Master research Internship

Internship report

Une approche géométrique pour le calcul d'espaces de Riemann-Roch : algorithme et complexité

Domain: Symbolic Computation - Computational Complexity

Author:
Aude Le Gluher

Supervisor:
Pierre-Jean Spaenlehauer

Inria Nancy-Grand Est,
équipe CARAMBA

Abstract: Les espaces de Riemann-Roch sont des espaces vectoriels de dimension finie de fonctions sur une courbe algébrique dont les zéros et les pôles sont contraints. Ce document présente un algorithme géométrique probabiliste de type Las Vegas pour en calculer une base dans le cas de courbes lisses. On y prouve sa correction et on montre qu'il nécessite au plus $O((d^2 + |D|)^\omega)$ opérations arithmétiques dans le corps de base où d est le degré de la courbe et $|D|$ le nombre de points du diviseur pris en entrée comptés avec multiplicité. Deux implémentations prototypes de cet algorithme ont également été réalisées dans le langage de calcul formel Magma.

Table des matières

1 Introduction

Un résultat théorique fondamental pour les courbes algébriques est le théorème de Riemann-Roch, qui met en lien le genre d'une courbe et la dimension de certains espaces de fonctions : les espaces de Riemann-Roch. Ces derniers sont des espaces vectoriels de fonctions sur une courbe algébrique auxquelles on demande de satisfaire un certain nombre de conditions quant à la localisation et l'ordre de leurs zéros et de leurs pôles. Le calcul effectif de bases de ces espaces intervient dans des domaines variés en informatique. Du calcul dans les jacobiennes de courbes [**?**, **?**, **?**] à l'intégration symbolique de fonctions algébriques [**?**] en passant par la cryptographie [**?**] et certains codes correcteurs [**?**], le calcul d'espaces de Riemann-Roch permet de répondre à de nombreuses questions pratiques.

Deux approches sont possibles lors du calcul d'un espace de Riemann-Roch. L'une est dite arithmétique et repose sur la manipulation directe du corps de fonctions de la courbe considérée ; c'est typiquement l'approche développée par Hess dans [**?**]. L'autre est dite géométrique et s'attache plus à la manipulation de la courbe en tant qu'objet géométrique ; c'est celle adoptée entre autres par Huang et Ierardi dans [**?**] et celle sur laquelle on se concentrera dans ce document.

Donnons nous une courbe projective plane C de degré d et de genre g sur un corps $\mathbf{K}$ ainsi qu'un diviseur D sur cette courbe — c'est-à-dire une somme formelle finie à coefficients dans $\mathbf{Z}$ de points de la courbe — dont la taille $|D|$ correspond au nombre de points y intervenant, comptés avec multiplicité. Sous des hypothèses sur les singularités de la courbe, le calcul de l'espace de Riemann-Roch associé à D se fait en temps polynomial en ces trois paramètres. Plus précisément, si C est une courbe dont les points singuliers sont tous ordinaires et ont été pré-calculés, l'approche géométrique de Huang et Ierardi [**?**] donne une complexité en $O(d^6|D|^6)$ pour cette opération. Le calcul dans la jacobienne de courbes étant un cas particulier de calcul d'espaces de Riemann-Roch (en particulier dans ce cas, $|D| = O(g)$), on peut également souligner les résultats de Khuri-Makdisi [**?**], qui obtient une complexité pour l'addition et l'inversion dans la Jacobienne en $O(g^\omega)$ par un algorithme probabiliste (où $\omega \leqslant 2,38$ est la constante de l'algèbre linéaire, i.e. le plus petit k connu permettant de multiplier deux matrices de taille n en $O(n^k)$ [**?**]). Ceci améliore la complexité en $O(g^4)$ pour les mêmes opérations obtenue par Khuri-Makdisi [**?**] d'une part et Hess [**?**] d'autre part ainsi que la complexité de Volcheck en $O(\max(d, g)^7)$ [**?**]. On peut encore améliorer cette complexité de calcul dans la jacobienne pour peu que les courbes sur lesquelles on travaille présentant des spécificités ; par exemple, on peut obtenir une complexité en $\widetilde{O}(g)$ pour des courbes hyperelliptiques en utilisant l'algorithme classique de Cantor [**?**].

Dans ce document, on propose une approche géométrique pour le calcul d'espaces de Riemann-Roch dans le cas des courbes lisses. On aboutit à un algorithme probabiliste de type Las Vegas dont la complexité finale (estimée par le nombre d'opération dans le corps $\mathbf{K}$) est

$$O((d^2 + |D|)^\omega)$$

En se plaçant sous les contraintes utilisées par Huang et Ierardi [**?**] (à savoir $|D| \geqslant d^2$), on obtient donc une complexité en $O(|D|^\omega)$ qui améliore leur complexité dans le cas des courbes lisses tout du moins. Si on applique cet algorithme au calcul dans les jacobiennes de courbes planes lisses (dans ce cas, $g = \Theta(d^2)$; on suppose cette fois $|D| \leqslant d^2$) on retrouve via cet algorithme géométrique la complexité obtenue par l'algorithme arithmétique de Khuri-Makdisi en $O(g^\omega)$ [**?**]. Puisqu'on travaille sur des courbes plane lisses et que dans

ce cas $g = (d-2)(d-1)/2$, notons qu'on peut reformuler notre complexité sous la forme $O(\max(g, |D|)^\omega)$: tant que la taille du diviseur est petite devant le genre de la courbe, la complexité de l'algorithme repose sur le genre ; dès que la taille du diviseur est suffisamment grande, c'est elle qui dicte la complexité. Lors de ce stage, j'ai implémenté en Magma deux prototypes de l'algorithme décrit dans ce document disponibles aux adresses suivantes : `http://perso.eleves.ens-rennes.fr/people/Aude.Legluher/RR_ideaux.mgm` et `http://perso.eleves.ens-rennes.fr/people/Aude.Legluher/RR_polynomes.mgm`. L'une utilise une représentation des diviseurs par idéaux et semble sensiblement plus rapide que la fonction dédiée de Magma sur certains exemples ; des tests sont toujours en cours à ce sujet. L'autre utilise la représentation de diviseurs par couples de polynômes ; l'implémentation naïve du calcul de résultants et sous-résultants ne permet pas à ce code prototype de rivaliser avec les performances de l'algorithme de Magma mais une version plus efficace en C est en projet.

Dans ce rapport, on a supposé que le corps $\mathbf{K}$ de définition de nos courbes est algébriquement clos. Les expériences pratiques ont en revanche été réalisées sur des corps finis dont on a supposé le cardinal suffisamment grand. Les résultats avancés continuent d'être vérifiés dans ce cas modulo une légère adaptation des preuves proposées ici. Mais, certaines opérations comme le calcul de résultant par évaluation-interpolation deviennent problématiques lorsqu'on travaille dans un corps de trop petit cardinal. Dans ce cas, on se place classiquement dans une petite extension du corps afin d'augmenter le nombre de points disponibles : ceci n'influe que peu sur la complexité mais rajoute une technicité qui n'a pas été abordée pendant le stage. Notons aussi que certains lemmes techniques tels le lemme 22 n'ont pas encore été démontrés : il est prévu de le faire durant la fin du stage. D'autre part, on ne s'intéresse dans ce rapport qu'aux courbes lisses. Il s'agirait à l'avenir de se pencher également sur le cas des courbes singulières, notamment sur celui des courbes singulières pour lesquelles tous les points singuliers sont ordinaires à la manière de Huang et Ierardi dans [**?**]. Il serait ainsi intéressant de voir si notre algorithme (probablement légèrement modifié) continue de soutenir la comparaison avec celui de Huang et Ierardi dans ce cas. Enfin, pour ce qui est du cas des courbes singulières générales, tout reste encore à faire.

La section 2 présente les outils théoriques dont nous aurons besoin par la suite. On y introduit tout d'abord les notions nécessaires à la définition d'un espace de Riemann-Roch : courbes planes, points sur une courbe, corps des fonctions, diviseurs en suivant les définitions et preuves de [**?**]. Puis on donne un certain nombre de résultats [**?**] autour des polynômes univariés qui permettront d'une part de justifier la représentation choisie pour les diviseurs dans l'algorithme de la section 3 et d'autre part la complexité dudit algorithme. La section 3 présente les contributions. On y développe un algorithme géométrique pour le calcul d'espaces de Riemann-Roch qui a été implémenté en Magma durant le stage. On y prouve sa correction et on y détaille sa complexité.

2 Préliminaires mathématiques

Dans ce document, et pour tout la théorie, on se donne un corps $\mathbf{K}$ algébriquement clos. En pratique néanmoins on travaillera sur des corps finis (ou de petites extensions de corps finis) de sorte que les temps de calcul reflètent le nombre d'opérations dans $\mathbf{K}$. Travailler dans un corps fini demande une adaptation des notions présentées ci-dessous qu'on ne détaillera que peu dans ce rapport.

2.1 Courbes, diviseurs

Pour plus de détails sur les objets introduits dans cette partie, consulter [**?**].

2.1.1 Courbes affines, courbes projectives

On rappelle que le plan projectif $\mathbf{P}^2(\mathbf{K})$ est le quotient de $\mathbf{K}^3\backslash\{0\}$ par la relation de colinéarité sur $\mathbf{K}^3$. Autrement dit, les points de coordonnées (x, y, z) et (kx, ky, kz) avec $k \neq 0$ sont confondus dans cet espace et on notera les coordonnées (homogènes) de ce point $(x : y : z)$. Plus intuitivement, on peut voir cet espace comme le plan affine classique $\mathbf{K}^2$ auquel on rajoute on rajoute une droite de points à l'infini : ceux de coordonnées homogènes $(x : y : 0)$.

On rappelle également qu'un polynôme à n indéterminées est dit *homogène de degré d* si chacun des monômes avec un coefficient non nul y intervenant a pour degré d. Par exemple, le polynôme $X^2Z + 2YXZ - Z^3$ est homogène de degré 3 car la somme des exposants de chacun de ses monômes vaut 3. Notons qu'un polynôme P homogène de degré d à n indéterminées vérifie ainsi pour tout $\lambda \in \mathbf{K}$, $P(\lambda X_1, ..., \lambda X_n) = \lambda^d P(X_1, ...X_n)$. Cette égalité caractérise d'ailleurs les polynômes homogènes de degré d.

Une courbe projective plane est décrite par un élément de l'ensemble

$$\bigcup_{d\in\mathbf{N}^\star} \mathbf{K}_d[X, Y, Z]/\sim$$

où $\mathbf{K}_d[X, Y, Z]$ est l'ensemble des polynômes homogènes de degré d en trois variables et $\sim$ est une relation d'équivalence sur cet ensemble telle que $F \sim G \Leftrightarrow \exists\lambda \in \mathbf{K}^\star,\ F = \lambda G$. De façon similaire, une courbe affine plane est un élément non constant de $\mathbf{K}[X, Y]/\sim$. Dans un cas comme dans l'autre, le degré d'une courbe est le degré du polynôme la décrivant. On dit qu'une courbe (projective ou affine) est irréductible si le polynôme qui la décrit l'est.

Pour des raisons de lisibilité ou de praticité, on confondra parfois courbe et polynôme décrivant la courbe. Les termes *courbe affine* et *courbe projective* seront parfois confondus sous la dénomination commune courbe. Toutes les courbes seront supposées irréductibles.

On explicite à présent les liens entre courbes projectives planes et courbes affines planes :

- L'homogénéisation est une application de $\mathbf{K}[X, Y]$ dans $\mathbf{K}[X, Y, Z]$ qui à tout polynôme $\widetilde{P}(X, Y)$ associe le polynôme $P(X, Y, Z) = Z^d P(\frac{X}{Z}, \frac{Y}{Z})$ où $d = \deg(\widetilde{P})$. A priori, le polynôme homogénéisé P est un élément de $\mathbf{K}(Z)[X, Y]$ mais on peut facilement vérifier qu'il s'identifie à un élément de $\mathbf{K}[X, Y, Z]$. Le nom du processus vient du fait que le polynôme P en résultant est homogène de degré d.

- La déshomogénéisation est une application de $\mathbf{K}[X,Y,Z]$ dans $\mathbf{K}[X,Y]$ qui à tout polynôme $P(X,Y,Z)$ associe le polynôme $\widetilde{P}(X,Y) = P(X,Y,1)$.

Ces deux opérations permettent de transformer l'équation d'une courbe projective en celle d'une courbe plane et inversement. La déshomogénéisation en particulier permet de considérer uniquement la "partie affine" d'une courbe a priori projective et d'oublier toute l'information sur le comportement de la courbe à l'infini.

Exemple 1. *On considère la parabole classique dans le plan. Les points (x,y) sur cette parabole doivent vérifier $y - x^2 = 0$. Autrement dit, la courbe affine plane qu'est la parabole est le lieu des points d'annulation du polynôme $\widetilde{P}(X,Y) = Y - X^2$ (et on dit que $\widetilde{P}$ décrit la parabole). Lorsqu'on homogénéise cette courbe (i.e. qu'on homogénéise le polynôme décrivant cette courbe) on obtient d'après la définition ci-dessus $P(X,Y,Z) = YZ - X^2$. Ce polynôme décrit une courbe projective, à savoir la parabole classique projective.*

A contrario, supposons que la courbe projective décrite par $P = XZ - Y^2$ nous soit donnée de prime abord. Afin de retrouver le pendant affine de cette courbe et ainsi oublier ce qui se passe à l'infini, on aurait alors déshomogénéisé P en $\widetilde{P} = P(X,Y,1) = X - Y^2$ pour retrouver notre parabole affine.

Dans la suite, les définitions sont généralement données dans le cadre des courbes projectives. Toutefois, il est possible de ne travailler (algorithmiquement du moins, et on ne s'en privera pas dans la partie 3.2) qu'avec des courbes affines. En effet, on verra en 2.1.3 puis en 3.2 que seul un nombre fini de points d'une courbe algébrique donnée sont pertinents à nos constructions.

Si tous ces points sont affines (i.e. pas sur la droite à l'infini $Z = 0$), alors on peut alors se permettre "d'oublier" tout ce qui se passe sur la droite à l'infini sans perdre de renseignements utiles en déshomogénéisant la courbe donnée en entrée. On se retrouve ainsi à travailler avec une courbe affine.

Si certains des points pertinents sont sur la droite à l'infini, alors on peut se ramener au cas favorable où tous ces points sont affines par changement de coordonnées linéaire et inversible (voir la définition précise en section 2.3 de [**?**]). En effet, comme démontré dans [**?**] dès que le corps $\mathbf{K}$ est suffisamment grand par rapport au nombre (fini) de points pertinents, il existe un changement de coordonnées permettant à la droite à l'infini $Z = 0$ d'éviter ces points. Ce changement de coordonnées permet donc de rendre affines tous les points pertinents et d'appliquer le raisonnement précédent. Dans le cas où la taille du corps $\mathbf{K}$ ne permet pas d'utiliser ce résultat (corps trop petit), on travaille plutôt avec de petites extensions de $\mathbf{K}$. Ceci augmente le nombre de points disponibles dans le corps sans augmenter outre mesure la complexité des calculs dans ce dernier.

Définition 2. *Soit C une courbe projective plane irréductible qu'on identifie à son polynôme de définition. Le* corps des fonctions *de C est par définition*

$$\mathbf{K}(C) = \left\{ \frac{R}{S} \mid \frac{R}{S} \in \mathrm{Frac}\left(\frac{\mathbf{K}[X,Y,Z]}{(C)}\right) \text{ et } R \text{ et } S \text{ sont homogènes de même degré} \right\}$$

Remarquons que cette définition fait sens. En effet, l'irréductibilité de C implique que l'anneau $\frac{\mathbf{K}[X,Y,Z]}{(C)}$ est intègre [**?**]. On peut donc construire le corps des fractions $\mathrm{Frac}\left(\frac{\mathbf{K}[X,Y,Z]}{(C)}\right)$ de cet anneau [**?**]. On vérifie ensuite que $\mathbf{K}(C)$ est effectivement en corps.

Autrement dit, cet ensemble est formé des fractions rationnelles $\frac{R}{S}$ telles que les polynômes R et S sont considérés modulo P c'est à dire que toutes les occurrences de P dans R et S sont remplacées par 0. On peut bien sûr évaluer $\frac{R}{S}$ en tout point Q de C n'annulant pas S et ceci a un sens puisque les points de C sont justement ceux qui annulent P. Si $R(Q) = 0$ on dit que Q est un zéro de $\frac{R}{S}$ et si $S(Q) = 0$ on dit que Q est un pôle de $\frac{R}{S}$.

Exemple 3. *Reprenons l'exemple 1 et notre parabole homogénéisée, qu'on note C. Alors $\frac{YZ-2X}{X-YZ}$ est le même objet dans son corps des fonctions $\mathbf{K}(C)$ que $\frac{X^2-2X}{X-X^2}$. Le point $(1:1:1) \in C$ est un pôle de cette fonction et le point $(2:4:1) \in C$ en est un zéro.*

On notera $\mathcal{O}_Q(\mathbf{P}^2)$ l'ensemble des fonctions bien définies en le point Q ; i.e. l'ensemble des fractions rationnelles qui n'ont pas de pôle en Q.

2.1.2 Points singuliers, courbes lisses

Si C est une courbe projective décrite par $P \in \mathbf{K}[X,Y,Z]$, on note $C(\mathbf{K}) = \{(x:y:z) \in \mathbf{P}^2(\mathbf{K}) \mid P(x,y,z) = 0\}$ l'ensemble des points de C.

On observe ici l'intérêt d'avoir défini une courbe projective comme étant décrite par un polynôme *homogène*. En effet, cette propriété permet de garantir que le choix de coordonnées homogènes pour un point projectif n'influe pas sur son appartenance à une courbe projective. En effet, si $Q = (x,y,z)$ et $Q' = (\lambda x, \lambda y, \lambda z)$ (avec $\lambda \neq 0$) désignent le même point projectif, on a bien

$$\begin{aligned} Q' \in C(\mathbf{K}) &\Leftrightarrow P(Q') = 0 \Leftrightarrow P(\lambda x, \lambda y, \lambda z) = 0 \\ &\Leftrightarrow \lambda^3 P(x,y,z) = 0 \text{ par homogénéité de } P \\ &\Leftrightarrow P(Q) = 0 \Leftrightarrow Q \in C \text{ car } \lambda \neq 0 \end{aligned}$$

Un point projectif $(x:y:z)$ est dit singulier s'il est tel que

$$\frac{\partial P}{\partial X}(x,y,z) = \frac{\partial P}{\partial Y}(x,y,z) = \frac{\partial P}{\partial Z}(x,y,z) = 0$$

On dit qu'une courbe est lisse si tous ses points sont non singuliers (on dit aussi *réguliers*).

De même, on définit les points d'une courbe affine par C décrite par $P \in \mathbf{K}[X,Y]$ par $C(\mathbf{K}) = \{(x,y) \in \mathbf{K}^2 \mid P(x,y) = 0\}$. Un point affine de la courbe est dit singulier s'il vérifie $\partial P/\partial X(x,y) = \partial P/\partial Y(x,y) = 0$ et régulier sinon.

Remarque 4. *La notion de point telle que définie ci-dessus ne vaut que lorsque $\mathbf{K}$ est algébriquement clos. Un point affine (par exemple) est en fait défini comme un idéal maximal de $\mathbf{K}[X,Y]/(P)$. Dans le cas où $\mathbf{K}$ est algébriquement clos, un tel idéal est nécessairement de la forme $\langle X-u, Y-v\rangle$ et on peut donc l'assimiler à (u,v).*

Lorsque $\mathbf{K}$ est fini, les points affines sont toujours les idéaux maximaux $\mathbf{K}[X,Y]/(P)$ mais il n'ont plus forcément cette forme particulière. On donne d'ailleurs à ces objets le nom de

places *plutôt que de* points. *Points et places se comportent similairement : afin de ne pas brouiller le propos, on continue de considérer* $\mathbf{K}$ *algébriquement clos afin de ne parler que de points. Pour plus de détails voir [?].*

On présente ci-après une bonne propriété des points réguliers.

Définition 5. *Un anneau* A *est dit* anneau de valuation discrète *(DVR) si*

$$\exists u \in A, \forall a \in A \backslash \{0\}, \exists k \in \mathbf{N} \text{ et } a' \in A^\star \text{ tels que } a = u^k a'$$

L'élément u est appelé une uniformisante et l'entier k est la valuation de a. Cet entier ne dépend en fait pas du choix de u et on utilisera sans démonstration toutes ses propriétés (plus détails en section 2.5 de [?]) . Par exemple, l'anneau $\mathbf{R}[[X]]$ est un anneau de valuation discrète dont X est une uniformisante. On peut penser à ces anneaux comme à des structures dans lesquelles, dans tout élément, on peut factoriser au maximum vis-a-vis d'un certain même élément de l'anneau. Un avantage des points réguliers est le suivant (énoncé et preuve du fait suivant peuvent être trouvés en section 3.2 de [?])

Proposition 6. *Soit* $Q = (u, v)$ *un point régulier d'une courbe* C *décrite par* $P \in \mathbf{K}[X, Y]$. *Alors, le localisé de l'anneau* $\mathbf{K}[X, Y]/(P)$ *par rapport à l'idéal* $\langle X - u, Y - v \rangle$ *correspondant au point* Q, *c'est-à dire l'anneau* $\mathcal{O}_Q(C) = \{R/S \in \mathbf{K}(C) \mid S(Q) \neq 0\}$ *est un anneau de valuation discrète.*

Remarque 7. *Cette propriété permet de définir la multiplicité d'un point pour un élément de* $\mathbf{K}(C)$. *Si* f *est une fonction sur la courbe* C *et* Q *un point régulier de* C *qui n'est pas un pôle de* f, *on peut alors considérer* f *comme un élément du localisé de* $\mathbf{K}[X, Y]/(F)$ *par rapport à* Q. *Comme* Q *est régulier, ce localisé est un DVR par la proposition 6. On peut donc parler de la valuation de* f *dans ce DVR et on lui donne le nom de* multiplicité de P dans f. *On note cet entier* $\mathrm{ord}_P(f)$.

Par la suite, on ne travaillera qu'avec des courbes non seulement irréductibles mais aussi lisses.

2.1.3 Diviseurs

On se donne une courbe projective lisse et irréductible C.

Un diviseur D de la courbe C est une somme formelle de points de C à coefficients dans $\mathbf{Z}$ et à support fini i.e. une somme du type $\sum_{P \in C(\mathbf{K})} n_P P$ où les n_P sont des entiers tous nuls sauf pour un nombre fini de points P. L'ensemble des diviseurs d'une courbe muni de la loi $+$ forme un groupe abélien noté $\mathrm{Div}(C)$. On définit aussi :

- Le degré du diviseur D, noté $\deg(D)$ par : $\deg(D) = \sum_{P \in C(\mathbf{K})} n_P$.
- La taille du diviseur D, notée $|D|$ par : $|D| = \sum_{P \in C(\mathbf{K})} |n_P|$.
- Le support du diviseur D, noté $\mathrm{Supp}(D)$ par $\mathrm{Supp}(D) = \{P \in C(\mathbf{K}) \mid n_P \neq 0\}$.

- Un ordre sur $\mathrm{Div}(C)$: $D' = \sum_{P \in C(\mathbf{K})} n'_P P$ est plus grand que le diviseur D si pour tout P, $n'_P \geqslant n_P$.
- Un diviseur est dit effectif si tous les n_P non nuls sont positifs.

Remarque 8. *Tout diviseur peut s'écrire sous la forme $D = D_+ - D_-$ avec D_+ et D_- deux diviseurs effectifs : il suffit de regrouper les termes ayant un coefficient positif dans D_+ et ceux ayant un coefficient négatif dans D_- par exemple. Si les supports de D_+ et D_- sont disjoints, cette décomposition est même unique. Comme on le verra dans la section 3.1, on préfère travailler avec des diviseurs effectifs qu'avec des diviseurs quelconques ; aussi, on utilisera systématiquement cette décomposition.*

Exemple 9. *On continue de filer l'exemple 1. Les deux points (projectifs) $P = (0 : 1 : 1)$ et $Q = (3 : 4 : 5)$ sont sur la courbe $X^2 + Y^2 - Z^2 = 0$. La somme formelle $D = 3P - 2Q$ est donc un diviseur de cette courbe. Son degré vaut* 1. *Il est plus grand que le diviseur $-4Q$.*

On définit aussi le diviseur associé à un élément f de $\mathbf{K}(C)$. Il s'agit de la somme formelle

$$(f) = \sum_{P \in C(\mathbf{K})} \mathrm{val}_P(f) P$$

où $\mathrm{val}_P(f)$ est l'ordre de P pour f et vaut la multiplicité de P dans f si P n'est pas un pôle de f et l'opposé de la multiplicité de P dans $1/f$ sinon. Intuitivement, l'entier $\mathrm{val}_P(f)$ correspond à combien de fois il est possible de factoriser le facteur relatif à P dans f, à la manière dont on dirait que 3 est l'ordre de 4 dans le polynôme $(X-4)^3(X+2)^2$.

Proposition 10. *Soit C une courbe projective irréductible lisse et $f \in \mathbf{K}(C)$. Alors :*
- *Le diviseur (f) est bien défini.*
- *Le degré du diviseur (f) est nul.*
- *Pour toutes fonctions $f, g \in \mathbf{K}(C)$, $(fg) = (f) + (g)$ et $(f/g) = (f) - (g)$.*
- *Deux fonctions non nulles ont même diviseur si et seulement si elles sont proportionnelles.*

Démonstration. Soit $f \in \mathbf{K}(C)$. Comme f a un nombre fini de zéros et de pôles et que la valuation de f en un point qui n'est ni zéro ni pôle est nulle, la somme $\sum_{P \in C(\mathbf{K})} \mathrm{val}_P(f) P$ est effectivement à support fini : c'est donc bien un diviseur de C.

Comme $f \in \mathbf{K}(C)$, il existe R et S deux polynômes homogènes de même degrés (modulo le polynôme décrivant C) tel que $f = R/S$. Le théorème de Bézout (section 5.3 de [**?**]) assure que le nombre de points d'intersection comptés avec multiplicité entre la courbe décrite par R et C — c'est-à-dire le nombre de zéros de R comptés avec multiplicité — vaut $\deg(R)\deg(C)$. De la même façon, le nombre de zéros de S vaut $\deg(S)\deg(C)$. Comme $\deg(R) = \deg(S)$, on obtient que R et S ont le même nombre de zéros comptés avec multiplicités donc que f a exactement autant de pôles que de zéros, toujours comptés avec multiplicités. D'où un degré nul pour (f).

Le troisième point découle immédiatement des propriétés d'une valuation (voir [**?**]).

Le quatrième se déduit du troisième. Si $(f) = (g)$ alors $(f/g) = 0$ donc f/g n'a ni zéros ni pôles donc est constante. Réciproquement, deux fonctions proportionnelles ont exactement les mêmes zéros et pôles donc même diviseur.

□

Un diviseur D de C est dit principal si il existe $f \in \mathbf{K}(C)$ tel que $D = (f)$. On peut alors quotienter le groupe des diviseurs de C par le sous groupe des diviseurs principaux de C. Ce quotient est le groupe de Picard de C. Deux diviseurs D et D' tels qu'il existe $f \in \mathbf{K}(C)$ vérifiant $D - D' = (f)$ sont donc confondus dans le groupe de Picard de C : on dit qu'ils sont équivalents et on note $D \sim D'$.

On définit enfin le diviseur associé à un polynôme homogène $f \in \mathbf{K}[X, Y, Z]$ non multiple de C : c'est le diviseur $(f) = \sum_{P \in C(\mathbf{K})} \mathrm{ord}_P(f)P$.

C'est une définition identique à celle pour une fonction à l'exception de l'absence de pôles.

2.1.4 Espaces et théorème de Riemann-Roch

Définition 11. *Soit D est un diviseur d'une courbe projective irréductible et lisse C. L'espace de Riemann-Roch $L(D)$ associé à D est l'espace vectoriel*

$$L(D) = \{f \in \mathbf{K}(C)\backslash\{0\} | (f) + D \geqslant 0\} \cup \{0\}$$

Démonstration. Pour que cette définition fasse sens, il faut vérifier que l'ensemble décrit est effectivement un espace vectoriel (pour l'addition et la multiplication par un élément de $\mathbf{K}$). L'addition est interne par propriété d'une valuation ([**?**]) ; la multiplication par un scalaire aussi puisqu'elle ne change pas les zéros et pôles d'une fonction. La structure $(L(D), +)$ est effectivement un groupe dont 0 est le neutre. La multiplication par un scalaire est associative, distributive par rapport à + et dispose d'un neutre : l'élément neutre de $\mathbf{K}$. Tous les axiomes d'un espace vectoriel sont ainsi vérifiés.

□

Exemple 12.

- *Si $D = 0$ alors $L(D) = \mathbf{K}$. En effet, si $f \in L(D)$ n'est pas nul, on doit avoir $(f) \geqslant 0$. Cela implique que $\deg((f)) \geqslant \deg(0) = 0$. Or, (f) est principal donc de degré nul donc le degré de f est exactement égal à zéro : f est une fraction rationnelle n'ayant aucun zéro et aucun pôle. Donc $f \in \mathbf{K}(C)^\times$. D'où le résultat.*
- *Si $\deg(D) < 0$ alors $L(D) = \{0\}$. Par l'absurde, si $f \in L(D)\backslash\{0\}$ alors $(f) \geqslant -D$ et en prenant les degrés, tout en se rappelant que (f) est principal, on a $0 \geqslant -\deg(D)$ c'est-à-dire $\deg(D) \geqslant 0$ ce qui est une contradiction.*
- *Un exemple moins trivial : Pour $D = 3P - 2Q$ (cf exemple précédent), si $f \in L(D)$, on doit avoir $(f) \geqslant -D$ donc $\mathrm{ord}_f(P) \geqslant -3$ et $\mathrm{ord}_f(Q) \geqslant 2$. Autrement dit, $L(D)$ est l'ensemble des fractions rationnelles qui ont un pôle en P d'ordre au plus 3 et un zéro d'ordre au moins 2 en Q.*

Observons que si on utilise la décomposition d'un diviseur D en $D_+ - D_-$ comme vu à la remarque 8, une fonction f appartient à $L(D)$ si $(f) \geqslant D_- - D_+$. Ainsi, le diviseur D_+ contraint les pôles de f et le diviseur D_- en contraint les zéros.

Ces espaces de Riemann-Roch sont non seulement des espaces vectoriels mais des espaces vectoriels de dimension finie. Le théorème de Riemann (section 8.3 de [**?**]) donne un minorant de la dimension de ces espaces :

Théorème 13. *Soit D un diviseur d'une courbe projective lisse et irréductible C de genre g. Alors,*

$$\dim(L(D)) \geqslant \deg(D) + 1 - g$$

Cette inégalité devient d'ailleurs une égalité lorsque $\deg(D) > 2g - 2$. Le théorème de Riemann-Roch (section 8.6 de [**?**]) explicite la différence entre $\dim(L(D))$ et $\deg(D) + 1 - g$ permettant ainsi d'avoir une égalité pour $\dim(L(D))$ dans tous les cas.

Ce résultat est théorique : il n'exhibe pas explicitement une base de $L(D)$ ayant le bon cardinal. L'objectif de ce stage est de construire explicitement une telle base de manière efficace.

2.1.5 Autour du théorème des résidus

L'algorithme 1 présenté en 3.2 consiste à construire des éléments de l'espace de Riemann-Roch $L(D)$ qu'on souhaite déterminer. Afin de montrer que ces éléments engendrent tout $L(D)$ on aura besoin d'un résultat technique : le théorème des résidus. On énonce ce théorème dans le cas de courbes lisses en adaptant et reformulant la preuve que l'on peut trouver dans [**?**] à la section 8.1. Il s'appuie sur le théorème de Max Noether qu'on énonce sans démontrer (preuve dans la section 5.5 de [**?**]). Dans cette partie on identifie courbe plane et polynôme la définissant par abus de notation.

Définition 14. *Si F est une courbe de degré d et P un point de $\mathbf{P}^2$, on note $F_\star = F/L^d \in \mathbf{K}(\mathbf{P}^2)$ où L est un polynôme homogène de degré un ne s'annulant pas en P.*

Cette définition appelle plusieurs remarques :

- On remarque que $F_\star \in \mathcal{O}_P(\mathbf{P}^2)$ puisque L est choisie justement pour que $F_\star$ n'ait pas de pôle en P. Cette transformation de F permet de la considérer comme une fonction rationnelle bien définie localement en P.
- La fonction $F_\star$ dépend du choix de L. Toutefois si on choisit une autre droite $L' \neq L$ ne passant pas par P, on a alors $\frac{F}{L'^d} = \left(\frac{L}{L'}\right)^d F_\star$. Or $\left(\frac{L}{L'}\right)^d$ est un élément inversible dans $\mathcal{O}_P(\mathbf{P}^2)$. Ainsi, $\frac{F}{L^d}$ et $\frac{F}{L'^d}$ ont le même comportement localement en P.

Définition 15. *(Conditions de Noether) Soit $P \in \mathbf{P}^2$, F et G deux courbes sans composante commune (i.e. ces polynômes n'ont pas de facteur commun non trivial) et H une troisième courbe. On dit que les conditions de Max Noether sont vérifiées en P pour F, G et H si $H_\star \in \langle F_\star, G_\star \rangle$. Cette condition signifie qu'il existe A et $B \in \mathcal{O}_P(\mathbf{P}^2)$ tels que $H_\star = AF_\star + BG_\star$ dans $\mathcal{O}_P(\mathbf{P}^2)$.*

Théorème 16. *(Théorème de Max Noether)*
Soit F,G et H trois courbes projectives planes telles que F et G n'ont pas de composantes communes. Alors les deux propositions sont équivalentes :

(1) Les conditions de Noether sont satisfaites en tout point de $F \cap G$;

(2) Il existe deux polynômes homogènes A et B de degrés respectifs $\deg(H) - \deg(F)$ *et* $\deg(H) - \deg(G)$ *tels que $H = AF + BG$.*

La démonstration de ce théorème est ici admise ; on peut la trouver à la section 5.5 de [**?**]. Voici néanmoins quelques explications à son propos :

- L'implication de (1) vers (2) est le sens qui permet de démontrer le théorème des résidus et donc celui qui nous intéresse ici. Plus intuitivement, elle signifie que, dès lors que H est localement en tout point dans l'idéal engendré par F et G on a en fait que H est globalement dans l'idéal engendré par F et G.
- L'implication de (2) vers (1) est plus directe. En effet, si $H = AF + BG$ et $P \in F \cap G$, choisissons une droite L ne passant pas par P. En divisant notre égalité par $L^{\deg(H)}$ on obtient immédiatement que

$$\frac{H}{L^{\deg(H)}} = \frac{A}{L^{\deg(H)-\deg(F)}} \times \frac{F}{L^{\deg(F)}} + \frac{B}{L^{\deg(H)-\deg(G)}} \times \frac{G}{L^{\deg(G)}}$$

  ce qui se réécrit

$$H_\star = \underbrace{\frac{A}{L^{\deg(H)-\deg(F)}}}_{\in \mathcal{O}_P(\mathbf{P}^2) \text{ car } L(P)\neq 0} \times F_\star + \underbrace{\frac{B}{L^{\deg(H)-\deg(G)}}}_{\in \mathcal{O}_P(\mathbf{P}^2) \text{ car } L(P)\neq 0} \times G_\star$$

  ce qui veut exactement dire que les conditions de Noether sont vérifiées en P.
- Lorsque $P \notin F \cap G$, les conditions de Noether en P sont obligatoirement vérifiées pour F, G et H. En effet, supposons par symétrie que $P \notin F$. Alors $F(P) \neq 0$ se qui signifie que F est inversible dans $\mathcal{O}(\mathbf{P}^2)$ et implique qu'il existe $A \in \mathcal{O}(\mathbf{P}^2)$ tels que $AF_\star = 1$ (où 1 est l'élément neutre de $\mathcal{O}(\mathbf{P}^2)$). On en déduit que $H_\star = 1 \times H_\star = (AF_\star) \times H_\star = (AH_\star) \times F_\star + 0 \times G_\star$: c'est la condition de Noether en P.

Théorème 17. *(Théorème des résidus) Soit C une courbe projective plane et lisse. Soit D et D' deux diviseurs effectifs et équivalents de C et A un diviseur effectif de C. S'il existe un polynôme homogène G tel que $(G) = D + A$ alors il existe un polynôme G' de même degré que G vérifiant $(G) = D' + A$.*

Démonstration. Notons F le polynôme décrivant la courbe C.

Comme D et D' sont équivalents, il existe H et H' de même degré (voir la définition 2) tels que $D - D' = \left(\frac{H}{H'}\right)$ ce qui se réécrit $D + (H) = D' + (H')$

L'idée de la démonstration est de montrer qu'on peut appliquer le théorème de Max Noether aux polynômes (décrivant certaines courbes planes) GH, H' et F. En effet si les conditions de Noether sont vérifiées pour ces trois polynômes, ledit théorème garantit alors l'existence de deux polynômes G' et F' tels que $GH = G'H' + FF'$ avec $\deg(G') = \deg(G)$ en particulier. Cette égalité permet de conclure en remarquant que :

$$\begin{aligned}(G') &= (GH) - (H') = (G) + (H) - (H') \\ &= D + A + (H) - (H') \text{ par définition de } (G) \\ &= D' + (H') + A - (H') \text{ puisque } D + (H) = D' + (H') \\ &= D' + A\end{aligned}$$

Il ne reste donc plus qu'à montrer que les conditions de Noether sont vérifiées pour tout point d'intersection des courbes décrites par H' et F. Ce fait vient d'une inégalité due au caractère effectif des diviseurs A et D'. En effet, de l'effectivité de ces deux diviseurs il découle :

$$(GH) = (G) + (H) = D + (H) + A = D' + (H') + A \geqslant (H')$$

On en déduit que pour tout point $P \in H' \cap F$, la multiplicité de P dans GH est supérieure à celle de P dans H' et garantit que les conditions de Noether sont vérifiées en P.

□

2.2 Polynômes univariés et complexité

2.2.1 Lemme de Hensel

On présente ici un lemme théorique qui permettra de justifier l'utilisation de la représentation pour les diviseurs décrite dans la section 3.1. Pour plus de précisions sur le complété d'un anneau et sur le lemme de Hensel en général consulter [**?**].

Lemme 18. *(lemme de Hensel)*
Soit f un polynôme irréductible de $\mathbf{K}[X]$ et A l'anneau $\mathbf{K}[X]$ complété par rapport à l'idéal $\langle f \rangle$. Soit $F \in A[Y]$ et $g \in A$ tels que $F(g(X)) \equiv 0$ mod $F'(g(X))^2 f(X)$ et $F'(g(X))$ n'est pas un diviseur de zéro dans A. Alors il existe un unique $\tilde{g} \in A$ tel que $F(\tilde{g}(X)) = 0$ dans A et vérifiant de plus $\tilde{g} \equiv g$ mod $F'(g(X))f(X)$.

On admet ce lemme (pour une preuve, voir le théorème 7.3 de [**?**]). Afin de l'exploiter plus facilement dans la section 3.1, on travaille dans la suite de cette partie pour aboutir à une formulation plus simple et directement utilisable.

Lemme 19. *Soit f un polynôme irréductible de $\mathbf{K}[X]$, A l'anneau $\mathbf{K}[X]$ complété par rapport à l'idéal $\langle f \rangle$ et g un élément de A. Si $g \not\equiv 0$ mod f, alors g est inversible dans A.*

Démonstration. Comme f est irréductible, l'hypothèse $g \not\equiv 0 \bmod f$ se réécrit g est inversible modulo f. Afin de montrer que g est inversible dans A il suffit de montrer que pour tout $k \in \mathbf{N}^\star$, g est inversible modulo f^k.

Pour ce faire, on montre par récurrence sur $k \in \mathbf{N}$ que g est inversible modulo f^{2^k}.

Cette propriété est effectivement vérifiée pour $k = 0$ par hypothèse. Montrons l'hérédité. Supposons que g est inversible modulo f^{2^k}. Alors il existe $h, l \in A$ tels que $gh = 1 + f^{2^k} l$. Montrons que $\tilde{h} = h - (gh - 1)h$ est un inverse pour g modulo $f^{2^{k+1}}$. C'est effectivement le cas car

$$\begin{aligned}
\tilde{h}g &= hg - (gh - 1)hg \\
&= hg - (gh - 1)(1 + f^{2^k} l) \\
&= 1 + f^{2^k} l(1 - gh) \text{ après simplification} \\
&= 1 - (l f^{2^k})^2 \\
&= 1 + l^2 f^{2^{k+1}} \equiv 1 \bmod f^{2^{k+1}}
\end{aligned}$$

On déduit immédiatement de cette récurrence que pour tout $k \in \mathbf{N}^\star$, g est inversible modulo f^k ce qui conclut.

□

Corollaire 20. *Soit C une courbe affine plane lisse et irréductible sur $\mathbf{K}$, f un polynôme irréductible de $\mathbf{K}[X]$, k un entier naturel non nul et D un diviseur de C. On note (x_i, y_i) les coordonnées des n points P_i distincts intervenant dans le diviseur D et $f = \prod_{i=1}^{n}(X - x_i)$. On suppose que pour tout $i \in [\![1, n]\!]$, la tangente à C en P_i n'est pas verticale.*

Si il existe $g \in \mathbf{K}[X]$ vérifiant la congruence $C(X, g(X)) \equiv 0$ mod $f(X)$ et les égalités $g(x_i) = y_i$ pour tout i alors il existe un unique $\tilde{g}$ vérifiant la congruence $C(X, \tilde{g}(X)) \equiv 0$ mod $f^k(X)$ et les mêmes égalités que g.

Démonstration. Cette propriété découle du lemme de Hensel (lemme 18) et du lemme 19.

On cherche à appliquer le lemme de Hensel au polynôme $C(X, Y) \in A[Y]$ où A est le complété de $\mathbf{K}[X]$ par rapport à f. Pour ce faire, il suffit de vérifier que $C(X, g(X)) \equiv 0 \bmod \partial C/\partial Y(X, g(X))^2 f(X)$. Comme on sait déjà que $C(X, g(X)) \equiv 0 \bmod f(X)$, il ne reste qu'à montrer que $\partial C/\partial Y(X, g(X))$ est inversible dans A. D'après le lemme 19, ce fait sera acquis si on montre que $\partial C/\partial Y(X, g(X)) \not\equiv 0 \bmod f(X)$.

Or, pour tout $i \in [\![1, n]\!]$, l'évaluation de $\partial C/\partial Y(X, g(X))$ modulo $(X - x_i)$ donne

$$\frac{\partial C}{\partial Y}(x_i, g(x_i)) = \frac{\partial C}{\partial Y}(x_i, y_i)) \neq 0$$

par définition de g et en utilisant le fait que la tangente à C en $P_i = (x_i, y_i)$ n'est pas verticale. Comme les x_i sont deux à deux distincts, les $X - x_i$ sont deux à deux premiers entre eux et des congruences $\partial C/\partial Y(X, g(X)) \not\equiv 0 \bmod (X - x_i)$ on peut ainsi déduire par théorème chinois [**?**] que $\partial C/\partial Y(X, g(X)) \not\equiv 0 \bmod f(X)$.

On peut donc bien appliquer le lemme de Hensel et ce dernier assure l'existence et l'unicité (car $\partial C/\partial Y(X, g(X))$ n'est pas un diviseur de zéro puisque inversible) d'un $\tilde{g} \in A$ vérifiant $C(X, \tilde{g}(X)) = 0$ dans A et $\tilde{g} \equiv g \bmod \partial C/\partial Y(X, g(X))f(X)$. Comme $\partial C/\partial Y(X, g(X))$ est inversible, cette dernière congruence peut se réécrire $\tilde{g} \equiv g \bmod f$.

Ne reste qu'à vérifier que $\tilde{g}$ vérifie les propriétés attendues. Comme pour tout i on a $X - x_i | f$, on a que $\tilde{g} \equiv g \bmod X - x_i$ ce qui se réécrit $\tilde{g}(x_i) = g(x_i) = y_i$ par hypothèse sur g. D'autre part, par définition du complété de $\mathbf{K}[X]$ par rapport à f, l'égalité $C(X, \tilde{g}(X)) = 0$ implique que pour tout $k \in \mathbf{N}^\star$ la congruence $C(X, g(X)) \equiv 0 \bmod f^k$ est vérifiée, ce qui conclut. □

2.2.2 Résultants et sous-résultants

On présente ici rapidement les notions de résultant et de sous-résultant tout d'abord dans le cas de polynômes univariés puis bivariés. Pour plus de précisions sur la théorie et la pratique des résultants, consulter la section I.6 de [**?**] ou encore [**?**].

Soit $\mathbf{A}$ un anneau commutatif unitaire [**?**]. On se donne deux polynômes non constants de $\mathbf{A}[X]$, $f = \sum_{i=0}^{m} \alpha_i X^i$ et $g = \sum_{i=0}^{n} \beta_i X^i$ de degrés respectifs m et n tous deux non nuls.

On appelle résultant de f et g, noté $\mathrm{Res}(f, g)$, le déterminant suivant :

$$\left.\begin{vmatrix}
\alpha_m & 0 & \cdots & 0 & 0 & \beta_n & 0 & \cdots & 0 & 0 \\
\alpha_{m-1} & \alpha_m & \ddots & \vdots & \vdots & \beta_{n-1} & \beta_n & \ddots & \vdots & \vdots \\
\vdots & \alpha_{m-1} & \ddots & 0 & \vdots & \vdots & \beta_{n-1} & \ddots & 0 & \vdots \\
\vdots & \vdots & \ddots & \alpha_m & 0 & \vdots & \vdots & \ddots & \beta_n & 0 \\
\alpha_1 & \vdots & \vdots & \alpha_{m-1} & \alpha_m & \beta_1 & \vdots & \vdots & \beta_{n-1} & \beta_n \\
\alpha_0 & \alpha_1 & \vdots & \vdots & \alpha_{m-1} & \beta_0 & \beta_1 & \vdots & \vdots & \beta_{n-1} \\
0 & \alpha_0 & \ddots & \vdots & \vdots & 0 & \beta_0 & \ddots & \vdots & \vdots \\
\vdots & 0 & \ddots & \alpha_1 & . & \vdots & 0 & \ddots & \beta_1 & 0 \\
\vdots & \vdots & \ddots & \alpha_0 & \alpha_1 & \vdots & \vdots & \ddots & \beta_0 & \beta_1 \\
0 & 0 & \cdots & 0 & \alpha_0 & 0 & 0 & \cdots & 0 & \beta_0
\end{vmatrix}\right\} m{+}n \text{ lignes}$$

n colonnes — m colonnes

La matrice dont le résultant est le déterminant est appelé matrice de Sylvester. tu

On définit de façon semblable le dernier sous-résultant de f et g. C'est un élément de $\mathbf{A}[Y]$ égal au déterminant de la matrice suivante :

$$\left.\begin{vmatrix}
\alpha_m & 0 & \cdots & 0 & 0 & \beta_n & 0 & \cdots & 0 & 0 \\
\alpha_{m-1} & \alpha_m & \ddots & \vdots & \vdots & \beta_{n-1} & \beta_n & \ddots & \vdots & \vdots \\
\vdots & \alpha_{m-1} & \ddots & 0 & \vdots & \vdots & \beta_{n-1} & \ddots & 0 & \vdots \\
\vdots & \vdots & \ddots & \alpha_m & 0 & \vdots & \vdots & \ddots & \beta_n & 0 \\
\alpha_2 & \vdots & \vdots & \alpha_{m-1} & \alpha_m & \beta_2 & \vdots & \vdots & \beta_{n-1} & \beta_n \\
\alpha_1 & \alpha_2 & \vdots & \vdots & \alpha_{m-1} & \beta_1 & \beta_2 & \vdots & \vdots & \beta_{n-1} \\
\alpha_0 & \alpha_1 & \ddots & \vdots & \vdots & \beta_0 & \beta_1 & \ddots & \vdots & \vdots \\
\vdots & \alpha_0 & \ddots & \alpha_2 & . & \vdots & \beta_0 & \ddots & \beta_1 & 0 \\
\vdots & \vdots & \ddots & \alpha_1 & \alpha_2 & \vdots & \vdots & \ddots & \beta_1 & \beta_2 \\
0 & 0 & \cdots & \alpha_0 Y & \alpha_1 Y + \alpha_0 & 0 & 0 & \cdots & \beta_0 Y & \beta_1 Y + \beta_0
\end{vmatrix}\right\} m{+}n\text{-}2 \text{ lignes}$$

$n{-}1$ colonnes — $m{-}1$ colonnes

En développant ce déterminant par rapport à la dernière ligne on constate que le dernier sous-résultant de f et g est linéaire en Y.

Si maintenant f et g sont deux polynômes de $\mathbf{K}[X, Y]$. Le résultant par rapport à Y de f et g noté $\mathrm{Res}_Y(f, g)$ est par définition le résultant (au sens vu précédemment) de f et g vus comme éléments de $\mathbf{K}[X][Y]$. Ce résultant est ainsi le déterminant d'une matrice ayant pour coefficients des éléments de $\mathbf{K}[X]$. On en déduit que $\mathrm{Res}_Y(f, g)$ est un polynôme de $\mathbf{K}[X]$. De même pour le dernier sous-résultant de f et g qui est ainsi un polynôme de $\mathbf{K}[X, Y]$, linéaire en Y.

On présente ici deux lemmes permettant pour l'un de justifier une étape de la complexité de l'algorithme 1 et pour l'autre d'éclairer un étape de la correction du même algorithme. La formalisation des preuves de ces lemmes n'a pas été entièrement faite durant le stage, on pourra néanmoins trouver de bonnes pistes de preuves dans [**?**].

Lemme 21. *Le résultant de deux polynômes f et g de $\mathbf{K}[X,Y]$ a un degré inférieur à $\deg_X(f)\deg_Y(g) + \deg_Y(f)\deg_X(g)$ où $\deg_X$ et $\deg_Y$ donnent respectivement les degrés en X et en Y de leur argument. Le dernier sous-résultant de f et g est un polynôme de la forme $a(X)Y - b(X)$ avec a inversible modulo $\mathrm{Res}_Y(f,g)$ et b/a mod $\mathrm{Res}_Y(f,g)$ un polynôme de degré en $O(\deg_X(f)\deg_Y(g) + \deg_Y(f)\deg_X(g))$.*

Démonstration. La première partie du résultat peut se montrer à partir de l'expression du résultant donnée ci-dessus. Ce résultant est par définition le déterminant d'une matrice carrée de taille $\deg_Y(f) + \deg_Y(g)$ contenant pour les $\deg_Y(g)$ premières colonnes des polynômes de degré majoré par $\deg_X(f)$ et dans des $\deg_Y(f)$ dernières colonnes des polynômes de degré majoré par $\deg_X(g)$. En utilisant l'expression $\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$ pour le déterminant d'une matrice A de taille n, on constate que chaque terme de cette somme dans le cas du résultant a un degré inférieur à $\deg_X(f)\deg_Y(g) + \deg_Y(f)\deg_X(g)$ ce qui conclut.

Pour la deuxième partie, il s'agit de montrer que le coefficient de Y dans le sous-résultant est inversible (puisqu'on sait déjà que le sous-résultant est linéaire en Y). Cette partie a été abordée pendant le stage mais pas formalisée.

□

Lemme 22. *Soit $C(X,Y) = Y^k + f(X,Y)$ un polynôme de $\mathbf{K}[X,Y]$ tel que le degré en Y de f soit strictement inférieur à k et h un polynôme de $\mathbf{K}[X,Y]$. Notons I l'idéal $\langle C\rangle + \langle h\rangle$. Alors $\mathrm{Res}_Y(C,h)$ est un générateur de $I \cap \mathbf{K}[X]$ et le dernier sous-résultant de C et h est un élément de I.*

Démonstration. Le fait que $\mathrm{Res}_Y(C,h)$ appartienne à $I \cap \mathbf{K}[X]$ découle immédiatement des propriétés du résultant (voir [**?**], proposition 6.7) ; de même pour l'appartenance du dernier sous-résultant à I. Il resterait encore à montrer que tout élément de $I \cap \mathbf{K}[X]$ est multiple du résultant pour conclure.

□

2.2.3 Complexité d'opérations polynomiales

Comme on le verra en section 3.2, l'algorithme de calcul d'espaces de Riemann-Roch qu'on y présente utilise intensivement un certain nombre d'opérations sur les polynômes univariés. Afin d'étudier la complexité de cet algorithme (en section 3.4), on expose ici brièvement les complexités des opérations qui y interviennent. Pour plus de détails on pourra consulter [**?**] notamment la section I.

On se donne f et g deux polynômes de $\mathbf{K}[X]$. Les complexités des opérations suivantes seront exprimées en fonction des degrés de ces polynômes et correspondent au nombre d'opérations réalisées dans $\mathbf{K}$ lors du calcul.

Le calcul de $f \wedge g$ et de $g \bmod f$ et de l'inverse de g modulo f reviennent à faire un algorithme d'Euclide (éventuellement étendu) ce qui peut se faire en $\widetilde{O}(\max(\deg(f),\deg(g)) = \widetilde{O}(\deg(f) + \deg(g))$ grâce à des algorithmes rapides [**?**]. On obtient la même complexité pour le calcul du produit de f et g.

Pour calculer une solution d'un système de trois congruences $\begin{cases} h \equiv g_1 \bmod f_1 \\ h \equiv g_2 \bmod f_2 \\ h \equiv g_3 \bmod f_3 \end{cases}$

on peut procéder de la manière suivante. On cherche la solution sous la forme $h = \alpha + \beta f_1 + \gamma f_1 f_2$ et on injecte cette expression dans la première équation pour trouver que $\alpha = g_1$ convient. Forts de cette information, on injecte notre nouvelle expression pour trouver que $\beta f_1 \equiv g_2 - \alpha \bmod f_2$ et on s'est donc ramené à un calcul de l'inverse de f_1 modulo f_2 pour trouver un β qui convienne (puisque α est maintenant connu). Puis, on remplace dans la dernière équation ce qui donne $\gamma f_1 f_2 \equiv g_3 - \alpha - \beta f_1 \bmod f_3$. Tout est connu ici sauf γ qui s'obtient en calculant l'inverse de $f_1 f_2$ modulo f_3. On constate donc que trouver une solution à un tel système revient à calculer deux inverses c'est-à-dire à appliquer deux fois un algorithme d'Euclide étendu dont on a déjà donné la complexité ci-dessus.

On aura également besoin dans cet algorithme de calculer certains résultants et sous-résultants de polynômes f et g de $\mathbf{K}[X, Y]$.

Pour calculer le résultant des polynômes f et g on ne calcule pas le déterminant présenté en section 2.2.2. A la place, on procède par évaluation-interpolation [**?**] : on estime le degré que devra avoir le résultant de f et g puis on évalue ce résultant en un nombre suffisant de points vis à vis du degré qu'il doit avoir en calculant des résultants de polynômes qui cette fois sont univariés. Ces opérations peuvent se faire en $\widetilde{O}(\deg(\mathrm{Res}_Y(f,g)) \times \max(\deg_X(f), \deg_X(g)))$ [**?**]. Il en va de même pour le calcul de sous-résultants ; en particulier pour le dernier qui sera celui qui nous intéressera en section 3.2.

En résumé :

Opération	Complexité
Pgcd de f et g et coefficients de Bézout	$\widetilde{O}(\deg(f) + \deg(g))$
g mod f	$\widetilde{O}(\deg(f) + \deg(g))$
Inverse de g modulo f	$\widetilde{O}(\deg(f) + \deg(g))$
Système de trois congruences	Deux calculs d'inverse modulo
Résultant et sous-résultant de f et g	$\widetilde{O}(\deg(\mathrm{Res}_Y(f,g)) \times \max(\deg_X(f), \deg_X(g)))$

Enfin, on aura besoin du petit lemme suivant sur le nombre de polynômes d'un certain degré pour expliciter la correction de l'algorithme de la section 3.2 :

Lemme 23. *L'espace vectoriel des polynômes de* $\mathbf{K}[X, Y]$ *de degré* d *est de dimension* $\binom{d+2}{2}$.

Démonstration. Il s'agit de dénombrer le nombre de monômes de $\mathbf{K}[X, Y]$ de degré inférieur ou égal à d. Cela revient à calculer le cardinal de $E_d = \{(i, j) \in [\![0, d]\!]^2 \mid i + j \leqslant d\}$. Or, l'application $\varphi : \begin{cases} E_d & \longrightarrow U = \{(i,j) \in [\![1, d+2]\!] \mid i < j\} \\ (i,j) & \longmapsto (i+1, i+j+2) \end{cases}$ est bijective.

L'injectivité est claire. De plus, si $(\alpha, \beta) \in U$ alors $(\alpha - 1, \beta - \alpha - 1) \in E_d$ en est un antécédent, d'où la surjectivité. On en déduit que le cardinal de E_d est égal à celui de U ; or ce dernier est égal à $\binom{2+d}{2}$ puisque chaque partie à deux éléments choisis parmi $d + 2$ donne un couple d'entiers dont l'un est strictement plus petit que l'autre.

□

3 Un algorithme géométrique efficace

3.1 Représentations de diviseurs

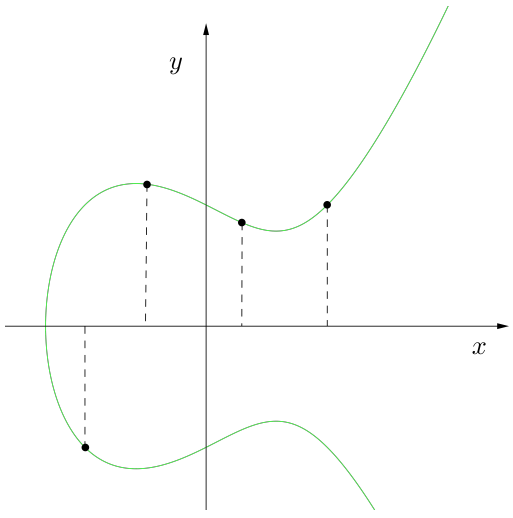
L'algorithme présenté dans la section 3.2 prendra en entrée une courbe (affine) et un diviseur sur cette courbe. Assez naturellement, la courbe sera représentée par son équation donc par un polynôme de $\mathbf{K}[X,Y]$. La représentation utilisée pour le diviseur est en revanche moins évidente ; c'est ce dont on discute dans cette partie.

Dans la suite de cette partie, C est une courbe plane affine irréductible et lisse qu'on confond avec son polynôme de définition (noté également C). Comme annoncé dans la remarque 8, on commence par représenter tout diviseur de C par un couple de diviseurs effectifs. La question est désormais de représenter un tel diviseur. On se donne donc un diviseur D sur C effectif. Initialement (comme vu dans la section 2.1.3) ce diviseur D est défini comme étant une somme formelle de points de C à coefficients entiers (positifs puisque D est effectif). On va voir par la suite que ce diviseur peut également être représenté par un idéal ou encore par un couple de polynômes.

Si $D = \sum_{P \in \mathbf{C}(\mathbf{K})} n_P P$ est effectif sur C, on peut lui associer l'ensemble suivant : $I_D = \{f \in \mathbf{K}[X,Y]/(C) \mid \mathrm{ord}_P(f) \geqslant n_P\}$. Grâce aux propriétés d'une valuation [**?**], on constate que cet ensemble est en fait un idéal de $\mathbf{K}[X,Y]/(C)$. Il contient tous les polynômes ayant une multiplicité en chaque point P de C au moins aussi grande que n_P. En particulier, un élément de I_D s'annule en tous les points du support de D avec une multiplicité au moins celle requise par D. Remarquons qu'on peut plutôt considérer I_D comme un idéal de $\mathbf{K}[X,Y]$ contenant C puisqu'il existe une bijection entre les idéaux de $\mathbf{K}[X,Y]/(C)$ et les idéaux de $\mathbf{K}[X,Y]$ contenant C.

Sous certaines hypothèses vérifiées lorsqu'on se place en coordonnées génériques, on peut également représenter D par deux polynômes de $\mathbf{K}[X]$, qu'on note f_D et g_D et dont on va donner l'intuition de la construction avant de prouver l'existence. On note (x_i, y_i) les coordonnées du i-ème des n points intervenant dans le diviseur D et n_i la multiplicité qui est associée à ce point.

On suppose que les x_i sont tous différents. Si ce n'est pas le cas, on peut toujours faire un changement de coordonnées pour que ce le soit (on sera donc toujours dans une situation semblable à celle de droite ; les points noirs représentent les points de D). On construit alors $f_D = \prod_{i=1}^{n} (X - x_i)^{n_i}$. On construit aussi g_D de degré inférieur à f_D tel que pour tout $i \in [\![1, n]\!]$ on a $g(x_i) = y_i$ et tel que la congruence $C(x, g(x)) \equiv 0 \bmod f(x)$ soit vérifiée.



Plus simplement, le polynôme f_D a exactement pour zéros les abscisses des points de D et ce avec la multiplicité propre au point correspondant. Le polynôme g_D quant à lui encode les ordonnées des points de D. La dernière condition sur g_D permet entre autres d'assurer l'unicité de f_D et g_D comme on le verra en proposition 24. Ces deux polynômes renferment ainsi l'information relatives aux ordonnées, aux abscisses et aux multiplicités de chacun des points de D c'est-à-dire exactement toute l'information que donnerait D vu comme une somme formelle. Dans la suite, on s'attache à prouver l'existence est l'unicité de tels f_D et g_D pour chaque diviseur D.

Proposition 24. *Soit C une courbe plane affine lisse et irréductible sur $\mathbf{K}$ qu'on confond avec son polynôme de définition et $D = \sum_{i=1}^{n} n_i P_i$ un diviseur de C. On note (x_i, y_i) les coordonnées du point P_i ; on suppose que les x_i sont deux à deux distincts et que pour tout $i \in [\![1, n]\!]$, la tangente à C en P_i n'est pas verticale. Alors il existe un unique (à multiplication par un inversible près) polynôme $f \in \mathbf{K}[X]$ et un unique polynôme $g \in \mathbf{K}[X]$ vérifiant les propriétés suivantes :*

(1) Les zéros de f sont exactement les abscisses x_i et la multiplicité de x_i dans f_D est exactement n_i.

(2) Le degré de g est inférieur strictement au degré de f_D.

(3) On a pour tout $i \in [\![1, n]\!]$, $g(x_i) = y_i$.

(4) La congruence $C(X, g(X)) \equiv 0 \ mod \ f(X)$ est vérifiée.

Démonstration. Remarquons qu'on peut toujours s'assurer que la condition $i \in [\![1, n]\!]$, la tangente à C en P_i n'est pas verticale est vérifiée en faisant au besoin un changement de coordonnées.

L'existence et l'unicité à produit par un inversible de $\mathbf{K}$ d'un polynôme vérifiant (1) est immédiate : $f = \prod_{i=1}^{n} (X - x_i)^{n_i}$ convient.

Remarquons d'ailleurs que si on trouve un polynôme g satisfaisant (3) et (4) alors on peut en trouver un satisfaisant de surcroît la propriété (2). Pour ce faire, réduisons g modulo f : $g = \tilde{g} + hf$ avec $\deg(\tilde{g}) < \deg(f)$ et $h \in \mathbf{K}[X]$. Alors $\tilde{g}$ continue de vérifier (3) et (4). En effet, pour tout $i \in [\![1, n]\!]$,

$$\tilde{g}(x_i) = g(x_i) - h(x_i)f(x_i) = g(x_i) + 0 = y_i$$

puisque x_i annule f et que g vérifie (3). De même

$$C(x, \tilde{g}(x)) \equiv C(x, g(x) - h(x)f(x)) \equiv C(x, g(x)) \equiv 0 \bmod f(x)$$

puisque g vérifie (4).

Il ne reste donc qu'à montrer l'existence et l'unicité d'un polynôme g vérifiant (3) et (4) pour conclure. On sait déjà qu'on dispose d'un polynôme f vérifiant (1). Commençons par déterminer un g correct dans des cas où f est particulier.

Soit $i \in [\![1, n]\!]$. Si on avait $f = X - x_i$ alors $g = y_i$ conviendrait (et c'est le seul polynôme de degré strictement inférieur à celui de $X - x_i$ qui convienne, d'où l'unicité). En effet, la propriété (3) est immédiatement vérifiée et évaluer $C(X, g(X))$ modulo $X - x_i$ revient à

calculer $C(x_i, g(x_i))$. Or $C(x_i, g(x_i)) = C(x_i, y_i) = 0$ car (x_i, y_i) est par définition un point de la courbe C.

Maintenant qu'on sait construire un polynôme $g \in \mathbf{K}[X]$ tel que $g(x_i) = y_i$ et $C(X, g(X)) \equiv 0 \bmod X - x_i$, on utilise le corollaire 20 (et on peut car on a pris soin de faire un changement de coordonnées approprié) qui donne aussitôt l'existence et l'unicité d'un polynôme $\tilde{g}$ tel que $\tilde{g}(x_i) = y_i$ et $C(X, \tilde{g}(X)) \equiv 0 \bmod (X - x_i)^{n_i}$.

On sait désormais que pour tout $i \in [\![1, n]\!]$, il existe un unique polynôme g_i vérifiant $g_i(x_i) = y_i$ et $C(X, g_i(X)) \equiv 0 \bmod (X - x_i)^{n_i}$. Considérons le système de congruences $\{g \equiv g_i \bmod (X - x_i)^{n_i} \mid i \in [\![1, n]\!]\}$. Comme les x_i sont deux à deux distincts, les $(X - x_i)^{n_i}$ sont deux à deux premiers entre eux et une application du théorème des restes chinois [**?**] assure alors l'existence d'un unique polynôme g de degré strictement inférieur à $\deg(f)$ solution de ce système.

Or, pour tout $i \in [\![1, n]\!]$, comme $X - x_i$ divise $(X - x_i)^{n_i}$, on a $g \equiv g_i \bmod X - x_i$ ce qui se réécrit $g(x_i) = g_i(x_i) = y_i$. De plus, pour tout $i \in [\![1, n]\!]$, $C(X, g(X)) \equiv C(X, g_i(X)) \equiv 0 \bmod (X - x_i)^{n_i}$. Comme les $(X - x_i)^{n_i}$ sont premiers entre eux, on a bien $C(X, g(X)) \equiv 0 \bmod \prod_{i=1}^{n} (X - x_i)^{n_i} = f(X)$. Le polynôme g qu'on vient de construire vérifie les propriétés (3) et (4) ce qui conclut.

Remarque 25. *Si on écrit $D = D_+ - D_-$ avec D_+ et D_- effectifs et à supports disjoints et qu'on construit les représentations polynomiales de (f_+, g_+) et (f_-, g_-) de D_+ et D_-, on constate que $\deg(f_+) + \deg(f_-)$ est exactement le nombre de points dans D comptés avec multiplicité, c'est à dire, est égal à $|D|$.*

□

3.1.1 Traduction des opérations sur les diviseurs selon la représentation

Les opérations que l'on souhaite faire dans l'algorithme 1 (section 3.2) sont initialement pensées comme des opérations sur des diviseurs effectifs représentés comme sommes formelles de points. Toutefois, cet algorithme utilise pour un diviseur effectif sa représentation polynomiale plutôt que cette somme formelle. On établit dès lors dans cette partie un dictionnaire entre les opérations sur les diviseurs comme sommes formelles et celles effectuées sur ces mêmes diviseurs représentés polynomialement.

Dans la suite, $D = \sum_{P \in C(\mathbf{K})} n_P P$ et $\tilde{D} = \sum_{P \in C(\mathbf{K})} m_P P$ sont deux diviseurs effectifs sur une courbe C. On note et (f, g) (respectivement $(\tilde{f}, \tilde{g})$) la représentation polynomiale de D (respectivement $\tilde{D}$). On suppose que $g \equiv \tilde{g} \bmod f \wedge \tilde{f}$. Ainsi, la situation où deux points différents — l'un sur D et l'autre sur $\tilde{D}$ — ont même projection sur l'axe des abscisses n'arrive jamais. Si par malchance ce n'était pas le cas, on change de direction de projection afin que cette condition soit vérifiée comme vu en 3.1. Pour chaque opération, afin de prouver que les polynômes construits sont effectivement ceux représentant le diviseur annoncé, il suffit de vérifier qu'ils vérifient les propriétés (1) à (4) de la proposition 24 : l'unicité montrée dans cette même proposition assurera alors la correction de nos constructions.

Commençons par traduire la construction du diviseur intersection de D et $\tilde{D}$, qui est $\sum_{P \in C(\mathbf{K})} \min(n_P, m_P) P$. Dans ce diviseur, on ne conserve pour chaque point que la contrainte

de multiplicité la moins forte entre celle donnée par D et celle donnée par $\tilde{D}$. En termes de représentations polynomiales, il nous faut construire (F, G) tels que F la multiplicité de tout $P \in C(\mathbf{K})$ vaut $\min(n_P, m_P)$ et G ne conserve que les ordonnées des points dans le support du diviseur intersection. Comme $f = \prod_P (X - x_P)^{n_P}$ (où x_P est l'abscisse du point $P \in C(\mathbf{K})$) et $\tilde{f} = \prod_P (X - x_P)^{m_P}$ par construction, on a immédiatement $F = f \wedge \tilde{f}$. Il ne reste alors qu'à prendre $G = g \bmod F$ (ou $G = \tilde{g} \bmod F$).

Continuons par la construction de la différence positive $[D - \tilde{D}]_+ = \sum_{P \in C(\mathbf{K})} \max(0, n_P - m_P)P$. Intuitivement, cela revient à retirer de D les points (comptés avec multiplicité) que ce diviseur a en commun avec $\tilde{D}$. On constate que $[D - \tilde{D}]_+$ est effectif ce qui autorise à parler de l'idéal qui lui est associé ainsi que de sa représentation polynomiale (section 3.1). En termes de représentations polynomiales, il s'agit de construire (F, G) tels que F s'annule exactement en les points P du support de $D - \tilde{D}$ avec la multiplicité $n_P - m_P$ et G ne conserve que les ordonnées des points dans le support de $D - \tilde{D}$. Pour ce faire, il suffit d'éliminer de f les facteurs communs à f et $\tilde{f}$ c'est-à-dire de prendre $F = f/(f \wedge \tilde{f})$. Il ne reste plus qu'à réduire g modulo F pour obtenir G.

Terminons par la construction du diviseur somme $D + \tilde{D} = \sum_{P \in C(\mathbf{K})} (n_P + m_P)P$. En termes de représentations polynomiales, il s'agit de construire (F, G) tels que F s'annule en l'abscisse de P avec multiplicité $n_P + m_P$: il suffit donc de prendre $F = f\tilde{f}$. Pour ce qui est de G, on veut que G coïncide avec g modulo f et avec $\tilde{g}$ modulo $\tilde{f}$ de façon à ce que G encode les ordonnées des points de D et celles des points de $\tilde{D}$. Il suffit donc de trouver pour G une solution au système de congruences $\begin{cases} G \equiv g \bmod f \\ G \equiv \tilde{g} \bmod \tilde{f} \end{cases}$

Si f et $\tilde{f}$ sont premiers entre eux, le théorème chinois donne immédiatement un polynôme G qui convient. Sinon, remarquons qu'on peut remplacer sans pertes f par $F = f/(f \wedge f')$ et $\tilde{f}$ par $\tilde{F} = \tilde{f}/(\tilde{f} \wedge \tilde{f}')$ dans les congruences ci-dessus : on n'a fait qu'éliminer l'information sur les multiplicités, inutile à la construction de G. Ces nouveaux polynômes peuvent encore avoir des facteurs communs. Mais on peut supprimer ce problème de la façon suivante. On demande simplement à G de donner les bonnes ordonnées pour les points exclusivement dans le support de D, exclusivement dans le support de $\tilde{D}$ et dans l'intersection des supports de D et $\tilde{D}$ (ces trois ensembles ont une union disjointe égale à $\mathrm{Supp}(D + \tilde{D})$). Pour que ces conditions soient vérifiées, il suffit donc de construire G vérifiant $\begin{cases} G \equiv g \bmod \frac{F}{F \wedge \tilde{F}} \\ G \equiv \tilde{g} \bmod \frac{\tilde{F}}{F \wedge \tilde{F}} \\ G \equiv g \bmod F \wedge \tilde{F} \end{cases}$

Cette fois nos trois polynômes sont bien premiers entre eux et le théorème chinois donne un polynôme $\tilde{G}$ solution de ce système modulo $P = F\tilde{F}/(F \wedge \tilde{F})$. Or, par construction de P, il existe un entier $k \in \mathbf{N}^\star$ tel que $f\tilde{f} | P^k$. En utilisant le lemme de Hensel (lemme 18) on peut calculer (via un algorithme de Newton décrit en [**?**]) un polynôme G tel que $G \equiv \tilde{G} \bmod P^k$ et $C(X, G(X)) \equiv 0 \bmod P^k$. Le polynôme G ainsi construit vérifie donc $C(X, G(X)) \equiv 0 \bmod f\tilde{f}$ ce qui permet de conclure qu'il vérifie effectivement toutes les conditions de la proposition 24.

Remarquons que l'entier k ci-dessus est nécessairement majoré par $\deg(f) + \deg(\tilde{f})$. L'algorithme donnant G à partir de $\tilde{G}$ étant logarithmique en k (voir [**?**]), la complexité de la

résolution du système de congruences domine celle dudit algorithme.

Pour résumer :

Opération	Somme formelle	Représentation polynomiale
Union	$D + \tilde{D}$	$(f\tilde{f}, CRT([g,\tilde{g}],[f,\tilde{f}])$
Différence positive	$[D - \tilde{D}]_+$	$(\frac{f}{f\wedge\tilde{f}}, g \bmod \frac{\tilde{f}}{f\wedge\tilde{f}})$
Intersection	$\sum_{P\in C(\mathbf{K})} \min(n_P, m_P)P$	$(f \wedge \tilde{f}, g \bmod (f \wedge \tilde{f}))$

3.2 Algorithme de calcul d'espaces de Riemann-Roch

Commençons par présenter une esquisse d'un algorithme de calcul d'espaces de Riemann-Roch avec le vocabulaire des idéaux. On nous donne une courbe C et un diviseur $D = D_+ - D_-$ où D_+ et D_- sont effectifs. Comme vu en section 3.1 à chacun de ces deux diviseurs effectifs correspond un idéal, respectivement I_+ et I_-. Rappelons que I_+ contraint les pôles des fonctions de $L(D)$ et que I_- en contraint les zéros. On cherche une base de $L(D)$.

On commence par trouver un dénominateur commun à tous les éléments de $\mathbf{K}(C)$ constituant la base cherchée. Pour ce faire, on choisit un polynôme h au hasard dans I_+ qui n'est pas divisible par l'équation de la courbe C (sinon, ce polynôme sera nul modulo C et ne peut donc pas être un dénominateur correct). Un polynôme de I_+ passant en particulier par tous les points de D_+ avec les bonnes multiplicités, on en déduit que h s'annule effectivement avec bonne multiplicité en tout point indiqué par D_+. Mais, h peut également s'annuler en d'autres points que ceux de D_+ (et a priori c'est le cas) : notre polynôme pris au hasard a des zéros en trop (ce qui se traduirait par des pôles en trop par rapport à ce qu'indique D_+ si on utilisait directement h comme dénominateur commun des éléments d'une base de $L(D)$).

La seconde étape est ainsi d'identifier ces zéros en trop. Pour ce faire, on fait la différence entre le diviseur associé à h et D_+. Afin de contrebalancer les zéros en trop introduits par h au dénominateur, on ajoute ces zéros en trop au numérateur des éléments de la base recherchée en les ajoutant à I_- pour donner I'. De cette façon, ces zéros en trop apparaîtront avec même multiplicité au numérateur et au dénominateur des éléments que nous construisons d'où simplification.

La dernière étape est alors de calculer une base des polynômes appartenant à l'idéal I' décrivant les nouveaux zéros et de degré celui de h (puisque une fonction rationnelle doit avoir un numérateur et un dénominateur de mêmes degrés 10). On obtient alors un ensemble E d'éléments qui, par construction, appartiennent à $L(D)$. On a donc $\mathrm{Vect}(E) \subset L(D)$, et, comme on le verra en 3.3, le théorème des résidus (théorème 17) garantit l'égalité de ces deux ensembles. Les fonctions que nous avons construites forment donc effectivement une base de $L(D)$.

3.2.1 Algorithme principal

On présente ici un algorithme de calcul de bases d'espaces de Riemann-Roch utilisant les représentations polynomiales introduites dans la section 3.1 pour décrire les diviseurs. L'idée est de manipuler ces représentations de sorte à effectuer les opérations décrites ci-dessus sur les idéaux qu'elles représentent (à l'aide de 3.1). On commencera par exposer

l'algorithme global puis on détaillera les diverses sous-fonctions qui y interviennent. Deux versions prototypes en Magma de cet algorithme sont disponibles aux adresses suivantes :
`http://perso.eleves.ens-rennes.fr/people/Aude.Legluher/RR_ideaux.mgm`
`http://perso.eleves.ens-rennes.fr/people/Aude.Legluher/RR_polynomes.mgm`

L'algorithme suivant prend en entrée l'équation C d'une courbe affine plane lisse et irréductible mise sous la forme $C = Y^{d_C} + P(X, Y)$ avec P de degré en Y strictement inférieur à d_C et $\deg(Y^{d_C} + P(X, Y)) = d_C$ (toujours possible par changement linéaire de coordonnées), ainsi que les représentations polynomiales (f_+, g_+) et (f_-, g_-) de deux diviseurs effectifs D_+ et D_- de C. La sortie de cet algorithme est une base de l'espace de Riemann-Roch $L(D)$ où $D = D_+ - D_-$.

Algorithm 1 Calcul d'une base d'un espace de Riemann Roch

1: **function** BaseRR$(C, (f_+, g_+), (f_-, g_-))$
2: $h \leftarrow$ RandomDenom(f_+, g_+, C)
3: $(f_s, g_s) \leftarrow$ RepPol(C, h)
4: $(f_p, g_p) \leftarrow$ Diff$((f_s, g_s), (f_+, g_+))$
5: $(f_z, g_z) \leftarrow$ Union$((f_p, g_p), (f_-, g_-))$
6: $N \leftarrow$ Base$((f_z, g_z), h, C)$
7: **Return** $\{h'/h \mid h' \in N\}$
8: **end function**

Avant de développer précisément les différentes étapes de cet algorithme, explicitons les fonctions qui y interviennent. La fonction RandomDenom prend en entrée la représentation polynomiale d'un diviseur effectif D et renvoie un polynôme h non multiple de C et s'annulant au moins en tous les points ayant une multiplicité non nulle dans D et ce avec ladite multiplicité. La fonction RepPol prend en entrée deux polynômes (ici C et h) de $\mathbf{K}[X, Y]$ et renvoie la représentation polynomiale du diviseur (h) sur la courbe C. La fonction Diff prend en entrée deux représentations polynomiales de diviseurs effectifs D et D' et renvoie celle de $[D - D']_+$. La fonction Union prend également en entrée les représentations polynomiales de deux diviseurs effectifs D et D' et renvoie celle de $D + D'$. Enfin, la fonction Base prend en entrée la représentation polynomiale (f, g) d'un diviseur et un polynôme $h \in \mathbf{K}[X]$ et donne une base de l'espace vectoriel des polynômes P de $\mathbf{K}[X, Y]$ ayant un degré inférieur à celui de h, non multiples de la courbe C et vérifiant $P(x, g(x)) \equiv 0 \mod f(x)$. Il est temps maintenant de détailler chacune de ces sous-fonctions.

3.2.2 Choix d'un dénominateur adéquat

Intuitivement voici l'objectif de cet algorithme : on veut trouver un polynôme $h \neq 0$, satisfaisant la condition $h(x, g_+(x)) \mod f_+(x) = 0$ et non multiple de l'équation de la courbe C. La ligne 2 de l'algorithme 2 permet de déterminer un degré pour h qui soit le plus petit possible mais permettant de satisfaire les conditions voulues. Les valeurs choisies pour ce degré seront explicitées en 3.3.1. Le polynôme h ainsi trouvé sera en fait le dénominateur commun à tous les éléments de la base d'espace de Riemann-Roch que l'on recherche. Il s'agit en particulier d'un polynôme qui a pour pôles au moins ceux requis par D_+.

Algorithm 2 Calcul d'un polynôme h passant par les points de D_+

function RandomDenom($(f_+, g_+), C$)
  if $\binom{d_C+1}{2} \leqslant \deg(f_+)$ **then** $D \leftarrow \lfloor \frac{\deg(f_+)}{d_C} + \frac{d_C-3}{2} + 1 \rfloor$
  else $D \leftarrow \lfloor \frac{\sqrt{1+8\deg(f_+)}-3}{2} + 1 \rfloor$
  end if
  $h \leftarrow \sum_{\substack{0 \leqslant i+j \leqslant D \\ j < d_C}} a_{i,j} X^i Y^j$ où les $a_{i,j}$ sont des inconnues
  Construire le système linéaire S donné par $h(x, g_+(x)) \bmod f_+(x) = 0$
  Return une solution non nulle de S
end function

3.2.3 Calcul de la représentation polynomiale de (h)

Algorithm 3 Calcul de la représentation polynomiale du diviseur (h)

function RepPol(C, h)
  $f_s \leftarrow$ résultant de C et h
  Calculer le sous-résultant $a(X)Y - b(X)$ de C et h
  $g_s \leftarrow Y - b(X) \times$ inverse de $a(X) \bmod \mathrm{Res}_Y(C, h)$
  Return (f_s, g_s)
end function

Ici, on construit la représentation associée au diviseur (h) en s'aidant des lemmes 21 et 22. Ce diviseur regroupe tous les zéros de h avec leurs multiplicités. Parmi ceux ci, il faut maintenant éliminer les zéros de h qui ne sont pas des points indiqués par D_+.

3.2.4 Construction des nouveaux zéros

On commence par isoler les zéros de h qui ne sont pas des points indiqués par D_+ avec Diff. Puis on y ajoute les points indiqués par D_- avec Union.

Algorithm 4 Calcul des pôles de h non indiqués par D_+

function Diff($(f_s, g_s), (f_+, g_+)$)
  $f \leftarrow \frac{f_s}{f_s \wedge f_+}$
  $g \leftarrow g_s \bmod f$
  Return (f, g)
end function

3.2.5 Calcul d'une base de l'espace de Riemann-Roch

Cet algorithme suit exactement le même principe que RandomDenom ; simplement on ne se contente plus d'un seul polynôme dans le noyau de la matrice construite, on en calcule une base.

Algorithm 5 Calcul du diviseur donnant les nouveaux zéros

function UNION($(f_p, g_p), (f_-, g_-)$)
    $f \leftarrow f_p \times f_-$
    $g \leftarrow$ un polynôme tel que $g \equiv g_p \bmod f_p$, $g \equiv g_- \bmod f_-$ calculé avec le théorème chinois
    Return (f, g)
end function

Algorithm 6 Calcul d'une base des numérateurs

function BASE($(f_z, g_z), h, C$)
    $D \leftarrow \deg(h)$
    $h \leftarrow \sum_{\substack{0 \leqslant i+j \leqslant D \\ j < d_C}} a_{i,j} X^i Y^j$ où les $a_{i,j}$ sont des inconnues
    Construire le système linéaire S donné par $h(x, g_z(x)) \bmod f_z(x) = 0$
    Return une base des solutions de S
end function

3.3 Correction

La correction des algorithmes Diff et Union a déjà été traitée dans la section 3.1.1. Il nous reste encore trois points à éclaircir :

- Vérifier que le degré choisi pour h dans l'algorithme RandomDenom est suffisamment grand pour garantir qu'il existe une solution non nulle au système linéaire
- Vérifier que les calculs effectués dans RepPol construisent effectivement la représentation polynomiale du diviseur (h)
- Vérifier que l'espace de Riemann-Roch associé au diviseur D en entrée de l'algorithme BaseRR est bien inclus dans l'espace vectoriel engendré par les éléments en sortie de cet algorithme

3.3.1 Correction de RandomDenom

Soit C une courbe affine plane irréductible qu'on confond avec son polynôme de définition dont l'équation est de la forme $Y^{d_C} + P(X, Y)$ avec P de degré en Y strictement inférieur à d_C et (f, g) la représentation polynomiale d'un diviseur effectif D. On prouve ici que l'algorithme 2 renvoie un polynôme h bivarié, non multiple de la courbe C, non nul et vérifiant

$$h(x, g_+(x)) \bmod f_+(x) = 0 \tag{1}$$

D'après le corps de cet algorithme, RandomDenom renvoie un polynôme bivarié h vérifiant (1). De plus h ne peut pas être multiple de C puisque son degré en Y est strictement inférieur à celui de la courbe C par construction. La seule chose à vérifier est donc la non nullité de h. Pour ce faire, on montre que le degré D choisi pour h dans l'algorithme 2 implique que le système linéaire homogène que doit vérifier h admet une solution non nulle. Ce système a par définition $\deg(f)$ équations et $N = \text{Card}\{(i, j) \in \mathbf{N}^2 \mid i + j \leqslant D \text{ et } j < d_C\}$. Pour qu'il ait une solution non nulle il suffit donc de vérifier que $N > \deg(f)$ (plus d'inconnues que d'équations).

Proposition 26. *On reprend les notations précédentes pour C, d_C et f.*

La fonction $\varphi : (x,y) \longmapsto \begin{cases} \left\lfloor \frac{\sqrt{1+8x}-3}{2} + 1 \right\rfloor & \text{si } \binom{y+1}{2} > x \\ \left\lfloor \frac{x}{y} + \frac{y-3}{2} + 1 \right\rfloor & \text{sinon} \end{cases}$ *vérifie que*

$$N(\deg(f), d_C) = \mathrm{Card}\{(i,j) \in \mathbf{N}^2 \mid i + j \leqslant \varphi(\deg(f), d_C) \text{ et } j < d_C\} > \deg(f)$$

Démonstration. Remarquons que $\binom{(d_C-1)+2}{2}$ est la dimension de l'espace vectoriel des polynômes de $\mathbf{K}[X,Y]$ de degré $d_C - 1$ d'après le lemme 23. Intuitivement, si cette quantité est strictement supérieure à $\deg(f)$ c'est qu'il existe un polynôme non nul de degré inférieur à $d_C - 1$ solution de 1. Comme le degré de ce polynôme est strictement inférieur à d_C, il vérifiera automatiquement la non divisibilité par C. Dans l'autre cas, il faudra nécessairement autoriser un degré au moins égal à d_C pour trouver un polynôme non nul satisfaisant nos conditions.

Notons également que le lemme 23 assure que

$$N(\deg(f), d_C) = \binom{\varphi(\deg(f), d_C) + 2}{2} - \binom{\varphi(\deg(f), d_C) - d_C + 2}{2}$$

si $\varphi(\deg(f), d_C) - d_C + 2 \geqslant 2$ et $N(x) = \binom{\varphi(\deg(f),d_C)+2}{2}$ sinon (en effet, le nombre de monômes bivariés de degré inférieur à $\varphi(\deg(f), d_C)$ divisibles par Y^{d_C} est égal au nombre de monômes de degré inférieur à $\varphi(\deg(f), d_C) - d_C$ via la bijection
$M \in \{$ monômes de degré inférieur à $\varphi(\deg(f), d_C) - d_C$ et non divisibles par $Y^{d_C}\} \longmapsto Y^{d_C} M$).

Vérifions la propriété dans le cas $\binom{d_C+1}{2} > \deg(f)$. Dans ce cas, un rapide calcul montre que $\varphi(\deg(f), d_C) < d_C$ et on a donc $N(\deg(f), d_C) = \binom{\varphi(\deg(f),d_C)+2}{2}$. Or, en calculant les racines du polynôme $\frac{X^2}{2} + \frac{3X}{2} + (1 - \deg(f))$, on constate que pour tout $x > \frac{\sqrt{1+8\deg(f)}-3}{2}$ ce polynôme est strictement positif. En particulier, comme $\varphi(\deg(f), d_C) > \frac{\sqrt{1+8\deg(f)}-3}{2}$ dans notre cas, on ainsi que $\varphi(\deg(f), d_C)^2/2 + 3\varphi(\deg(f), d_C)/2 + 1 > \deg(f)$ ce qui se réécrit $\binom{\varphi(\deg(f),d_C)+2}{2} > \deg(f)$ c'est-à-dire $N(\deg(f), d_C) > \deg(f)$ comme attendu.

Dans le cas où $\binom{d_C+1}{2} \leqslant \deg(f)$, en remplaçant $\varphi(\deg(f), d_C)$ par sa valeur, on constate que $\varphi(\deg(f), d_C) \geqslant d_C$ et on a donc $N(\deg(f), d_C) = \binom{\varphi(\deg(f),d_C)+2}{2} - \binom{\varphi(\deg(f),d_C)-d_C+2}{2} = d_C(\varphi(\deg(f), d_C) + (3 - d_C)/2)$ en développant. En remplaçant $\varphi(\deg(f), d_C)$ par sa valeur dans cette dernière expression, on trouve immédiatement que $N(\deg(f), d_C) > \deg(f)$.

□

Remarque 27.

- *La proposition 26 prouve que le degré choisi pour h dans l'algorithme 2 est suffisant pour assurer la non nullité de h*
- *En pratique les valeurs proposées pour le degré de h on été trouvées en recherchant quel degré minimal suffisait à avoir une solution non nulle du système 1.*
- *Dans un cas comme dans l'autre, en remplaçant $\varphi(x)$ par sa valeur dans l'expression de $N(x)$, on remarque que le polynôme recherché h de degré $\varphi(x)$ a un nombre de coefficients en $O(\deg(f))$.*
- *Le degré de h est dans tous les cas inférieur à $\frac{\deg(f)}{d_C} + \frac{d_C-3}{2} + 1$.*

3.3.2 Correction de RepPol

On prouve dans cette partie la correction de l'algorithme RepPol. On rappelle que cet algorithme prend en entrée un polynôme bivarié C sous la forme $Y^{d_C}+p(X,Y)$ et un polynôme bivarié h. Pour prouver que le couple $(\mathrm{Res}_Y(C,h),g)$ où $\mathrm{SubRes}(C,h) = a(X)Y - b(X)$ et $g = b/a \bmod \mathrm{Res}_Y(C,h)$ est effectivement la représentation polynomiale du diviseur (h), il suffit de vérifier que ces polynômes vérifient les propriétés (1) à (4) de la proposition 24 : l'unicité prouvée dans cette proposition conclura alors.

On note I l'idéal $\langle h\rangle + \langle C\rangle$ correspondant à (h). D'après le lemme 22, $\mathrm{Res}(C,h)$ est un générateur de $I \cap \mathbf{K}[X]$ et $\mathrm{SubRes}(C,h) \in I$. Le fait que $\mathrm{Res}(C,h)$ engendre $I \cap \mathbf{K}[X]$ implique immédiatement qu'il vérifie la propriété (1). La propriété (2) découle de l'étude fine du degré de $\mathrm{SubRes}(C,h)$. La propriété (3) vient de ce que $\mathrm{SubRes}(C,h) \in I$: ceci implique que pour tout point (x,y) du diviseur associé à h on a $\mathrm{SubRes}(C,h)(x,y) = 0$ ce qui se réécrit effectivement $g(x) = y$.

Enfin, il reste à monter que $C(X,g(X)) \equiv 0 \bmod \mathrm{Res}(C,h)$. Comme $\mathrm{Res}(C,h)$ engendre $I \cap \mathbf{K}[X]$, il suffit de montrer que $C(X,g(X)) \in I$ pour conclure que la propriété (4) est vérifiée. Or, $Y - g(X) = \mathrm{SubRes}(C,h) \times (a^{-1} \bmod \mathrm{Res}_Y(C,h))$ est un élément de I puisque c'est le cas de $\mathrm{SubRes}(C,h)$. On en déduit que pour tous $(i,j) \in \mathbf{N}^2$,

$$X^iY^j - X^ig(Y)^j = X^i(Y-g(Y))\sum_{i=0}^{j-1}(-1)^k g(Y)^k Y^{j-1-k} \in I$$

par absorption. Par stabilité par somme, on en déduit que $C(X,Y) - C(X,g(Y)) \in I$. Comme $C \in I$, la stabilité par somme assure que $C(X,g(X)) \in I$ ce qui conclut.

3.3.3 Correction de l'algorithme final BaseRR

On montre ici que l'ensemble E des éléments en sortie de l'algorithme 1 vérifie bien $\mathrm{Vect}(E) = L(D)$ où D est le diviseur en entrée.

Théorème 28. *Soit C une courbe plane irréductible lisse et $D = D_+ - D_-$ un diviseur sur cette courbe tel que D_+ et D_- sont effectifs (et à supports disjoints). Si G_0 est un polynôme de degré m tel que C ne divise pas G_0 et $(G_0) \geqslant D_+$, alors*

$L(D) = \{\frac{G}{G_0} \mid G$ *est un polynôme de degré m, C ne divise pas G et $(G) \geqslant (G_0) - D\}$*

Démonstration. On montre ce résultat par double inclusion.

Si G est un polynôme de degré m tel que $G \notin I(C)$ et $(G) \geqslant (G_0) - D$ alors on a immédiatement

$$\left(\frac{G}{G_0}\right) = (G) - (G_0) \geqslant (G_0) - D - (G_0) = -D$$

Donc on a bien $\left(\frac{G}{G_0}\right) \in L(D)$.

Réciproquement, si $\varphi \in L(D)$ alors par définition $(\varphi) \geqslant -D$ ce qui signifie aussi qu'il existe un diviseur effectif D' tel que $(\varphi) = D' - D$. En se rappelant de la définition de D, on constate que alors que $(\varphi) = (D' + D_-) - D_+$ et on en déduit que $D' + D_- \sim D_+$ $(\star)$

De plus, par hypothèse, $(G_0) \geqslant D_+$ ce qui signifie qu'il existe un diviseur effectif D'' tels que $(G_0) = D_+ + D''$. En ajoutant D'' de part et d'autre de l'équivalence $(\star)$, on obtient que $D' + D_- + D'' \sim D_+ + D''$. D'autre part, ces diviseurs tous deux effectifs car somme de diviseurs positifs (par hypothèse pour D_+ et D_- et par construction pour D' et D'').

Ceci nous autorise à appliquer le théorème des résidus à $D' + D_- + D''$, $D_+ + D''$ et G_0 (dans notre cas, le diviseur A du théorème des résidus est nul) et donc à en déduire l'existence d'un polynôme G de degré m tel que $G = D' + D_- + D''$. Remarquons d'ailleurs que $(G_0) - D = D'' + D_-$ et qu'on a donc bien $(G) \geqslant (G_0) - D$ par effectivité de D'.

Enfin,

$$\left(\frac{G}{G_0}\right) = (G) - (G_0) = (D' + D_- + D'') - (D_+ + D'') = D' - D = (\varphi)$$

ce qui assure la proportionnalité des fonctions φ et $\left(\frac{G}{G_0}\right)$ et par suite l'autre inclusion.

□

Ceci conclut quant à la correction de l'algorithme BaseRR : ce dernier renvoie bien une base de l'espace de Riemann-Roch associé au diviseur pris en entrée.

3.4 Complexité

On cherche ici à déterminer une complexité asymptotique pour l'algorithme BaseRR vu en section 3.2 en termes de nombres d'opérations effectuées dans le corps $\mathbf{K}$. Pour ce faire, on utilisera intensivement les résultats énoncés dans la section 2.2.3. On rappelle que $f(n)$ est un $\widetilde{O}(g(n))$ s'il existe k tels que $f(n)$ est un $O(\log(n)^k g(n))$: cette notation permet d'ignorer les facteurs logarithmiques.

Rappelons que l'algorithme BaseRR prend en entrée l'équation d'une courbe affine lisse (donc un polynôme en deux variables sur un certain corps fini $\mathbf{K}$) C dont on note le degré d_C ainsi que deux couples de polynômes univariés sur $\mathbf{K}$, (f_+, g_+) et (f_-, g_-), représentant respectivement les diviseurs D_+ et D_- d'un certain diviseur $D = D_+ - D_-$ sur la courbe C.

On estime que la complexité de BaseRR est le nombre d'opérations effectuées dans $\mathbf{K}$ lors de son exécution. L'objectif ici est d'exprimer cette complexité en fonction de d_C et $\deg(f_+)$. Le degré de f_- n'interviendra pas dans la complexité finale de BaseRR car on peut supposer sans perte de généralité que $\deg(f_-) \leqslant \deg(f_+)$ d'après le lemme 29 ci après.

Lemme 29. *Si* $\deg(f_-) > \deg(f_+)$ *alors* $L(D) = \{0\}$.

Démonstration. On montre la contraposée. Si il existe $\varphi \in L(D)\backslash\{0\}$, par définition, $(\varphi) + D \geqslant 0$. On en déduit en prenant le degré dans cette inégalité que $0 + \deg(D) \geqslant 0$. Or, $\deg(D) = \deg(f_+) - \deg(f_-)$ ce qui conclut. On en déduit que par la suite on peut toujours supposer que $\deg(f_-) \leqslant \deg(f_+)$. □

Afin de clarifier l'analyse de la complexité de BaseRR, examinons les différentes étapes rencontrées lors de son exécution :

1. Construction d'un polynôme h passant par le diviseur représenté par (f_+, g_+)

2. Calcul de la représentation polynomiale, notée (f_s, g_s), du diviseur (h)
3. Calcul de la représentation polynomiale, notée (f_p, g_p), du diviseur des pôles en trop (introduits à cause du choix de h au hasard)
4. Calcul de la représentation polynomiale, notée (f_z, g_z), du diviseur fixant les nouveaux zéros des fonctions cherchées
5. Calcul de la dimension du noyau d'une application linéaire construite à partir de (f_z, g_z)

Les sections suivantes détaillent les complexités de ces différentes étapes.

3.4.1 Complexité de la première étape

Lors de cette première étape, on cherche un certain polynôme $h = \sum_{\substack{0 \leqslant i+j \leqslant D \\ j < d_C}} a_{i,j} X^i Y^j$ vérifiant l'équation 1 présentée en section 3.3.1. On doit d'abord construire le système linéaire découlant de cette équation puis le résoudre.

Pour la construction, il suffit de calculer $\sum_{\substack{0 \leqslant i+j \leqslant D \\ j < d_C}} a_{i,j} x^i g_+(x)^j \bmod f_+(x)$ et d'égaler chacun des $\deg(f_+)$ coefficients de cette expression à zéro. Pour ce faire, on calcule récursivement les $x^i g_+(x)^j \bmod f_+(x)$ pour tout $i + j \leqslant D$. Chacune de ces multiplications modulaires se calcule en $\widetilde{O}(\deg(f_+))$ et il y en a autant que de $a_{i,j}$ c'est-à-dire un $O(\deg(f_+))$ d'après la remarque 27. Calculer tous ces termes se fait donc en $\widetilde{O}(\deg(f_+)^2)$. Il ne reste plus qu'à sommer les termes ainsi construits (multipliés par l'inconnue $a_{i,j}$ correspondante), à réduire cette somme modulo f_+ et à isoler chacun des $\deg(f_+)$ coefficients du polynôme ainsi construit ce qui se fait en $\widetilde{O}(\deg(f_+))$. Ainsi, la construction du système linéaire se fait en $\widetilde{O}(\deg(f_+)^2)$ (théorème 2.10 de [**?**]).

On obtient alors un système linéaire à $\deg(f_+)$ équations et de l'ordre de $\deg(f_+)$ inconnues qui se résout en $O(\deg(f_+)^\omega)$. D'où une complexité totale pour la première étape en $O(\deg(f_+)^\omega)$.

3.4.2 Complexité de la deuxième étape

Le polynôme f_s est le résultant des polynômes C et h et g_s en est leur sous-résultant. Le polynôme f_s a donc un degré inférieur à $\deg_x(C)\deg_y(h) + \deg_x(h)\deg_y(C)$ et le degré du polynôme g_s est un $O(\deg_x(C)\deg_y(h) + \deg_x(h)\deg_y(C)))$ d'après le lemme 21.

Or, par construction de h, on a $deg_y(h) \leqslant d_C$. De plus, on peut brutalement majorer $deg_x(C)$ et $deg_y(C)$ par d_C d'une part et $deg_x(h)$ par D d'autre part. De ces remarques et du fait que $D \leqslant \frac{\deg(f_+)}{d_C} + \frac{d_C - 3}{2} + 1$ comme vu en remarque 27 on déduit que f_s et g_s ont un degré en $O(d_C^2 + deg(f_+))$. Remarquons qu'on peut être plus précis en soulignant que $\deg(f_s) \leqslant d_C^2 + deg(f_+)$

En calculant f_s et g_s par évaluation-interpolation, on obtient un coût pour cette deuxième étape en $\widetilde{O}(d_C(d_C^2 + deg(f_+))$.

3.4.3 Complexité de la troisième étape

D'après l'algorithme BaseRR, $f_p = \frac{f_s}{f_s \wedge f_+}$ et $g_p = g_s \bmod \frac{f_s}{f_s \wedge f_+}$. Ces deux calculs se font en $\widetilde{O}(deg(f_s)) = \widetilde{O}(d_C^2 + deg(f_+))$.

Déterminons les degrés des polynômes f_p et g_p ainsi obtenus. Tout d'abord, remarquons que f_+ divise f_s. En effet, comme expliqué en 3.1, on a $\langle f_s, Y - g_s\rangle = \langle C\rangle + \langle h\rangle$ et, par construction, cet idéal est inclus dans $\langle f_+, Y - g_+\rangle$ puisqu'on a précisément choisi h dans cet idéal. En particulier, on a donc $\langle f_s, Y - g_s\rangle \cap \mathbf{K}[X] \subset \langle f_+, Y - g_+\rangle \cap \mathbf{K}[X]$ ce qui se réécrit $\langle f_s\rangle \subset \langle f_+\rangle$ et implique bien que f_+ divise f_s. Dès lors, $\deg(f_p) = \deg(f_s/f_+) = \deg(f_s) - \deg(f_+) \leqslant d_C^2 + \deg(f_+) - \deg(f_+) = d_C^2$. On a donc $\deg(f_p) \leqslant d_C^2$ et $\deg(g_s) = \widetilde{O}(d_C^2 + \deg(f_+))$.

3.4.4 Complexité de la quatrième étape

Toujours en suivant l'algorithme BaseRR, $f_z = f_p \times f_-$ ce qui se calcule en $\widetilde{O}(\deg(f_p) + \deg(f_-)) = \widetilde{O}(d_C^2 + \deg(f_+))$ de par la partie précédente et le lemme 29.

D'autre part, g_z est solution du système de congruence $\begin{cases} g_z \equiv g_s \bmod f_p \\ g_z \equiv g_- \bmod f_- \end{cases}$

La résolution de ce système se fait en $\widetilde{O}(d_C^2 + \deg(f_+))$ toujours à cause du lemme 29 et de l'expression de $\deg(f_p)$ si f_p et f_- sont premiers entre eux. Si ce n'est pas le cas, on réfère à la section 3.1.1. Dans ce cas, en plus de résoudre un système de congruences similaire à celui ci-dessus, il faut encore utiliser le lemme de Hensel pour trouver un g_z convenable. Comme expliqué dans la section 3.1.1 la convergence quadratique de la méthode de Newton-Hensel [**?**] permet d'aboutir à la même complexité que dans le cas où on ne fait que résoudre un système de congruences : $\widetilde{O}(d_C^2 + \deg(f_+))$.

Les polynômes f_z et g_z qu'on obtient à la suite de ce calcul sont de degré inférieur à celui de f_p donc on un degré en $O(d_C^2)$.

3.4.5 Complexité de la dernière étape

Il s'agit ici de trouver le cardinal d'une base de l'espace vectoriel des polynômes bivariés q vérifiant $q(x, g_z(x)) \bmod f_z(x) = 0$ et de degré inférieur à celui de h. Cela revient à trouver une base de l'espace des solutions d'un système linéaire à $\deg(f_z)$ équations et ayant un nombre d'inconnues en Dd_C. Rappelons que les degrés de f_z et g_z sont en $\widetilde{O}(d_C^2)$ et que le degré de h est D. En réutilisant les raisonnements de la section 3.4.1, la construction de ce système se fait en $\widetilde{O}(Dd_C^3) = \widetilde{O}(d_C^3 + d_C\deg f_+)$ et sa résolution se fait en $O((d_C^2 + d_C\deg(f_+)) \times (d_C^2)^{\omega-1}) = O(d_C^{2\omega} + d_C^{2\omega-1}\deg(f_+))$ [**?**]. On en déduit une complexité pour cette étape en $O(d_C^{2\omega} + d_C^{2\omega-1}\deg(f_+))$.

3.4.6 Conclusion et comparaisons

Résumons les résultats obtenues dans les 5 sous-sections précédentes :

Étape	Complexité
1	$O(deg(f_+)^\omega)$
2	$\widetilde{O}(d_C^3 + d_C deg(f_+))$
3	$\widetilde{O}(d_C^2 + deg(f_+))$
4	$\widetilde{O}(d_C^2 + deg(f_+))$
5	$O(d_C^{2\omega} + d_C^{2\omega-1}\deg(f_+))$

En sommant, on obtient une complexité finale en $O((d_C^2 + \deg(f_+))^\omega)$ (les étapes 1 et 5 dominent les autres).

Remarquons que ce qui pèse le plus dans notre algorithme est le coût de l'algèbre linéaire. Comparons cette complexité avec celle obtenue dans le cas de courbes lisses par Huang et Ierardi dans [**?**]. Ces derniers trouvaient une complexité en $O(d_C^6|D|^6)$ dès lors que $|D| \geqslant d_C$. En particulier, si on se place dans le cas où $|D| \geqslant d_C^2$ et en rappelant que $|D| = \deg(f_+) + \deg(f_-) = O(\deg(f_+))$ comme vu dans la remarque 25, on peut réécrire la complexité que nous venons de trouver selon les mêmes paramètres que dans l'article de Huang et Ierardi et on trouve une complexité en $O(|D|^\omega)$.

Dans le cas d'une courbe lisse, $g = (d_C - 1)(d_C - 2)/2$ [**?**]. Ainsi, si on applique notre algorithme au calcul dans une jacobienne de courbe lisse dans le cas où $|D| \leqslant d_C^2$, on retrouve la complexité en $O(d_C^{2\omega}) = O(g^\omega)$ de Khuri-Makdisi [**?**] avec un algorithme géométrique.

4 Conclusion

Ce rapport décrit un algorithme géométrique de calcul de bases d'espaces de Riemann-Roch dans le cas des courbes lisses. Il est probabiliste de type Las Vegas : on change de système de coordonnées tant qu'on n'en a pas trouvé un qui satisfait les contraintes nécessaires à l'existence de la représentation polynomiale du diviseur en entrée, à savoir, pas de tangente verticale aux points du diviseur et pas de points du diviseur ayant même abscisse. Il prend en entrée une courbe de degré d sur un corps $\mathbf{K}$ et un diviseur D de cette courbe de taille $|D|$ sous représentation polynomiale et renvoie une base de $L(D)$. La complexité théorique de cet algorithme en terme de nombre d'opérations dans le corps de base est en $O((d^2 + |D|)^\omega)$. Cette complexité améliore celle de l'algorithme géométrique de Huang et Ierardi [**?**] dans le cas des courbes lisses et coïncide avec celle de l'algorithme arithmétique de Khuri-Makdisi [**?**] dans le cas particulier où on applique notre algorithme à l'arithmétique dans les jacobiennes de courbes.

Deux implémentations prototypes de cet algorithme ont été réalisées en Magma, une avec une représentation des diviseurs par idéaux qui paraît plus rapide dans certains cas pratiques que la fonction consacrée en Magma et une avec une représentation des diviseurs par polynômes qu'on attendrait encore plus rapide mais dont les performances sont pour l'instant modestes en pratique ; ceci est dû au moins en partie à l'implémentation naïve du calcul de résultants. La conception d'une version plus optimisée du dernier algorithme est prévue.

Quelques points théoriques au sujet des résultants et sous-résultants restent à éclaircir afin de justifier rigoureusement la construction de la représentation polynomiale du diviseur associé à un polynôme (algorithme RepPol). Une réécriture des preuves dans le cadre des corps qui ne sont pas algébriquement clos est également prévue. Enfin, le cas des courbes singulières est encore à traiter ; il nécessite une adaptation de l'algorithme présenté ici et potentiellement une nouvelle étude de complexité.