha^1 t^1 + \alpha^4 t^{19} + \alpha^1 t^{24} \cdots \\
u_2 &= t^{-1} + \alpha^2 t^2 + \alpha^8 t^{19} + \alpha^2 t^{24} \cdots \\
u_3 &= t^{-1} + \alpha^4 t^4 + \alpha^1 t^{19} + \alpha^4 t^{24} \cdots \\
u_4 &= t^{-1} + \alpha^8 t^8 + \alpha^2 t^{19} + \alpha^8 t^{24} \cdots.
\end{aligned}$$

Au total, $\mathcal{IS}_1^4$ possède 12 séquences de valuation.

Calculons maintenant une base de $\mathcal{L}(521\mathfrak{P}_\infty)$. On a évidement $1 \in \mathcal{L}(521\mathfrak{P}_\infty)$. Notons respectivement par $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ et $\mathfrak{P}'_1, \mathfrak{P}'_2, \mathfrak{P}'_3$ les places correspondant aux s.d.v. de $\mathcal{S}_3^4$ et $\mathcal{IS}_3^4$ et par $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_{12}$ les places correspondant aux s.d.v. de $\mathcal{S}_1^4$. Soit l'ensemble de places

$$\mathcal{V} := \{ \mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}'_1, \mathfrak{P}'_2, \mathfrak{P}'_3, \mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_{12} \}.$$

On a

$$\mathbb{P}_4^{\infty} = \{\, \mathfrak{P} \in \mathbb{P}_{\overline{F}_4} \mid \overline{K}[x_1, x_2, x_3, x_4] \not\subset \mathcal{O}_{\mathfrak{P}} \,\} = \mathcal{V} \cup \{\, \mathfrak{P}_\infty \,\}.$$

D'après la Proposition 4.2.3, on a

$$\mathcal{L}(521\mathfrak{P}_\infty) \subset \overline{K}[x_1, x_2, x_3, x_4].$$

Par conséquent, si $u \in \overline{K}[x_1, x_2, x_3, x_4]$, alors

$$u \in \mathcal{L}(521\mathfrak{P}_\infty) \iff \nu_{\mathfrak{P}_\infty}(u) \geq -521 \text{ et } \nu_{\mathfrak{P}}(u) \geq 0 \text{ pour tout } \mathfrak{P} \in \mathcal{V}.$$

On peut trouver facilement tous les monômes $x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}$ appartenant à $\mathcal{L}(521\mathfrak{P}_\infty)$. En effet, considérons le tableau suivant donnant les valuations de x_1, x_2, x_3, x_4 pour chacune des places de $\mathcal{V}$:

	$\mathfrak{P}_\infty$	$\mathfrak{P}_1$	$\mathfrak{P}_2$	$\mathfrak{P}_3$	$\mathfrak{P}'_1$	$\mathfrak{P}'_2$	$\mathfrak{P}'_3$	$\mathfrak{Q}_1$	$\mathfrak{Q}_2$	$\cdots$	$\mathfrak{Q}_{12}$
x_1	-64	1	1	1	16	16	16	1	1	$\cdots$	1
x_2	-16	4	4	4	-16	-16	-16	4	4	$\cdots$	4
x_3	-4	16	16	16	-4	-4	-4	-4	-4	$\cdots$	-4
x_4	-1	-16	-16	-16	-1	-1	-1	-1	-1	$\cdots$	-1

Alors

$$x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} \in \mathcal{L}(521\mathfrak{P}_\infty) \iff \left\{ \begin{array}{rcrcrcrcr} -64i_1 & + & -16i_2 & + & -4i_3 & + & -i_1 & \geq & -521 \\ i_1 & + & 4i_2 & + & 16i_3 & + & -16i_1 & \geq & 0 \\ 16i_1 & + & -16i_2 & + & -4i_3 & + & -i_1 & \geq & 0 \\ i_1 & + & 4i_2 & + & -4i_3 & + & -i_1 & \geq & 0 \end{array} \right.$$

Quel que soit $n \in \mathbb{Z}$, il n'existe qu'un nombre fini de monômes $x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}$ tels que $\nu_{\mathfrak{P}_\infty}(x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}) = n$. En parcourant tous les monômes tels que $\nu_{\mathfrak{P}_\infty}(x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}) = n$ pour $-521 \leq n \leq -1$, on trouve exactement 217 monômes appartenant à $\mathcal{L}(521\mathfrak{P}_\infty)$. D'après le Théorème 1.5.4, on a

$$\ell\,(521\mathfrak{P}_\infty) = 521 - 261 + 1 = 261.$$

Ainsi, les 217 monômes trouvés ne suffisent pas à déterminer une base de $\mathcal{L}(521\mathfrak{P}_\infty)$. De plus, ces 217 monômes ne sont pas linéairement indépendants. Soit V l'espace vectoriel engendré par ces 217 monômes. En appliquant le Corollaire 4.4.13 à ces 217 monômes, on calcule une base de V et on en déduit que $\dim_{\overline{K}} V = 175$. Observons aussi que parmi ces 217 monômes il y en a 175, disons $M_1, M_2, \ldots, M_{175}$, tels que

$$\nu_{\mathfrak{P}_\infty}(M_1) > \nu_{\mathfrak{P}_\infty}(M_2) > \cdots > \nu_{\mathfrak{P}_\infty}(M_{175}) \geq -521 \tag{4.11}$$

et il est clair alors

$$B_1 := \{ M_1, M_2, \ldots, M_{175} \}$$

est une base du sous-espace vectoriel $V \subset \mathcal{L}(521\mathfrak{P}_\infty)$. On en déduit aussi que toute base de $\mathcal{L}(D)$ ne peut avoir plus de 175 éléments qui sont des monômes de $\overline{K}[x_1, x_2, x_3, x_4]$.

Puisque $1 \in \mathcal{L}(521\mathfrak{P}_\infty)$, on doit trouver $261-175-1 = 85$ fonctions pour compléter la base B_1 en une base de $\mathcal{L}(521\mathfrak{P}_\infty)$. Les 85 fonctions manquantes (voir Table 4.2 page 157) ont été trouvées en considérant l'espace vectoriel $W \subset \overline{K}[x_1, x_2, x_3, x_4] \subset \overline{F}_4$ engendré par l'ensemble

$$M := \left\{ x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4} \;\middle|\; 1 \leq i_1 + i_2 + i_3 + i_4 \leq 15 \right\}.$$

Observons qu'il existe 4845 monômes à 4 variables de degré ≤ 15. Or il est clair que $\dim_{\overline{K}} W < 4845$. Par des calculs de base de Groebner on peut déduire une base $B' := \{ H_1, H_2, \ldots, H_l \} \subset M$ qui engendre l'espace vectoriel W : de ces calculs on a déduit que $l := \dim_{\overline{K}} W = 1887$. En appliquant le Corollaire 4.4.13 avec les monômes $H_1, H_2, \ldots, H_{1887}$, on obtient une base de l'espace vectoriel

$$W' := W \cap \mathcal{L}(521\mathfrak{P}_\infty)$$

et on en déduit que $\dim_{\overline{K}} W' = 259$. Puisque $W' \subset \mathcal{L}(521\mathfrak{P}_\infty)$ et que $\ell\,(521\mathfrak{P}_\infty) = 261$, il ne manque que deux éléments à la base de W' pour qu'elle soit une base de $\mathcal{L}(521\mathfrak{P}_\infty)$. En fait, on a $1 \in \mathcal{L}(521\mathfrak{P}_\infty) \setminus W$ et on peut montrer que $x_1^7 x_2^3 x_3^3 x_4^3 \in B_1$ est tel que

$$x_1^7 x_2^3 x_3^3 x_4^3 \in \mathcal{L}(521\mathfrak{P}_\infty) \setminus W.$$

Par conséquent, W' possède bien les 85 fonctions manquantes, disons $f_1, f_2, \ldots, f_{85}$. Ces fonctions sont données dans les Tables 4.2, 4.3 et 4.4. En ajoutant ces fonctions à la base B_1, on obtient

$$B := \{ 1, M_1, M_2, \ldots, M_{175}, f_1, f_2, \ldots, f_{85} \}$$

qui est une base de $\mathcal{L}(521\mathfrak{P}_\infty)$. De plus, on peut choisir les fonctions f_i de sorte que $f_i \in K[x_1, x_2, x_3, x_4]$ pour $i = 1, 2, \ldots, 85$. D'après le Théorème 2.8.7, B est une base de

$$\mathcal{L}(521\mathfrak{P}'_\infty) \subset K(x_1, x_2, x_3, x_4)$$

où

$$\mathfrak{P}'_\infty := \mathfrak{P}_\infty \cap F_4.$$

Déterminons l'ensemble de toutes les places de degré 1 de F_4. On considère d'abord les places correspondant aux points simples de la courbe affine lisse $\mathcal{C}_4 \subset \mathbb{A}^4$

comme définie au Corollaire 4.2.2. Soient $Q \in \mathcal{C}_4$ et $\mathfrak{Q} \in \mathbb{P}_{\overline{F}_4}$ tels que $\mathfrak{Q} \equiv Q$ et posons $\mathfrak{P} = \mathfrak{Q} \cap F_4$. Alors $\deg \mathfrak{P} = 1$ si et seulement si Q est rationnel sur K. Observons que si $Q := (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathcal{C}_4$ est tel que $\alpha_1 \in K \setminus \{0\}$, alors $\alpha_i \in K \setminus \{0\}$ pour $i = 1, 2, 3$: en effet, considérons

$$\beta := \alpha_1 \alpha_2.$$

Alors

$$\beta^4 + \beta = \alpha_1^5. \tag{4.12}$$

On a

$$\beta^{16} + \beta = (\beta^{16} + \beta^4) + (\beta^4 + \beta) = (\alpha_1^5)^4 + \alpha_1^5 = \alpha_1^5 + \alpha_1^5 = 0$$

d'où $\beta \in K$. Par conséquent,

$$\alpha_2 = \beta_1 \alpha_1^{-1} \in K \setminus \{0\}.$$

De plus, puisque $\alpha_1 \neq 0$, on déduit de (4.12) que $\beta \neq 0$ et donc $\alpha_2 \neq 0$. De la même façon, on montre que $\alpha_i \in K \setminus \{0\}$ pour $i = 3, 4$. D'autre part, si $\mathfrak{Q}$ est une place de $\overline{F}_4$ telle que $\mathfrak{Q} \equiv Q = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ et $\alpha_1 \neq 0$, alors il est clair que $\nu_{\mathfrak{Q}}(x_1) = \nu_{\mathfrak{P}}(x_1) = 0$. Par conséquent, l'ensemble de toutes les places $\mathfrak{P} \in \mathbb{P}_{F_4}$ de degré 1 telles que $\nu_{\mathfrak{P}}(x_1) = 0$ est exactement l'ensemble

$$\mathcal{W} := \{ \mathfrak{Q} \cap F_4 \mid \mathfrak{Q} \equiv Q \in \mathcal{C}_4(K) \setminus \{ (0,0,0,0) \} \}$$

et on montre aisément que

$$\#\mathcal{W} = (4^2 - 1)4^3 = 960.$$

Il nous reste maintenant à dénombrer toutes les places $\mathfrak{P}$ de F_4 de degré 1 telles que $\nu_{\mathfrak{P}}(x_1) \neq 0$. Les places $\mathfrak{P}'_\infty$ et $\mathfrak{P}'_0 := \mathfrak{P}_0 \cap F_4$ sont toutes deux de degré 1. On observera que pour tout $S \in \mathcal{S} := \mathcal{S}_1^4 \cup \mathcal{S}_3^4 \cup \mathcal{IS}_3^4$, on a $S \in K((t))$. De plus, chacune des s.d.v. a été construite en fonction d'un paramètre local appartenant à F_4. On en déduit donc que si $\mathcal{V}$ est l'ensemble des places correspondant aux s.d.v. de $\mathcal{S}$, alors chacune des places de l'ensemble

$$\mathcal{V}' := \{ \mathfrak{Q} \cap F_4 \mid \mathfrak{Q} \in \mathcal{V} \}$$

est une place de degré 1. On déduira des Corollaires 4.4.9 et 4.4.12 que

$$\{ \mathfrak{P}' \in \mathbb{P}_{F_4} \mid \nu_{\mathfrak{P}'}(x_1) \neq 0 \} = \{ \mathfrak{P}'_0, \mathfrak{P}'_\infty \} \cup \mathcal{V}'.$$

Ainsi,

$$\mathcal{Q} := \mathcal{W} \cup \{ \mathfrak{P}'_0, \mathfrak{P}'_\infty \} \cup \mathcal{V}'$$

est exactement l'ensemble de toutes les places[5] de degré 1 de F_4 et

$$\#\mathcal{Q} = 960 + 2 + \#\mathcal{S}_1^4 + \#\mathcal{S}_3^4 + \#\mathcal{IS}_3^4 = 960 + 2 + 12 + 3 + 3 = 980$$

Si

$$\mathcal{P} := \sum_{\mathfrak{P} \in \mathcal{Q} \setminus \{ \mathfrak{P}'_\infty \}} \mathfrak{P}$$

et

$$D := 521\mathfrak{P}'_\infty,$$

alors le code géométrique $C_{\mathcal{L}}(F_4, \mathcal{P}, \mathcal{D})$ est un $(979, 261, d)$-code où $d \geq 979 - 521 = 458$.

Observons qu'il est facile de construire la matrice génératrice du code $C_{\mathcal{L}}(F_4, \mathcal{P}, \mathcal{D})$. Soit $B := \{ 1, M_1, M_2, \ldots, M_{175}, f_1, f_2, \ldots, f_{85} \}$ la base de $\mathcal{L}(D)$. Il faut évaluer toutes les fonctions de B en chacune des 979 places de $\mathcal{Q}$. Soient $g \in B$ et $G \in K[X_1, X_2, X_3, X_4]$ tels que $g = G(x_1, x_2, x_3, x_4)$. Il est clair que si $\mathfrak{P} \in \mathcal{Q}$ correspond à un point simple de $P \in \mathcal{C}_4$, alors $g(\mathfrak{P}) = G(P)$. De même, pour la place $\mathfrak{P}'_0$ qui est l'unique zéro commun de x_1, x_2, x_3 et x_4, on a

$$g(\mathfrak{P}'_0) = G(x_1(\mathfrak{P}'_0), x_2(\mathfrak{P}'_0), x_3(\mathfrak{P}'_0), x_4(\mathfrak{P}'_0)) = G(0,0,0,0).$$

Soient maintenant $\mathfrak{P}' \in \mathcal{V}'$ et $\mathfrak{P} \in \mathcal{V}$ l'unique place de $\overline{F}_4$ dominant la place $\mathfrak{P}'$. Alors $g(\mathfrak{P}') = g(\mathfrak{P})$. Pour évaluer $g(\mathfrak{P})$, il suffit d'utiliser $S \in \mathcal{S}$ telle que $\nu_S = \nu_{\mathfrak{P}}$ car $g(\mathfrak{P})$ est égal au terme constant de la série $G[S]$.

5. Soulignons que dans [11] on donne une formule exacte pour le nombre de places du corps de fonctions $\overline{F}_n$ pour tout n.

−64	1 0 0 0	−300	4 2 3 0	−368	5 3 0 0	−409	6 1 2 1	−456	6 4 2 0	−493	7 2 3 1
−80	1 1 0 0	−304	4 3 0 0	−369	5 3 0 1	−410	6 1 2 2	−457	6 4 2 1	−494	7 2 3 2
−128	2 0 0 0	−305	4 3 0 1	−372	5 3 1 0	−416	6 2 0 0	−458	6 4 2 2	−495	7 2 3 3
−144	2 1 0 0	−308	4 3 1 0	−373	5 3 1 1	−420	6 2 1 0	−459	6 4 2 3	−496	7 3 0 0
−148	2 1 1 0	−309	4 3 1 1	−374	5 3 1 2	−421	6 2 1 1	−460	6 4 3 0	−497	7 3 0 1
−149	2 1 1 1	−310	4 3 1 2	−376	5 3 2 0	−424	6 2 2 0	−461	6 4 3 1	−500	7 3 1 0
−160	2 2 0 0	−312	4 3 2 0	−377	5 3 2 1	−425	6 2 2 1	−462	6 4 3 2	−501	7 3 1 1
−192	3 0 0 0	−313	4 3 2 1	−378	5 3 2 2	−426	6 2 2 2	−463	6 4 3 3	−502	7 3 1 2
−208	3 1 0 0	−314	4 3 2 2	−379	5 3 2 3	−428	6 2 3 0	−464	6 4 3 4	−504	7 3 2 0
−212	3 1 1 0	−315	4 3 2 3	−380	5 3 3 0	−429	6 2 3 1	−465	6 4 4 1	−505	7 3 2 1
−213	3 1 1 1	−316	4 3 3 0	−381	5 3 3 1	−430	6 2 3 2	−466	6 4 4 2	−506	7 3 2 2
−224	3 2 0 0	−317	4 3 3 1	−382	5 3 3 2	−432	6 3 0 0	−467	6 4 4 3	−507	7 3 2 3
−228	3 2 1 0	−318	4 3 3 2	−383	5 3 3 3	−433	6 3 0 1	−468	6 4 4 4	−508	7 3 3 0
−229	3 2 1 1	−319	4 3 3 3	−384	5 3 3 4	−436	6 3 1 0	−469	6 4 4 5	−509	7 3 3 1
−232	3 2 2 0	−320	4 3 3 4	−385	5 3 4 1	−437	6 3 1 1	−470	6 4 5 2	−510	7 3 3 2
−233	3 2 2 1	−324	5 0 1 0	−388	5 4 1 0	−438	6 3 1 2	−472	6 5 2 0	−511	7 3 3 3
−234	3 2 2 2	−325	5 0 1 1	−389	5 4 1 1	−440	6 3 2 0	−473	6 5 2 1	−512	7 3 3 4
−240	3 3 0 0	−336	5 1 0 0	−390	5 4 1 2	−441	6 3 2 1	−474	6 5 2 2	−513	7 3 4 1
−256	4 0 0 0	−340	5 1 1 0	−392	5 4 2 0	−442	6 3 2 2	−475	6 5 2 3	−514	7 3 4 2
−260	4 0 1 0	−341	5 1 1 1	−393	5 4 2 1	−443	6 3 2 3	−476	6 5 3 0	−515	7 3 4 3
−272	4 1 0 0	−344	5 1 2 0	−394	5 4 2 2	−444	6 3 3 0	−477	6 5 3 1	−516	7 4 1 0
−276	4 1 1 0	−345	5 1 2 1	−395	5 4 2 3	−445	6 3 3 1	−478	6 5 3 2	−517	7 4 1 1
−277	4 1 1 1	−352	5 2 0 0	−396	5 4 3 0	−446	6 3 3 2	−479	6 5 3 3	−518	7 4 1 2
−280	4 1 2 0	−356	5 2 1 0	−397	5 4 3 1	−447	6 3 3 3	−480	6 5 3 4	−520	7 4 2 0
−288	4 2 0 0	−357	5 2 1 1	−398	5 4 3 2	−448	6 3 3 4	−484	7 2 1 0	−521	7 4 2 1
−292	4 2 1 0	−360	5 2 2 0	−399	5 4 3 3	−449	6 3 4 1	−485	7 2 1 1		
−293	4 2 1 1	−361	5 2 2 1	−400	5 4 3 4	−450	6 3 4 2	−488	7 2 2 0		
−296	4 2 2 0	−362	5 2 2 2	−404	6 1 1 0	−452	6 4 1 0	−489	7 2 2 1		
−297	4 2 2 1	−364	5 2 3 0	−405	6 1 1 1	−453	6 4 1 1	−490	7 2 2 2		
−298	4 2 2 2	−365	5 2 3 1	−408	6 1 2 0	−454	6 4 1 2	−492	7 2 3 0		

TAB. 4.1 – *Table de tous les monômes* $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4} \in \mathcal{L}(521\mathfrak{P}_\infty)$ *en fonction de la valuation* $\nu_{\mathfrak{P}_\infty}(x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4})$. *Par exemple, à l'entier* -149 *correspond le quadruplet* 2 1 1 1 *signifiant que* $x_1^2x_2x_3x_4 \in \mathcal{L}(521\mathfrak{P}_\infty)$ *et* $\nu_{\mathfrak{P}_\infty}(x_1^2x_2x_3x_4) = -149$.

−138	0 2 4 0 2 0 2 2 0 3 0 0
−164	3 1 4 0 3 2 0 0 1 0 2 2
−197	2 1 2 0 3 0 1 1
−202	1 2 4 0 3 0 2 2 1 3 0 0
−218	3 1 2 2 1 0 1 0
−222	3 1 3 2 1 0 2 0
−223	3 1 3 3 1 0 2 1
−237	3 2 3 1 2 0 1 0
−238	3 2 3 2 2 0 1 1
−244	3 3 1 0 2 1 2 2 0 0 1 0
−245	4 0 0 4 3 0 1 4 4 0 1 0 0 1 0 4 0 1 1 0 0 0 1 1
−248	3 3 2 0 2 1 3 2 0 0 2 0
−249	2 1 3 3 4 0 1 4 3 0 2 4 4 0 2 0 3 0 3 0 0 1 1 4 0 1 2 0 0 0 2 1
−250	4 0 1 5 3 0 2 5 2 1 4 0 4 0 2 1 3 0 3 1 0 1 1 5 0 1 2 1 0 0 2 2
−255	4 0 2 6 1 2 6 0 2 1 5 1 4 0 3 2 3 0 4 2 0 1 2 6 1 3 2 0 2 2 1 1 0 1 3 2 3 0 0 3 0 0 3 3
−261	3 1 2 0 4 0 1 1
−264	4 0 2 0 1 0 1 1
−265	3 1 3 0 4 0 2 1
−266	2 2 4 0 4 0 2 2 2 3 0 0
−270	2 2 5 0 4 0 3 2 2 3 1 0
−271	2 2 5 1 3 1 4 2 4 0 3 3 2 3 1 1 1 0 3 0
−274	2 2 6 0 3 1 5 1 2 3 2 0 4 1 0 2 3 1 1 2 0 1 4 2 1 0 3 3 0 2 0 2
−275	2 2 6 1 3 1 5 2 2 3 2 1 4 1 0 3 3 1 1 3 0 1 4 3 1 0 4 0 0 2 0 3
−281	3 2 3 0 4 1 2 1
−282	4 1 2 2 2 0 1 0
−284	3 2 3 3 4 1 3 0
−285	3 2 4 0 4 1 3 1
−286	4 1 3 2 2 0 2 0
−287	4 1 3 3 2 0 2 1
−290	4 2 0 2 3 2 1 2 0 2 4 2 2 0 3 0 0 3 0 2
−295	3 2 6 2 4 2 1 3 3 2 2 3 0 2 5 3 2 1 4 0 1 1 5 0 2 0 4 1 0 3 1 3 1 2 1 0 0 0 2 2

TAB. 4.2 – *Table des fonctions de* $\mathcal{L}(521\mathfrak{P}_\infty)$ *en fonction de leur valuation en la place* $\mathfrak{P}_\infty$. *Par exemple, à l'entier* -197 *correspond les deux quadruplets* 2 1 2 0 3 0 1 1 *représentant la fonction* $x_1^2x_2x_3^2 + x_1^3x_3x_4 \in \mathcal{L}(521\mathfrak{P}_\infty)$ *qui est d'ordre* -197 *en la place* $\mathfrak{P}_\infty$.

−301	4 2 3 1 3 0 1 0
−302	4 2 3 2 2 1 2 0
−303	4 2 3 3 2 1 2 1
−306	4 3 0 2 4 0 0 5 3 0 1 5 2 1 3 0 4 0 1 1 3 0 2 1 0 1 0 5 0 1 1 1 0 0 1 2
−307	4 3 0 3 4 0 0 6 3 0 1 6 2 1 3 1 4 0 1 2 3 0 2 2 0 1 0 6 0 1 1 2 0 0 1 3
−328	5 0 1 4 4 0 2 4 4 0 3 0 1 1 1 4 1 1 2 0 2 0 1 1
−329	3 2 3 3 5 0 2 1
−330	4 1 3 1 5 0 2 2
−334	3 2 5 0 5 0 3 2 2 1 2 2 0 0 1 0
−335	3 2 5 1 5 0 3 3 3 0 2 0 0 0 1 1
−338	3 2 6 0 0 2 5 1 5 1 0 2 4 1 1 2 2 1 3 2 1 1 4 2 2 0 3 3 0 3 1 1 1 2 0 2 0 0 2 0
−339	3 2 6 1 4 2 1 2 0 2 5 2 5 1 0 3 4 1 1 3 2 1 3 3 1 1 4 3 2 0 4 0 0 3 1 2 1 2 0 3 0 0 2 1
−346	5 1 2 2 3 0 1 0
−348	5 1 3 0 2 1 2 1
−349	5 1 3 1 2 1 2 2
−350	5 1 3 2 3 0 2 0
−351	5 1 3 3 3 0 2 1
−354	5 2 0 2 4 2 1 2 1 2 4 2 3 0 3 0 1 3 0 2
−355	3 2 6 2 5 2 0 3 3 2 2 3 1 2 4 3 0 2 5 3 2 1 4 0 1 1 5 0 3 0 3 1 2 0 4 1 1 3 0 3 0 3 1 3 1 2 1 0 0 0 2 2
−359	5 2 1 3 4 2 2 3 1 2 5 3 4 0 2 5 2 1 5 0 4 0 3 1 3 0 4 1 1 3 1 3 0 1 2 5 2 2 1 0 0 1 3 1 3 0 0 2 0 0 3 2
−366	5 2 3 2 3 1 2 0
−367	5 2 3 3 3 1 2 1
−370	5 3 0 2 3 1 3 0 1 0 1 2
−371	5 3 0 3 5 0 0 6 4 0 1 6 3 1 3 1 5 0 1 2 4 0 2 2 1 1 0 6 1 1 1 2 1 0 1 3
−375	6 0 0 6 5 0 1 6 3 1 4 1 6 0 1 2 5 0 2 2 2 1 0 6 2 1 1 2 1 0 2 3
−386	3 2 3 0 6 0 0 2 5 0 1 2 2 1 0 2
−387	6 0 0 3 5 0 1 3 2 1 0 3 2 0 1 0

TAB. 4.3 – *Suite de la Table 4.2.*

−401	5006 3026 1250 6101 2141 5012 1106 0116 1310 2201 1112 0122 0023
−402	3330 1251 6102 5112 2142 3033 1311 2202 0030
−403	5212 1252 6103 5113 2143 4024 4030 3040 1312 2203 0124 0130 3001 0031
−412	6130 3121
−413	6131 1010
−414	6132 1011
−415	6133 3130
−418	6202 5212 2242 4030 2302
−419	6203 4223 2243 1253 4025 2150 3041 2303 1313 0125 2210 0131 3002 0032
−422	6212 2252 3143 2312 0140 1031 0200
−423	6213 5223 2253 3150 2313 4101 0141 1032 0201
−431	6233 3230
−434	6302 3233 2012
−435	6303 3240 3141 2013 1023
−439	7006 6016 7012 3106 4201 0241 3112 2122 2023 0301
−451	7003 6013 3103 3010
−455	7013 6023 3113 3020
−471	7113 6123 3213 3120
−481	7201 3241 6013 5023 3301 2113
−482	7202 3242 2252 3143 5024 3302 2312 1124 1130 0140 4001 1031 0200
−483	7203 5223 3243 2253 5025 3150 3303 2313 1125 4101 1131 0141 4002 1032 0201
−486	7212 3252 7113 6123 5133 4203 0243 4005 3015 1140 2031 0303 0105 1200 0111
−487	7213 6223 3253 4006 3016 0250 5101 1141 4012 3022 2032 0106 0310 1201 0112
−498	7302 2121 3012
−499	7303 4201 0241 2122 3013 2023 0301
−503	8006 8012 2126 5201 1241 2132 5003 4013 3023 0206 1301 0212 0113
−519	8013 4113 3123 1011

TAB. 4.4 – *Suite et fin de la Table 4.3.*

Conclusion

Deux méthodes de construction effective de codes géométriques ont été présentées. Toutes deux concernent le calcul d'une base de l'espace vectoriel associé à un diviseur d'un corps de fonctions. La première méthode utilise l'algorithme de Brill-Noether et est applicable à tout code géométrique défini à partir d'un corps de fonctions dont on connaît un modèle plan. La deuxième méthode de construction effective est particulière aux codes géométriques définis à partir des corps de fonctions d'une tour d'extensions du type d'Artin-Schreier obtenue par A. Garcia et H. Stichtenoth [11].

Les codes géométriques ont été présentés d'un point vue algébrique, c'est-à-dire du point de vue de la théorie des corps de fonctions algébriques à une variable. Toujours en utilisant un point vue algébrique et inspiré de l'article de H. Hironaka [22], l'algorithme de Brill-Noether a été entièrement décrit au Chapitre 2. L'étude détaillée de l'algorithme par une approche algébrique a permis de définir de façon évidente les algorithmes sous-jacents à l'algorithme de Brill-Noether (Chapitre 3).

Le choix d'utiliser l'algorithme de Brill-Noether est clairement justifié par le fait qu'on peut l'appliquer à toute courbe plane $\mathcal{C}$ pour une base de l'espace vectoriel $\mathcal{L}(D)$ quel que soit le diviseur D du corps des fonctions de la courbe. De plus, on a montré comment utiliser l'algorithme de Brill-Noether avec les extensions dynamiques de corps et on en a surtout déduit un résultat important : d'une part, les calculs se font toujours dans la plus petite extension possible et d'autre part, si n est le degré de la courbe et d est le degré d'un diviseur $D \geq 0$ pour lequel on veut calculer une base de $\mathcal{L}(D)$, le degré de toutes tours d'extensions dynamiques utilisées pour les calculs est borné par un même entier N qui est d'ordre $O(n^2 + d)$.

Il était tout à fait naturel de choisir le système de calcul formel Axiom pour réaliser le logiciel qui implante l'algorithme de Brill-Noether. En effet, bien que l'algorithme de Brill-Noether et ses algorithmes sous-jacents soient relativement simples, ils font intervenir plusieurs objets à la fois. Le caractère "orienté-objet" et générique d'Axiom permet de définir de façon formelle tous les objets utilisés et par suite de ne plus se soucier de l'implantation particulière des objets pour réaliser un algorithme. Ainsi, le logiciel qui réalise l'algorithme de Brill-Noether est utilisable avec tout corps pour lequel l'algorithme de Brill-Noether est défini (en l'occurence tous les corps parfaits). De plus, Axiom a permis de réaliser un logiciel facile à utiliser ; en ce sens, le logiciel n'est pas entièrement dédié à la construction de codes géométriques, il se veut aussi un outil d'aide à la recherche. Il fut utile par exemple pour déterminer la méthode de construction effective de codes géométriques sur les extensions du type d'Artin-Schreier proposée au Chapitre 4. Aussi, dans [34], le genre de certaines courbes a été calculé avec le logiciel.

Rappelons que l'objectif principal de ce travail de thèse était de réaliser un logiciel qui implante l'algorithme de Brill-Noether comme décrit par D. Le Brigand et J.J. Risler [28] et il est permis de croire qu'il a été atteint. De plus, il s'avère par la pratique que le logiciel a des performances très raisonnables grâce à une attention particulière quant à la programmation. Il faut dire qu'il y a eu une évolution constante du logiciel depuis la première version opérationnelle (realisée en 1993) et ce tant du point de vue de l'efficacité que du point de vue de la souplesse d'utilisation. Il est évident néanmoins qu'il y a place pour certaines améliorations et recherches en perspective. Par exemple, il serait utile de faire en sorte que soit le plus efficace possible :

1. la recherche des points singuliers et des points rationnels,

2. la résolution des systèmes d'équations linéaires.

Notons qu'un premier pas a été fait pour la recherche des points singuliers car une interface a été créée pour calculer les bases de Groebner avec le logiciel "GB" de J.C. Faugères. Aussi, il serait intéressant de considérer, pour le calcul des arbres de désingularisation et le calcul des séries $\mathfrak{P}$-adiques, les techniques d'évaluations paresseuses comme proposées par J.-P. Henry et M. Merle [21]. Il y a aussi un travail de recherche non négligeable qui consisterait à faire une étude approfondie de la complexité des calculs.

Au Chapitre 4, on a donné une méthode de construction effective d'une base de l'espace vectoriel $\mathcal{L}(D)$ associé à un diviseur D d'un corps de fonctions F_n/K d'une tour d'extensions

$$F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots$$

du type d'Artin-Schreier. On a montré en particulier qu'il existe des diviseurs D dont une base de $\mathcal{L}(D)$ est formée de polynômes et non de fractions rationnelles comme c'est le cas en général. La méthode de calcul d'une base de $\mathcal{L}(D)$ utilise ce fait et consiste à calculer pour certaines places $\mathfrak{P}$ et certaines fonctions f les séries

$\mathfrak{P}$-adiques de f. Il s'avère que le calcul de ces séries est très simple et efficace. Par contre, pour appliquer cette méthode, il faut déterminer espace vectoriel V tel que $V \supset \mathcal{L}(D)$ et de préférence tel que $\dim_K V - \ell(D)$ soit petit. Ce problème n'est toujours pas résolu et constituerait un travail de recherche intéressant.

Annexe A

Codes correcteurs d'erreurs

On rappelle ici de façon très sommaire quelques définitions et généralités sur les codes correcteurs d'erreurs. Pour plus de détails on se reportera à [29, 37].

Soit A un ensemble fini de q symboles appelé alphabet. Tout sous-ensemble $C \subseteq A^n$ $(n \in \mathbb{N})$ est un code de longueur n, dont les éléments $c \in C$ sont appelés mots du code C. L'ensemble A^n est muni d'une distance appelé distance de Hamming définie comme suit : pour

$$x = (x_1, \ldots, x_n) \in A^n \text{ et } y = (y_1, \ldots, y_n) \in A^n,$$

on a

$$d(x, y) = \#\, \{\, i \mid x_i \neq y_i, i = 1, 2, \ldots, n \,\} .$$

À un code C est associée sa distance minimale

$$d(C) = \min \{\, d(x, y) \mid x, y \in C,\ x \neq y \,\} .$$

Un code C de paramètre (n, M, d), ou simplement un (n, M, d)-code, est un code de longueur n, de cardinal $M := \#C$ et de distance minimale $d := d(C)$. Un code C est dit e-correcteur $(e \in \mathbb{N})$ si $d(C) \geq 2e + 1$.

Si A est le corps fini $\mathbb{F}_q$ et C un sous-espace vectoriel de $\mathbb{F}_q^n$, on dit du code C qu'il est un $[n, k, d]_q$-code linéaire où n désigne sa longueur, $k := \dim_{\mathbb{F}_q} C$ sa dimension et d sa distance minimale. Un code linéaire de longueur n sur $\mathbb{F}_q$ n'est ni plus ni moins qu'un sous-espace vectoriel de $\mathbb{F}_q^n$. À tout $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, on associe son poids

$$w(x) = \#\, \{\, i \mid x_i \neq 0 \,\} .$$

Par linéarité, on a

$$d(C) = \min \{\, w(x) \mid x \in C \setminus \{\, 0 \,\} \,\} .$$

Soit C un $[n,k,d]_q$-code linéaire. Une matrice génératrice du code C est une matrice $k \times n$ à coefficients dans $\mathbb{F}_q$,

$$G = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \cdots & \alpha_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k,1} & \alpha_{k,2} & \cdots & \alpha_{k,n} \end{bmatrix},$$

dont les lignes engendrent le code $C \subset \mathbb{F}_q^n$. De la sorte,

$$C = \left\{ uG \mid u = (u_1, u_2, \ldots, u_k) \in \mathbb{F}_q^k \right\}.$$

Une matrice de contrôle du code C est une matrice H de taille $(n-k)\times n$ à coefficients dans $\mathbb{F}_q$ telle que

$$x \in C \iff Hx^t = 0.$$

On peut définir alors un code linéaire, appelé le dual de C et noté $C^\perp$, donné par

$$C^\perp := \left\{ vH \mid v = (v_1, v_2, \ldots, v_{n-k}) \in \mathbb{F}_q^{n-k} \right\}.$$

Le code $C^\perp$ est un code de longueur n et de dimension $n-k$. En fait,

$$C^\perp = \left\{ (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} x_i y_i = 0 \text{ pour tout } (x_1, x_2, \ldots, x_n) \in C \right\}$$

et il est clair qu'une matrice génératrice G de C est une matrice de contrôle du code $C^\perp$.

Annexe B

Un peu de géométrie algébrique

Cette annexe contient un bref rappel de quelques notions de géométrie algébrique. On réfère à Silverman [41]. Dans toute cette annexe, K est un corps parfait, $\overline{K}$ une clôture algébrique de K et $\mathcal{G}(\overline{K}/K)$ le groupe de Galois de l'extension $\overline{K}/K$.

B.1 Espace affine

DÉFINITION B.1.1 *L'*espace affine *de dimension n sur $\overline{K}$, noté $\mathbb{A}^n$, est l'ensemble*

$$\mathbb{A}^n := \left\{ (a_1, a_2, \ldots, a_n) \mid a_i \in \overline{K} \right\}.$$

On appelle point affine *un élément $P \in \mathbb{A}^n$ et si $P = (a_1, a_2, \ldots, a_n)$ avec $a_i \in \overline{K}$, les éléments a_i sont appelés les* coordonnées *de P. Le point P est dit* rationnel *sur K si $a_i \in K$ pour $i = 1, 2, \ldots, n$. L'ensemble de tous les points de $\mathbb{A}^n$ rationnels sur K est noté $\mathbb{A}^n(K)$.*

Observons que le groupe de Galois $\mathcal{G}(\overline{K}/K)$ agit sur $\mathbb{A}^n$ comme suit :

$$\text{si } P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n \text{ et } \sigma \in \mathcal{G}(\overline{K}/K),$$

alors

$$P^\sigma := (a_1^\sigma, a_2^\sigma, \ldots, a_n^\sigma).$$

Il est clair alors que

$$\mathbb{A}^n(K) = \{ P \in \mathbb{A}^n \mid P^\sigma = P \}.$$

Soit $\overline{K}[\underline{X}] := \overline{K}[X_1, X_2, \ldots, X_n]$ l'anneau des polynômes à n variables. On considère un élément $G \in \overline{K}[\underline{X}]$ comme une fonction $G : \mathbb{A}^n \to \overline{K}$ définie par $G(P) := G(a_1, a_2, \ldots, a_n)$. Si $G(P) = 0$, on dit que P est un zéro de G. Plus généralement, à tout $T \subseteq \overline{K}[\underline{X}]$, on associe son ensemble des zéros

$$\mathcal{Z}(T) := \{ P \in \mathbb{A}^n \mid G(P) = 0 \text{ pour tout } G \in T \}.$$

Définition B.1.2 *Un ensemble $V \subseteq \mathbb{A}^n$ est un* ensemble algébrique *s'il existe $T \subseteq \overline{K}[\underline{X}]$ tel que $V = \mathcal{Z}(T)$.*

Définition B.1.3 *Soit $V \subseteq \mathbb{A}^n$ un ensemble algébrique. On appelle* idéal *de V l'ensemble*

$$\mathcal{I}(V) := \left\{ G \in \overline{K}[\underline{X}] \mid G(P) = 0 \text{ pour tout } P \in V \right\}.$$

On vérifie aisément que $\mathcal{I}(V)$ est effectivement un idéal de $\overline{K}[\underline{X}]$. Rappelons que l'anneau $\overline{K}[\underline{X}]$ est noethérien, c'est-à-dire que tout idéal propre de $\overline{K}[\underline{X}]$ est engendré par un nombre fini de polynômes de $\overline{K}[\underline{X}]$.

Lemme B.1.4 *Tout idéal maximal de $\overline{K}[\underline{X}]$ est de la forme*

$$\langle X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n \rangle$$

où $a_i \in \overline{K}$ pour $i = 1, 2, \ldots, n$. En conséquence, pour tout $P := (a_1, a_2, \ldots, a_n) \in \mathbb{A}^2$, le singleton $V_P := \{ P \}$ est un ensemble algébrique ayant pour idéal $I_P := \langle X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n \rangle$.

Démonstration : Malliavin [30, Chap. 11, Prop. 2.2].

Définition B.1.5 *Une* variété affine *V (ou simplement* variété *lorsque le contexte est clair) de $\mathbb{A}^n$ est un ensemble algébrique $V \subset \mathbb{A}^n$ dont l'idéal $\mathcal{I}(V)$ est premier. L'ensemble des points de V rationnels sur K est noté $V(K)$. On dit que la variété V est* définie *sur K, et on note alors V/K, si $\mathcal{I}(V)$ possède un ensemble de générateurs contenu dans $K[\underline{X}]$. Dans ce cas, on associe à la variété V/K l'idéal de $K[\underline{X}]$*

$$\mathcal{I}(V/K) := \mathcal{I}(V) \cap K[\underline{X}].$$

Soient V une variété et $\sigma \in \mathcal{G}(\overline{K}/K)$. Considérons l'idéal

$$\mathcal{I}(V)^\sigma := \{ G^\sigma \mid G \in \mathcal{I}(V) \}$$

où G^σ est défini en faisant agir σ sur les coefficients de G. Il est clair que

$$V \text{ est définie sur } K \iff \mathcal{I}(V) = \mathcal{I}(V)^\sigma \text{ pour tout } \sigma \in \mathcal{G}(\overline{K}/K).$$

On en déduit que

$$V \text{ est définie sur } K \iff V = V^\sigma := \{ P^\sigma \mid P \in V \} \text{ pour tout } \sigma \in \mathcal{G}(\overline{K}/K).$$

Définition B.1.6 *Soit V une variété affine. On appelle l'anneau quotient*

$$\overline{K}[V] := \overline{K}[\underline{X}]/\mathcal{I}(V)$$

*l'*anneau de coordonnées *de V. Si V est définie sur K, l'anneau quotient*

$$K[V] := K[\underline{X}]/\mathcal{I}(V/K)$$

*est appelé l'*anneau de coordonnées *de V/K.*

Remarque B.1.7 L'anneau de coordonnées d'une variété V peut être considéré comme un ensemble de fonctions à valeurs dans $\overline{K}$ définies en tout point de V : soient $g \in \overline{K}[V]$ et $G \in \overline{K}[\underline{X}]$ tel que $g = G + \mathcal{I}(V)$. On pose $g(P) := G(P)$. Cette définition est indépendante du choix du représentant G : si $G' \in \overline{K}[\underline{X}]$ est tel que $G' + \mathcal{I}(V) = G + \mathcal{I}(V)$, alors $G' - G \in \mathcal{I}(V)$. On a donc $0 = (G' - G)(P) = G'(P) - G(P)$ d'où $G'(P) = G(P)$.

Puisque l'idéal d'une variété est un idéal premier, l'anneau de coordonnées $\overline{K}[V]$ est intègre. On peut donc définir ce qui suit.

Définition B.1.8 *Soit V une variété affine. Le corps des fractions de $\overline{K}[V]$, noté $\overline{K}(V)$, est le* corps des fonctions *de V. Si V est définie sur K, on définit le* corps des fonctions *de V/K, noté $K(V)$, comme étant le corps des fractions de $K[V]$.*

Définition B.1.9 *Soient deux variétés $V \subseteq \mathbb{A}^m$ et $W \subseteq \mathbb{A}^n$. On dit que V est* birationnelle *à W si $\overline{K}(V)$ est $\overline{K}$-isomorphe à $\overline{K}(W)$.*

Remarque B.1.10 Soit V/K une variété. Il est clair que $K[V]$ et $K(V)$ se plongent naturellement dans $\overline{K}[V]$ et $\overline{K}(V)$ respectivement. On considérera donc $K[V]$ comme un sous-anneau de $\overline{K}[V]$ et $K(V)$ comme un sous-corps de $\overline{K}(V)$. Soit $\varphi \in \mathcal{G}(\overline{K}/K)$. Puisque $\mathcal{I}(V) = \mathcal{I}(V)^{\varphi}$, l'application

$$\begin{array}{rccc} \varphi^* : & \overline{K}[V] & \longrightarrow & \overline{K}[V] \\ & g = G + \mathcal{I}(V) & \mapsto & g^{\varphi^*} := G^{\varphi} + \mathcal{I}(V) \end{array}$$

est bien définie et c'est un K-isomorphisme d'anneaux. On peut alors prolonger φ^* à $\overline{K}(V)$ pour obtenir l'automorphisme

$$\begin{array}{rccc} \sigma : & \overline{K}(V) & \longrightarrow & \overline{K}(V) \\ & g/h & \mapsto & g^{\varphi^*}/h^{\varphi^*}. \end{array}$$

On vérifie aisément que

$$K[V] \;=\; \left\{ g \in \overline{K}[V] \mid g = g^{\varphi^*} \text{ pour tout } \varphi \in \mathcal{G}(\overline{K}/K) \right\}.$$

On en déduit que l'automorphisme σ laisse le corps $K(V)$ fixe.

B.2 Anneau local d'un point

Définition B.2.1 *Soient V une variété et $P \in V$. L'anneau*

$$\mathcal{O}_P(V) := \{ f/g \in \overline{K}(V) \mid f, g \in \overline{K}[V], g(P) \neq 0 \}.$$

est appelé l'anneau local du point *P. Soient $u \in \mathcal{O}_P(V)$ et $f, g \in \overline{K}[V]$ tels que $u = f/g$ et $g(P) \neq 0$. On appelle $u(P) := f(P)/g(P)$* l'évaluation *de u au point P (cf. Remarque B.1.7).*

Remarque B.2.2 Soit $u := f/g \in \mathcal{O}_P(V)$. Il est clair que la définition de $u(P)$ est indépendante du choix de f et g où g est tel que $g(P) \neq 0$; si $f', g' \in \overline{K}[V]$ sont tels que $u = f'/g'$ et $g'(P) \neq 0$, alors $f(P)/g(P) = f'(P)/g'(P)$ puisque $fg' = f'g$. On peut donc considérer $\mathcal{O}_P(V)$ comme l'ensemble de toutes les fonctions de $\overline{K}(V)$ définies au point P. D'autre part, soit I_P idéal maximal de l'ensemble algébrique $\{ P \}$. Alors $\mathcal{I}(V) \subseteq I_P$ et donc $M_P := I_P + \mathcal{I}(V) \subset \overline{K}[V]$ est un idéal maximal de $\overline{K}[V]$. Par suite, on a

$$\mathcal{O}_P(V) = \{ f/g \mid f, g \in \overline{K}[V], g \notin M_P \}.$$

L'anneau $\mathcal{O}_P(V)$ est donc le localisé de $\overline{K}[V]$ en l'idéal maximal M_P et a pour unique idéal maximal

$$\begin{aligned} \mathcal{M}_P(V) &:= \{ f/g \in \overline{K}(V) \mid f, g \in \overline{K}[V], f \in M_P, g \notin M_P \} \\ &= \{ f/g \in \overline{K}(V) \mid f, g \in \overline{K}[V], f(P) = 0, g(P) \neq 0 \}. \end{aligned}$$

La proposition suivante montre que l'ensemble des fonctions définies en tous les points de V est exactement l'anneau de coordonnées $\overline{K}[V]$.

Proposition B.2.3 *Soit V une variété affine. Alors*

$$\overline{K}[V] = \bigcap_{P \in V} \mathcal{O}_P(V).$$

Démonstration : C'est une conséquence du fait qu'un anneau intègre est égal à l'intersection des localisés en tous ses idéaux maximaux (voir Matsumura [31, Lemme 2, page 8])

B.3 Dimension d'une variété

Par définition, le corps des fonctions $\overline{K}(V)$ d'une variété V est une extension de type fini de $\overline{K}$, c'est-à-dire qu'il existe $x_1, x_2, \ldots, x_n \in \overline{K}(V)$ tels que $\overline{K}(V) = \overline{K}(x_1, x_2, \ldots, x_n)$. En particulier, le degré de transcendance de $\overline{K}(V)$ sur K est fini.

Définition B.3.1 *Soit V une variété. La* dimension *de V, notée* $\dim V$*, est le degré de transcendance de $\overline{K}(V)$ sur $\overline{K}$.*

Définition B.3.2 *Soit I un idéal premier d'un anneau A. La* hauteur *de l'idéal I, notée* $\mathrm{ht}\,(I)$*, est le maximum des longueurs des chaînes d'idéaux premiers*

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n = I.$$

La dimension *d'un anneau A est définie par*

$$\dim A := \sup \{\, \mathrm{ht}\,(I) \mid I \text{ un idéal premier de } A \,\}.$$

Théorème B.3.3 *Soit $V \subset \mathbb{A}^n$ une variété. Alors*

$$n - \mathrm{ht}\,(\mathcal{I}(V)) = \dim V.$$

De plus, pour tout $P \in V$, on a

$$\dim \mathcal{O}_P(V) = \dim V.$$

Démonstration : Atiyah-Macdonald [1, Théorème 11.25 et Corollaire 11.27].

Définition B.3.4 *Une* courbe affine *$\mathcal{C} \subset \mathbb{A}^n$ est une variété affine de dimension 1.*

Exemple B.3.5 Soit $C \in \overline{K}[X,Y]$ un polynôme irréductible et considérons la variété

$$\mathcal{C} := \{\, C = 0 \,\} = \left\{\, P \in \mathbb{A}^2 \mid C(P) = 0 \,\right\}.$$

Il est clair que le corps des fonctions $\overline{K}(\mathcal{C})$ a un degré de transcendance sur $\overline{K}$ égal à 1. La variété $\mathcal{C}$ est donc une courbe et puisque qu'elle est contenue dans le plan affine $\mathbb{A}^2$, on dit alors que $\mathcal{C}$ est une courbe affine plane.

Dans le cas des courbes affines, le Théorème B.3.3 a pour corollaire :

Corollaire B.3.6 *Soit P un point d'une courbe $\mathcal{C}$. Les seuls idéaux premiers propres de l'anneau local $\mathcal{O}_P(\mathcal{C})$ sont les idéaux $\{\, 0 \,\}$ et $\mathcal{M}_P$.*

B.4 Points non-singuliers d'une variété

Définition B.4.1 *Soient $V \subseteq \mathbb{A}^n$ une variété, $\{\, G_1, G_2, \ldots, G_s \,\}$ un ensemble de générateur de l'idéal $\mathcal{I}(V)$. Soit $P \in V$ et considérons la matrice $\mathcal{J}_{V,P} := ||a_{i,j}||$ où $a_{i,j} := (\partial G_i / \partial X_j)(P)$ pour $i = 1, 2, \ldots, s$ et $j = 1, 2, \ldots, n$. On dit que P est un point* non-singulier *(on dit aussi* simple*) si*

$$\mathrm{rang} \mathcal{J}_{V,P} = n - \dim V,$$

sinon le point P est dit singulier*. La variété V est* singulière *si elle possède au moins un point singulier, sinon elle est* lisse.

La matrice $\mathcal{J}_{V,P}$ est appelée matrice jacobienne au point $P \in V$. Il est aisé de montrer que le rang de la matrice $\mathcal{J}_{V,P}$ ne dépend pas du choix de l'ensemble des générateurs de l'idéal $\mathcal{J}_{V,P}$.

La définition suivante est équivalente à la définition précédente dans le cas des courbes affines planes.

DÉFINITION B.4.2 *Soit $\mathcal{C} := \{ C = 0 \}$ une courbe affine plane. Soient C_X et C_Y les dérivés usuelles de C par rapport à X et Y respectivement. Alors*

$$P = (a, b) \in \mathcal{C} \text{ est simple } \iff C_X(a, b) \neq 0 \text{ ou } C_Y(a, b) \neq 0.$$

DÉFINITION B.4.3 *Soit A un anneau local noethérien et $\mathcal{M}$ son unique idéal maximal. Soit le corps résiduel $K := A/\mathcal{M}$. On dit que l'anneau A est* régulier *si*

$$\dim_K \mathcal{M}/\mathcal{M}^2 = \dim A.$$

Le théorème suivant montre que les points non-singuliers d'une variété sont exactement ceux dont l'anneau local est un anneau local régulier.

THÉORÈME B.4.4 *Soient V une variété et $P \in V$. Alors*

$$P \text{ est non-singulier} \iff \mathcal{O}_P(V) \text{ est régulier.}$$

Démonstration : Hartshorne [20, Chap.1 Th. 5.1].

La caractérisation la plus remarquable d'un point simple d'une courbe est la suivante.

PROPOSITION B.4.5 *Soient $\mathcal{C}$ une courbe et $P \in \mathcal{C}$. Le point P est simple si et seulement si $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète.*

Démonstration : On peut montrer que $\mathcal{O}_P(\mathcal{C})$ est un anneau de valuation discrète si et seulement si $\dim_{\overline{K}} \mathcal{M}_P(\mathcal{C})/\mathcal{M}_P^2(\mathcal{C}) = 1$ (cf. [1, Prop. 9.2]). La proposition est alors une conséquence des Théorèmes B.3.3 et B.4.4. □

B.5 Courbes projectives planes

Le plan projectif sur $\overline{K}$, noté $\mathbb{P}^2$, est l'ensemble quotient

$$\mathbb{P}^2 := \mathbb{A}^3 \setminus \{ (0, 0, 0) \}/\equiv$$

où pour deux points $P = (a_0, a_1, a_2)$ et $Q = (b_0, b_1, b_2)$ la relation d'équivalence $\equiv$ est donnée par

$$P \equiv Q \iff \text{il existe } 0 \neq \lambda \in \overline{K} \text{ tel que } a_i = \lambda b_i \text{ pour } i = 0, 1, 2.$$

Un élément $P \in \mathbb{P}^2$ est appelé point et tout point $(a_0, a_1, a_2) \in \mathbb{A}^3$ dans la classe d'équivalence de P est appelé ensemble de coordonnées homogènes. Il est d'usage d'écrire

$$P = (a_0 : a_1 : a_2).$$

On dit d'un point $P = (a_0 : a_1 : a_2)$ qu'il est à l'infini si $a_2 = 0$. Si $V \subset \mathbb{P}^2$, on note V_∞ l'ensemble $V_\infty := \{ (a_0 : a_1 : a_2) \in V \mid a_2 = 0 \}$. Pour $i = 0, 1, 2$, posons

$$U_i := \left\{ (a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid a_i \neq 0 \right\}.$$

On appelle les ensembles U_i les ouverts standards de $\mathbb{P}^2$ (au sens de la topologie de Zariski, les ensembles U_i sont des ouverts de $\mathbb{P}^2$). Pour $i = 0, 1, 2$, on a les applications bijectives

$$\begin{array}{cccc} \pi_i : & \mathbb{A}^2 & \longrightarrow & U_i \\ & (a, b) & \mapsto & \begin{cases} (1 : a : b) & \text{si } i = 0, \\ (a : 1 : b) & \text{si } i = 1, \\ (a : b : 1) & \text{si } i = 2. \end{cases} \end{array}$$

Le plan $\mathbb{P}^2$ est recouvert par les ouverts U_0, U_1 et U_2. Chacun des U_i est canoniquement isomorphe à $\mathbb{A}^2$.

Au plan $\mathbb{P}^2$ on fait correspondre l'anneau de polynômes $S := \overline{K}[X_0, X_1, X_2]$. À la différence du plan affine, les éléments de S ne peuvent être considérés comme des fonctions définies sur $\mathbb{P}^2$ car tout point de $\mathbb{P}^2$ admet une infinité d'ensembles de coordonnées homogènes. Pour $d \in \mathbb{N}$, on pose

$$S_d := \{ G \in S \mid G \text{ est un polynôme homogène de degré } d \}.$$

Si $G \in S_d$, on dit que $P = (a_0 : a_1 : a_2) \in \mathbb{P}^n$ est un zéro de G, noté $G(P) = 0$, si $G(a_0, a_1, a_2) = 0$. Puisque G est homogène, cette définition ne dépend pas de l'ensemble de coordonnées de P car $G(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^d G(a_0, a_1, a_2)$ pour tout $\lambda \in \overline{K} \setminus \{ 0 \}$.

Définition B.5.1 *Une* courbe projective plane $\mathcal{C} \subset \mathbb{P}^2$ *est l'ensemble des zéros d'un polynôme homogène irréductible $C \in \overline{K}[X_0, X_1, X_2]$. Si $C \in K[X_0, X_1, X_2]$, on dit alors que la courbe $\mathcal{C}$ est* définie *sur K et on écrit $\mathcal{C}/K$ pour signifier cette propriété.*

Soit $C \in S$ un polynôme homogène irréductible. Il sera d'usage d'écrire $\mathcal{C} := \{ C = 0 \}$ pour désigner la courbe projective $\mathcal{C} := \{ P \in \mathbb{P}^2 \mid C(P) = 0 \}$. Soit l'idéal $\mathcal{I}(\mathcal{C}) := \langle C \rangle \subset S$. Puisque I est un idéal premier, l'anneau

$$\overline{K}[\mathcal{C}] := \overline{K}[X_0, X_1, X_2]/\mathcal{I}(\mathcal{C})$$

est intègre et est appelé anneau de coordonnées de la courbe $\mathcal{C}$. Si $\mathcal{C}$ est définie sur K, on définit alors l'idéal $\mathcal{I}(\mathcal{C}/K)$ engendré par C dans $K[X_0, X_1, X_2]$. L'anneau de coordonnées de $\mathcal{C}/K$ est donné par

$$K[\mathcal{C}] := K[X_0, X_1, X_2]/\mathcal{I}(\mathcal{C}/K).$$

DÉFINITION B.5.2 *Soit $\mathcal{C} := \{ C = 0 \}$ une courbe projective plane. On dit que $g \in \overline{K}[\mathcal{C}] \setminus \{ 0 \}$ est une* forme de degré *d s'il existe un polynôme homogène $G \in S$ de degré d tel que $g = G + \langle C \rangle$. On note alors* $\deg g := d$. *On écrit $g(P) \neq 0$ si $P \in \mathcal{C}$ est tel que $G(P) \neq 0$. La même définition s'applique aux éléments de $K[\mathcal{C}]$ si $\mathcal{C}$ est définie sur K.*

Le degré d'une forme est bien défini : si G et G' sont deux polynômes homogènes non nuls de degrés distincts tels que $G - G' \in \langle C \rangle$, alors $G \in \langle C \rangle$ et $G' \in \langle C \rangle$ car sinon le polynôme C ne serait pas homogène.

On ne peut pas considérer les éléments de $\overline{K}[\mathcal{C}]$ comme des fonctions définies sur $\mathcal{C}$. Par contre, soient $d \in \mathbb{N}$ et $G, H \in S_d$. Soit $P = (a_0 : a_1 : a_2) \in \mathcal{C}$ et supposons que $H(P) \neq 0$. Alors quel que soit $\lambda \in \overline{K} \setminus \{ 0 \}$, on a

$$\frac{G(\lambda a_0, \lambda a_1, \lambda a_2)}{H(\lambda a_0, \lambda a_1, \lambda a_2)} = \frac{\lambda^d G(a_0, a_1, a_2)}{\lambda^d H(a_0, a_1, a_2)} = \frac{G(a_0, a_1, a_2)}{H(a_0, a_1, a_2)}.$$

De la sorte, l'application $G/H \mapsto (G/H)(P) := \frac{G(a_0,a_1,a_2)}{H(a_0,a_1,a_2)}$ est bien définie.

DÉFINITION B.5.3 *Soit $\mathcal{C}$ une courbe projective plane. Le* corps des fonctions *de la courbe $\mathcal{C}$ est le sous-corps du corps des fractions de $\overline{K}[\mathcal{C}]$ donné par*

$$\overline{K}(\mathcal{C}) := \left\{ f/g \mid f, g \in \overline{K}[\mathcal{C}] \text{ sont des formes de même degré et } g \neq 0 \right\}.$$

Si $\mathcal{C}$ est définie sur K, le corps des fonctions *de $\mathcal{C}/K$ est donné par*

$$K(\mathcal{C}) := \{ f/g \mid f, g \in K[\mathcal{C}] \text{ sont des formes de même degré et } g \neq 0 \}.$$

On dit que $u \in \overline{K}(\mathcal{C})$ est défini au point $P \in \mathcal{C}$ s'il existe deux formes g et h de même degré telles que $u = g/h$ et $h(P) \neq 0$. Dans ce cas, si $G, H \in S$ sont tels que $g = G + \langle C \rangle$ et $h = H + \langle C \rangle$, on évalue u au point P en posant[1] $u(P) := (G/H)(P)$.

DÉFINITION B.5.4 *Soient $\mathcal{C}$ une courbe projective plane et $P \in \mathcal{C}$.* L'anneau local du point *P est défini par*

$$\mathcal{O}_P(\mathcal{C}) := \left\{ f/g \mid f, g \in \overline{K}[\mathcal{C}] \text{ sont des formes de même degré et } g(P) \neq 0 \right\}.$$

1. Il est clair que $u(P)$ ne dépend pas du choix des coordonnées homogènes du point P ni des représentants G et H.

L'anneau local d'un point P est donc l'ensemble de toutes les fonctions définies au point P. Il est clair que $\mathcal{O}_P(\mathcal{C})$ est un anneau local et que son unique idéal maximal est donné par

$$\mathcal{M}_P(\mathcal{C}) := \{\, f/g \in \mathcal{O}_P(\mathcal{C}) \ \mid \ f(P) = 0 \text{ et } g(P) \neq 0 \,\}$$

DÉFINITION B.5.5 *Soient $\mathcal{C}$ et $\mathcal{C}'$ deux courbes planes (affines ou projectives). On dit que $\mathcal{C}$ est* birationnelle *à la courbe $\mathcal{C}'$ si leurs corps de fonctions sont $\overline{K}$-isomorphes.*

Toute courbe projective plane est birationnelle à une courbe plane affine et réciproquement : soit $\mathcal{C} := \{\, C = 0 \,\}$ une courbe projective plane et supposons que $C \neq X_2$. Posons $C_2 := C(X, Y, 1)$. On a

$$\mathcal{C}_2 := \pi_2^{-1}(\mathcal{C}) = \left\{\, Q \in \mathbb{A}^2 \ \mid \ C_2(Q) = 0 \,\right\}.$$

En fait, $\mathcal{C}_2$ est une courbe affine plane car l'irréductibilité de C entraîne celle de C_2. De plus, $\mathcal{C}_2$ est birationnelle à $\mathcal{C}$. Pour s'en convaincre, considérons x et y les images résiduelles de X et Y dans $\overline{K}[\mathcal{C}_2] := \overline{K}[X, Y]/\langle C_2 \rangle$. Soient aussi x_0, x_1, x_2 les images résiduelles respectives de X_0, X_1, X_2 dans $\overline{K}[\mathcal{C}]$. Il est aisé de montrer que

$$\begin{array}{rccc} \varphi_2 : & \overline{K}(\mathcal{C}) & \longrightarrow & \overline{K}(\mathcal{C}_2) \\ & \frac{G(x_0,x_1,x_2)}{H(x_0,x_1,x_2)} & \longmapsto & \frac{G(x,y,1)}{H(x,y,1)} \end{array}$$

est un $\overline{K}$-isomorphisme. De façon similaire, en considérant respectivement les ouverts standards U_i pour $i = 0, 1$, on définira les $\overline{K}$-isomorphismes φ_i pour en déduire que $\mathcal{C}_i := \pi_i^{-1}(\mathcal{C})$ est une courbe affine plane birationnelle à $\mathcal{C}$.

Réciproquement, si $\mathcal{C} := \{\, C = 0 \,\}$ est une courbe affine plane et

$$C = \sum_{l=0}^{d} \sum_{l=i+j} \alpha_{i,j} X^i Y^j \in \overline{K}[X, Y],$$

en posant

$$C^* := \sum_{l=0}^{d} \sum_{l=i+j} \alpha_{i,j} X_0^i X_1^j X_2^{(d-l)},$$

on vérifie que C^* est un polynôme homogène irréductible et que $\mathcal{C}$ est birationnelle à la courbe projective plane $\mathcal{C}^* := \{\, C^* = 0 \,\}$.

REMARQUE B.5.6 Soit $\mathcal{C}$ une courbe projective plane. Pour $i = 0, 1, 2$, on vient de montrer que $\mathcal{C}_i := \pi_i^{-1}(\mathcal{C})$ est une courbe affine plane birationnelle à $\mathcal{C}$. On observera aussi que $\mathcal{C}_i$ est en bijection avec $\mathcal{C} \cap U_i$. En particulier, si $P \in \mathcal{C} \cap U_i$ et $P_i \in \mathcal{C}_i$ est tel que $\pi_i(P_i) = P$, alors

$$\varphi_i\left(\mathcal{O}_P(\mathcal{C})\right) = \mathcal{O}_{P_i}(\mathcal{C}_i).$$

On observera aussi que $\Gamma_2 := \{\, x_0/x_2, x_1/x_2 \,\}$ est un ensemble de coordonnées du corps de fonctions $\overline{K}(\mathcal{C})$ (cf. Définition 2.1.5) car $\varphi_2(x_0/x_2) = x$, $\varphi_2(x_1/x_2) = y$ et $\overline{K}(x,y) = \overline{K}(\mathcal{C}_2)$. En intervertissant les rôles de x_0, x_1 et x_2, on vérifie que $\Gamma_1 := \{\, x_0/x_1, x_2/x_1 \,\}$ et $\Gamma_0 := \{\, x_1/x_0, x_2/x_0 \,\}$ sont aussi des ensembles de coordonnées de $\overline{K}(\mathcal{C})$. On appelle les ensembles Γ_i, $i = 0, 1, 2$, les ensembles de coordonnées standards du corps de fonctions $\overline{K}(\mathcal{C})$.

Puisque tout corps de fonctions d'une courbe affine plane est un corps de fonctions algébriques à une variable, on a la proposition suivante.

Proposition B.5.7 *Tout corps de fonctions d'une courbe projective plane est un corps de fonctions algébriques à une variable.*

B.6 Changement de coordonnées projectives

Soient $\mathcal{C} := \{\, C = 0 \,\}$ une courbe projective plane et $B \subset \mathcal{C}$ un ensemble fini de points. On peut supposer que $B \subset \mathcal{C} \cap U_2$, quitte à faire un *changement de coordonnées projectives.*

Soit M une matrice inversible de taille 3×3 à coefficients dans $\overline{K}$. Soit l'application

$$\begin{array}{cccc} T: & \mathbb{P}^2 & \longrightarrow & \mathbb{P}^2 \\ & P = (a_0 : a_1 : a_2) & \mapsto & T(P) := (a_0' : a_1' : a_2') \end{array}$$

où $(a_0' : a_1' : a_2')$ est donné par $(a_0', a_1', a_2') := (a_0, a_1, a_2)M$. Cette application est bien définie car $T(P)$ ne dépend pas du choix des coordonnées homogènes de P. On appelle l'application T un changement de coordonnées projectives. À T est associé l'application

$$\begin{array}{ccc} \overline{K}[X_0, X_1, X_2] & \longrightarrow & \overline{K}[X_0, X_1, X_2] \\ G(X_0, X_1, X_2) & \mapsto & G^T := G(X_0', X_1', X_2') \end{array}$$

où X_0', X_1', X_2' sont donnés par $(X_0', X_1', X_2') := (X_0, X_1, X_2)M^{-1}$. Il est clair que $G(P) = G^T(T(P))$ pour tout $P \in \mathbb{P}^2$ et pour tout polynôme homogène G. Soit maintenant $\mathcal{C} := \{\, C = 0 \,\}$ une courbe projective plane. Alors quel que soit le changement de coordonnées T, le polynôme C^T est irréductible. On vérifie aisément que $\mathcal{C}$ est birationnelle à $\mathcal{C}^T := \left\{\, C^T = 0 \,\right\}$.

Lemme B.6.1 *Soient $P_i = (a_i : b_i : c_i) \in \mathbb{P}^2$ pour $i = 1, 2, \ldots, n$. Il existe un changement de coordonnées projectives T tel que $T(P_i) \in \mathbb{P}^2 \cap U_2$ pour $i = 1, 2, \ldots, n$.*

Démonstration : On peut toujours choisir $\beta, \gamma \in \overline{K}$ avec $\lambda \neq 0$ tels que $a_i + \beta b_i + \gamma c_i \neq 0$ pour $i = 1, 2, \ldots, n$. On conclut en appliquant le changement de coordonnées défini par la matrice inversible

$$M := \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & \beta \\ 0 & 0 & \gamma \end{bmatrix}.$$

□

B.7 Le Théorème de Bézout

Soient $G, H \in \overline{K}[X_0, X_1, X_2]$ deux polynômes homogènes et

$$\mathcal{V}(G \cap H) := \{\, P \in \mathbb{P}^2 \mid G(P) = H(P) = 0 \,\}$$

qu'on appelle ensemble des points d'intersection de G et H. Le Théorème de Bézout permet de "compter" avec multiplicité le nombre de points de $\mathcal{V}(G \cap H)$.

Soient $G \in \overline{K}[X_0, X_1, X_2]$ un polynôme homogène et $P := (a_0 : a_1 : a_2) \in \mathbb{P}^2$. Posons

$$G^P(X, Y) := \begin{cases} G(X, Y, 1) & \text{si } a_2 \neq 0, \text{ sinon} \\ G(X, 1, Y) & \text{si } a_2 = 0 \text{ et } a_1 \neq 0, \\ G(1, X, Y) & \text{sinon.} \end{cases}$$

Définition B.7.1 *On dit que deux polynômes homogènes $G, H \in \overline{K}[X_0, X_1, X_2]$ sont* transverses *au point $P \in \mathbb{P}^2$ si*

1. *$G(P) = H(P) = 0$ et*
2. *$\mathrm{Init}(G^P)$ et $\mathrm{Init}(H^P)$ n'ont pas de facteur commun.*

Géométriquement, deux polynômes homogènes G et H sont transverses au point P s'il n'existe pas au point P de tangente commune aux courbes $\{\, G = 0 \,\}$ et $\{\, H = 0 \,\}$.

Définition B.7.2 *Soient $G, H \in S$ deux polynômes homogènes de degrés respectif m et n.* L'indice d'intersection *est une application*

$$\begin{array}{ccc} \mathbb{P}^2 \times S \times S & \longrightarrow & \mathbb{N} \cup \{\, \infty \,\} \\ (P, G, H) & \mapsto & I_P(G, H) \end{array}$$

ayant les propriétés suivantes :

1. *$I_P(G, H) = \infty$ si et seulement si G et H ont un facteur commun H' tel que $H'(P) = 0$, sinon $I_P(G, H) \in \mathbb{N}$,*

2. $I_P(G,H) = 0$ *si et seulement si* $P \notin \mathcal{V}(G \cap H)$,

3. $I_P(G,H) = I_P(H,G)$,

4. $I_P(G,H) = I_{T(P)}(G^T, H^T)$ *quel que soit le changement de coordonnées projectives* T,

5. $I_P(G,H) \geq \mathrm{m}_P(G)\mathrm{m}_P(H)$ *avec égalité si et seulement si* G *et* H *sont transverses au point* P.

6. *si* $G = \prod G_i^{r_i}$ *et* $H = \prod H_j^{s_j}$, *alors* $I_P(G,H) = \sum_{i,j} r_i s_j I_P(G_i, H_j)$,

7. *si* $\deg G \geq \deg H$, *alors pour tout polynôme homogène* $B \in \overline{K}[X_0, X_1, X_2]$ *tel que* $\deg B = \deg G - \deg H$, *on a* $I_P(G,H) = I_P(G + BH, H)$.

THÉORÈME B.7.3 *Il existe une unique application de* $\mathbb{P}^2 \times S \times S$ *dans* $\mathbb{N} \cup \{ \infty \}$ *qui satisfait les propriétés de l'indice d'intersection.*

Démonstration : Fulton [10, Th. 3 page 75].

THÉORÈME B.7.4 (BÉZOUT) *Soient* $G, H \in \overline{K}[X_0, X_1, X_2]$ *deux polynômes homogènes n'ayant pas de facteur commun. Alors*

$$\sum_{P \in \mathcal{V}(G \cap H)} I_P(G,H) = \deg G \times \deg H.$$

Démonstration : Fulton [10, page 112.]

Annexe C

Complétions $\mathfrak{P}$-adiques

Un corps valué (L, ν) est un corps L muni d'une valuation discrète ν. Une suite $(s_n)_{n\geq 0} \subset L$ converge vers $s \in L$ si quel que soit $c \in \mathbb{R}$, il existe $N_c \in \mathbb{N}$ tel que pour tout $n \geq N_c$ on ait $\nu(s - s_n) > c$. Dans ce cas on dit que la suite est convergente et on écrit

$$\lim_{n\to\infty} s_n = s.$$

Une suite de Cauchy est une suite $(s_n)_{n\geq 0}$ telle que pour tout $c \in \mathbb{R}$, il existe $N_c \in \mathbb{N}$ tel que quelles que soient $m, n \geq N_c$ on ait $\nu(s_n - s_m) > c$. Soit $(z_n)_{n\geq 0}$ une suite de L et soit la série $s = \sum_{i=0}^{\infty} z_i$. On dit que la série s est convergente L si la suite $(s_m := \sum_{i=0}^{m} z_i)_{m\geq 0}$ est convergente.

Définition C.1 *Soit (L, ν) un corps valué.*

1. *(L, ν) est dit* complet *si toute suite de Cauchy de L est convergente.*
2. *Un* complété *de (L, ν) est un corps valué $(\hat{L}, \hat{\nu})$ tel que*
   (a) *$L \subseteq \hat{L}$ et ν est la restriction de $\hat{\nu}$ à L.*
   (b) *$(\hat{L}, \hat{\nu})$ est complet.*
   (c) *L est* dense *dans $\hat{L}$, c'est-à-dire que pour tout $s \in \hat{L}$ il existe une suite $(s_n)_{n\geq 0}$ de L telle que $\lim_{n\to\infty} s_n = s$.*

Tout corps valué possède un complété qui est unique à isomorphisme près. Plus précisément on a :

Proposition C.2 *Soit (L, ν) un corps valué et soit $(\hat{L}, \hat{\nu})$ un complété de (L, ν). Si (L', ν') est un autre complété de (L, ν), alors il existe un unique isomorphisme $\varphi : \hat{L} \to L'$ tel que $\nu' \circ \varphi = \hat{\nu}$.*

Démonstration : Stichtenoth [43, Proposition IV.2.3].

Soient F/K un corps de fonctions et $\nu_{\mathfrak{P}}$ la valuation discrète d'une place $\mathfrak{P}$ de F/K. Alors $(F, \nu_{\mathfrak{P}})$ est un corps valué. On note $(\hat{F}_{\mathfrak{P}}, \hat{\nu}_{\mathfrak{P}})$ le complété de $(F, \nu_{\mathfrak{P}})$.

Théorème C.3 *Soient $\mathfrak{P}$ une place de degré 1 du corps F/K et t un paramètre local de $\mathfrak{P}$. Soit $(\hat{F}_{\mathfrak{P}}, \hat{\nu}_{\mathfrak{P}})$ le complété de $(F, \nu_{\mathfrak{P}})$. Alors tout élément $z \in \hat{F}_{\mathfrak{P}}$ se représente de façon unique par la série formelle*

$$z(t) := \sum_{i=n}^{\infty} c_i t^i, \quad n \in \mathbb{Z}, \quad c_i \in K.$$

Cette représentation s'appelle la série $\mathfrak{P}$-adique *de z en fonction de t. D'autre part, si $(c_i)_{i \geq n}$ est une suite d'éléments de K, alors $\sum_{i=n}^{\infty} c_i t^i$ converge dans $\hat{F}_{\mathfrak{P}}$ et*

$$\hat{\nu}_{\mathfrak{P}} \left(\sum_{i=n}^{\infty} c_i t^i \right) = \min \{ i \mid c_i \neq 0 \}.$$

Démonstration : Stichtenoth [43, Th. IV.2.6].

Remarque C.4 Soient $\mathfrak{P}$ une place de degré 1 du corps F/K et t un paramètre local de la place $\mathfrak{P}$. Soit $z \in \hat{F}_{\mathfrak{P}}$. Pour déterminer la série $\mathfrak{P}$-adique de z en fonction de t on procède comme suit. Puisque $\deg \mathfrak{P} = 1$, on peut identifier le corps résiduel $F_{\mathfrak{P}}$ au corps K. Soit $n_1 := \hat{\nu}_{\mathfrak{P}}(z)$. Puisque F est dense dans $\hat{F}_{\mathfrak{P}}$, il existe $z' \in F$ tel que $\hat{\nu}_{\mathfrak{P}}(z - z') > n_1$. En particulier, on a $\nu_{\mathfrak{P}}(z) = \hat{\nu}_{\mathfrak{P}}(z')$. Soit donc $u_1 \in \mathcal{O}_{\mathfrak{P}}^*$ tel que $z' = u_1 t^{n_1}$. Alors $a_1 := u_1(\mathfrak{P}) \in K \setminus \{0\}$ et $\nu_{\mathfrak{P}}(u_1 - a_1) > 0$. Soit $z_1' := t^{n_1}(u_1 - a_1) \in F$. On a

$$z = a_1 t^{n_1} + (z' - a_1 t^{n_1}) + (z - z') = a_1 t^{n_1} + t^{n_1}(u_1 - a_1) + (z - z') = a_1 t^{n_1} + z_1' + (z - z').$$

Posons $z_1 := z_1' + (z - z') \in \hat{F}_{\mathfrak{P}}$. On a donc

$$\left\{ \begin{array}{rcl} z & = & a_1 t^{n_1} + z_1 \\ n_2 & := & \hat{\nu}_{\mathfrak{P}}(z_1) > n_1. \end{array} \right.$$

De la même façon, on trouve $a_2 \in K$ et $z_2 \in \hat{F}_{\mathfrak{P}}$ tels que

$$\left\{ \begin{array}{rcl} z & = & a_1 t^{n_1} + a_2 t^{n_2} + z_2 \\ n_3 & := & \hat{\nu}_{\mathfrak{P}}(z_2) > n_2. \end{array} \right.$$

En répétant ce processus, on obtient une représentation de z de la forme $\sum_{i=1}^{\infty} a_i t^{n_1}$. D'après le théorème précédent, cette représentation est unique d'où $\sum_{i=1}^{\infty} a_i t^{n_1}$ est la série $\mathfrak{P}$-adique de z en fonction de t. De plus, en utilisant les propriétés de convergence connues, on montre aisément que pour tout $x, y \in \hat{F}_{\mathfrak{P}}$ alors $(x + y)(t) =$

$x(t)+y(t)$ et $(xy)(t) = x(t)y(t)$ où l'addition et la multiplication sont celles définies dans le corps des séries de Laurent

$$K((t)) = \left\{ \sum_{i=n}^{\infty} c_i t^i \;\middle|\; n \in \mathbb{Z}, c_i \in K \right\}.$$

Par conséquent, $\hat{F}_{\mathfrak{P}}$ est isomorphe au corps $K((t))$.

Annexe D

Un peu d'Axiom

> On retrouvera dans cette annexe quelques rudiments du langage de programmation utilisé par le compilateur du système de calcul formel Axiom. L'objectif est d'introduire le lecteur non-initié à quelques notions de base nécessaires à la compréhension du Chapitre 3. Pour plus de détails, on se reportera à [26].

Axiom est un système de calcul formel utilisant les outils de programmation fonctionnelle et de programmation par objet. Il se différencie des autres systèmes de calcul formel du fait qu'il permet d'écrire du code *générique* et *compilable*. Pour ce faire, Axiom utilise trois types de constructeurs : les catégories, les domaines et les paquetages :

1. une catégorie sert à définir une classe d'objets et elle le fait en regroupant un ensemble d'opérations propres à la classe d'objets ; on dit alors que les opérations sont *exportées* par la catégorie.

2. Les domaines quant à eux réalisent les objets et appartiennent aux catégories. Par exemple, la classe des anneaux est définie par la catégorie "`Ring`" et l'anneau des entiers $\mathbb{Z}$ est réalisé par le domaine "`Integer`" qui appartient à la catégorie "`Ring`". Un domaine aura à sa charge d'implanter les opérations exportées par la catégorie à laquelle il appartient.

3. Un paquetage implante des algorithmes relatifs à un ou plusieurs domaines. Par exemple, dans le paquetage "`GroebnerPackage`" on retrouvera l'implantation de l'algorithme de calcul d'une base de Groebner.

Notons qu'un domaine appartient toujours à une catégorie, mais qu'une catégorie peut appartenir à une autre : la catégorie "`Ring`" appartient à la catégorie "`Monoid`" qui définit la classe des monoïdes multiplicatifs qui sont des semi-groupes multiplicatifs avec un élément neutre. Par suite, la catégorie "`Monoid`" appartient à la catégorie "`SemiGroup`". L'opération de multiplication de deux éléments d'un anneau est alors exportée par la catégorie "`SemiGroup`" et la catégorie "`Ring`" y a accès par *héritage*.

Voici un exemple simple de programmation en Axiom. On veut faire des calculs[1] sur les matrices de taille 2×2 à coefficients dans le corps $\mathbb{F}_2$. On est en présence de deux d'objets : le corps $\mathbb{F}_2$ et l'anneau des matrices de taille 2×2. Un corps étant un anneau, il sera judicieux de créer d'abord une catégorie pour la classe des anneaux. Ensuite, on utilisera cette catégorie pour construire la catégorie qui définira la classe des corps. Voici ce que pourrait être le code d'une catégorie pour la classe des anneaux :

```
MyRing:Category == SetCategory with
    "+" : (%,%) -> %
    "*" : (%,%) -> %
    "-" : (%,%) -> %
    "-" :   %   -> %
    1   :   ()  -> %
    0   :   ()  -> %
```

Le code débute avec "`MyRing`" : c'est le nom qu'aura la catégorie. Vient ensuite "`:Category`" qui déclare que "`MyRing`" est une catégorie. Ce qui suit le "`==`" est la définition même de la catégorie. La première partie indique à quelle catégorie "`MyRing`" appartient. Ici, la catégorie "`SetCategory`" est la catégorie d'Axiom qui définit la classe de tous les objets "mathématiques" : cette catégorie exporte entre autres la fonction du test d'égalité. Après le "`with`", on retrouve la liste des opérations exportées par la catégorie "`MyRing`". Ces opérations sont déclarées en leur attribuant une *signature*. Par exemple, l'opération d'addition a pour signature :

```
    "+" : (%,%) -> %
```

Le symbole "`%`" (on utilise aussi "`$`") représente un domaine (quelconque) qui appartiendra à la catégorie. La signature de l'opérations "`+`" signifie que "`+`" prend pour argument deux éléments du domaine "`%`" et retourne un élément de "`%`". On remarquera les signatures des opérations "`1`" et "`0`" : ce sont des opérations constantes représentant respectivement les éléments 1 et 0 d'un anneau. La catégorie qui définit la classe des corps aura pour codes :

```
MyField:Category == MyRing with
```

1. Bien évidemment, il existe déjà en Axiom tout ce qu'il faut pour faire ces calculs.

```
    inv : % -> %
    "/" : (%,%) -> %
```

La catégorie “`MyField`” est donc la catégorie “`MyRing`” augmentée des opérations “`inv`” (inverse) et “`/`” (division).

On définit maintenant le domaine “`Matrice22`” qui réalisera les matrices de taille 2×2. Une matrice est en général définie sur un anneau. Le domaine “`Matrice22`” aura donc pour paramètre générique un domaine appartenant à la catégorie “`MyRing`” :

```
Matrice22(R:MyRing) : Export == Implementation where
  Export ==> MyRing with
    determinant: % -> R
    matrice: (R,R,R,R) -> %
  Implementation ==> add
    Rep :=  List R
    a:% = b:% == a =$Rep b
    1 == [1,0,0,1]
    0 == [0,0,0,0]
    a:% * b:% ==
      [ a.1*b.1 + a.2*b.3 ,_
        a.1*b.2 + a.2*b.4 ,_
        a.3*b.1 + a.4*b.3 ,_
        a.3*b.2 + a.4*b.4 ]
    a:% + b:% ==
      [ (ca + cb)  for ca in a   for cb in b ]
    matrice(a,b,c,d)==[a,b,c,d]
    determinant(a)==
      a.1*a.4 - a.2*a.3
```

Le code débute avec “`Matrice22(R:MyRing)`”. C’est le nom du domaine suivi de ses paramètres : ici, “`Matrice22`” prend pour unique paramètre un domaine “`R`” qui appartient à la catégorie “`MyRing`”. On déclare ensuite à quelle catégorie appartiendra le domaine : ceci est réalisé par la *macro* “`Export`”. On voit à la ligne suivante que la macro “`Export`” pointe sur la catégorie “`MyRing`” : le domaine exporte donc les opérations de “`MyRing`”. On ajoute ensuite les opérations propres au domaine : “`determinant`” calculera le déterminant d’une matrice et “`matrice`” sera utilisée par l’utilisateur pour créer une matrice. Ici, le symbole “`%`” représente le domaine en construction, soit le domaine “`Matrice22`”.

Revenons à la première ligne de code. Ce qui suit le "`==`" concerne l'implantation du domaine et est réalisé par la macro "`Implementation`". Comme on le voit, "`Implementation`" pointe sur "`List R`" : cela signifie que "`Matrice22`" utilisera pour son implantation le domaine "`List`" d'Axiom avec le paramètre "`R`". Ce qui suit le "`add`" est l'implantation même du domaine. La variable "`Rep`" est une variable réservée : elle contient le domaine qui sera utilisé pour représenté les éléments du domaines "`Matrice22`".

On portera une attention particulière à l'implantation du test d'égalité :

```
a:% = b:% == a =$Rep b
```

Ce qui précède "`==`" est la déclaration de l'opération : ici, l'opération "`=`" prendra un argument à gauche et un autre à droite. Après "`==`" on retrouve la définition de l'opération. Le symbole "`$`" est utilisé pour indiquer au compilateur qu'il devra utiliser une opération d'un domaine (ou paquetage) particulier : ici par exemple, on indique au compilateur d'utiliser le test d'égalité du domaine "`List R`" représenté par "`Rep`". Notons que si l'on avait écrit "`a = b`" au lieu de "`a =$Rep b`", alors le test d'égalité de "`Matrice22`" se serait appelé recursivement sans jamais s'arrêter (boucle infini!). Je laisse le soin au lecteur d'interpréter le reste du code de "`Matrice22`" de même que le code pour un corps à deux éléments qui suit :

```
CorpsDeuxElem : Exports == Implementation where
  Exports ==> MyField

  Implementation ==> Integer add

    Rep := Integer

    1 == 1$Integer
    0 == 0$Integer

    a:% = b:% == a =$Rep b
    a:% + b:% ==
      a = 0 => b
      b = 0 => a
      0

    a:% - b:% == a + (-b)
```

```
  a:% * b:% ==
    a = 0 => 0
    b = 0 => 0
    1

  -a:% == a

  inv(a) ==
    a = 0 => error "Je ne connais pas l'inverse de zero"
    a
```

Sous l'interpréteur d'Axiom, on utilise les domaines que nous venons de construire comme suit.

```
(1) ->F:=CorpsDeuxElem


   (1)  CorpsDeuxElem
                                                  Type: Domain
(2) ->M:=Matrice22 F


   (2)  Matrice22 CorpsDeuxElem
                                                  Type: Domain
(3) ->a:=1$M


        +1  0+
   (3)  |    |
        +0  1+
                              Type: Matrice22 CorpsDeuxElem
(4) ->a:=1$M


   (4)  1
                                           Type: CorpsDeuxElem
```

Rien n'empêche de définir les matrices à coefficients dans l'anneau “`M`” :

```
(5) ->MM:=Matrice22 M


   (5)  Matrice22 Matrice22 CorpsDeuxElem
                                                  Type: Domain
```

```
(6) ->a:=1$MM

         ++1  0+  +0  0++
         ||    |  |    ||
         |+0  1+  +0  0+|
     (6) |              |
         |+0  0+  +1  0+|
         ||    |  |    ||
         ++0  0+  +0  1++
                     Type: Matrice22 Matrice22 CorpsDeuxElem
```

Il faut évidement implanter toute les fonctions car sinon :

```
(6) ->determinant(a)
Function:  ?-? : (%,%) -> %
is missing from domain: Matrice22 CorpsDeuxElem
   Internal Error
```

En voulant calculer le déterminant de la matrice "`a`", Axiom a essayé de soustraire deux matrices de "`Matrice22 CorpsDeuxElem`" : or dans le domaine "`Matrice22`" l'opération "`-`" n'a pas été implantée.

Bibliographie

[1] Atiyah (M.F.) et MacDonald (I.G.). – *Introduction to commutative algebra.* – London, Addison-Wesley, 1969.

[2] Bronstein (M.), Hassner (M.), Vasquez (A.) et Wiliamson (C.J.). – Algebraic algorithms for the construction of error correction codes on algebraic curves. *Proccedings of IEEE International Symposium on Information Theory*, June 1991.

[3] Camion (P.). – Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur $\mathbb{F}_q$. *C. R. Acad. Sc. Paris*, vol. 291, 1980, p. 479.

[4] Cantor (D.) et Zassenhaus (H.). – A new algorithm for factoring polynomials over finite fields. *Math. comp.*, no36, 1981, pp. 587–592.

[5] Chevalley (C.). – *Introduction to the theory of algebraic functions of one variable.* – New-York, American Mathematical Society, 1951, *Mathematical Survey.*

[6] Driencourt (Y.) et Michon (J.-F.). – Remarques sur les codes géométriques. *C.R. Acad. Sc. Paris*, vol. 301 Serie I, n° 1, 1985, pp. 15–17.

[7] Driencourt (Y.) et Stichtenoth (H.). – A criterion for self-duality of geometric codes. *Com. in Algebra*, vol. 17, n° 4, 1989, pp. 885–898.

[8] Duval (D.). – Évaluation dynamique et clôture algébrique en Axiom. *Journal of Pure and Applied Algebra*, no99, 1995, pp. 267–295.

[9] Fried (M.D.) et Jarden (M.). – *Field Arithmetic.* – Springer-Verlag, 1986.

[10] Fulton (W.). – *Algebraic curves: An introduction to algebraic geometry.* – New-York, Amsterdam, W.A. Benjamin, Inc, 1969.

[11] Garcia (A.) et Stichtenoth (H.). – A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Invent. Math.*, vol. 121, 1995, pp. 211–222.

[12] Goppa (V.D.). – Codes associated with divisors. *Probl. Peredach. infor.*, vol. 13, n° 1, 1977, pp. 33–39.

[13] Goppa (V.D.). – Codes on algebraic curves. *Soviet Math Dokl*, vol. 24, n° 1, 1981, pp. 170–172.

[14] Goppa (V.D.). – Algebraico-geometric codes. *Math. USSR Izv.*, vol. 21, 1983, pp. 75–91.

[15] Goppa (V.D.). – Codes and information. *Russian Math. Surveys*, vol. 24, 1984, pp. 87–141.

[16] Gorenstein (D.). – An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc*, vol. 72, 1952, pp. 414–436.

[17] Haché (G.). – Computation in algebraic function fields for effective construction of algebraic-geometric codes. *Lecture Notes in Computer Science*, vol. 948, 1995, pp. 262–278.

[18] Haché (G.). – Effective construction of self-dual geometric goppa codes. *In : Proceeding ISIT-95*. IEEE.

[19] Haché (G.) et Le Brigand (D.). – Effective construction of algebraic geometry codes. *IEEE Transaction on Information Theory*, vol. 41, n° 6, November 1995, pp. 1615–1628.

[20] Hartshorne (R.). – *Algebraic Geometry*. – Springer-Verlag, 1977.

[21] Henry (J.-P.) et Merle (M.). – Complexity of computation of embedded resolution of algebraic curves. *Lect. Notes in Comp. Sc*, no378, 1987, pp. 381–390.

[22] Hironaka (H.). – On the arithmetic genera and the effective genera of algebraic curves. *Memoirs of the College of Sciences of Kyoto*, 1957, pp. 177–195.

[23] Høholdt (T.) et Voss (C.). – *An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound. The first steps.* – Rapport technique n° 1995-10, Math. Institute, Tech. Univ. of Denmark, May 1995.

[24] Huang (M.D.) et Ierardi (D.). – Efficient algorithms for Riemann-Roch problem and for addition in the jacobian of a curve. *In : Proceedings 32nd Annual Symposium on Foundations of Computer Sciences*. IEEE Comput. Soc. Press, pp. 678–687.

[25] Ihara (Y.). – Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo*, no28, 1981, pp. 721–724.

[26] Jenks (R.D.) et Sutor (R.S.). – *Axiom, the scientific computation system.* – Springer-Verlag, 1992.

[27] Kirfel (C.) et Pellikaan (R.). – The minimum distance of codes in an array comming from telescopic semigroups. *IEEE Trans. Info. Th.*, vol. 41, n° 6, November 1995, pp. 1720–1732.

[28] Le Brigand (D.) et Risler (J.J.). – Algorithme de Brill-Noether et codes de Goppa. *Bull. Soc. Math. France*, vol. 116, 1988, pp. 231–253.

[29] MacWilliams (F.J.) et Sloane (N.J.A.). – *The theory of error-correcting codes.* – Amsterdam, North-Holland, 1977, *North-Holland Math.*

[30] Malliavin (M.P.). – *Algèbre Commutative.* – Paris, Masson, 1984.

[31] Matsumura (H.). – *Commutative algebra.* – Benjamin/Cumming, 1980, 2-ième édition. 1-ière éd. de 1969.

[32] Menezes (A. J.) et *al.* – *Applications of finite fields.* – Kluwer Academic Publishers, 1993.

[33] Moreno (G.). – Lazy resolution of plane curves. – Notes informelles de calcul formel 11.

[34] Moreno (O.), Zinoviev (D.) et Zinoviev (V.). – On several new projective curves over $\mathbb{F}_2$ of genus 3,4 and 5. *IEEE Trans. on Info. Theory*, vol. 41, n° 6, November 1995, pp. 1643–1648.

[35] Munuera (C.) et Pellikaan (R.). – Equality of geometric Goppa codes and equivalence of divisors. *Journal of Pure and Applied Algebra*, 1993, pp. 229–252.

[36] Munuera (C.) et Pellikaan (R.). – Self-dual and decomposable geometric Goppa codes. *EUROCODE 92*, 1993.

[37] Papini (O.) et Wolfmann (J.). – *Algèbre discrète et codes correcteurs.* – Springer-Verlag, 1994.

[38] Perrin (D.). – *Géométrie Algébrique.* – Paris, InterÉditions / CNRS Édition, 1995.

[39] Scharlau (W.). – Selbstdual Goppa codes. *Math. Nachr.*, vol. 143, 1989, pp. 119–122.

[40] Shafarevich (I.). – *Basic Algebraic Geometry 1.* – Springer-Verlag, 1994, 2-ième édition.

[41] Silverman (J.H.). – *The Arithmetic of Elliptic Curves.* – New-York, Springer-Verlag, 1986, *Graduate texts in Matehmatics.*

[42] Stichtenoth (H.). – Self-dual goppa dodes. *Journal of Pure and Applied Algebra*, no55, 1988.

[43] Stichtenoth (H.). – *Algebraic function fields and codes.* – Springer-Verlag, 1993, *University Text.*

[44] Tsfasman (M. A.), Vlăduţ (S. G.) et Zink (T.). – Modular curves, Shimura curves, and Goppa codes better than Varshamov-Gilbert bound. *Math. Nachr.*, vol. 109, 1982, pp. 21–28.

[45] Tsfasman (M.A.) et Vlăduţ (S.G.). – *Algebraic-geometric codes.* – Kluwer Academic Pub., 1991, *Math. and its Appl.*, volume 58.

[46] Vasquez (A.T.). – *Rational desingularization of a curve defined over a finite field.* – New York, London, Springer-Verlag, 1992, *Number Theory*, 229–250p. N. Y. Seminar 1989-1990.

[47] Zariski (O.) et Samuel (P.). – *Commutative Algebra.* – New-York, Springer-Verlag, 1958, *Graduate texts in mathematics*, volume II. 2nd Printing.

Liste des notations

Index