



**Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation**  
ESA - CNRS 6090

---

L'algorithme de Brill-Noether appliqué aux courbes réduites

**Gaétan Haché**

Rapport de recherche n° 1998-01

---

Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex  
Tél. 05 55 45 73 23 - Fax. 05 55 45 73 22 - laco@unilim.fr

<http://www.unilim.fr/laco/>



# L'algorithme de Brill-Noether appliqué aux courbes réduites

Gaétan Haché

## Introduction

Ce travail de recherche est motivé par l'utilisation de l'algorithme de Brill-Noether pour factoriser des polynômes à deux variables en utilisant une approche géométrique identique à celle proposée par D. Duval [1]. Déjà dans [1], D. Duval souligne qu'il est sûrement possible d'utiliser l'algorithme de Brill-Noether pour factoriser des polynômes ce qu'a confirmé D. LeBrigand [11] en adaptant l'algorithme de Brill-Noether à la factorisation absolue.

À priori, l'algorithme de Brill-Noether est défini pour calculer une base de l'espace vectoriel associé à un diviseur du corps des fonctions d'une courbe algébrique plane absolument irréductible définie sur un corps parfait, en l'occurrence les corps de caractéristique 0 et les corps finis. Par exemple, on peut utiliser l'algorithme de Brill-Noether pour construire des codes géométriques à partir de courbes planes absolument irréductibles définies sur un corps fini. À ce sujet le lecteur pourra consulter [6, 5] et ma thèse de doctorat [4] consacrée en majeure partie à l'implantation de l'algorithme de Brill-Noether que j'ai réalisée dans le langage de calcul formel AXIOM.

Peu de modifications seraient nécessaires à mon implantation pour réaliser l'algorithme de factorisation proposé par D. LeBrigand [11]. Cependant, on peut se demander si ces modifications sont réellement nécessaires – la réponse est non et le but principal de ce travail de recherche est de montrer que l'algorithme de Brill-Noether est aussi valide pour les courbes réduites, c'est-à-dire à sans composantes multiples. Plus généralement, nous verrons que tous les théorèmes, propositions ou lemmes, à priori énoncés pour des courbes irréductibles et sur lesquels repose l'algorithme de Brill-Noether, sont vrais pour des courbes réduites.

Voici comment ce rapport est organisé. Dans un premier temps on voit comment des notions de base liées aux courbes irréductibles sont généralisées aux courbes réduites. Cette généralisation se fait au passage du corps des fonctions d'une courbe irréductible à *l'anneau des fonctions* d'une courbe réduite. À la Section 1.1 j'introduis les notions de place et de diviseur comme dans [1]. La Section 1.2 est consacrée aux anneaux locaux de points d'une courbe réduite. On verra tout particulièrement, à la différence des anneaux locaux de points d'une courbe irréductible, que l'anneau local d'un point d'une courbe réduite n'est pas nécessairement contenu dans l'anneau des fonctions de la courbe. Les Sections 1.3 à 1.6 reprennent les notions déjà exposées

dans [4] qui sont inhérentes à l'algorithme de Brill-Noether. Par exemple, la notion de *point de corps de fonctions* devient celle de *point d'anneau des fonctions*.

La deuxième partie est consacrée à la preuve que l'algorithme de Brill-Noether peut calculer une base de l'espace vectoriel associé à un diviseur d'un anneau des fonctions d'une courbe réduite. On donnera alors un exemple d'utilisation de l'algorithme pour calculer la factorisation absolue d'un polynôme à deux variables à coefficients dans un corps fini.

## 1 Anneaux des fonctions de courbes planes réduites

Soient  $K$  un corps parfait<sup>1</sup> et  $\bar{K}$  une clôture algébrique de  $K$ . Soit  $C \in \bar{K}[X, Y]$  un polynôme non-irréductible sans facteur carré et considérons sa factorisation

$$C = \prod_{i=1}^r C^{(i)},$$

où pour  $i = 1, 2, \dots, r$  les polynômes  $C^{(i)} \in \bar{K}[X, Y]$  sont irréductibles. Chacun des polynômes  $C^{(i)}$  définit une courbe affine plane irréductible

$$\mathcal{C}^{(i)} : = \{ P \in \mathbb{A}^2 \mid C^{(i)}(P) = 0 \}$$

à laquelle sont associés l'anneau de coordonnées

$$\Gamma(\mathcal{C}^{(i)}) : = \bar{K}[X, Y]/\langle C^{(i)} \rangle$$

et le corps des fractions

$$\bar{K}(\mathcal{C}^{(i)}) : = \{ f/g \mid f, g \in \Gamma(\mathcal{C}^{(i)}), g \neq 0 \}$$

appelé le corps des fonctions de  $\mathcal{C}^{(i)}$ . À la courbe affine plane réduite<sup>2</sup>

$$\mathcal{C} : = \{ P \in \mathbb{A}^2 \mid C(P) = 0 \}$$

est aussi associé son anneau de coordonnées

$$\Gamma(\mathcal{C}) : = \bar{K}[X, Y]/\langle C \rangle.$$

L'anneau  $\Gamma(\mathcal{C})$  n'étant pas intègre, on considère  $\Gamma(\mathcal{C})^*$  l'ensemble des éléments réguliers<sup>3</sup> de  $\Gamma(\mathcal{C})$  et on construit<sup>4</sup> l'anneau total des fractions de  $\Gamma(\mathcal{C})$ , soit l'anneau

$$\bar{K}[\mathcal{C}] : = \{ g/h \mid g \in \Gamma(\mathcal{C}) \text{ et } h \in \Gamma(\mathcal{C})^* \}$$

---

1. Un corps  $K$  est parfait si toute extension algébrique de  $K$  est séparable. C'est le cas de tout corps de caractéristique 0, les corps finis et évidemment des corps algébriquement clos.

2. On dit d'une courbe qu'elle est réduite lorsque celle-ci est sans composante multiple, ce qui est le cas pour la courbe  $\mathcal{C}$  car  $C$  est sans facteur carré.

3. Un élément  $a$  d'un anneau  $A$  est dit régulier si quel que soit  $b \in A$  tel que  $ab = 0$  alors  $b = 0$ .

4. Il est intéressant de noter que pour une courbe irréductible cette même construction fournit le corps de fonctions de la courbe.

que nous appellerons **anneau des fonctions** de la courbe  $\mathcal{C}$ .

L'anneau de coordonnées  $\Gamma(\mathcal{C})$  peut être considéré comme un ensemble de fonctions à valeurs dans  $\overline{K}$  définies en tout point de  $\mathcal{C}$ . En effet, soient  $g \in \Gamma(\mathcal{C})$  et  $G \in \overline{K}[X, Y]$  tel que  $g = G + \langle C \rangle$ . Si  $P \in \mathcal{C}$ , on pose  $g(P) := G(P)$ , appelé l'évaluation de  $g$  au point  $P$ , et cette définition est indépendante du choix du représentant de  $g$ .

L'anneau  $\overline{K}[\mathcal{C}]$  possède exactement  $r$  idéaux premiers, soient les idéaux

$$\mathfrak{e}^{(i)} := (\overline{C}^{(i)}/1)\overline{K}[\mathcal{C}]$$

où  $\overline{C}^{(i)} := C^{(i)} + \langle C \rangle \in \Gamma(\mathcal{C})$ . En effet, via le  $\overline{K}$ -homomorphisme

$$\begin{aligned} \Gamma(\mathcal{C}) &\longrightarrow \overline{K}[\mathcal{C}] \\ g &\longmapsto g/1, \end{aligned}$$

les idéaux premiers de  $\overline{K}[\mathcal{C}]$  sont en correspondance biunivoque avec les idéaux premiers de  $\Gamma(\mathcal{C})$  formés que d'éléments non-réguliers de  $\Gamma(\mathcal{C})$  et il est aisé de vérifier que ces derniers sont exactement les idéaux  $\overline{C}^{(i)}\Gamma(\mathcal{C})$ .

Les idéaux  $\mathfrak{e}^{(i)}$  sont tous maximaux, tels que  $\mathfrak{e}^{(i)} + \mathfrak{e}^{(j)} = \overline{K}[\mathcal{C}]$  pour  $i \neq j$  et vérifient  $\bigcap_{i=1}^r \mathfrak{e}^{(i)} = \{0\}$ . En appliquant le théorème du reste chinois on a donc

$$\overline{K}[\mathcal{C}] \cong \overline{K}[\mathcal{C}]/\mathfrak{e}^{(1)} \times \dots \times \overline{K}[\mathcal{C}]/\mathfrak{e}^{(r)}.$$

En fait, pour  $i = 1, 2, \dots, r$ , le corps de fonctions  $\overline{K}(\mathcal{C}^{(i)})$  est  $\overline{K}$ -isomorphe au corps  $\overline{K}[\mathcal{C}]/\mathfrak{e}^{(i)}$ . Plus précisément, on a l'isomorphisme de  $\overline{K}$ -algèbre

$$\begin{aligned} \varphi : \overline{K}[\mathcal{C}] &\longrightarrow \overline{K}(\mathcal{C}^{(1)}) \times \dots \times \overline{K}(\mathcal{C}^{(r)}) \\ \frac{G(x,y)}{H(x,y)} &\longmapsto \left( \frac{G(x^{(1)},y^{(1)})}{H(x^{(1)},y^{(1)})}, \dots, \frac{G(x^{(r)},y^{(r)})}{H(x^{(r)},y^{(r)})} \right) \end{aligned} \quad (1)$$

où  $G, H \in \overline{K}[X, Y]$ , dont  $H$  n'a pas de composante commune avec  $C$ , et où  $x, x^{(i)}$  et  $y, y^{(i)}$  pour  $i = 1, 2, \dots, r$  sont les images résiduelles respectives de  $X$  et  $Y$  dans les anneaux  $\Gamma(\mathcal{C}), \Gamma(\mathcal{C}^{(1)}), \dots, \Gamma(\mathcal{C}^{(r)})$  respectivement.

Dans la suite, pour  $u \in \overline{K}[\mathcal{C}]$  on notera  $u^{(i)}$  la  $i$ -ème coordonnée de  $\varphi(u)$ .

**REMARQUE 1.1** Dans [1] on suppose que le polynôme  $C$  est unitaire en  $Y$  et on considère l'anneau quotient

$$\overline{K}(x)[Y]/\langle C(x, Y) \rangle$$

où  $x$  est l'image résiduelle de  $X$  dans le corps des fractions de  $\overline{K}[X]$ . En fait  $\overline{K}(x)[Y]/\langle C(x, Y) \rangle \cong \overline{K}[\mathcal{C}]$  car en appliquant le théorème du reste chinois on a

$$\overline{K}(x)[Y]/\langle C(x, Y) \rangle \cong \prod_{i=1}^r \overline{K}(x)[Y]/\langle C^{(i)}(x, Y) \rangle$$

et chacun des corps  $\overline{K}(x)[Y]/\langle C^{(i)}(x, Y) \rangle$  est isomorphe à  $\overline{K}(\mathcal{C}^{(i)})$ . Dans [11] on utilise aussi cette représentation de l'anneau des fonctions. Nous verrons à la deuxième section que ce choix n'est pas adéquat pour généraliser l'algorithme de Brill-Noether (voir Remarque 2.6).

## 1.1 Places et diviseurs

Puisque l'anneau des fonctions d'une courbe réduite s'identifie à un produit de corps des fonctions de courbes irréductibles, on peut généraliser à l'anneau des fonctions d'une courbe les notions de place et de diviseur d'un corps de fonctions algébriques à une variable. Pour plus de détails sur ces notions, on se reportera au livre de Henning Stichtenoth "Algebraic Function Fields and Codes" [14].

Rappelons qu'un anneau de valuation d'un corps de fonctions algébriques à une variable  $F$  de corps de base  $K$  est un anneau  $\mathcal{O}$  tel que

1.  $K \subsetneq \mathcal{O} \subsetneq F$ ,
2. si  $x \in F \setminus \mathcal{O}$  alors  $x^{-1} \in \mathcal{O}$ .

Tout anneau de valuation est local. Une **place** de  $F$  est l'unique idéal maximal d'un anneau de valuation de  $F$ . L'ensemble des places de  $F$  est noté  $\mathbb{P}_F$  et si  $\mathfrak{P} \in \mathbb{P}_F$ , il existe un et un seul anneau de valuation dont  $\mathfrak{P}$  est l'idéal maximal. On note donc  $\mathcal{O}_{\mathfrak{P}}$  l'anneau de valuation de la place  $\mathfrak{P}$ . Une place  $\mathfrak{P}$  possède un élément remarquable  $t$ , appelé **paramètre local**, tel que  $\mathfrak{P} = t\mathcal{O}_{\mathfrak{P}}$ . Tout élément  $v \in F$  peut s'écrire de la forme

$$v = ut^n$$

où  $n \in \mathbb{Z}$  et  $u \in \mathcal{O}_{\mathfrak{P}}^* := \mathcal{O}_{\mathfrak{P}} \setminus \mathfrak{P}$ . En particulier, l'application  $\nu_{\mathfrak{P}} : F \rightarrow \mathbb{Z} \cup \{\infty\}$  donnée par

$$\nu_{\mathfrak{P}}(v) := \begin{cases} n & \text{si } v \neq 0 \text{ et } v = t^n u \text{ où } u \in \mathcal{O}_{\mathfrak{P}}^*, \\ \infty & \text{si } v = 0 \end{cases} \quad (2)$$

est bien définie et ne dépend pas du choix du paramètre local de la place  $\mathfrak{P}$ . L'application  $\nu_{\mathfrak{P}}$  est une **valuation discrète** de  $F$  car elle est surjective sur  $\mathbb{Z} \cup \{\infty\}$  et possède les trois propriétés suivantes :

1.  $\nu_{\mathfrak{P}}(u) = \infty \iff u = 0$ ,
2.  $\nu_{\mathfrak{P}}(uv) = \nu_{\mathfrak{P}}(u) + \nu_{\mathfrak{P}}(v)$  quels que soient  $u, v \in F$ ,
3.  $\nu_{\mathfrak{P}}(u+v) \geq \min \{ \nu_{\mathfrak{P}}(u), \nu_{\mathfrak{P}}(v) \}$  quels que soient  $u, v \in F$  (inégalité du triangle).

Dans le contexte qui nous intéresse on considère les corps des fonctions de chacune des composantes irréductibles de  $\mathcal{C}$ .

**DÉFINITION 1.2** Une place de  $\overline{K}[\mathcal{C}]$  est une place du corps des fonctions d'une des composantes irréductibles de  $\mathcal{C}$ . On note  $\mathbb{P}_{\mathcal{C}}$  l'ensemble des places de  $\overline{K}[\mathcal{C}]$ .

Soient  $\mathfrak{P}$  une place de  $\overline{K}[\mathcal{C}]$  et  $i_{\mathfrak{P}} \in \{1, 2, \dots, r\}$  l'unique indice tel que  $\mathfrak{P}$  soit une place de  $\overline{K}(\mathcal{C}^{(i_{\mathfrak{P}})})$  et considérons la valuation discrète correspondante :

$$\nu_{\mathfrak{P}}^{(i_{\mathfrak{P}})} : \overline{K}(\mathcal{C}^{(i_{\mathfrak{P}})}) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

En projetant  $\overline{K}[\mathcal{C}]$  sur  $\overline{K}(\mathcal{C}^{(i_{\mathfrak{P}})})$ , on peut définir l'application

$$\begin{aligned} \nu_{\mathfrak{P}} : \overline{K}[\mathcal{C}] &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ u &\longmapsto \nu_{\mathfrak{P}}^{(i_{\mathfrak{P}})}(u^{(i_{\mathfrak{P}})}). \end{aligned} \quad (3)$$

Cette application est surjective et vérifie les trois propriétés suivantes :

1.  $\nu_{\mathfrak{P}}(u) = \infty$  si et seulement si  $u^{(i_{\mathfrak{P}})} = 0$ ,
2.  $\nu_{\mathfrak{P}}(uv) = \nu_{\mathfrak{P}}(u) + \nu_{\mathfrak{P}}(v)$  quels que soient  $u, v \in \overline{K}[\mathcal{C}]$ ,
3.  $\nu_{\mathfrak{P}}(u + v) \geq \min \{ \nu_{\mathfrak{P}}(u), \nu_{\mathfrak{P}}(v) \}$  quels que soient  $u, v \in \overline{K}[\mathcal{C}]$ .

L'application  $\nu_{\mathfrak{P}}$  ne possède pas toutes les propriétés qui font d'une application une valuation discrète car il existe évidemment  $u \in \overline{K}[\mathcal{C}] \setminus \{0\}$  tel que  $u^{(i_{\mathfrak{P}})} = 0$ , d'où  $\nu_{\mathfrak{P}}(u) = \infty$  avec  $u \neq 0$ . Néanmoins, par abus de langage on acceptera la définition suivante :

**DÉFINITION 1.3** Une valuation discrète de  $\overline{K}[\mathcal{C}]$  est une application surjective

$$\nu : \overline{K}[\mathcal{C}] \longrightarrow \mathbb{Z} \cup \{ \infty \}$$

vérifiant les propriétés suivantes :

1. il existe  $i \in \{1, 2, \dots, r\}$  tel que  $\nu(u) = \infty$  si et seulement si  $u^{(i)} = 0$ ,
2.  $\nu(uv) = \nu(u) + \nu(v)$  quels que soient  $u, v \in \overline{K}[\mathcal{C}]$ ,
3.  $\nu(u + v) \geq \min \{ \nu(u), \nu(v) \}$  quels que soient  $u, v \in \overline{K}[\mathcal{C}]$ .

Soit  $\nu$  une valuation de  $\overline{K}[\mathcal{C}]$ . L'entier  $i$  vérifiant  $\nu(u) = \infty$  si et seulement si  $u^{(i)} = 0$  est unique. En effet, puisque  $\nu$  est surjective, il existe  $u \in \overline{K}[\mathcal{C}]$  tel que  $\nu(u) \neq \infty$  et alors  $u^{(i)} \neq 0$ . En prenant  $j \neq i$ ,  $1 \leq j \leq r$ , on peut choisir  $u$  tel que  $u^{(j)} = 0$  et toujours tel que  $\nu(u) \neq \infty$  ce qui montre que l'entier  $j$  ne vérifie pas  $\nu(u) = \infty$  si et seulement si  $u^{(j)} = 0$ . Sachant qu'une place d'un corps de fonctions est entièrement et uniquement déterminée par une valuation discrète, la proposition suivante est évidente.

**PROPOSITION 1.4** Pour toute place  $\mathfrak{P} \in \mathbb{P}_{\mathcal{C}}$ , l'application  $\nu_{\mathfrak{P}}$  définie en (3) est une valuation discrète de  $\overline{K}[\mathcal{C}]$ . Réciproquement, si  $\nu : \overline{K}[\mathcal{C}] \rightarrow \mathbb{Z} \cup \{ \infty \}$  est une valuation discrète alors il existe une unique place  $\mathfrak{P} \in \mathbb{P}_{\mathcal{C}}$  telle que  $\nu = \nu_{\mathfrak{P}}$ .

On peut maintenant généraliser à l'anneau des fonctions d'une courbe la notion de diviseur d'un corps de fonctions.

**DÉFINITION 1.5** Un diviseur de  $\overline{K}[\mathcal{C}]$  est une somme formelle

$$D := \sum_{\mathfrak{P} \in \mathbb{P}_{\mathcal{C}}} n_{\mathfrak{P}} \mathfrak{P}$$

où  $n_{\mathfrak{P}} \in \mathbb{Z} \cup \{ \infty \}$ . On note  $\mathcal{D}_{\mathcal{C}}$  l'ensemble de tous les diviseurs de  $\overline{K}[\mathcal{C}]$ .

Contrairement aux diviseurs d'un corps de fonctions, le support d'un diviseur  $D : = \sum_{\mathfrak{p} \in \mathbb{P}_C} n_{\mathfrak{p}} \mathfrak{p}$  de  $\overline{K}[\mathcal{C}]$  n'est pas nécessairement fini. Il en est de même du degré<sup>5</sup> de  $D$ ,

$$\deg D : = \sum_{\mathfrak{p} \in \mathbb{P}_C} n_{\mathfrak{p}},$$

qui prend sa valeur dans  $\mathbb{Z} \cup \{\infty\}$ .

L'ensemble des diviseurs  $\mathcal{D}_C$  est muni d'une relation d'ordre : si  $D' : = \sum_{\mathfrak{p} \in \mathbb{P}_C} n'_{\mathfrak{p}} \mathfrak{p}$  est un autre diviseur de  $\overline{K}[\mathcal{C}]$  alors

$$D' \geq D \iff n_{\mathfrak{p}} \geq n'_{\mathfrak{p}} \text{ pour tout } \mathfrak{p} \in \mathbb{P}_C.$$

On définit l'addition de  $D$  et  $D'$  par

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

où l'addition dans  $\mathbb{Z} \cup \{\infty\}$  est l'addition usuelle dans  $\mathbb{Z}$  si  $n_{\mathfrak{p}} \in \mathbb{Z}$  et  $n'_{\mathfrak{p}} \in \mathbb{Z}$  et dans le cas où  $n_{\mathfrak{p}} = \infty$  ou  $n'_{\mathfrak{p}} = \infty$ , alors  $n_{\mathfrak{p}} + n'_{\mathfrak{p}} = \infty$ . On note 0 l'élément neutre de l'addition dans  $\mathcal{D}_C$  et du fait que

$$\deg(D + D') = \deg(D) + \deg(D'),$$

il est clair que  $D$  possède un inverse dans  $\mathcal{D}_C$  si et seulement si  $\deg D < \infty$ . Muni de cette addition, l'ensemble des diviseurs  $\mathcal{D}_C$  n'est pas un groupe mais un monoïde seulement.

Il est naturel maintenant de généraliser aux anneaux des fonctions d'une courbe les notions de diviseur principal et d'espace vectoriel associé à un diviseur. Soit  $u \in \overline{K}[\mathcal{C}]$ . On appelle

$$(u) : = \sum_{\mathfrak{p} \in \mathbb{P}_C} \nu_{\mathfrak{p}}(u) \mathfrak{p}$$

le **diviseur principal** de la fonction  $u$ . On remarquera qu'il existe des diviseurs principaux de degré infini : ce sont les diviseurs principaux des éléments non-inversibles de  $\overline{K}[\mathcal{C}]$ . Si par contre  $u \in \overline{K}[\mathcal{C}]$  est inversible alors  $\deg(u) = 0$ .

Soit maintenant  $D$  un diviseur de  $\overline{K}[\mathcal{C}]$ . On vérifie aisément que

$$\mathcal{L}(D) : = \{ u \in \overline{K}[\mathcal{C}] \mid D + (u) \geq 0 \}$$

est un  $\overline{K}$ -espace vectoriel. Sa dimension sur  $\overline{K}$  est notée  $\ell(D) : = \dim_{\overline{K}} \mathcal{L}(D)$ .

C'est sur la proposition suivante que s'appuie l'algorithme de factorisation proposé par D. Duval [1].

**PROPOSITION 1.6** (cf. [1]) *Soit  $r$  le nombre de composantes irréductibles de  $\mathcal{C}$ . Alors*

1.  $\ell(0) = r$ ,

---

5. Habituellement, le degré d'un diviseur est pondéré par le degré des places. Or ici, toutes les places sont de degré 1 car tous les corps de fonctions considérés ont pour corps de base le corps algébriquement clos  $\overline{K}$ .

2. pour toute place  $\mathfrak{P}$  de  $\overline{K}[\mathcal{C}]$  et un entier  $n > 0$ , on a  $\ell(-n\mathfrak{P}) = r - 1$ .

Démonstration : Soit  $D$  un diviseur tel que  $\deg D < \infty$ . Il est clair que

$$\mathcal{L}(D) \cong \mathcal{L}(D^{(1)}) \times \dots \times \mathcal{L}(D^{(r)})$$

via l'isomorphisme de  $\overline{K}$ -algèbre  $\overline{K}[\mathcal{C}] \cong \overline{K}(\mathcal{C}^{(1)}) \times \dots \times \overline{K}(\mathcal{C}^{(r)})$  (voir (1) page 3). Les  $\overline{K}$ -espaces vectoriels  $\mathcal{L}(D^{(i)}) \subset \overline{K}(\mathcal{C}^{(i)})$  étant tous de dimension finie on a  $\ell(D) = \sum_{i=1}^r \ell(D^{(i)})$ . En particulier,  $\ell(0) = \sum_{i=1}^r \ell(0^{(i)}) = r$  car dans les corps de fonctions  $\overline{K}(\mathcal{C}^{(i)})$  on a  $\mathcal{L}(0^{(i)}) \cong \overline{K}$ . Pour finir, supposons sans perte de généralité que  $\mathfrak{P}$  soit une place de  $\mathcal{C}^{(1)}$  et soit un entier  $n > 0$ . Il est clair que  $u \in \mathcal{L}(-n\mathfrak{P})$  si et seulement si  $u^{(1)} = 0$  et  $u^{(i)} \in \overline{K}$  pour  $i \neq 1$ , d'où  $\ell(-n\mathfrak{P}) = r - 1$ .  $\square$

## 1.2 Anneaux locaux de points

Soient  $\mathcal{C} : \{C = 0\}$  une courbe affine plane réduite et  $P \in \mathcal{C}$ . Nous allons maintenant étudier les propriétés locales de la courbe  $\mathcal{C}$ , c'est-à-dire les propriétés intrinsèques "au voisinage" de points de la courbe  $\mathcal{C}$ . Dans le cas des courbes irréductibles, on considère l'ensemble des fonctions de  $\Gamma(\mathcal{C})$  définies au point  $P$ , soit

$$\Gamma(\mathcal{C})_P := \{g/h \mid g \in \Gamma(\mathcal{C}), h \in \Gamma(\mathcal{C})^* \text{ et } h(P) \neq 0\} \quad (4)$$

qui est un sous-anneau de  $\overline{K}[\mathcal{C}]$ . Or pour les courbes réduites, cet anneau ne convient pas à l'étude des propriétés de  $\mathcal{C}$  au voisinage de  $P$  car il dépend de toutes les composantes de  $\mathcal{C}$  et, le cas échéant, de celles ne passant pas par  $P$ . Comme le montre la proposition suivante, ceci est caractérisé algébriquement par le fait que  $\Gamma(\mathcal{C})_P$  soit un anneau local ou non.

**PROPOSITION 1.7** *Soient  $\mathcal{C}$  une courbe affine plane réduite,  $\mathcal{C}^{(1)}, \dots, \mathcal{C}^{(r)}$  ses composantes irréductibles deux à deux distinctes et  $P \in \mathcal{C}$ . Alors  $\Gamma(\mathcal{C})_P$  est un anneau local si et seulement si  $P \in \bigcap_{i=1}^r \mathcal{C}^{(i)}$ .*

Démonstration : Soit

$$M_P := \{g/h \mid g \in \Gamma(\mathcal{C}), h \in \Gamma(\mathcal{C})^*, g(P) = 0 \text{ et } h(P) \neq 0\}$$

qui est un idéal maximal de  $\Gamma(\mathcal{C})_P$ . Supposons que  $P \in \bigcap_{i=1}^r \mathcal{C}^{(i)}$  et soit  $u \in \Gamma(\mathcal{C})_P \setminus M_P$ . Dans ce cas,  $u = g/h$  avec  $g \in \Gamma(\mathcal{C})$  tel que  $g(P) \neq 0$  et  $h \in \Gamma(\mathcal{C})^*$  et  $h(P) \neq 0$ . Le fait que  $P \in \bigcap_{i=1}^r \mathcal{C}^{(i)}$  et  $g(P) \neq 0$  entraîne que  $g^{-1} \in \Gamma(\mathcal{C})_P$  car dans ce cas un représentant de  $g$  n'est divisible par aucun des polynômes définissant l'une des composantes irréductibles de  $\mathcal{C}$  d'où  $g$  est régulier dans  $\Gamma(\mathcal{C})_P$ . Par conséquent  $u^{-1} = h/g \in \Gamma(\mathcal{C})_P \setminus M_P$  d'où  $M_P$  est exactement l'ensemble des éléments non-inversibles de  $\Gamma(\mathcal{C})_P$  et donc l'unique idéal maximal. Réciproquement, supposons qu'il existe  $i$  tel que  $P \notin \mathcal{C}^{(i)}$  et soit  $c_i := C^{(i)} + \langle C \rangle$  où  $C^{(i)}$  est le polynôme définissant la courbe  $\mathcal{C}^{(i)}$ . Alors  $c_i \in \Gamma(\mathcal{C})_P$  n'est pas régulier et  $c_i \notin M_P$ . Il est alors clair que  $c_i$  engendre un idéal propre de  $\Gamma(\mathcal{C})_P$  qui n'est pas contenu dans  $M_P$ , c'est-à-dire que  $M_P$  n'est pas l'unique idéal maximal de  $\Gamma(\mathcal{C})_P$ .  $\square$

Avant de poursuivre, voici quelques notations très utiles dans la suite. À une partie  $S$  de  $\{1, 2, \dots, r\}$  sont associés le polynôme

$$C^{(S)} : = \prod_{i \in S} C^{(i)}$$

et la courbe

$$\mathcal{C}^{(S)} : = \{ C^{(S)} = 0 \}.$$

On associe aussi à la partie  $S$  le  $\overline{K}$ -homomorphisme

$$\varphi^{(S)} : \overline{K}[\mathcal{C}] \longrightarrow \overline{K}[\mathcal{C}^{(S)}],$$

soit la projection de  $\overline{K}[\mathcal{C}]$  sur  $\overline{K}[\mathcal{C}^{(S)}]$  via l'isomorphisme défini en (1) (page 3). À tout point  $P \in \mathcal{C}$  est associé le **support** du point  $P$

$$S_P : = \{ i \in \{1, 2, \dots, r\} \mid P \in \mathcal{C}^{(i)} \}.$$

Si  $\#S_P = 1$ , c'est-à-dire que le point  $P$  n'appartient qu'à une seule composante de  $\mathcal{C}$ , on dit alors que le point est **isolé**. Si  $\mathfrak{P}$  est une place de  $\overline{K}[\mathcal{C}]$ , on note  $\mathcal{C}^{(\mathfrak{P})}$  l'unique composante irréductible de  $\mathcal{C}$  dont  $\mathfrak{P}$  est une place du corps de fonctions  $\overline{K}(\mathcal{C}^{(\mathfrak{P})})$ .

**DÉFINITION 1.8** Soient  $P$  un point de  $\mathcal{C}$  et  $S_P$  le support de  $P$ . L'anneau

$$\mathcal{O}_P(\mathcal{C}) : = \{ g/h \mid g \in \Gamma(\mathcal{C}^{(S_P)}), h \in \Gamma(\mathcal{C}^{(S_P)})^* \text{ et } h(P) \neq 0 \}$$

est appelé l'anneau local du point  $P$ .

D'après la Proposition 1.7, l'anneau  $\mathcal{O}_P(\mathcal{C})$  est bien un anneau local. Il a

$$\mathcal{M}_P(\mathcal{C}) : = \{ g/h \mid g \in \Gamma(\mathcal{C}^{(S_P)}), h \in \Gamma(\mathcal{C}^{(S_P)})^*, g(P) = 0 \text{ et } h(P) \neq 0 \}$$

pour unique idéal maximal.

**REMARQUE 1.9** Supposons que  $P$  soit un point de chacune des  $r \geq 2$  composantes  $\mathcal{C}^{(1)}, \dots, \mathcal{C}^{(r)}$  et considérons les anneaux locaux  $\mathcal{O}_P(\mathcal{C}^{(i)})$ . L'anneau produit  $B : = \mathcal{O}_P(\mathcal{C}^{(1)}) \times \dots \times \mathcal{O}_P(\mathcal{C}^{(r)})$  n'est pas isomorphe à  $\mathcal{O}_P(\mathcal{C})$  tout simplement parce que  $B$  n'est pas local. En effet,  $B$  possède  $r$  idéaux maximaux deux à deux distincts, tous de la forme

$$\mathcal{O}_P(\mathcal{C}^{(1)}) \times \dots \times \mathcal{M}_P(\mathcal{C}^{(i)}) \times \dots \times \mathcal{O}_P(\mathcal{C}^{(r)})$$

où seule la  $i$ -ième composante de  $B$  est remplacée par  $\mathcal{M}_P(\mathcal{C}^{(i)})$ .

Il est évident que la définition précédente d'un anneau local n'est pas souhaitable si la factorisation de  $C$  n'est pas connue. Or comme le montre la proposition suivante, il n'est pas nécessaire de connaître cette factorisation pour décrire l'anneau  $\mathcal{O}_P(\mathcal{C})$ , on peut le faire au passage de l'anneau local d'un point affine  $P \in \mathbb{A}^2$  défini comme suit :

$$\mathcal{O}_P(\mathbb{A}^2) : = \{ G/H \mid G, H \in \overline{K}[X, Y], H(P) \neq 0 \}.$$

**PROPOSITION 1.10** Soit  $P$  un point de la courbe affine plane réduite  $\mathcal{C} : = \{ C = 0 \}$ . Alors

$$\mathcal{O}_P(\mathcal{C}) \cong \mathcal{O}_P(\mathbb{A}^2) / C \mathcal{O}_P(\mathbb{A}^2).$$

Démonstration : Notons  $\overline{G}, \overline{H}$  les images résiduelles respectives de  $G, H \in \overline{K}[X, Y]$  dans  $\Gamma(\mathcal{C}^{(S_P)}) = \overline{K}[X, Y]/\langle C^{(S_P)} \rangle$ . L'application

$$\begin{aligned} \varphi : \mathcal{O}_P(\mathbb{A}^2) &\longrightarrow \mathcal{O}_P(\mathcal{C}) \\ G/H &\mapsto \overline{G}/\overline{H} \end{aligned}$$

est un  $\overline{K}$ -homomorphisme de noyau  $\ker \varphi = C^{(S_P)}\mathcal{O}_P(\mathbb{A}^2)$ . Posons  $C' := C/C^{(S_P)} \in \overline{K}[X, Y]$ . Puisque  $C'(P) \neq 0$ , il est clair que  $C' \in \mathcal{O}_P(\mathbb{A}^2)$  est inversible dans  $\mathcal{O}_P(\mathbb{A}^2)$  d'où  $\ker \varphi = C' \ker \varphi = C\mathcal{O}_P(\mathbb{A}^2)$ . L'homomorphisme  $\varphi$  étant surjectif on a comme voulu  $\mathcal{O}_P(\mathcal{C}) \cong \mathcal{O}_P(\mathbb{A}^2)/C\mathcal{O}_P(\mathbb{A}^2)$ .  $\square$

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  $C \in \overline{K}[X, Y]$ . On peut écrire

$$C = C_{m_1} + C_{m_2} + \cdots + C_{m_d}, \quad m_1 < m_2 < \cdots < m_d,$$

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

REMARQUE 1.11 Rappelons que tout polynôme homogène de  $\overline{K}[X, Y]$  se factorise en un produit de formes linéaires. Si  $P = (0, 0)$  et  $m_P(C) > 0$ , on peut donc écrire

$$\text{Init}(C) = \prod_{i=1}^{m_P(C)} (\alpha_i X + \beta_i Y).$$

Géométriquement, les facteurs distincts  $L_i := \alpha_i X + \beta_i Y$  de  $\text{Init}(C)$  définissent les tangentes distinctes en  $P$  à la courbe affine plane  $\mathcal{C} = \{C = 0\}$ .

DÉFINITION 1.12 Soient  $\mathcal{C} := \{C = 0\}$  une courbe affine plane et  $P \in \mathcal{C}$ . On appelle  $m_P(\mathcal{C}) := m_P(C)$  la *multiplicité* du point  $P$ .

Il est clair que la forme initiale d'un produit de polynômes est égale au produit des formes initiales de ces mêmes polynômes d'où le lemme suivant.

LEMME 1.13 Soient  $\mathcal{C}^{(1)}, \dots, \mathcal{C}^{(r)}$  les composantes irréductibles de  $\mathcal{C}$  et  $P \in \mathcal{C}$ . On a

$$m_P(\mathcal{C}) = \sum_{i=1}^r m_P(\mathcal{C}^{(i)}).$$

Soient  $C_X$  et  $C_Y$  les dérivés usuelles de  $C$  par rapport à  $X$  et  $Y$  respectivement. Quel que soit  $P := (a, b) \in \mathcal{C}$ , il est clair que

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

Le membre de droite de cette équivalence correspond exactement à la définition d'un point simple (on dit aussi non-singulier) d'une courbe affine plane. Si  $P$  est simple, il est clair qu'une seule composante de  $\mathcal{C}$  passe par  $P$ . Dans ce cas  $\mathcal{C}^{(S_P)}$  est une courbe irréductible et  $\mathcal{O}_P(\mathcal{C})$  est un anneau de valuation discrète du corps de fonctions  $\overline{K}(\mathcal{C}^{(S_P)})$ .

REMARQUE 1.14 La multiplicité d'un point  $P \in \mathcal{C}$  dépend uniquement de l'anneau local  $\mathcal{O}_P(\mathcal{C})$ . En effet, il existe un entier  $N$  assez grand tel que pour tout  $n \geq N$ ,

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

Voir [2, Théorème 2, page 71] pour une démonstration<sup>6</sup>.

### 1.3 Points d'un anneau des fonctions d'une courbe

Dans ma thèse [4] j'ai introduit les notions d'ensemble de coordonnées et de point d'un corps de fonctions algébriques à une variable. Ces notions sont très commodes pour l'étude ainsi que l'implantation de l'algorithme d'éclatement de points. Dans ce qui suit ces notions sont généralisées à l'anneau des fonctions d'une courbe réduite  $\mathcal{C}$ .

DÉFINITION 1.15 Soit  $\overline{K}[\mathcal{C}]$  l'anneau des fonctions de  $\mathcal{C}$ . Le doublet  $\Gamma := \{x, y\} \subset \overline{K}[\mathcal{C}]$  est appelé un ensemble de coordonnées de  $\overline{K}[\mathcal{C}]$  si

1. les éléments réguliers de  $\overline{K}[x, y]$  sont inversibles dans  $\overline{K}[\mathcal{C}]$ ,
2. l'anneau total des fractions de  $\overline{K}[x, y]$  est égal à  $\overline{K}[\mathcal{C}]$ .

Un polynôme de définition de  $\Gamma := \{x, y\}$  est un polynôme<sup>7</sup>  $C_\Gamma \in \overline{K}[X, Y]$  de plus petit degré tel que  $C_\Gamma(x, y) = 0$ . À l'ensemble de coordonnées  $\Gamma$  est associée la courbe  $\mathcal{C}_\Gamma := \{C_\Gamma = 0\}$ .

Dans la remarque qui suit on voit qu'en appliquant un changement de coordonnées affine à un ensemble de coordonnées on obtient un autre ensemble de coordonnées qui est en quelque sorte équivalent au premier.

REMARQUE 1.16 Soit  $\mathcal{C} := \{C = 0\}$  où  $C \in \overline{K}[X, Y]$  et notons respectivement  $x$  et  $y$  les images résiduelles de  $X$  et  $Y$  dans  $\overline{K}[\mathcal{C}]$ . Il est clair que  $\{x, y\}$  est un ensemble de coordonnées de  $\overline{K}[\mathcal{C}]$  admettant  $C$  pour polynôme de définition. Quels que soient  $\alpha, \beta \in \overline{K}$  on a  $\overline{K}[x, y] = \overline{K}[x - \alpha, y - \beta]$  d'où  $\{x - \alpha, y - \beta\}$  est un ensemble de coordonnées de  $\overline{K}[\mathcal{C}]$  admettant le polynôme de définition  $C(X + \alpha, Y + \beta)$ . De plus, si  $P := (a, b; x, y)$  est un point de  $\overline{K}[\mathcal{C}]$  alors

$$P' := (a - \alpha, b - \beta; x - \alpha, y - \beta)$$

6. Dans [2], ce résultat est énoncé pour une courbe irréductible seulement mais la démonstration qu'on y trouve ne fait pas intervenir cette propriété.

7. Ce polynôme est unique à multiplication près par un élément de  $\overline{K} \setminus \{0\}$ .

est aussi un point de  $\overline{K}[\mathcal{C}]$  et il est aisé de montrer que  $\mathcal{O}_P = \mathcal{O}_{P'}$ . De même, soient  $\alpha_i, \beta_i \in \overline{K}$ ,  $i = 1, 2$ , et posons

$$\begin{cases} x_1 & : = & \alpha_1 x + \beta_1 y \\ y_1 & : = & \alpha_2 x + \beta_2 y. \end{cases}$$

Si  $\gamma := \alpha_1 \beta_2 - \beta_1 \alpha_2 \neq 0$  alors  $\overline{K}[x, y] = \overline{K}[x_1, y_1]$  d'où  $\{x_1, y_1\}$  est un ensemble de coordonnées admettant le polynôme de définition  $C(\gamma \beta_2 X - \gamma \beta_1 Y, -\gamma \alpha_2 X + \alpha_1 \beta_2 Y)$ . Comme plus haut, si  $P := (a, b; x, y)$  est un point de  $\overline{K}[\mathcal{C}]$  alors

$$P' := (\alpha_1 a + \beta_1 b, \alpha_2 a + \beta_2 b; x_1, y_1)$$

est un point de  $\overline{K}[\mathcal{C}]$  et  $\mathcal{O}_P = \mathcal{O}_{P'}$ .

Par conséquent, pour étudier les propriétés locales d'un point  $P$  de  $\overline{K}[\mathcal{C}]$  on peut toujours supposer que  $P$  soit à l'origine, c'est-à-dire que  $P$  soit de la forme  $(0, 0; x, y)$ . De plus, une fois à l'origine, on pourra toujours supposer que ni  $X$  ni  $Y$  ne divisent la forme initiale du polynôme de définition de  $\{x, y\}$ .

Soit  $\Gamma$  un ensemble de coordonnées de  $\overline{K}[\mathcal{C}]$ . Par définition de  $\Gamma$ , l'anneau  $\overline{K}[\mathcal{C}_\Gamma]$  est isomorphe à  $\overline{K}[\mathcal{C}]$  et il est naturel d'identifier  $\overline{K}[\mathcal{C}_\Gamma]$  à  $\overline{K}[\mathcal{C}]$ . En particulier, si  $\mathcal{C}^{(1)}, \dots, \mathcal{C}^{(r)}$  sont les  $r$  composantes irréductibles de  $\mathcal{C}$ , alors  $\mathcal{C}_\Gamma$  possède aussi exactement  $r$  composantes irréductibles  $\mathcal{C}_\Gamma^{(1)}, \dots, \mathcal{C}_\Gamma^{(r)}$ . De plus, les composantes de  $\mathcal{C}$  sont deux à deux birationnelles avec les composantes de  $\mathcal{C}_\Gamma$ , et quitte à réordonner les indices, on supposera toujours que  $\mathcal{C}^{(i)}$  est birationnelle à  $\mathcal{C}_\Gamma^{(i)}$  pour  $i = 1, 2, \dots, r$ . Ainsi, si  $S$  est une partie de  $\{1, 2, \dots, r\}$ , l'anneau des fonctions  $\overline{K}[\mathcal{C}_\Gamma^{(S)}]$  s'identifie à  $\overline{K}[\mathcal{C}^{(S)}]$ .

**DÉFINITION 1.17** Soit  $\overline{K}[\mathcal{C}]$  l'anneau des fonctions de  $\mathcal{C}$ . Un point de  $\overline{K}[\mathcal{C}]$  est le couple  $P := (a, b; x, y)$  où  $\Gamma := \{x, y\}$  est un ensemble de coordonnées de  $\overline{K}[\mathcal{C}]$  et  $(a, b) \in \mathcal{C}_\Gamma$ . Si  $\mathcal{C}^{(i)}$ ,  $i = 1, 2, \dots, r$ , sont les composantes irréductibles de  $\mathcal{C}$  respectivement birationnelles aux composantes  $\mathcal{C}_\Gamma^{(i)}$  de  $\mathcal{C}_\Gamma$ , on appelle

$$S_P := \left\{ i \mid (a, b) \in \mathcal{C}_\Gamma^{(i)} \right\}$$

le support de  $P$ . L'entier  $m_P := m_{(a,b)}(\mathcal{C}_\Gamma)$  est appelé la **multiplicité** du point  $P$ .

La définition précédente est une généralisation aux anneaux de fonctions de la notion de *point de corps de fonctions* (voir [4, Définition 2.1.8]). Étant donné un corps de fonctions  $F$ , la notion de points de  $F$  permet de fixer une fois pour toutes le corps  $F$  et de comparer dans  $F$  les anneaux locaux de points de différentes courbes ayant un corps de fonctions isomorphe à  $F$ . On fera de même pour l'anneau  $\overline{K}[\mathcal{C}]$  mais ce sera un peu plus délicat car l'anneau local d'un point  $P$  d'une courbe  $\mathcal{C}$  réduite n'est pas a priori contenu dans  $\overline{K}[\mathcal{C}]$  mais dans  $\overline{K}[\mathcal{C}^{(S)}]$  où  $S$  est le support du point  $P$ . Cette dernière remarque devrait aider à justifier la prochaine définition.

**DÉFINITION 1.18** Soient  $P := (a, b; x, y)$  un point de  $\overline{K}[\mathcal{C}]$  et  $S_P$  le support de  $P$ . L'anneau local d'un point  $P := (a, b; x, y)$  de  $\overline{K}[\mathcal{C}]$ , noté  $\mathcal{O}_P$ , est le sous-anneau de  $\overline{K}[\mathcal{C}^{(S_P)}]$  isomorphe à l'anneau local  $\mathcal{O}_{(a,b)}(\mathcal{C}_\Gamma) \subset \overline{K}[\mathcal{C}_\Gamma^{(S_P)}]$ . On note  $\mathcal{M}_P$  l'unique idéal maximal de  $\mathcal{O}_P$ .

Soient  $P$  un point de  $\overline{K}[\mathcal{C}]$  et  $S_P$  le support de  $P$ . Il sera utile de considérer l'élément  $\varphi^{(S_P)}(u) \in \overline{K}[\mathcal{C}^{(S_P)}]$ . Plus particulièrement si  $\varphi^{(S_P)}(u) \in \mathcal{O}_P \subset \overline{K}[\mathcal{C}^{(S_P)}]$  on écrira  $u \overline{\in} \mathcal{O}_P$  afin d'alléger l'écriture.

De même, étant donnée une place  $\mathfrak{P}$ , on notera  $u \overline{\in} \mathcal{O}_{\mathfrak{P}}$  (resp.  $u \overline{\in} \mathfrak{P}$ ) pour indiquer que  $\varphi^{(\mathfrak{P})}(u) \in \mathcal{O}_{\mathfrak{P}}$  (resp.  $\varphi^{(\mathfrak{P})}(u) \in \mathfrak{P}$ ). Aussi, si  $u \overline{\in} \mathcal{O}_{\mathfrak{P}}$ , l'unique  $\alpha \in \overline{K}$  tel que  $u - \alpha \overline{\in} \mathfrak{P}$  est appelé l'évaluation de  $u$  à la place  $\mathfrak{P}$  et est noté  $u(\mathfrak{P})$ .

La définition qui suit est dans le cas irréductible équivalente à celle que l'on trouve dans [4] (voir [4, Définition 2.1.10 et Proposition 2.1.14]).

**DÉFINITION 1.19** *Soit  $P := (a, b; x, y)$  un point de  $\overline{K}[\mathcal{C}]$ . Soit  $Q$  un point (resp. une place  $\mathfrak{P}$ ) de  $\overline{K}[\mathcal{C}]$ . On dit que  $Q$  (resp.  $\mathfrak{P}$ ) domine  $P$ , et on note  $Q|P$  (resp.  $\mathfrak{P}|P$ ), si*

$$x - a \overline{\in} \mathcal{M}_Q \text{ et } y - b \overline{\in} \mathcal{M}_Q \text{ (resp. } x - a \overline{\in} \mathfrak{P} \text{ et } y - b \overline{\in} \mathfrak{P})$$

Dans le cas d'une courbe irréductible, il est facile de montrer qu'un point d'une courbe est dominé par au moins une et au plus un nombre fini de places du corps des fonctions de la courbe (voir [4, Cor. 2.1.15]) Il est clair alors qu'un point d'une courbe réduite  $\mathcal{C}$  est aussi dominé par au moins une et au plus un nombre fini de places. Si le point est simple, il existe une place  $\mathfrak{P}$  telle que  $\mathcal{O}_P = \mathcal{O}_{\mathfrak{P}}$ . Cette place est unique car l'anneau de valuation de tout autre place dominant le point  $P$  devrait contenir  $\mathcal{O}_{\mathfrak{P}}$ , or tout anneau de valuation est un sous-anneau maximal propre du corps de fonctions dans lequel il est contenu (voir [14, Th. I.1.12]).

## 1.4 Éclatements de points

On se contentera ici de rappeler quelques faits sur les éclatements de points qui sont abordés d'un point de vue strictement algébrique comme dans [4] en s'inspirant du point de vue de Hironaka [9]. Pour une approche géométrique, on se reportera par exemple à [7, 12, 13].

Soient  $C \in \overline{K}[X, Y]$  et  $m := \deg \text{Init}(C)$ . Il est aisé de montrer que  $m$  est le plus grand entier tel que  $X^m$  divise  $C(X, XY) \in \overline{K}[X, Y]$ . De même,  $m$  est le plus grand entier tel que  $Y^m$  divise  $C(XY, Y) \in \overline{K}[X, Y]$ . On pose

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

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

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

que l'on appelle transformé stricte de  $C$  de coordonnée exceptionnelle  $y$ . On appelle aussi la courbe  $\mathcal{C}^{[x]} := \{C^{[x]} = 0\}$  (resp.  $\mathcal{C}^{[y]} := \{C^{[y]} = 0\}$ ) la transformée stricte de  $\mathcal{C}$  de coordonnée exceptionnelle  $x$  (resp.  $y$ ).

Si  $C = \prod_{i=1}^r C^{(i)}$  alors

$$C^{[x]} = \prod_{i=1}^r C^{(i)[x]} \text{ et } C^{[y]} = \prod_{i=1}^r C^{(i)[y]}. \quad (5)$$

On en déduit que si  $C$  n'est pas divisible par  $X$  (resp.  $Y$ ) alors  $C$  est irréductible si et seulement si  $C^{[x]}$  (resp.  $C^{[y]}$ ) est irréductible. Plus particulièrement, si  $C$  n'est pas divisible par  $X$  (resp.  $Y$ ) alors  $\overline{K}[C] \cong \overline{K}[C^{[x]}]$  (resp.  $\overline{K}[C] \cong \overline{K}[C^{[y]}]$ ). Plus précisément, on a :

**PROPOSITION 1.20** *Soient  $\Gamma : = \{x, y\}$  un ensemble de coordonnées de  $\overline{K}[C]$  et  $C$  un polynôme de définition de  $\Gamma$ . Si  $C$  n'est pas divisible par  $X$  (resp.  $Y$ ) alors  $\{x, y/x\}$  (resp.  $\{x/y, x\}$ ) est un ensemble de coordonnées de  $\overline{K}[C]$  qui admet  $C^{[x]}$  (resp.  $C^{[y]}$ ) pour polynôme de définition. L'ensemble de coordonnées  $\{x, y/x\}$  (resp.  $\{x/y, x\}$ ) est appelé le transformé monoïdale de  $\{x, y\}$  de coordonnée exceptionnelle  $x$  (resp.  $y$ ).*

Démonstration : Montrons pour  $\{x, y/x\}$  et supposons que  $X$  ne divise pas  $C$ . D'abord, il est clair que si  $\{x, y/x\}$  est un ensemble de coordonnées alors  $C^{[x]}$  en est un polynôme de définition. Le fait que  $X$  ne divise pas  $C$  entraîne que  $x$  est régulier dans  $\overline{K}[X, Y]$  d'où  $1/x \in \overline{K}[C]$  et donc  $\overline{K}[x, y] \subset \overline{K}[x, y/x] \subset \overline{K}[C]$ . Pour terminer il suffit donc de montrer qu'un élément régulier de  $\overline{K}[x, y/x]$  soit inversible dans  $\overline{K}[C]$  car alors l'anneau total des fractions de  $\overline{K}[x, y/x]$  sera égal à  $\overline{K}[C]$ . On observera qu'un diviseur de zéro dans  $\overline{K}[x, y]$  reste un diviseur de zéro dans  $\overline{K}[x, y/x]$ . On en déduit que si  $g$  est un élément régulier de  $\overline{K}[x, y/x]$  et  $n$  un entier assez grand tel que  $g' : = x^n g \in \overline{K}[x, y]$  alors  $g'$  est un élément régulier de  $\overline{K}[x, y]$ . Par conséquent  $g = g'/x^n$  est inversible dans  $\overline{K}[C]$ .  $\square$

Soient  $\mathfrak{P}$  une place de  $\overline{K}[C]$  et  $P$  un point de  $\overline{K}[C]$  dominé par  $\mathfrak{P}$ . Supposons sans perte de généralité que  $P : = (0, 0 ; x, y)$  (voir remarque 1.16) et soit  $C(X, Y) \in \overline{K}[X, Y]$  un polynôme de définition de  $\{x, y\}$ . Supposons de plus que  $C$  ne soit divisible ni par  $X$  ni par  $Y$ . Soit  $\text{Init}(C)$  la forme initiale de  $C$  qui est de degré  $m : = m_P > 0$  et considérons sa factorisation (voir Remarque 1.11)

$$\text{Init}(C) = \prod_{i=1}^m (\alpha_i X + \beta_i Y).$$

Soit  $\{x, y/x\}$  (resp.  $\{x/y, y\}$ ) le transformé monoïdale de  $\{x, y\}$  de coordonnée exceptionnelle  $x$  (resp.  $y$ ) qui admet  $C^{[x]}$  (resp.  $C^{[y]}$ ) comme polynôme de définition. Soit  $H = C - \text{Init}(C)$ . Alors  $l : = \deg \text{Init}(H) > m$  et on peut écrire

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

de même que

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

Considérons maintenant  $\mathfrak{P}$  qui domine  $P$ . Par définition d'un anneau de valuation, on doit avoir  $y_1 : = y/x \in \mathcal{O}_{\mathfrak{P}}$  ou  $x_1 : = x/y \in \mathcal{O}_{\mathfrak{P}}$ .

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

$$0 = 0(\mathfrak{P}) = C^{[x]}(x, y_1)(\mathfrak{P}) = \prod_{i=1}^m (\alpha_i + \beta_i y_1(\mathfrak{P})). \quad (6)$$

Il existe donc  $i$  tel que  $\beta_i \neq 0$  et  $y_1(\mathfrak{P}) = -\alpha_i/\beta_i$ . En particulier

$$P^{\mathfrak{P}} := (0, -\alpha_i/\beta_i; x, y_1)$$

est un point de  $\overline{K}[C]$ .

2. Si  $y_1 \notin \mathcal{O}_{\mathfrak{P}}$ , et donc  $x_1 \in \mathfrak{P}$ , alors  $x_1(\mathfrak{P}) = 0$ . Dans ce cas

$$0 = C^{[y]}(x_1, y)(\mathfrak{P}) = \prod_{i=1}^m (\alpha_i x_1(\mathfrak{P}) + \beta_i) = \prod_{i=1}^m \beta_i \quad (7)$$

d'où il existe  $i$  tel que  $\beta_i = 0$ . En particulier

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

est un point de  $\overline{K}[C]$ .

Le point  $P^{\mathfrak{P}}$  défini plus haut est appelé le **point infiniment voisin** de  $P$  vers la place  $\mathfrak{P}$ . On remarquera que l'ensemble des valeurs  $-\alpha_i/\beta_i$ , pour lesquelles évidemment  $\beta_i \neq 0$ , est exactement l'ensemble des racines distinctes du polynôme  $\text{Init}(C)(1, Y)$ . Il est clair aussi qu'il existe  $i$  tel que  $\beta_i = 0$  si et seulement si  $\text{Init}(C)(0, 1) = 0$  ce qui est équivalent à dire que  $X$  divise  $\text{Init}(C)$ .

**DÉFINITION 1.21** *Supposons que  $P := (0, 0; x, y)$  soit un point de  $\overline{K}[C]$  et soit  $C$  un polynôme de définition de  $\{x, y\}$ .*

1. On appelle **éclatement** du point  $P$  l'ensemble

$$\mathcal{E}(P) := \{ (0, \gamma; x, y/x) \mid \gamma \in \overline{K}, \text{Init}(C)(1, \gamma) = 0 \} \cup \mathcal{E}_{\infty}(P)$$

où

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

2. Si  $P := (a, b; x, y)$ , l'éclatement du point  $P$  se définit en ramenant le point à  $P$  à l'origine, c'est-à-dire  $\mathcal{E}(P) := \mathcal{E}((0, 0; x - a, y - b))$ .

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

**REMARQUE 1.22** 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  $\mathcal{E}(P)$  sont en correspondance biunivoque avec les facteurs linéaires distincts de  $\text{Init}(C)$  et donc avec les tangentes à la courbe  $\mathcal{C}_{\Gamma}$  au point  $P$  (voir Remarque 1.11). Plus précisément,  $Q := (0, \gamma; x, y_1) \in \mathcal{E}(P)$  si et seulement si la droite  $\{\gamma X - Y = 0\}$  est tangente à la courbe  $\mathcal{C}_{\Gamma}$  en  $P$ . De même,  $Q' := (0, 0; x_1, y) \in \mathcal{E}(P)$  si et seulement si la droite  $\{X = 0\}$  est tangente à la courbe  $\mathcal{C}_{\Gamma}$  en  $P$ .

**PROPOSITION 1.23** *Soit  $P$  un point de  $\overline{K}[C]$ . Alors*

1.  $\mathcal{E}(P) = \{ P^{\mathfrak{P}} \mid \mathfrak{P} | P \}$ ,

2. quel que soit la place  $\mathfrak{P}$  dominant le point  $P$ , on a

$$\mathfrak{P}|P^{\mathfrak{P}} \quad \text{et} \quad P^{\mathfrak{P}}|P.$$

Démonstration : Soit  $Q \in \mathcal{E}(P)$  et supposons sans perte de généralité que  $P = (0, 0; x, y)$  et  $Q = (0, \gamma; x, y_1)$  où  $y_1 := y/x$ . Il est clair que  $x \in \mathcal{M}_Q$  et  $y = xy_1 \in \mathcal{M}_Q$  d'où  $Q$  domine  $P$ . Pour finir la démonstration, il suffit de montrer qu'il existe une place  $\mathfrak{P}$  telle que  $Q = P^{\mathfrak{P}}$ . Soit  $C$  un polynôme de définition de  $\{x, y\}$ . Par définition de  $Q$ , on a  $\text{Init}(C)(1, \gamma) = 0$ . En particulier, il existe un facteur irréductible  $C'$  de  $C$  tel que  $\text{Init}(C')(1, \gamma) = 0$ . Soit alors  $\mathcal{C}' := \{C' = 0\}$  qui est une composante irréductible de  $\mathcal{C}$  et notons respectivement  $x', y'$  et  $y'_1$  les projections de  $x, y$  et  $y_1$  sur  $\overline{K}(\mathcal{C}')$ . Alors  $P' := (0, 0; x', y')$  et  $Q' := (0, \gamma; x', y'_1) \in \mathcal{E}(P')$  sont des points du corps de fonctions  $\overline{K}(\mathcal{C}')$ . Il existe une place  $\mathfrak{P}$  de  $\overline{K}(\mathcal{C}')$  telle que  $\mathfrak{P} \supset \mathcal{M}_{Q'}$  (voir [14, Th.I.1.18]) d'où  $Q' = P'^{\mathfrak{P}}$ . Or  $\mathfrak{P}$  est aussi par définition une place de  $\overline{K}[\mathcal{C}]$  et il est clair que  $Q' = P'^{\mathfrak{P}}$  entraîne  $Q = P^{\mathfrak{P}}$ .  $\square$

PROPOSITION 1.24 Soient  $P$  un point de  $\overline{K}[\mathcal{C}]$  et  $\mathfrak{P}$  une place dominant le point  $P$ . Alors il existe un entier  $N$  tel que pour tout  $n \geq N$ , le point  $P^{\mathfrak{P}^{(n)}}$  est un point isolé de  $\overline{K}[\mathcal{C}]$ .

Démonstration : Il n'y a rien à montrer si  $\mathcal{C}$  est irréductible. Soient donc  $\mathcal{C}^{(1)}, \dots, \mathcal{C}^{(r)}$  les  $r \geq 2$  composantes irréductibles de  $\mathcal{C}$ . Supposons que  $P = (0, 0; x, y)$  et soient  $C$  un polynôme de définition de  $\{x, y\}$  et  $C^{(1)}, \dots, C^{(r)}$  les  $r$  facteurs irréductibles de  $C$  (dans l'ordre adéquat par rapport aux composantes  $\mathcal{C}^{(i)}$ ). Supposons que  $\mathfrak{P}$  soit une place de  $\overline{K}(\mathcal{C}^{(1)})$  et posons

$$G_1(X, Y) := C/C^{(1)} = \prod_{i=2}^r C^{(i)} \in \overline{K}[X, Y].$$

Si  $G_1(0, 0) \neq 0$  alors évidemment le point  $P$  est isolé et la démonstration est finie. Sinon, soit  $Q := P^{\mathfrak{P}}$  et supposons que  $Q = (0, \gamma; x, y_1)$  où  $y_1 := y/x$ . Rappelons que dans ce cas l'ensemble de coordonnées  $\{x, y_1\}$  admet  $C^{[x]}$  comme polynôme de définition. Posons

$$G_2(X, Y) := G_1^{[x]} = C^{[x]}/C^{(1)[x]}.$$

Si  $G_2(0, \gamma) \neq 0$  alors  $Q$  est un point isolé et la démonstration est terminée. Sinon considérons les fonctions

$$g_1 := G_1(x, y) \quad \text{et} \quad g_2 := G_2(x, y_1).$$

Elles sont liées par la relation

$$g_1 = x^m g_2$$

où  $m := \deg \text{Init}(G_1)$ . Par conséquent  $\nu_{\mathfrak{P}}(g_1) > \nu_{\mathfrak{P}}(g_2)$  car  $m > 0$  et  $\nu_{\mathfrak{P}}(x) > 0$ . En répétant ce processus, après avoir remplacé  $P$  par  $Q$  (qu'on prendra soin de ramener à l'origine), on trouvera  $g_3 \in \overline{K}[\mathcal{C}]$  avec  $\nu_{\mathfrak{P}}(g_2) > \nu_{\mathfrak{P}}(g_3)$  et ainsi de suite. Après un nombre fini d'itérations, disons  $N$ , on trouvera  $g_N$  avec  $\nu_{\mathfrak{P}}(g_N) = 0$  et alors le point  $P^{\mathfrak{P}^{(n)}}$  est isolé pour tout  $n \geq N$ .  $\square$

COROLLAIRE 1.25 Soient  $P$  un point de  $\overline{K}[\mathcal{C}]$  et  $\mathfrak{P}$  une place dominant le point  $P$ . Alors il existe un entier  $N$  tel que pour tout  $n \geq N$ , le point  $P^{\mathfrak{P}^{(n)}}$  est simple.

Démonstration : On sait que le corollaire est vrai si  $\mathcal{C}$  est irréductible (cf. [4, Th. 2.5.2]). Cela suffit à démontrer le corollaire car d'après la proposition précédente on peut supposer que le point  $P$  est isolé et dans ce cas l'anneau  $\mathcal{O}_P$  est contenu dans le corps des fonctions de la composante irréductible contenant le point  $P$ .  $\square$

À tout point  $P$  de  $\overline{K}[\mathcal{C}]$  on associe son **arbre de désingularisation**, noté  $\mathcal{T}_P$ , défini récursivement comme suit :

1. Si  $P$  est simple alors on pose

$$\mathcal{T}_P := \{ [P] \}.$$

Ici  $\mathcal{T}_P$  est un arbre formé du seul noeud  $[P]$ .

2. Sinon  $P$  est singulier et on pose alors

$$\mathcal{T}_P := \{ P, \{ \mathcal{T}_Q \mid Q \in \mathcal{E}(P) \} \}.$$

Ici  $\mathcal{T}_P$  est un arbre formé du noeud  $[P]$  auquel sont liés les arbres de désingularisation de chacun des points infiniment voisins de  $P$ .

**PROPOSITION 1.26** *Pour tout point  $P$  de  $\overline{K}[\mathcal{C}]$ , l'arbre de désingularisation  $\mathcal{T}_P$  est fini. En particulier, si  $Q$  est un point de  $\overline{K}[\mathcal{C}]$  correspondant à une feuille de  $\mathcal{T}_P$  alors il existe une place de  $\overline{K}[\mathcal{C}]$  dominant le point  $P$  telle que  $\mathcal{O}_Q = \mathcal{O}_{\mathfrak{P}}$ . Réciproquement, si  $\mathfrak{P}$  est une place dominant le point  $P$  alors il existe une feuille de  $\mathcal{T}_P$  dont le point correspondant  $Q$  est tel que  $\mathcal{O}_Q = \mathcal{O}_{\mathfrak{P}}$ . Ainsi, les feuilles de  $\mathcal{T}_P$  sont en correspondance biunivoque avec les places dominant le point  $P$ .*

Démonstration : C'est une conséquence de la Proposition 1.23 et du Corollaire 1.25.  $\square$

## 1.5 Diviseurs exceptionnels

Dans cette section on définit le *diviseur exceptionnel* d'un point de  $\overline{K}[\mathcal{C}]$ . Ce diviseur joue un rôle essentiel pour le calcul d'une base de l'espace vectoriel associé à un diviseur de  $\overline{K}[\mathcal{C}]$ . La notion de diviseur exceptionnel est exactement la même que dans le cas irréductible et on se reportera à [4, Section 2.3] pour plus de détails.

**DÉFINITION 1.27** *Soient  $P \in \mathcal{C}$  et  $u \in \overline{K}[\mathcal{C}] \setminus \{0\}$ . 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 déduit facilement des propriétés d'une valuation discrète que si  $u, v \in \overline{K}[\mathcal{C}] \setminus \{0\}$  alors  $(uv)_P = (u)_P + (v)_P$  pour tout point  $P \in \mathcal{C}$ .

**DÉFINITION 1.28** *Soit  $P$  un point de  $\overline{K}[\mathcal{C}]$ . Le diviseur exceptionnel du point  $P$ , noté  $E_P$ , est défini par*

$$E_P := \sum_{\mathfrak{P}|P} m_{\mathfrak{P}} \mathfrak{P}$$

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

$$m_{\mathfrak{P}} := \min \{ \nu_{\mathfrak{P}}(z) \mid z \in \overline{\mathcal{M}}_P \}.$$

Le diviseur exceptionnel d'un point intervient dans le calcul des diviseurs locaux : supposons que  $P := (0, 0; x, y)$  soit un point de  $\overline{K}[\mathcal{C}]$  et soit  $g \in \overline{K}[x, y]$ . Puisque toute place dominant  $P$  domine un seul point de  $\mathcal{E}(P)$ , on a

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

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

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

Mais  $l_Q$  étant une coordonnée exceptionnelle du point  $Q \in \mathcal{E}(P)$ , 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  $Q$ . Par conséquent,

$$E_P = \sum_{Q \in \mathcal{E}(P)} (l_Q)_Q \tag{8}$$

d'où

$$(g)_P = m_P(G)E_P + \sum_{Q \in \mathcal{E}(P)} (g^{[l_Q]})_Q. \tag{9}$$

**PROPOSITION 1.29** *Soient  $P := (a, b; x, y)$  un point de  $\overline{K}[\mathcal{C}]$  et  $C$  un 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*

$$(g)_P = m_P(G)E_P.$$

Démonstration : C'est clair en considérant l'équation (9) et la Remarque 1.22.  $\square$

**COROLLAIRE 1.30** *Si  $P := (0, 0; x, y)$  est un point de  $\overline{K}[\mathcal{C}]$  et ni  $X$  ni  $Y$  ne divisent la forme initiale du polynôme de définition de  $\{x, y\}$  alors*

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

Avant de passer à la section suivante on donne la définition du *diviseur d'adjonction* d'un point d'un anneau des fonctions d'une courbe. Cette définition est exactement la même que celle donnée dans [4] pour les points d'un corps de fonctions. Comme on le verra plus loin, les diviseurs d'adjonction jouent un rôle essentiel dans l'algorithme de Brill-Noether.

**DÉFINITION 1.31** *Soit  $P$  un point de l'anneau des fonctions d'une courbe réduite. On appelle diviseur d'adjonction du point  $P$  le diviseur défini récursivement*

$$\mathcal{A}_P := (m_P - 1)E_P + \sum_{Q \in \mathcal{E}(P)} \mathcal{A}_Q$$

où  $m_P$  est la multiplicité du point  $P$  et  $E_P$  est le diviseur exceptionnel du point  $P$ .

On observera que le diviseur d'adjonction d'un point  $P$  est fini car les points correspondant aux feuilles de l'arbre de désingularisation  $\mathcal{T}_P$  sont des points simples et donc de multiplicité égale à 1.

La proposition suivante fournit les conditions suffisantes pour appliquer le Théorème fondamental de Max Noether sur lequel repose l'algorithme de Brill-Noether (voir Théorème 2.1). On sait déjà que cette proposition est vraie pour les courbes irréductibles (cf. [4, Prop. 2.6.3]) et la démonstration est beaucoup plus simple que celle qui suit pour les courbes réduites. Pour saisir cette différence, considérons un point singulier  $P$  d'une courbe  $\mathcal{C}$ . Si  $\mathcal{C}$  est irréductible alors les anneaux locaux de tous les points infiniment voisins de  $P$  sont contenus dans le corps des fonctions de la courbe. La démonstration repose alors sur un élément appartenant à l'intersection de ces anneaux locaux. Dans le cas d'une courbe réduite  $\mathcal{C}$ , le point singulier  $P \in \mathcal{C}$  peut être un point d'intersection de différentes composantes irréductibles de  $\mathcal{C}$ . Dans ce cas les anneaux locaux des points infiniment voisins de  $P$  ne sont pas tous contenus dans le même anneaux des fonctions et on ne peut pas en prendre l'intersection. Il était donc nécessaire de contourner cette différence car autrement il ne serait pas possible d'appliquer l'algorithme de Brill-Noether aux courbes réduites.

**PROPOSITION 1.32** *Si  $\mathcal{C} := \{C = 0\}$  est une courbe réduite,  $P$  un point de  $\overline{K}[\mathcal{C}]$  et  $u \in \overline{K}[\mathcal{C}]$  alors*

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

*Démonstration :* Montrons par récurrence sur le degré du diviseur  $\mathcal{A}_P$  et supposons sans perte de généralité que le point  $P$  appartient à chacune des composantes de la courbe. Soit  $u \in \overline{K}[\mathcal{C}]$  tel que  $(u)_P \geq \mathcal{A}_P$ . Si  $\deg \mathcal{A}_P = 0$ , et donc  $\mathcal{A}_P = 0$ , alors  $P$  est simple. Dans ce cas il existe une place  $\mathfrak{P}$  telle que  $\mathcal{O}_{\mathfrak{P}} = \mathcal{O}_P$  et  $(u)_P = \nu_{\mathfrak{P}}(u)\mathfrak{P}$ . Or  $\nu_{\mathfrak{P}}(u) \geq 0$  si et seulement si  $u \in \overline{\mathcal{O}}_P$  d'où  $(u)_P \geq \mathcal{A}_P = 0$  entraîne  $u \in \overline{\mathcal{O}}_P$ . Supposons maintenant que  $\deg \mathcal{A}_P > 0$ . Supposons de plus que  $P := (0, 0; x, y)$  et que ni  $X$  ni  $Y$  ne divisent  $\text{Init}(C)$ . Dans ce cas  $x$  est inversible dans  $\overline{K}[\mathcal{C}]$  et

$$x^{m_P-1} \mathcal{O}_P[y_1] \subseteq \mathcal{O}_P$$

où  $m_P$  est la multiplicité du point  $P$  et  $y_1 := y/x$  (voir [12, Ch. IX, Lemme 4.7] ou [2, pages 165–166] pour une démonstration de cette inclusion). Il suffit donc de

montrer que  $v := u/x^{(m_P-1)} \in \mathcal{O}_P[y_1]$ . Soient  $C' := C^{[x]}$  le polynôme de définition de  $\{x, y_1\}$  et  $G, H \in \overline{K}[X, Y]$  tels que

$$v = \frac{G(x, y_1)}{H(x, y_1)}.$$

Si  $H(Q) \neq 0$  pour tout  $Q \in \mathcal{E}(P)$  alors la démonstration est terminée car on peut alors montrer que  $H(x, y_1)$  n'appartient à aucun idéal maximal de  $\mathcal{O}_P[y_1]$ , et donc inversible, d'où  $v = G(x, y_1)H(x, y_1)^{-1} \in \mathcal{O}_P[y_1]$ . Sinon, il nous faut trouver  $G', H' \in \overline{K}[X, Y]$  tels que  $v = G'(x, y_1)/H'(x, y_1)$  avec  $H'(Q) \neq 0$  pour tout  $Q \in \mathcal{E}(P)$ . Observons que

$$(u)_P = \sum_{Q \in \mathcal{E}(P)} (u)_Q \geq \mathcal{A}_P = (m_P - 1)E_P + \sum_{Q \in \mathcal{E}(P)} \mathcal{A}_Q$$

et d'après le Corollaire 1.30 on a  $E_P = (x)_P$ . On peut donc écrire

$$(v)_Q = (u)_Q - (x^{(m_P-1)})_Q \geq \mathcal{A}_Q \quad \text{pour tout } Q \in \mathcal{E}(P).$$

Puisque  $\deg \mathcal{A}_Q < \deg \mathcal{A}_P$  quel que soit  $Q \in \mathcal{E}(P)$ , par hypothèse de récurrence on a

$$v \in \mathcal{O}_Q \quad \text{pour tout } Q \in \mathcal{E}(P).$$

Pour chacun des points  $Q \in \mathcal{E}(P)$  il existe donc trois polynômes  $G_Q, H_Q, A_Q \in \overline{K}[X, Y]$  tels que

$$H_Q(Q) \neq 0 \quad \text{et} \quad GH_Q = G_QH + A_Q C'^{(S_Q)}. \quad (10)$$

Pour  $Q \in \mathcal{E}(P)$  posons

$$\widehat{C}'_Q := C'/C'^{(S_Q)} \in \overline{K}[X, Y].$$

Puisque  $\widehat{C}'_Q(Q) \neq 0$  et  $H_Q(Q) \neq 0$ , on peut choisir  $\alpha_Q \in \overline{K}$  tels que le polynôme

$$H' := \sum_{Q \in \mathcal{E}(P)} \alpha_Q \widehat{C}'_Q H_Q$$

soit tel que  $H'(Q) \neq 0$  pour tout  $Q \in \mathcal{E}(P)$ . Pour chacun des points  $Q \in \mathcal{E}(P)$ , en multipliant l'égalité (10) par  $\alpha_Q \widehat{C}'_Q$  et en additionnant le tout, on trouve

$$GH' = G'H + \left( \sum_{Q \in \mathcal{E}(P)} \alpha_Q A_Q \right) C'$$

où

$$G' := \sum_{Q \in \mathcal{E}(P)} \alpha_Q \widehat{C}'_Q G_Q.$$

Par conséquent,

$$v = \frac{G'(x, y_1)}{H'(x, y_1)}$$

avec comme voulu  $H'(Q) \neq 0$  quel que soit  $Q \in \mathcal{E}(P)$ .  $\square$

**REMARQUE 1.33** La démonstration précédente est beaucoup plus simple si la courbe  $\mathcal{C}$  est irréductible. Dans ce cas, pour chacun des points  $Q \in \mathcal{E}(P)$ , l'anneau local  $\mathcal{O}_Q$  est contenu dans le corps des fonctions  $\overline{K}(\mathcal{C})$  et alors  $\mathcal{O}_P[y_1]$  est égal à l'intersection de tous ses localisés en chacun de ses idéaux maximaux. Or ces localisés sont exactement les anneaux locaux  $\mathcal{O}_Q$  d'où  $\mathcal{O}_P[y_1] = \bigcap_{Q \in \mathcal{E}(P)} \mathcal{O}_Q$ .

## 1.6 Diviseurs d'intersection

On donne dans cette section la définition du *diviseur d'intersection* d'un polynôme homogène  $G \in \overline{K}[X, Y, Z]$  avec une courbe projective plane sans composante multiple. Cette définition est essentiellement la même que celle que l'on retrouve dans [4, Section 2.4] pour le cas des courbes projectives planes irréductibles.

Soit la courbe affine place  $\mathcal{C} : = \{C = 0\}$  et considérons la courbe projective plane  $\mathcal{C}^* : = \{C^* = 0\}$  où  $C^*$  est le polynôme homogène associé au polynôme  $C \in \overline{K}[X, Y]$  : si  $C : = \sum_{i,j} a_{ij} X^i Y^j$  est de degré  $n$ , alors

$$C^* : = \sum_{i,j} a_{ij} X^i Y^j Z^{n-(i+j)}.$$

Comme dans le cas affine, on peut associer à la courbe projective  $\mathcal{C}^*$  un anneau des fonctions noté  $\overline{K}[\mathcal{C}^*]$ . Plus précisément, l'anneau  $\overline{K}[\mathcal{C}^*]$  est l'anneau total des fractions homogènes de  $\Gamma(\mathcal{C}^*) : = \overline{K}[X, Y, Z]/\langle C^* \rangle$ . On peut aussi décrire  $\overline{K}[\mathcal{C}^*]$  comme suit : soient  $x, y$  et  $z$  les images résiduelles respectives de  $X, Y$  et  $Z$  dans  $\Gamma(\mathcal{C}^*)$ . L'anneau  $\overline{K}[\mathcal{C}^*]$  est l'anneau total des fractions de l'anneau  $\overline{K}[x/z, y/z]$  contenu dans l'anneau total des fractions (pas nécessairement homogènes) de  $\Gamma(\mathcal{C}^*)$ .

Comme le lecteur l'a sûrement remarqué, l'anneau  $\overline{K}[\mathcal{C}^*]$  est isomorphe à  $\overline{K}[\mathcal{C}]$  et l'ensemble  $\{x/z, y/z\}$  est un ensemble de coordonnées de  $\overline{K}[\mathcal{C}^*]$ . De la même façon, si  $Y$  ne divise pas  $C^*$  alors  $\{x/y, z/y\}$  est un ensemble de coordonnées de  $\overline{K}[\mathcal{C}^*]$  de même que  $\{y/x, z/x\}$  si  $X$  ne divise pas  $C^*$ . On appelle ces ensembles de coordonnées les **ensembles de coordonnées standards** de  $\overline{K}[\mathcal{C}^*]$ . Ces trois ensembles de coordonnées admettent respectivement  $C^*(X, Y, 1)$ ,  $C^*(X, 1, Z)$  et  $C^*(1, Y, Z)$  comme polynômes de définition.

Soit  $P = (a : b : c) \in \mathcal{C}^*$ . Par définition, au moins une des coordonnées de  $P$  est non nulle. Supposons que  $c \neq 0$ . Alors  $P_* : = (a/c, b/c ; x/z, y/z)$  est un point de  $\overline{K}[\mathcal{C}^*]$ . Si par exemple on a aussi  $b \neq 0$ , alors  $P'_* : = (a/b, c/b ; x/y, z/y)$  est aussi un point de  $\overline{K}[\mathcal{C}]$  et on peut montrer sans trop de peine que  $\mathcal{O}_{P_*} = \mathcal{O}_{P'_*}$ . On peut ainsi identifier tout point de  $\mathcal{C}^*$  à un point de  $\overline{K}[\mathcal{C}^*]$ . Bien que  $\mathcal{O}_{P_*} = \mathcal{O}_{P'_*}$ , certains calculs liés au point  $P$  dépendent du choix de la coordonnée non nulle de  $P = (a : b : c)$ . On adopte donc la définition suivante :

**DÉFINITION 1.34** *Soit  $\mathcal{C}^* : = \{C^* = 0\}$  une courbe projective plane et considérons les ensembles de coordonnées standards correspondants. À tout point  $P : = (a : b : c) \in \mathcal{C}^*$  est associé un point de  $\overline{K}[\mathcal{C}^*]$  défini comme suit :*

$$P_* : = \begin{cases} (a/c, b/c ; x/z, y/z) & \text{si } c \neq 0 \\ (a/b, c/b ; x/y, z/y) & \text{si } c = 0 \text{ et } b \neq 0 \\ (0, 0 ; y/x, z/x) & \text{si } P = (1 : 0 : 0). \end{cases}$$

De plus, pour un polynôme homogène  $G \in \overline{K}[X, Y, Z]$ , on pose

$$\overline{G}^P : = \begin{cases} G(x, y, z)/z^{\deg G} & \text{si } c \neq 0 \\ G(x, y, z)/y^{\deg G} & \text{si } c = 0 \text{ et } b \neq 0 \\ G(x, y, z)/x^{\deg G} & \text{si } P = (1 : 0 : 0). \end{cases}$$

DÉFINITION 1.35 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  $P$ .

DÉFINITION 1.36 Soient  $\mathcal{C}^*$  une courbe projective plane et  $P \in \mathcal{C}^*$ . Soit  $G \in \overline{K}[X, Y, Z] \setminus \{0\}$  un polynôme homogène. 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 d'intersection d'un polynôme homogène  $G \in \overline{K}[X, Y, Z]$  avec  $\mathcal{C}^*$  est défini en fonction des points d'intersection de la courbe  $\mathcal{C}^*$  et de la courbe projective plane  $\mathcal{G} := \{G = 0\}$ . Par le Théorème de Bézout (voir [2, page 112]) on sait que si  $\mathcal{G}$  et  $\mathcal{C}^*$  n'ont pas de composante commune, alors  $\mathcal{G}$  et  $\mathcal{C}^*$  ont un nombre fini et non nul de points en commun. En particulier,  $\deg(G) < \infty$  si et seulement si  $\mathcal{G}$  et  $\mathcal{C}^*$  n'ont pas de composante commune.

Soit  $u \in \overline{K}[\mathcal{C}^*]$ . Le diviseur principal  $(u)$  peut s'écrire comme une différence de diviseurs d'intersection. En effet, il existe deux polynômes homogènes  $G, H \in \overline{K}[X, Y, Z]$  tels que  $u = G(x, y, z)/H(x, y, z)$  et  $H$  n'a pas de composante commune avec  $\mathcal{C}^*$ . Puisque  $H$  n'a pas de composante commune avec  $\mathcal{C}^*$ , on a  $\deg(H) < \infty$  et dans ce cas le diviseur  $-(H)$  est défini. En fait on a

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

Pour montrer cette égalité il suffit de considérer la fonction  $u$  localement en chacun des points de  $P \in \mathcal{C}^*$  et de constater que  $u = \overline{G}^P / \overline{H}^P$  quel que soit  $P \in \mathcal{C}^*$ . Pour plus de détails voir [4, Proposition 2.4.6].

## 1.7 Remarques sur les algorithmes de calculs

Nous verrons à la prochaine section que l'algorithme de Brill-Noether s'applique aux courbes réduites. Or pour appliquer l'algorithme de Brill-Noether il faut savoir calculer les éclatements de points, les diviseurs exceptionnels, les diviseurs d'adjonction et les diviseurs d'intersection.

Les éclatements de points d'un anneau des fonctions d'une courbe ont été définis exactement de la même façon qu'ont été définis dans [4] les éclatements de points d'un corps des fonctions d'une courbe irréductible. Il est clair que le calcul des points infiniment voisins de  $P$  ne dépend pas du fait que la courbe soit irréductible ou non. De plus, on a vu que si  $P$  est un point d'un anneau des fonctions d'une courbe réduite alors comme dans le cas irréductible, l'arbre de désingularisation  $\mathcal{T}_P$  est un arbre fini dont les feuilles sont des points simples (voir Proposition 1.26). Ces arguments suffisent à montrer que tout algorithme de calcul d'arbres de désingularisation a priori défini pour les points d'un corps des fonctions d'une courbe irréductible est aussi applicable, sans modification, aux points d'un anneau des fonctions d'une courbe réduite.

En utilisant les mêmes arguments que précédemment et sachant que tous les algorithmes de calcul de diviseurs décrits dans [4] reposent à la base sur l'équation (9) (page 17), qui est exactement la même dans le cas irréductible, on peut affirmer aussi que tous les algorithmes de calcul de diviseurs décrits dans [4] sont aussi applicables, sans modification, à une courbe réduite.

On sait maintenant que tous les objets utilisés par l'algorithme de Brill-Noether, soient tout particulièrement les diviseurs d'adjonction et d'intersection, sont calculables en utilisant exactement les mêmes algorithmes que l'on retrouve dans [4] à priori définis pour les courbes irréductibles.

Reste à voir que l'algorithme de Brill-Noether lui-même est applicable aux courbes réduites. C'est le sujet de la prochaine section.

## 2 L'algorithme de Brill-Noether et les courbes réduites

Étant donné un diviseur  $D$  de  $\overline{K}[\mathcal{C}^*]$  tel que  $\deg D < \infty$ , l'algorithme de Brill-Noether calcule une base de l'espace vectoriel  $\mathcal{L}(D)$ . Cet algorithme retourne une base  $\{g_1, g_2, \dots, g_{\ell(D)}\}$  où les éléments  $g_i$  s'expriment comme un quotient de polynômes homogènes de même degré, soient  $G_i/G_0$  où  $G_0$  est commun à tous les quotients. Si  $g_i := \overline{G}_i/\overline{G}_0$  alors  $(g_i) + D = (G_i) - (G_0) + D \geq 0$  et donc  $(G_i) \geq (G_0) - D$ . Ainsi, l'algorithme de Brill-Noether peut se résumer en deux étapes :

1. l'algorithme trouve un polynôme homogène  $G_0 \in \overline{K}[X, Y, Z]$  qui sera le dénominateur commun des éléments de la base,
2. l'algorithme calcule une base  $\{G_1, G_2, \dots, G_{\ell(D)}\}$  de l'espace vectoriel des polynômes homogènes  $G \in \overline{K}[X, Y, Z]$  de degré  $\deg G_0$  tels que  $(G) \geq (G_0) - D$ .

Le but de cette section est de montrer que l'algorithme de Brill-Noether, à priori défini pour les courbes irréductibles, est toujours valide pour les courbes non-irréductibles sans facteur carré, c'est-à-dire réduites.

### 2.1 Le théorème fondamental de Max Noether

L'algorithme de Brill-Noether repose essentiellement sur le théorème suivant qui n'impose aucune contrainte d'irréductibilité sur la courbe  $\mathcal{C}^*$ .

**THÉORÈME 2.1 (THÉORÈME FONDAMENTAL DE MAX NOETHER)** *Soient  $\mathcal{C}^* := \{C^* = 0\}$  une courbe projective plane et  $G, H \in \overline{K}[X, Y, Z]$  deux polynômes homogènes où  $G$  n'a pas de facteur commun avec  $C^*$ . Les deux énoncés suivants sont équivalents :*

1. *Il existe deux polynômes homogènes  $A, B \in \overline{K}[X, Y, Z]$  tels que  $\deg A + \deg G = \deg B + \deg C = \deg H$  et*

$$H = AG + BC.$$

2.  *$\overline{H}^P / \overline{G}^P \in \mathcal{O}_P$  quel que soit  $P \in \mathcal{C}^*$ .*

Démonstration : Gorenstein [3, Th. 7]. Voir aussi Fulton [2, page 120].

La proposition qui suit fournit une condition suffisante pour appliquer le théorème précédent. Cette condition fait intervenir le *diviseur d'adjonction* d'une courbe projective plane dont voici la définition.

**DÉFINITION 2.2** *Soient  $\mathcal{C}^*$  une courbe projective plane réduite et  $\mathcal{S}$  l'ensemble des points singuliers de  $\mathcal{C}^*$ . On appelle le diviseur*

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

*le diviseur d'adjonction de la courbe  $\mathcal{C}^*$ .*

**THÉORÈME 2.3** *Soient  $\mathcal{C}^* : = \{C^* = 0\}$  une courbe réduite,  $\mathcal{A}$  le diviseur d'adjonction de  $\mathcal{C}^*$  et deux polynômes homogènes  $G, H \in \overline{K}[X, Y, Z]$ . Si  $G$  et  $\mathcal{C}^*$  n'ont pas de facteur commun et*

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

*alors il existe deux polynômes homogènes  $A, B \in \overline{K}[X, Y, Z]$  tels que  $\deg A + \deg G = \deg B + \deg C = \deg H$  et*

$$H = AG + BC.$$

Démonstration : C'est une conséquence du Théorème 2.1 car quel que soit  $P \in \mathcal{C}^*$ , l'inégalité  $(H) \geq \mathcal{A} + (G)$  entraîne  $(\overline{H}^P)_P \geq \mathcal{A}_P + (\overline{G}^P)_P$  et donc  $(\overline{H}^P / \overline{G}^P)_P \geq \mathcal{A}_P$  d'où  $\overline{H}^P / \overline{G}^P \in \mathcal{O}_P$  d'après la Proposition 1.32.  $\square$

**THÉORÈME 2.4** *Soient  $\mathcal{C}^* : = \{C^* = 0\}$  une courbe projective plane réduite et  $\mathcal{A}$  son diviseur d'adjonction. Soient  $D$  et  $D'$  deux diviseurs de  $\overline{K}[\mathcal{C}^*]$  et supposons que  $\deg D < \infty$  et que  $D'$  soit effectif ( $D' \geq 0$ ). S'il existe  $u \in \overline{K}[\mathcal{C}^*]$  tel que  $D' = (u) + D$  et un polynôme homogène  $G \in \overline{K}[X, Y, Z]$  tel que*

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

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

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

Démonstration : Puisqu'il existe  $u \in \overline{K}[\mathcal{C}^*]$  tel que  $D' = (u) + D$ , il existe deux polynômes homogènes  $H$  et  $H'$  tels que  $H$  n'a pas de composante commune avec  $\mathcal{C}^*$  et  $D' = (H') - (H) + D$  et donc  $(H) + D' = (H') + D$ . En additionnant  $(H')$  de part et d'autre de  $(G) = D + \mathcal{A} + R$  on trouve

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

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

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

Le polynôme  $H$  n'ayant pas de facteur commun avec  $C^*$ , il existe donc, d'après le Théorème 2.3, deux polynômes homogènes  $G', B$  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  $(G') = (H'G) - (H) = D' + \mathcal{A} + R$ .  $\square$

Le théorème qui suit est celui que l'algorithme de Brill-Noether met en oeuvre pour calculer une base de l'espace vectoriel associé à un diviseur. On se reportera à [4] pour sa démonstration car elle est exactement identique à celle donnée dans le cas des courbes irréductibles. Rappelons tout de même que ce théorème est une conséquence du Théorème 2.4 et repose sur la Proposition 1.32 dont la généralisation aux courbes réduites a nécessité une attention particulière.

**THÉORÈME 2.5** *Soient  $\mathcal{C}^* : = \{C^* = 0\}$  une courbe projective plane réduite,  $\mathcal{A}$  son diviseur d'adjonction et  $D$  un diviseur de  $\overline{K}[\mathcal{C}^*]$  tel que  $\deg D < \infty$ . Soit  $G_0 \in \overline{K}[X, Y, Z]$  un polynôme homogène n'ayant pas de facteur commun avec  $C^*$  tel que*

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

Alors

$$\mathcal{L}(D) = \{ \overline{G}/\overline{G}_0 \mid G \in S_{\deg G_0} \text{ tel que } (G) \geq (G_0) - D \}$$

où  $S_{\deg G_0} \subset \overline{K}[X, Y, Z]$  est l'ensemble des polynômes homogènes de degré  $\deg G_0$ .

**REMARQUE 2.6** Soit  $\mathcal{C} : = \{C = 0\}$  une courbe affine plane. Dans [11] on considère l'anneau  $\overline{K}(x)[Y]/\langle C(x, Y) \rangle$  (voir Remarque 1.1) et on identifie les éléments de  $\overline{K}[\mathcal{C}^*]$  à des quotients de polynômes homogènes  $\overline{G}/\overline{G}_0$  de même degré où  $G \in \overline{K}[X, Y, Z]$  mais  $G_0 \in \overline{K}[X, Z]$ . Supposons que l'on veuille calculer une base de  $\mathcal{L}(D)$  pour un diviseur  $D$  de  $\overline{K}[\mathcal{C}^*]$  et soit  $\mathcal{A}$  le diviseur d'adjonction de  $\mathcal{C}^*$ . Pour sauver du temps de calcul, il est clair qu'il faut choisir un polynôme homogène  $G_0$  tel que  $(G_0) \geq D + \mathcal{A}$  de degré le plus petit possible. D'après [11] il faut choisir  $G_0 \in \overline{K}[X, Z]$  tel que  $(G_0) \geq D + \mathcal{A}$ . Or, on peut montrer qu'en général le polynôme homogène  $G'$  de plus petit degré tel que  $(G') \geq D + \mathcal{A}$  ne se trouve pas dans  $\overline{K}[X, Z]$  mais dans  $\overline{K}[X, Y, Z]$ . Le temps de calcul de l'algorithme proposé dans [11] est donc plus élevé que celui de l'algorithme de Brill-Noether non modifié qui est valide pour les courbes réduites d'après le théorème précédent.

## 2.2 Exemple de factorisation absolue d'un polynôme à deux variables

Soit le polynôme

$$C : = X^6 + X^5 + X^4 + X^3 + X^2Y^4 + XY^4 + Y^6 \in \mathbb{F}_2[X, Y]$$

où  $\mathbb{F}_2$  est le corps fini à deux éléments. Pour calculer la factorisation absolue de  $C$ , on applique la Proposition 1.6 en calculant une base de  $\mathcal{L}(0)$  avec l'algorithme de

Brill-Noether. Pour se faire on considère la courbe projective plane  $\mathcal{C}^* : = \{ C^* = 0 \}$  définie sur  $\mathbb{F}_2$  où

$$C^* : = X^6 + X^5Z + X^4Z^2 + X^3Z^3 + X^2Y^4 + XY^4Z + Y^6 \in \mathbb{F}_2[X, Y, Z].$$

Cette courbe est réduite car elle possède un nombre fini de points singuliers, soient  $P_1 : = (1 : 0 : 1)$  et  $P_2 : = (0 : 0 : 1)$  tous deux de multiplicité égale à 3.

Il faut d'abord calculer les arbres de désingularisation de  $P_1$  et  $P_2$ . En accord avec la Définition 1.34 on éclatera les points  $P_{1*} : = (1, 0 ; x_1, y_1)$  et  $P_{2*} : = (0, 0 ; x_1, y_1)$  où  $x_1 : = x/z$  et  $y_1 : = y/z$ . L'ensemble de coordonnées  $\{x_1, y_1\}$  admet le polynôme de définition  $C : = C^*(X, Y, 1)$  et observons que  $C(X+1, Y) = C(X, Y)$ , d'où les calculs de l'éclatement du point  $P_{1*}$  seront exactement les mêmes<sup>8</sup> que ceux du point  $P_{2*}$ . Puisque  $\text{Init}(C) = X^3$ , le point  $P_{1*}$  n'a qu'un seul point infiniment voisin, soit le point  $Q_1 : = (0, 0 ; x_2, y_1)$  où  $x_2 : = x_1/y_1$ , et  $\{x_2, y_1\}$  admet le polynôme de définition

$$C_1 : = C^{[y]} = X^3 + XY^2 + Y^3 + X^2Y^3 + X^4Y + X^5Y^2 + X^6Y^3.$$

Puisque  $m_{Q_1} = \deg \text{Init}(C_1) = 3$ , il faut éclater le point  $Q_1$  et on trouve

$$\begin{aligned} \mathcal{E}(Q_1) &= \left\{ (\alpha, 0 ; x_2/y_1, y_1) \mid \alpha \in \overline{\mathbb{F}_2} \text{ et } \text{Init}(C_1)(\alpha, 1) = 0 \right\} \\ &= \left\{ (\alpha, 0 ; x_2/y_1, y_1) \mid \alpha \in \overline{\mathbb{F}_2} \text{ et } \alpha^3 + \alpha + 1 = 0 \right\}. \end{aligned}$$

Les points de  $\mathcal{E}(Q_1)$  sont définis dans une extension de degré 3 de  $\mathbb{F}_2$ , c'est-à-dire dans  $\mathbb{F}_{2^3}$ . Il en est de même de l'unique point infiniment voisin de  $P_{2*}$  que l'on note  $Q_2$ . Tous les points de  $\mathcal{E}(Q_1)$  sont simples. Par conséquent, l'arbre de désingularisation  $\mathcal{T}_{P_1}$  (resp.  $\mathcal{T}_{P_2}$ ) possède exactement 3 feuilles et celles-ci sont deux à deux conjuguées sur  $\mathbb{F}_2$  par l'application de Frobenius  $\alpha \mapsto \alpha^2$ . Si  $\mathcal{C}^*$  est absolument irréductible cela signifie que  $P_1$  (resp.  $P_2$ ) est dominé par une place de degré 3 du corps de fonctions  $\mathbb{F}_2(\mathcal{C}^*)$ . Par contre, si  $\mathcal{C}^*$  n'est pas absolument irréductible, alors il y a deux interprétations :

- $P_1$  (resp.  $P_2$ ) est dominé par une place de degré 3 du corps de fonctions d'une composante absolument irréductible définie sur  $\mathbb{F}_2$ ,
- $P_1$  (resp.  $P_2$ ) est dominé par 3 places de degré 1 appartenant respectivement aux corps des fonctions de trois courbes absolument irréductibles définies sur  $\mathbb{F}_{2^3}$  et deux à deux conjuguées sur  $\mathbb{F}_2$ .

Notons  $\mathfrak{P}_{i,1}$ ,  $\mathfrak{P}_{i,2}$  et  $\mathfrak{P}_{i,3}$  les places correspondant aux feuilles de  $\mathcal{T}_{P_{i*}}$ ,  $i = 1, 2$ . Les diviseurs exceptionnels sont

$$E_{P_{i*}} = \mathfrak{P}_{i,1} + \mathfrak{P}_{i,2} + \mathfrak{P}_{i,3}, \quad i = 1, 2$$

et

$$E_{Q_i} = \mathfrak{P}_{i,1} + \mathfrak{P}_{i,2} + \mathfrak{P}_{i,3}, \quad i = 1, 2.$$

---

<sup>8</sup> Les calculs seront les mêmes car ils ne dépendent que des polynômes de définitions, mais les points obtenus se distinguent par leur ensembles coordonnées

Le diviseur d'adjonction de  $C^*$  est donc

$$\begin{aligned} \mathcal{A} = \mathcal{A}_{P_1} + \mathcal{A}_{P_2} & := (2E_{P_{1^*}} + 2E_{Q_1}) + (2E_{P_{2^*}} + 2E_{Q_2}) \\ & = 4(\mathfrak{P}_{1,1} + \mathfrak{P}_{1,2} + \mathfrak{P}_{1,3}) + 4(\mathfrak{P}_{2,1} + \mathfrak{P}_{2,2} + \mathfrak{P}_{2,3}). \end{aligned}$$

La droite  $\{Y = 0\}$  passe par les points  $P_1$  et  $P_2$  : Puisque  $m_P(P_i) = 3$  pour  $i = 1, 2$  on doit avoir  $\deg(Y) \geq 6$ . Or par le théorème de Bézout on doit avoir  $\deg(Y) = 6$  d'où

$$(Y) = \sum_{i=1}^2 \mathfrak{P}_{i,1} + \mathfrak{P}_{i,2} + \mathfrak{P}_{i,3}.$$

Par conséquent  $G_0 := Y^4$  est tel que  $(G_0) \geq \mathcal{A}$  (en fait  $(G_0) = \mathcal{A}$ ). Pour finir on trouve une base des polynômes homogènes  $G$  de degré 4 tels que  $(G) \geq (G_0)$ . On trouve

$$\{G_1, G_2, G_3\} := \{Y^4, (X^2 + XZ)Y^2, X^4 + X^2Z^2\}$$

d'où

$$\left\{ 1, \frac{x^2 + xz}{y^2}, \frac{x^4 + x^2z^2}{y^4} \right\}.$$

est une base de  $\mathcal{L}(0)$ . La courbe  $C^*$  possède donc exactement 3 facteurs absolument irréductibles (Proposition 1.6).

Pour trouver un facteur de  $C^*$  il faut choisir une place  $\mathfrak{P}$  de  $\overline{\mathbb{F}}_2[C^*]$  et calculer une base de  $\mathcal{L}(-\mathfrak{P})$ . Prenons  $\mathfrak{P} := \mathfrak{P}_{1,1}$ . Puisque  $\mathcal{L}(-\mathfrak{P}) \subset \mathcal{L}(0)$  on vérifie aisément que

$$\mathcal{L}(-\mathfrak{P}) = \left\{ \frac{\sum_{i=1}^3 \gamma_i \overline{G}_i}{\overline{G}_0} \mid \gamma_i \in \overline{\mathbb{F}}_2 \text{ et } \left( \sum_{i=1}^3 \gamma_i G_i \right) \geq (G_0) + \mathfrak{P} \right\}.$$

On trouve

$$\left\{ \frac{\alpha^5 x^4 + \alpha^5 x^2 z^2 + y^4}{y^4}, \frac{\alpha^6 x^4 + x^2 y^2 + \alpha^6 x^2 y^2 + x y^2 z}{y^4} \right\}$$

pour base de  $\mathcal{L}(-\mathfrak{P})$  où  $\alpha \in \mathbb{F}_{2^3}$  est tel que  $\alpha^3 + \alpha + 1 = 0$ . En calculant le plus grand commun diviseur de  $C^*$  avec les représentants des numérateurs des éléments de la base précédente, on trouve un facteur absolument irréductible de  $C^*$ , soit

$$X^2 + XZ + \alpha Y^2.$$

Le polynôme  $C^*$  étant défini sur  $\mathbb{Q}$ , les conjugués de  $X^2 + XZ + \alpha Y^2$ , obtenus par l'application de Frobenius  $\alpha \mapsto \alpha^2$ , sont aussi des facteurs de  $C^*$  : on obtient alors deux autres facteurs, soient  $(X^2 + XZ + \alpha^2 Y^2)$  et  $(X^2 + XZ + \alpha^4 Y^2)$ , et puisque  $\deg C^* = 36$  on a

$$C^* = (X^2 + XZ + \alpha Y^2)(X^2 + XZ + \alpha^2 Y^2)(X^2 + XZ + \alpha^4 Y^2).$$

## Conclusion

L'objectif de ce travail de recherche a été de montrer que l'algorithme de Brill-Noether tel que décrit dans ma thèse de doctorat [4] peut être appliqué aux courbes réduites dans le but de calculer la factorisation absolue de polynômes à deux variables. Pour se faire il a suffi de généraliser à l'anneau des fonctions d'une courbe les notions liées aux corps des fonctions d'une courbe. En quelque sorte, ce travail de recherche est une traduction de ma thèse dans le langage des anneaux des fonctions de courbes. Ainsi la première partie de ce travail a été consacrée à la généralisation des notions de place, de diviseur, d'espace vectoriel associé à un diviseur, etc. On a vu en particulier que cette généralisation a permis de définir les éclatements de points d'un anneau des fonctions d'une courbe réduite exactement de la même manière qu'a été défini les éclatements de points d'un corps des fonctions d'une courbe irréductible. Cela nous permet d'affirmer que tous les algorithmes de calculs inhérents à l'algorithme de Brill-Noether s'appliquent aussi aux courbes réduites et ce sans les modifier.

Ayant montré à la première section que les objets utilisés par l'algorithme de Brill-Noether sont aussi calculables dans le cas des courbes réduites, on montre à la deuxième section que l'algorithme de Brill-Noether s'applique aussi aux courbes réduites. Il a suffi pour cela de vérifier que les théorèmes sur lesquels repose l'algorithme de Brill-Noether sont aussi valides pour les courbes réduites. Pour terminer, en utilisant l'approche géométrique proposée par D. Duval [1], on montre comment utiliser l'algorithme de Brill-Noether pour calculer les facteurs absolument irréductibles d'un polynôme à deux variables à coefficients dans le corps fini à deux éléments.

Soulignons qu'il n'a pas été question dans ce travail d'évaluer la complexité de l'algorithme de factorisation absolue basé sur l'algorithme de Brill-Noether. Il faudrait d'abord évaluer celle de l'algorithme de Brill-Noether qui repose sur la complexité du calcul des arbres de désingularisation. Selon [15], mais sans donner de démonstration, cette complexité est polynomiale en le degré de la courbe. Pour les corps de caractéristique 0 et en utilisant des techniques dites d'évaluations paresseuses, J.-P. Henry et M. Merle [8] montrent que cette complexité est polynomiale. En utilisant des techniques similaires, mais cette fois-ci avec des corps finis, Kaj Laursen [10] a montré que cette complexité est aussi polynômial.

Pour terminer, des tests comparatifs pour factoriser un polynôme à deux variables définies sur  $\mathbb{Q}$  montrent que l'algorithme de Brill-Noether est moins efficace que l'algorithme de M. van Hoeij [16] basé sur le calcul de bases intégrales. En revanche, et ce contrairement à ce dernier, l'algorithme de Brill-Noether est défini pour tout corps premier, en particulier les corps finis, et non seulement pour  $\mathbb{Q}$ .

## Bibliographie

- [1] Duval (D.). – Absolute factorization of polynomials: a geometric approach. *SIAM J. Comput.*, vol. 20, n° 1, February 1991, pp. 1–21.
- [2] Fulton (W.). – *Algebraic curves: An introduction to algebraic geometry*. – New-York, Amsterdam, W.A. Benjamin, Inc, 1969.

- [3] Gorenstein (D.). – An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc.*, vol. 72, 1952, pp. 414–436.
- [4] Haché (G.). – *Construction effective des codes géométriques*. – Thèse de doctorat, Université Pierre et Marie Curie (Paris 6), Sept. 1996.
- [5] Haché (G.). – Computation in algebraic function fields for effective construction of algebraic-geometric codes. *Lecture Notes in Computer Science*, n° 948, 1995, pp. 262–278.
- [6] Haché (G.) et Le Brigand (D.) – Effective construction of algebraic geometry codes. *IEEE Transaction on Information Theory*, vol. : 41, n° 6, 1995, pp. 1615–1628.
- [7] Hartshorne (R.). – *Algebraic Geometry*. – Springer-Verlag, 1977.
- [8] Henry (J.-P.) et Merle (M.). – Complexity of computation of embedded resolution of algebraic curves. *Lect. Notes in Comp. Sc.*, n° 378, 1987, pp. 381–390.
- [9] 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.
- [10] Laursen (K.). – The computational complexity of effective construction of geometric goppa codes. *In: Proceedings ISIT-97. IEEE.* – Ulm, Germany, July 1997.
- [11] Le Brigand (D.). – Polynomial factorization using Brill-Noether algorithm. *Lect. Notes in Comp. Sc.*, vol. 388, 1989, pp. 37–46.
- [12] Perrin (D.). – *Géométrie Algébrique*. – Paris, InterÉditions / CNRS Édition, 1995.
- [13] Shafarevich (I.). – *Basic Algebraic Geometry 1*. – Springer-Verlag, 1994, 2-ième édition.
- [14] Stichtenoth (H.). – *Algebraic function fields and codes*. – Springer-Verlag, 1993, *University Text*.
- [15] Tsfasman (M.A.) et Vlăduț (S.G.). – *Algebraic-geometric codes*. – Kluwer Academic Pub., 1991, *Math. and its Appl.*, volume 58.
- [16] van Hoeij (M.). – An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Comput.*, vol. 18, n° 4, 1994, pp. 353–363.

# Table des matières

<b>Introduction</b>	<b>1</b>
<b>1 Anneaux des fonctions de courbes planes réduites</b>	<b>2</b>
1.1 Places et diviseurs . . . . .	4
1.2 Anneaux locaux de points . . . . .	7
1.3 Points d'un anneau des fonctions d'une courbe . . . . .	10
1.4 Éclatements de points . . . . .	12
1.5 Diviseurs exceptionnels . . . . .	16
1.6 Diviseurs d'intersection . . . . .	20
1.7 Remarques sur les algorithmes de calculs . . . . .	21
<b>2 L'algorithme de Brill-Noether et les courbes réduites</b>	<b>22</b>
2.1 Le théorème fondamental de Max Noether . . . . .	22
2.2 Exemple de factorisation absolue d'un polynôme à deux variables . . . . .	24
<b>Conclusion</b>	<b>26</b>
<b>Bibliographie</b>	<b>27</b>