Cubiques en trois variables : points d'inflexion, formes normales et dimension essentielle

Mélanie Raczek

Cubiques en trois variables : points d'inflexion, formes normales et dimension essentielle

Mélanie Raczek

Dissertation présentée en vue de l'obtention du Diplôme d'Etudes Approfondies, en août 2004, au Département de Mathématique de la Faculté des Sciences de l'Université Catholique de Louvain, à Louvain-la-Neuve.

Promoteur : Jean-Pierre Tignol

Lecteurs : Francis Borceux (UCL)
Enrico Vitale (UCL)

AMS Subject Classification (2000) : 11E76 (Forms of degree higher than two), 14H45 (Special curves and curves of low genus)

FNRS Classification des domaines scientifiques (1991) : P 120 (Théorie des nombres, théorie des champs, géométrie algébrique, algèbre, théorie des groupes)

Table des matières

Introduction

Ce mémoire de DEA traite d'un sujet déjà connu depuis longtemps, mais revenant à l'actualité : la théorie des cubiques. Une cubique est un polynôme homogène de degré 3 en 3 variables à coefficients dans un corps k, définie à un multiple scalaire près. Des résultats prouvés sur de tels polynômes ne manquent pas, mais ils se trouvent souvent éparpillés dans des livres datant du XIXème siècle, par exemple [Miller *et. al.*, 1916 ; Salmon, 1884 ; Serret, 1866 ; Weber, 1896], où la manière de présenter les mathématiques est particulière. Des références plus modernes comme [Brieskorn et Knörrer, 1986] considèrent les cubiques comme exemples de courbes projectives dans le cadre de la géometrie algébrique, mais ne s'intéressent qu'aux cubiques à coefficients dans les complexes. Pourtant, pour la compréhension d'un travail récent comme celui de G. Berhuy et G. Favi [2004] sur la "dimension essentielle" des cubiques, il est absolument nécessaire de bien maîtriser la théorie élémentaire des cubiques à coefficients dans un corps k quelconque. Il était donc intéressant de mettre les résultats principaux de la théorie des cubiques sur un corps k au goût du jour, et de les réunir dans un mémoire.

Dans un premier chapitre, nous faisons un inventaire des connaissances nécessaires pour comprendre le mémoire. Ainsi, nous rappelons les notions de résultants de polynômes, d'extensions de corps et d'espaces projectifs, les démonstrations des théorèmes et des propositions n'étant pas données.

Nous entrons dans le sujet du mémoire dans le deuxième chapitre. Nous y parlons de courbes projectives avant de définir les cubiques, et nous exposons des outils qui sont utilisés ultérieurement. Nous en donnons les démonstrations puisque nous n'avons pas trouvé de références les explicitant.

Le troisième chapitre contient une énumération de propriétés importantes vérifiées par les cubiques, avec des preuves détaillées. Le résultat principal est sans doute le fait que toute cubique sans points multiples, à coefficients dans un corps infini séparablement clos de caractéristique différente de 2 et de 3, peut s'écrire, à un changement de variables linéaire près, sous la forme $X_1^3 + X_2^3 + X_3^3 + \lambda \cdot X_1 X_2 X_3$, pour un certain λ dans le corps. Ce résultat est essentiel, puisqu'il permet d'obtenir une multitude d'autres résultats de la théorie des cubiques. Les cubiques avec points multiples possèdent moins de propriétés, mais on arrive quand-même à les classifier en huit types différents.

Dans le quatrième et dernier chapitre, nous parlons succinctement du résultat récent de G. Berhuy et G. Favi [2004] : la dimension essentielle des cubiques sur un corps de caractéristique différente de 2 et de 3 est égale à 3. Les notions manipulées dans cet article dépassant le cadre de notre travail, nous nous sommes bornées à ne donner qu'une esquisse du calcul. La notion de dimension essentielle étant très "prisée" ces dernières années, elle pourrait faire l'objet d'une éventuelle future recherche.

Remerciements. Je tiens à remercier Jean-Pierre Tignol pour la quantité de temps qu'il m'a consacré, malgré ses diverses occupations, et pour ses explications claires en réponse à toutes mes questions. Je remercie aussi les autres chercheurs qui m'ont aidé dans la réalisation de ce mémoire.

1

Préliminaires

Dans ce chapitre, nous allons introduire des notions utiles pour la suite. Nous allons parler des résultants de polynômes, des extensions de corps et des espaces projectifs. Nous ne démontrerons pas tous les résultats ; le lecteur intéressé pourra trouver les preuves dans les références classiques, e.g. [Walker, 1950] pour les polynômes, [Morandi, 1996] pour les extensions de corps et [Berger, 1977] pour les espaces projectifs.

1.1 Polynômes et résultants

Si f est un polynôme n r variables et $i_1, \ldots, i_l \in \{1, \ldots, r\}$, on note soit $\partial^l_{i_1 \ldots i_l} f$ soit $\frac{\partial^l f}{\partial X_{i_1} \ldots \partial X_{i_l}}$ la dérivée partielle de f par rapport aux variables $X_{i_1}, \ldots, X_{i_l}$.

Théorème 1.1.1 *Soient k un corps de caractéristique 0, $f(X_1, \ldots, X_r)$ un polynôme en r variables à coefficients dans k et $a_1, \ldots, a_r \in k$. Alors*

$$f(X_1, \ldots, X_r) = \sum_{l=0}^{\deg f} \frac{1}{l!} \sum_{i_1, \ldots, i_l = 1}^{r} \partial^l_{i_1 \ldots i_l} f(a_1, \ldots, a_r)(X_{i_1} - a_{i_1}) \ldots (X_{i_l} - a_{i_l})$$

et cette expression est appelée développement de Taylor de f en $(X_1, \ldots, X_r) = (a_1, \ldots, a_r)$. Le résultat est encore valable si la caractéristique de k vaut p, un nombre premier, et $\deg f < p$.

Dans le cas où $r = 2$,

$$f(X_1, X_2) = \sum_{l=0}^{\deg f} \frac{1}{l!} \sum_{i_1, \ldots, i_l = 1}^{2} \partial^l_{i_1 \ldots i_l} f(a_1, a_2)(X_{i_1} - a_{i_1}) \ldots (X_{i_l} - a_{i_l}).$$

Puisque, pour toute permutation σ de $\{1, \ldots, l\}$,

$\partial^l_{i_1 \ldots i_l} f = \partial_{i_{\sigma(1)} \ldots i_{\sigma(l)}} f$ et $(X_{i_{\sigma(1)}} - a_{i_{\sigma(1)}}) \ldots (X_{i_{\sigma(l)}} - a_{i_{\sigma(l)}}) = (X_{i_1} - a_{i_1}) \ldots (X_{i_l} - a_{i_l})$,

on a

$$f(X_1, X_2) = \sum_{l=1}^{\deg f} \frac{1}{l!} \sum_{j=1}^{l} \left(\begin{array}{c} l \\ j \end{array} \right) \frac{\partial^l f}{\partial X_1^j \partial X_2^{l-j}}(a_1, a_2)(X_1 - a_1)^j (X_2 - a_2)^{l-j},$$

où $\begin{pmatrix} l \\ j \end{pmatrix} = \frac{l\cdot(l-1)\cdot\ldots\cdot(l-j+1)}{j!}$ est le cardinal de l'ensemble des l-uplets $(i_1, \ldots, i_l) \in \{1,2\}^l$ tel que $\Big|\{s \mid i_s = 1\}\Big| = j$.

Définition 1.1.2 *Soient f et g deux polynômes non constants à une variable à coefficients dans un anneau A.*

$$\begin{array}{rcl} f(X) & = & a_0 + a_1 X + \ldots + a_n X^n \\ g(X) & = & b_0 + b_1 X + \ldots + b_m X_m \end{array}$$

où $a_n, b_m \neq 0$. On définit le résultant R de f et g par

$$R = \det \begin{pmatrix} a_0 & a_1 & \ldots & \ldots & \ldots & a_n & & & \\ & a_0 & \ldots & \ldots & \ldots & a_{n-1} & a_n & & \\ & & \ddots & & & & & \ddots & \\ & & & a_0 & \ldots & \ldots & \ldots & \ldots & a_n \\ b_0 & b_1 & \ldots & b_{m-1} & b_m & & & & \\ & b_0 & & & b_{m-1} & b_m & & & \\ & & \ddots & & & & \ddots & & \\ & & & \ddots & & & & \ddots & \\ & & & & b_0 & \ldots & \ldots & \ldots & b_m \end{pmatrix}$$

avec m lignes de a_i, n lignes de b_j et les lignes étant comblées avec des zéros.

On élargit la définition au cas où f est constant non nul et g est non constant ou f est non constant et g est constant non nul. On définit comme suit le résultant de deux polynômes à plusieurs variables.

Définition 1.1.3 *Si f et g sont des polynômes non nuls en r variables à coefficients dans un anneau A, le résultant de f et g par rapport à la variable X_r est le résultant de f et g où f et g sont considérés comme des polynômes en la variable X_r à coefficients dans $A[X_1, \ldots, X_{r-1}]$ (la définition étant valable à la condition que f ou g, considéré comme un polynôme de la variable X_r, ne soit pas constant).*

Théorème 1.1.4 *Soit A un anneau à factorisation unique. Deux polynômes f et g non constants à une variable à coefficients dans A ont un facteur commun non constant si et seulement si leur résultant est nul.*

Un polynôme en r variables à coefficients dans A est un polynôme homogène de degré n si le degré de tous ses termes vaut n. Par convention, on dit que le polynôme nul est un polynôme homogène de degré n, pour tout $n \geq 0$.

Lemme 1.1.5 *Soient f et g des polynômes homogènes de degré n et m respectivement. Alors fg est un polynôme homogène de degré nm et si $n = m$, $f + g$ est un polynôme homogène de degré n.*

Théorème 1.1.6 *Soit f un polynôme homogène en r variables de degré n à coefficients dans un anneau A. Alors*

$$\sum_{i=1}^{r} X_i \cdot \partial_i f = nf$$

Ce théorème est appelé le Théorème d'Euler.

Proposition 1.1.7 *Tout facteur d'un polynôme homogène est homogène.*

Théorème 1.1.8 *Soient f et g deux polynômes homogènes en r variables à coefficients dans un anneau A. Si f et g, en tant que polynômes de la variable X_r, sont de degré n et m respectivement et, alors notant R le résultant de f et g par rapport à X_r, on a soit $R = 0$, soit R est un polynôme homogène de degré nm.*

1.2 Extensions de corps

Dans cette section, les corps considérés seront toujours commutatifs. Soit k et L deux corps. L est une extension de k s'il existe un homomorphisme d'anneaux de k dans L. Pour simplifier, on dit aussi L/k est une extension. L'homomorphisme de k dans L est injectif puisque son noyau est un idéal de k différent de k et les seuls idéaux d'un corps sont $\{0\}$ et le corps lui-même. Ainsi on peut voir k comme étant contenu dans L. Par abus de language, on pourra dire que k est un sous-corps de L. Si L est une extension de k, alors en particulier L est une espace vectoriel de k. On note $[L\colon k]$ la dimension de L sur k. On dit que L est une extension finie de k, si $[L\colon k]$ est fini.

Soit L/k une extension et S un sous-ensemble de L. On définit le corps $k(S)$ comme étant l'intersection de tous les sous-corps de L contenant S et k. Si $X = \{a_1, \dots, a_r\}$, on écrit $k(a_1, \dots, a_r)$ pour $k(S)$.

Soit $a \in L$. On dit que a est algébrique sur k s'il existe un polynôme $f(X) \in k[X]$ non nul tel que $f(a) = 0$. Si a n'est pas algébrique sur k, on dit que a est transcendant sur k. Si $a \in L$ est un élément algébrique sur k, le polynôme minimal de a sur k, noté $\mathsf{min}(k, a)$, est le polynôme unitaire (donc non nul) $f(X) \in k[X]$ de degré minimal tel que $f(a) = 0$. Un moyen de se représenter ce polynôme est de considérer l'homomorphisme d'évaluation

$$\mathsf{ev}_a\colon k[X] \to k(a)$$

qui à un polynôme $f(X) \in k[X]$ associe l'évaluation $f(a)$ de $f(X)$ en a. Dire que a est algébrique est équivalent à dire que l'homomorphisme n'est pas injectif. Ainsi $\ker(\mathsf{ev}_a)$ est un idéal non nul de $k[X]$. Il est donc engendré par un unique polynôme de $k[X]$, à un scalaire près. Le polynôme minimal de a sur k est ainsi le polynôme unitaire qui engendre $\ker(\mathsf{ev}_a)$. On dit que L est algébrique sur k si tous les éléments de L sont algébriques sur k.

Soit E une autre extension de k. Un k-homomorphisme de L dans E est un homomorphisme d'anneaux $\sigma\colon L \to E$ laissant fixes les éléments de k. Si σ est bijectif, on dit que σ est un k-isomorphisme de L dans E et si en plus $E = L$, σ est appelé k-automorphisme de L. Le groupe de Galois $\mathsf{Gal}(L/k)$ est l'ensemble des k-automorphismes de L. Si S est un sous-ensemble de $\mathsf{Gal}(L/k)$, le corps fixé par S, noté $\mathcal{F}(S)$, est le sous-corps de L défini par

$$\mathcal{F}(S) = \{a \in L \mid \tau(a) = a \text{ pour tout } \tau \in S\}.$$

Définition 1.2.1 *Soit L/k une extension. L est une extension galoisienne de k si $k = \mathcal{F}(\mathsf{Gal}(L/k))$.*

Soit L/k une extension et $f(X) \in k[X]$. On dit que $f(X)$ se factorise linéairement sur L s'il existe $\alpha \in k$ et $a_1, \ldots, a_n \in L$ tel que

$$f(X) = \alpha \prod_{i=1}^{n} (X - a_i)$$

dans $L[X]$. Soit S un ensemble de polynômes non constants sur k. On dit que L est un corps de décomposition de S sur k si tout $f \in S$ se factorise linéairement sur L et si $L = k(T)$ où T est l'ensemble de toutes les racines de tous les polynômes de S.

On dit que k est algébriquement clos, s'il ne possède pas d'extension algébrique autre que k lui-même.

Lemme 1.2.2 *Soit k un corps. Alors les assertions suivantes sont équivalentes :*
1. k est algébriquement clos.
2. Tout polynôme $f(X) \in k[X]$ se factorise linéairement sur k.
3. Tout polynôme $f(X) \in k[X]$ possède une racine dans k.

Cette propriété des corps algébriquement clos est particulièrement intéressante et permet de déduire un résultat, cette fois-ci, sur les polynômes homogènes en deux variables.

Théorème 1.2.3 *Si k est un corps algébriquement clos et f est un polynôme homogène non nul de degré n en 2 variables, alors il existe n paires $\alpha_i, \beta_i \in k$, $i = 1, \ldots, n$ et $\alpha \in k$, $\alpha \neq 0$ tels que*

$$f(X_1, X_2) = \alpha \prod_{i=1}^{n} (\alpha_i X_2 - \beta_i X_1).$$

Chaque paire α_i, β_i est unique à la multiplication d'un scalaire commun non nul près. C'est-à-dire, s'il existe des paires $\gamma_i, \delta_i \in k$, $i = 1, \ldots, n$ et $\gamma \in k$, $\gamma \neq 0$ tels que

$$f(X_1, X_2) = \gamma \prod_{i=1}^{n} (\gamma_i X_2 - \delta_i X_1),$$

alors, il existe une permutation σ de $\{1, \ldots, n\}$ et pour tout $i = 1, \ldots, n$, il existe $\lambda_i \in k$ tels que $(\gamma_i, \delta_i) = (\lambda_i \alpha_{\sigma(i)}, \lambda_i \beta_{\sigma(i)})$.

Une extension algébrique L de k est une clôture algébrique de k si L est algébrique sur k et si L est algébriquement clos. On remarque que le corps de décomposition de l'ensemble de tous les polynômes non constants sur un corps k est une clôture algébrique de k.

Théorème 1.2.4 *Soit k un corps et S un ensemble de polynômes non constants sur k, alors il existe une clôture algébrique de k et un corps de décomposition de S sur k.*

Théorème 1.2.5 *Soit k un corps et S un sous-ensemble de $k[X]$. Alors tous les corps de décomposition de S sur k sont k-isomorphes. En particulier, toutes les clôtures algébriques de k sont k-isomorphes.*

Pour un corps k, on peut ainsi parler de la clôture algébrique de k, définie à un k-isomorphisme près. Celle-ci sera notée $\overline{k}$.

Soit L/k une extension de k, alors L est une extension normale de k si L est le corps de décomposition d'un ensemble de polynômes sur k.

Soit a un élément de L algébrique sur k. Alors a est séparable sur k si $\min(k, a)$ n'a que des racines simples dans son corps de décomposition. L est une extension séparable de k si, pour tout $a \in L$, a est séparable sur k.

Théorème 1.2.6 *Soit L une extension algébrique de k. Alors L est une extension galoisienne de k si et seulement L est une extension normale et séparable de k.*

Le théorème suivant est le théorème fondamental de la théorie de Galois.

Théorème 1.2.7 *Soient L une extension galoisienne finie et $G = \mathsf{Gal}(L/k)$. Alors on a une bijection qui inverse les inclusions, entre les corps intermédiaires de L/k et les sous-groupes de G, donnée par $E \mapsto \mathsf{Gal}(L/E)$ et $H \mapsto \mathcal{F}(H)$. De plus, si $H = \mathsf{Gal}(L/E)$, alors $[L\colon E] = |H|$ et $[E\colon k] = [G\colon H]$. Et, H est un sous-groupe normal de G si et seulement si E est une extension galoisienne de k. Dans ce cas, $\mathsf{Gal}(E/k) \cong G/H$.*

Un corps k est dit séparablement clos s'il n'existe pas d'extensions séparables propres de k. Si L est une extension de k, la clôture séparable de k dans L est le corps composé des éléments de L séparables sur k. On note k_s la clôture séparable de k dans $\overline{k}$. Alors k_s est séparablement clos et k_s est une extension galoisienne de k.

1.3 Espaces projectifs

Soit E un espace vectoriel de dimension finie sur un corps k. On appelle espace projectif issu de E, noté $\mathbb{P}(E)$, le quotient $(E \setminus \{0\})/\mathcal{R}$ par la relation d'équivalence $\mathcal{R}$, où $x\mathcal{R}y$ si et seulement si $y = \lambda x$ pour un certain $\lambda \in k$.

Les élément de $\mathbb{P}(E)$ sont appelés points. La dimension de $\mathbb{P}(E)$ est par définition $\dim E-1$. La projection canonique est notée $p: E\setminus\{0\} \to \mathbb{P}(E)$. Un exemple d'espaces projectifs est $\mathbb{P}(k^{n+1})$, pour tout $n \geq 1$, que l'on note $\mathbb{P}^n(k)$. On l'appelle espace projectif standard de dimension n sur le corps k. Un espace projectif de dimension 1 (respectivement 2) est appelé droite (resp. plan) projectif.

Soit $\{e_0, \ldots, e_n\}$ une base de E. Pour tout $m \in \mathbb{P}(E)$, il existe $x \in E$ tel que $m = p(x)$. Il existe $x_0, \ldots, x_n \in k$ tels que $x = x_0e_0 + \ldots + x_ne_n$. Alors on dit que $(x_0: \ldots : x_n)$ sont des coordonnées homogènes de m par rapport à la base considérée. Si la base $\{e_0, \ldots, e_n\}$ de E est fixée, on écrira $m = (x_0: \ldots : x_n)$. On remarque que si $(x_0: \ldots : x_n)$ sont des coordonnées homogènes d'un point $m \in \mathbb{P}(E)$, alors $(y_0: \ldots : y_n)$ sont aussi des coordonnées homogènes de m si et seulement s'il existe $\lambda \in k^\times$ tel que pour tout $i = 0, \ldots, n$, $y_i = \lambda x_i$.

Soit $\mathbb{P}(E)$ un espace projectif de dimension n. On appelle repère projectif de $\mathbb{P}(E)$ un système $\{m_0, \ldots, m_{n+1}\}$ de $m + 2$ points de $\mathbb{P}(E)$ tel qu'il existe une base $\{e_0, \ldots, e_n\}$ avec

$$m_i = p(e_i) \text{ pour tout } i = 0, \ldots, n \text{ et } m_{n+1} = p(e_0 + \ldots + e_n). \tag{1.1}$$

Soit $\{m_0, \ldots, m_{n+1}\}$ un repère projectif de $\mathbb{P}(E)$. Si $\{e_i\}$ et $\{e'_i\}$ sont deux bases vérifiant la propriété (1.1) alors il existe $\lambda \in k^\times$ tel que $e'_i = \lambda e_i$ pour tout $i = 0, \ldots, n$. Ainsi la donnée d'un repère de $\mathbb{P}(E)$ permet de lui associer des systèmes de coordonnées homogènes. Pour un point $m \in \mathbb{P}(E)$, un système de coordonnées homogènes $(x_0: \ldots : x_n)$ sera alors apellé coordonnées projectives de m par rapport au repère considéré. Une caractérisation des repères projectifs sera donnée plus tard.

Soient $\mathbb{P}(E)$ et $\mathbb{P}(E')$ deux espaces projectifs. Une application $g: \mathbb{P}(E) \to \mathbb{P}(E')$ est un isomorphisme d'espaces projectifs ou une homographie s'il existe un isomorphisme d'espaces vectoriels f de E dans E' tel que $g \circ p = p \circ f$. On note $\mathsf{Isom}(\mathbb{P}(E); \mathbb{P}(E'))$ l'ensemble des homographies de $\mathbb{P}(E)$ dans $\mathbb{P}(E')$. L'application g associée à f est notée $\underline{f}$. Alors

$$\underline{f} = \underline{f'} \iff \exists \lambda \in k^\times : f' = \lambda f$$

et si f est un isomorphisme de E dans E' et f' de E' dans E'', alors $\underline{f' \circ f} = \underline{f'} \circ \underline{f}$.

Proposition 1.3.1 *L'application*

$$\mathsf{Isom}(\mathbb{P}(E); \mathbb{P}(E)) \to \mathsf{GL}(E)/k^\times \mathsf{Id}_E : f \mapsto \underline{f} \cdot k^\times \mathsf{Id}_E$$

est un isomorphisme.

Ce résultat permet de travailler à l'aide de matrices à $n+1$ lignes et $n+1$ colonnes pour représenter les homographies (à un scalaire près). La proposition suivante est appelée Premier théorème fondamental de la géométrie projective.

Proposition 1.3.2 *Soient $\mathbb{P}(E)$ et $\mathbb{P}(E')$ deux espaces projectifs de même dimension et $\{m_i\}$, $\{m'_i\}$ deux repères projectifs de $\mathbb{P}(E)$, $\mathbb{P}(E')$ respectivement. Alors il existe une unique homographie $g\colon \mathbb{P}(E) \to \mathbb{P}(E')$ telle que pour tout i, $m'_i = g(m_i)$.*

Si F est un sous-espace vectoriel de E, $F \neq 0$, alors F est stable par la relation d'équivalence $\mathcal{R}$ de la définition de l'espace projectif $\mathbb{P}(E)$. Ainsi on peut identifier $p(F \setminus \{0\}) \subset \mathbb{P}(E)$ avec $\mathbb{P}(F)$. Une partie V d'un espace projectif $\mathbb{P}(E)$ est un sous-espace projectif s'il existe un sous-espace vectoriel F de E tel que $V = p(F \setminus \{0\})$. V est alors un espace projectif de dimension $\dim F - 1$.

Le sous-espace de dimension -1 est la partie vide. Les sous-espaces de dimension 1 (resp. 2) sont appelés droites (resp. plans) de $\mathbb{P}(E)$. Les sous-espaces projectifs de $\mathbb{P}(E)$ provenant des hyperplans vectoriels de E sont aussi appelés hyperplans de $\mathbb{P}(E)$. Si $V, W \subset \mathbb{P}(E)$, $V \subset W$ et $\dim V = \dim W$, alors $V = W$. L'intersection de sous-espaces projectifs est encore un sous-espace.

Soit S une partie quelconque d'un espace projectif. On appelle sous-espace projectif engendré par S, noté $\langle S \rangle$, le plus petit sous-espace contenant S (il est égal à l'intersection de tous les sous-espaces contenant S).

Si $\mathbb{P}(E)$ est un espace projectif de dimension supérieure ou égale à 2, alors le sous-espace projectif engendré par deux points distincts de $\mathbb{P}(E)$ est une droite et le sous-espace engendré par trois points non alignés (c'est-à-dire ne se trouvant pas dans une droite de $\mathbb{P}(E)$) est un plan.

Proposition 1.3.3 *Soient V et W deux sous-espaces d'un même espace projectif, alors*

$$\dim(\langle V \cup W \rangle) + \dim(V \cap W) = \dim V + \dim W.$$

La proposition montre en particulier que deux droites distinctes d'un plan projectif se rencontrent en un et un seul point.

Proposition 1.3.4 *Soit $\{m_0, \dots, m_{n+1}\}$ un système de $n+2$ points d'un espace projectif de dimension n. Alors $\{m_0, \dots, m_{n+1}\}$ est un repère si et seulement si tout espace projectif engendré par $n+1$ points parmi $\{m_0, \dots, m_{n+1}\}$ est de dimension n.*

Si $\mathbb{P}(E)$ est un plan projectif, alors un repère est un système de 4 points distincts tel que 3 points de ce système ne sont pas alignés. Rappelons que le Premier théorème fondamental de la géométrie projective nous dit que connaître l'image par une homographie des points d'un repère caractérise l'homographie. De plus, on sait qu'il existe une homographie qui envoie un repère sur un autre repère. Alors si on travaille dans un plan projectif et on voudrait une homographie qui envoie, par exemple, 2 points distincts sur 2 points distincts, on peut affirmer qu'il en existe une (mais pas une unique puisque seules les images de 2 points sont déterminées).

Nous allons maintenant définir les espaces affines et voir leur liaison avec les espaces projectifs. Soit X un ensemble non vide. On dit que X est un espace affine s'il existe un espace vectoriel $\overrightarrow{X}$ sur un corps k et une application

$$\Theta\colon X \times X \to \overrightarrow{X}\colon (x, y) \mapsto \overrightarrow{xy}$$

tels que pour tout $x \in X$, l'application $\Theta_x\colon X \to \overrightarrow{X}\colon y \mapsto \overrightarrow{xy}$ est bijective et pour tout $x, y, z \in X$, $\overrightarrow{xy} + \overrightarrow{yz} = \overrightarrow{xz}$.

La dimension de X, notée $\dim X$, est définie comme étant la dimension de l'espace vectoriel $\overrightarrow{X}$. Si la dimension de X est 1 (resp. 2), on dit que X est une droite (resp. un plan) affine. A chaque espace vectoriel, on peut faire correspondre un espace affine de la façon suivante : pour V un espace vectoriel, $(V, \overrightarrow{V}, \Theta)$ est un espace affine où $\overrightarrow{V} = V$ et

$$\Theta\colon V \times V \to V\colon (v, w) \mapsto w - v.$$

Un repère affine de l'espace affine X est la donnée de $d + 1$ points $\{x_0, \ldots, x_d\}$ de X tels que $\{\overrightarrow{x_0 x_i}\}_{i=1,\ldots,d}$ soit une base de $\overrightarrow{X}$. Les coordonnées de $x \in X$ dans ce repère sont les $\{\lambda_i\}_{i=1,\ldots,d}$ tels que

$$\overrightarrow{x_0 x} = \lambda_1 \overrightarrow{x_0 x_1} + \ldots + \lambda_d \overrightarrow{x_0 x_d}.$$

On écrira $x = (\lambda_1, \ldots, \lambda_d)$.

Soit $(X, \overrightarrow{X}, \Theta)$ et $(X', \overrightarrow{X'}, \Theta')$ deux espaces affines sur le même corps. Une application $f\colon X \to X'$ est un morphisme d'espaces affines s'il existe $a \in X$ tel que $\Theta'_{f(a)} \circ f \circ \Theta_a^{-1}$ soit une application linéaire de $\overrightarrow{X}$ dans $\overrightarrow{X'}$. En fait, $\Theta'_{f(a)} \circ f \circ \Theta_a^{-1}$ ne dépend que de f. On note $\overrightarrow{f}$ cette application. Ainsi, pour tout $x, y \in X$,

$$\overrightarrow{f(x)f(y)} = \overrightarrow{f}(\overrightarrow{xy}).$$

Si $f\colon X \to X'$ et $g\colon X' \to X''$ sont des morphismes d'espaces affines, alors $g \circ f$ est encore un morphisme d'espaces affines et

$$\overrightarrow{g \circ f} = \overrightarrow{g} \circ \overrightarrow{f}.$$

Si $f\colon X \to X'$ est un morphisme d'espace affine bijectif, alors on dit que f est un isomorphisme d'espaces affines ou encore que X et X' sont isomorphes.

Dans le cas où $X = k^n$, on sait que $(X, \overrightarrow{X}, \Theta)$ est un espace affine, où $\overrightarrow{X} = k^n$ et $\Theta\colon X \times X \to X\colon (v, w) \mapsto w - v$. Alors un morphisme d'espace affine $f\colon X \to X$ est toujours de la forme $v \mapsto A(v) + b$, pour un certain endomorphisme A de k^n et un certain $b \in k^n$. De plus, f est un isomorphisme de X dans X si et seulement si $A \in \mathsf{GL}_n(k)$.

Soient X un espace affine. Une partie non vide $Y \subset X$ est un sous-espace s'il existe un élément $a \in Y$ tel que $\Theta_a(Y)$ soit un sous-espace vectoriel de $\overrightarrow{X}$. Dans ce cas, pour tout $b \in X$, $\Theta_b(Y) = \Theta_a(Y)$. On note $\overrightarrow{Y}$ l'espace vectoriel $\Theta_a(Y)$ et on l'appelle direction de Y. Alors $(Y, \overrightarrow{Y}, \Theta\mid_{Y\times Y})$ est un espace affine et l'inclusion $i: Y \to X$ est un morphisme d'espaces affines.

Proposition 1.3.5 *Soient $\mathbb{P}(E)$ un espace projectif et H un hyperplan de E. Alors $\mathbb{P}(E) \setminus \mathbb{P}(H)$ possède une structure naturelle d'espace affine.*

Visualisons le passage de l'espace projectif à l'espace affine. Soient $\mathbb{P}(E)$ un espace projectif et H un hyperplan de E. On choisit une base $\{e_0, \ldots, e_n\}$ de E de telle sorte que $\{e_1, \ldots, e_n\}$ soit une base de H. Alors

$$\mathbb{P}(E) \setminus \mathbb{P}(H) = \Big\{m \in \mathbb{P}(E) \mid \exists v \in H \text{ avec } m = p(v + e_0)\Big\}$$

et on a une bijection

$$\mathbb{P}(E) \setminus \mathbb{P}(H) \to k^n : p(x_0, \ldots, x_n) \mapsto \Big(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\Big).$$

Un autre choix pour les bases de E et de H donnerait un espace affine isomorphe. Soit $(X, \overrightarrow{X}, \Theta)$ un espace affine. On pose $\hat{X} = \overrightarrow{X} \cup (k^\times \times X)$, où la réunion est disjointe. Alors $\hat{X}$ possède une structure d'espace vectoriel : si $\lambda \in k^\times$ et $(\mu, x) \in k^\times \times X$, alors

$$\lambda(\mu, x) = (\lambda\mu, x) \text{ et } 0(\mu, x) = 0,$$

si $(\lambda, x), (\lambda', x') \in k^\times \times X$ et $v \in \overrightarrow{X}$, alors

$$(\lambda, x) + v = (\lambda, x + \lambda^{-1}v), \text{ où } x + w \text{ désigne l'élément } y \in X \text{ tel que } \overrightarrow{xy} = w$$
$$\text{si } \lambda + \lambda' \neq 0, (\lambda, x) + (\lambda', x') = (\lambda + \lambda', x) + \lambda'\overrightarrow{xx'}$$
$$\text{si } \lambda + \lambda' = 0, (\lambda, x) + (\lambda', x') = \lambda\overrightarrow{x'x}.$$

Sur $\overrightarrow{X}$, on garde les lois déjà existantes. On appelle $\hat{X}$ vectoriel universel de X.

Théorème 1.3.6 *Soient X un espace affine et $\hat{X}$ son vectoriel universel. On pose $\tilde{X} = \mathbb{P}(\hat{X})$. Alors X s'identifie à une partie, encore notée X, de $\tilde{X}$. Cette partie X est le complémentaire de $\mathbb{P}(\overrightarrow{X}) = \infty_X$ dans $\tilde{X}$ et $\mathbb{P}(\overrightarrow{X})$ est un hyperplan de $\tilde{X}$.*

Les opérations de passages d'espace affine à espace projectif et d'espace projectif à espace affine, définies ci-dessus, sont inverses l'une de l'autre. On appelle $\tilde{X}$ le complété projectif de X et ∞_X est l'hyperplan à l'infini de X.

Théorème 1.3.7 *Si X, X' sont des espaces affines, $\tilde{X}, \tilde{X}'$ leurs complétés et f un morphisme d'espaces affines de X dans X', alors il existe un unique morphisme d'espaces projectifs $\tilde{f}$ de $\tilde{X}$ dans $\tilde{X}'$ tel que $\tilde{f}\mid_X = f$. En outre, $\tilde{f}(\infty_X) \subset \infty_{X'}$ et $\tilde{f}\mid_{\infty_X} = \underline{\overrightarrow{f}}$.*

Soit S un sous-espace affine de l'espace affine X. Alors S est plongé dans $\tilde{X}$. Le sous-espace projectif $\langle S\rangle$ de $\tilde{X}$ engendré par S s'identifie au complété $\tilde{S}$ de S. On a donc $\langle S\rangle = \tilde{S} = S \cup \infty_S$, où $\infty_S = \infty_X \cap \tilde{S}$.

Proposition 1.3.8 *L'application $S \mapsto \tilde{S}$ est une bijection de l'ensemble des sous-espaces affines de X dans l'ensemble des sous-espaces projectifs de $\tilde{X}$ qui ne sont pas contenus dans ∞_X. De plus,*

$$\infty_S = \infty_{S'} \Longleftrightarrow \overrightarrow{S} = \overrightarrow{S'} \text{ et } \infty_S \subset \infty_{S'} \Longleftrightarrow \overrightarrow{S} \subset \overrightarrow{S'}.$$

2

Définition des cubiques

Dans cette section, nous allons définir les courbes projectives. Nous parlerons de résultats sur les courbes projectives, qui nous servirons dans le chapitre suivant. Ces résultats se trouvent dans les références de la géométrie algébrique e.g. [Brieskorn et Knörrer, 1986]. Nous en donnons les démonstrations, puisque nous n'avons pas trouver de références les explicitant. Enfin, nous définissons les cubiques, des courbes projectives particulières, et les points singuliers des cubiques

2.1 Courbes projectives

Soit k un corps (commutatif).

Définition 2.1.1 *On appelle courbe projective (ou plus simplement courbe) à coefficients dans k de degré n, un polynôme homogène non nul de degré n en 3 variables à coefficients dans k, à un scalaire non nul près.*

On devra faire attention : une courbe peut être représentée par plusieurs polynômes, multiples par un scalaire l'un de l'autre. Par abus de langage, on confrondra souvent une courbe avec un de ces représentants. Ainsi, on parlera, par exemple, de la courbe C qui "est" le polynôme $C(X_1, X_2, X_3) = X_1^4 X_2 + X_3^5$ plutôt que de préciser que la courbe C est représentée par ce polynôme. A certains endroits, il faudra faire la distinction entre la courbe et un polynôme représentant, mais on le précisera à ce moment là.

Soit C une courbe. Les points $m = (a\colon b\colon c) = p(a, b, c) \in \mathbb{P}^2(k)$ (où p désigne la projection canonique $k^3 \setminus \{0\} \to \mathbb{P}^2(k)$) vérifiant $C(a, b, c) = 0$ sont appelés points[1] de la courbe C (si $\lambda \in k^\times$ et $\deg C = n$, $(\lambda a\colon \lambda b\colon \lambda c)$ désigne de nouvelles coordonnées homogènes de m, mais on a encore $C(\lambda a, \lambda b, \lambda c) = \lambda^n C(a, b, c) = 0$). On dit aussi que m appartient à C ou encore C passe par le point m. On écrit $m \in C$. Si C' est une autre courbe, on dit que $m \in \mathbb{P}^2(k)$ est un point d'intersection de C avec C', s'il est à la fois un point de C et un point de C'.

[1]Pour être rigoureux, on devrait définir les points d'une courbe C à l'aide d'un de ses polynômes représentants et vérifier que l'ensemble de ces points ne dépend pas du choix du représentant.

Si C est une courbe de degré n et $\varphi \in \mathsf{GL}_3(k)$, alors $C \circ \varphi$ est encore une courbe de degré n. En effet, si on écrit

$$\varphi = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ et } C(X_1, X_2, X_3) = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3},$$

où la somme se fait sur les indices i_1, i_2, i_3 tels que $i_1 + i_2 + i_3 = n$, alors

$$C \circ \varphi(X_1, X_2, X_3) = \sum \lambda_{i_1,i_2,i_3} \Big(\sum_{j_1=1}^{3} a_{1j_1} X_{j_1} \Big)^{i_1} \Big(\sum_{j_2=1}^{3} a_{2j_2} X_{j_2} \Big)^{i_2} \Big(\sum_{j_3=1}^{3} a_{3j_3} X_{j_3} \Big)^{i_3}$$

est une somme, sur les indices i_1, i_2, i_3 tels que $i_1 + i_2 + i_3 = n$, de produits de 3 polynômes homogènes de degrés i_1, i_2 et i_3 respectivement. Il est donc un polynôme homogène de degré n. Il faut voir aussi que $C \circ \varphi$ est bien défini. Si f et g sont des polynômes représentants de la courbe C, alors il existe $\alpha \in k^\times$ tels que $g = \alpha f$. Ainsi

$$g \circ \varphi = (\alpha f) \circ \varphi = \alpha(f \circ \varphi)$$

et donc $g \circ \varphi$ et $f \circ \varphi$ représentent la même courbe.

Lemme 2.1.2 *Si C est une courbe projective, m est un point de C et $\varphi \in \mathsf{GL}_3(k)$, alors $\underline{\varphi}^{-1}(m)$ est un point de la courbe $C \circ \varphi$.*

Preuve : On écrit $m = (a{:}\, b{:}\, c) = p(a, b, c)$. Alors

$$\underline{\varphi}^{-1}(m) = \underline{\varphi}^{-1}(p(a, b, c)) = p(\varphi^{-1}(a, b, c))$$

et $C \circ \varphi(\varphi^{-1}(a, b, c)) = C(a, b, c) = 0$. □

Proposition 2.1.3 *L'ensemble des points d'une courbe de degré 1 est une droite de $\mathbb{P}^2(k)$. Inversement, une droite de $\mathbb{P}^2(k)$ est l'ensemble des points d'une certaine courbe de degré 1.*

Preuve : Soit C une courbe de degré 1. On écrit $C = a_1X_1 + a_2X_2 + a_3X_3$, pour certains $a_1, a_2, a_3 \in k$. On note S l'ensemble des points de C. On vérifie qu'il existe 2 points m et m' de $\mathbb{P}^2(k)$ appartenant à C (en fait, une courbe projective de degré 1 passe par au moins 3 points, puisque la courbe X_1 passe par les points $(0{:}\,1{:}\,0)$, $(0{:}\,0{:}\,1)$ et $(0{:}\,1{:}\,1)$). Il existe $\varphi \in \mathsf{GL}_3(k)$ tel que $\underline{\varphi}(m) = (0{:}\,1{:}\,0)$ et $\underline{\varphi}(m') = (0{:}\,0{:}\,1)$. Ainsi $C \circ \varphi^{-1}$ est une courbe de degré 1 passant par $(0{:}\,1{:}\,0)$ et $(0{:}\,0{:}\,1)$ et donc $C \circ \varphi^{-1} = X_1$. Alors $S = p(F \setminus \{0\})$, où F est le sous-espace vectoriel de k^3 engendré par $\varphi^{-1}(0, 1, 0)$ et $\varphi^{-1}(0, 0, 1)$. En effet, pour $m'' \in \mathbb{P}^2(k)$,

$$\begin{aligned} m'' \in S &\iff \underline{\varphi}(m'') \in X_1 \\ &\iff \exists \alpha, \beta \in k \text{ non tous nuls tels que } \underline{\varphi}(m'') = p(\alpha(0, 1, 0) + \beta(0, 0, 1)) \end{aligned}$$

$$\begin{aligned}
&\iff m'' = \underline{\varphi}^{-1}(p(\alpha(0,1,0)+\beta(0,0,1))\\
&\iff m'' = p(\varphi^{-1}(\alpha(0,1,0)+\beta(0,0,1)))\\
&\iff m'' = p(\alpha\varphi^{-1}(0,1,0)+\beta\varphi^{-1}(0,0,1))\\
&\iff m'' \in p(F\setminus\{0\}).
\end{aligned}$$

Inversement, si $S \subset \mathbb{P}^2(k)$ est une droite, alors $S = p(F\setminus\{0\})$ pour un certain F, sous-espace vectoriel de k^3 de dimension 2. Ainsi F est engendré par 2 éléments (a,b,c) et (a',b',c'). Soit $\varphi \in \mathsf{GL}_3(k)$ tel que $\underline{\varphi}(a{:}b{:}c) = (0{:}1{:}0)$ et $\underline{\varphi}(a'{:}b'{:}c') = (0{:}0{:}1)$. Puisque $\underline{\varphi}(a{:}b{:}c) = (0{:}1{:}0)$, on a $p(\varphi(a,b,c)) = p(0,1,0)$, donc il existe $\lambda \in k$ tel que $\varphi(a,b,c) = \lambda(0,1,0)$. De même, il existe $\lambda' \in k$ tel que $\varphi(a',b',c') = \lambda'(0,0,1)$. Alors, pour tout $m'' \in \mathbb{P}^2(k)$,

$$\begin{aligned}
m'' \in S &\iff \exists \alpha,\beta \in k \text{ non tous nuls tels que } m'' = p(\alpha(a,b,c)+\beta(a',b',c'))\\
&\iff \underline{\varphi}(m'') = p(\alpha\varphi(a,b,c)+\beta\varphi(a',b',c'))\\
&\iff \underline{\varphi}(m'') = p(\alpha\lambda(0,1,0)+\beta\lambda'(0,0,1))\\
&\iff \underline{\varphi}(m'') \in X_1\\
&\iff m'' \in X_1\circ\varphi.
\end{aligned}$$

S est donc l'ensemble des points de la courbe $X_1 \circ \varphi$. □

On en déduit, en outre, que par 2 points distincts de $\mathbb{P}^2(k)$ passe une unique courbe de degré 1. On confondra les notions de courbes projectives de degré 1 et d'espaces projectifs de degré 1. Ainsi, on parlera de droite pour désigner une courbe de degré 1.

Pour une droite d, on voudrait définir la multiplicité d'un point d'intersection $p \in \mathbb{P}^2(k)$ de C avec d. On la note $m_p(C,d)$. Supposons que d divise C, alors on définit pour tout point $p \in d$, $m_p(C,d) = \infty$ et pour tout $p \notin d$, $m_p(C,d) = 0$. Maintenant, si d ne divise pas C, alors il existe $\varphi \in \mathsf{GL}_3(k)$ tel que $d\circ\varphi = X_3$. Alors $C\circ\varphi(X_1,X_2,0)$ est un polynôme homogène non nul de degré n en 2 variables. De plus, les points $\underline{\varphi}(a{:}b{:}0)$ avec $C\circ\varphi(a,b,0) = 0$ sont exactement les points d'intersection de C avec d. On sait qu'il existe des $\alpha_i, \beta_i \in \overline{k}$, $\alpha \in k$, $\alpha \neq 0$ tels que

$$C\circ\varphi(X_1,X_2,0) = \alpha\prod_{i=1}^{n}(\alpha_i X_2 - \beta_i X_1).$$

Si $p \in d$, $p = \underline{\varphi}(a{:}b{:}0)$ pour certains $a,b \in k$, on définit

$$m_p(C,d) = \left|\{i \mid (a{:}b{:}0) = (\alpha_i{:}\beta_i{:}0) \text{ dans } \mathbb{P}^2(\overline{k})\}\right|$$

et si $p \notin d$, alors $m_p(C,d) = 0$. Il faut voir que cette multiplicité est bien définie. Si $\psi \in \mathsf{GL}_3(k)$ est tel que $d\circ\psi = X_3$, alors $\varphi^{-1}\circ\psi \in \mathsf{GL}_3(k)$ et $X_3\circ\varphi^{-1}\circ\psi = d\circ\psi = X_3$. On pose

$$\varphi^{-1}\circ\psi = \begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}.$$

Puisque $X_3 \circ \varphi^{-1} \circ \psi = X_3$, alors $a_{31} = 0$, $a_{32} = 0$ et $a_{33} = 1$. On peut écrire

$$C \circ \psi(X_1, X_2, 0) = \gamma \prod_{i=1}^{n} (\gamma_i X_2 - \delta_i X_1)$$

pour certains $\gamma_i, \delta_i \in \overline{k}$, $\gamma \in k$, $\gamma \neq 0$. Puisque $C \circ \psi = C \circ \varphi \circ \varphi^{-1} \circ \psi$,

$$\begin{aligned} C \circ \psi(X_1, X_2, 0) &= C \circ \varphi(a_{11}X_1 + a_{12}X_2, a_{21}X_1 + a_{22}X_2, 0) \\ &= \alpha \prod_{i=1}^{n} \Big(\alpha_i(a_{21}X_1 + a_{22}X_2) - \beta_i(a_{11}X_1 + a_{12}X_2) \Big) \\ &= \alpha \prod_{i=1}^{n} \Big((\alpha_i a_{22} - \beta_i a_{12})X_2 - (-\alpha_i a_{21} + \beta_i a_{11})X_1 \Big). \end{aligned}$$

On peut réordonner les (γ_i, δ_i) de sorte que pour tout $i = 1, \ldots, n$,

$$(\gamma_i \colon \delta_i \colon 0) = (\alpha_i a_{22} - \beta_i a_{12} \colon -\alpha_i a_{21} + \beta_i a_{11} \colon 0).$$

Mais puisque

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \frac{1}{a_{11}a_{22} - a_{21}a_{12}} \begin{pmatrix} a_{22} & -a_{12} & b_{13} \\ -a_{21} & a_{11} & b_{23} \\ 0 & 0 & b_{33} \end{pmatrix},$$

pour certains $b_{13}, b_{23}, b_{33} \in k$, on a, pour tout $i = 1, \ldots, n$

$$(\gamma_i \colon \delta_i \colon 0) = \underline{(\varphi^{-1} \circ \psi)^{-1}}(\alpha_i \colon \beta_i \colon 0)$$

et donc

$$(\alpha_i \colon \beta_i \colon 0) = \underline{\varphi^{-1} \circ \psi}(\gamma_i \colon \delta_i \colon 0).$$

Alors, si $p = \underline{\varphi}(a \colon b \colon 0) = \underline{\psi}(c \colon d \colon 0)$, $i \in \{1, \ldots, n\}$,

$$\begin{aligned} (c \colon d \colon 0) = (\gamma_i \colon \delta_i \colon 0) &\iff \underline{\varphi^{-1} \circ \psi}(c \colon d \colon 0) = \underline{\varphi^{-1} \circ \psi}(\gamma_i \colon \delta_i \colon 0) \\ &\iff (a \colon b \colon 0) = (\alpha_i \colon \beta_i \colon 0). \end{aligned}$$

Ceci prouve que la multiplicité d'un point d'intersection d'une courbe avec une droite est bien définie. Soient C une courbe de degré n et p un point de C. On considère les droites passant par p et on s'intéresse à la multiplicité du point d'intersection p de C avec chacune de ces droites. La multiplicité d'intersection étant définie à un changement de variables linéaire près, on peut supposer que $p = (1 \colon a \colon b)$. Une droite $a_1X_1 + a_2X_2 + a_3X_3$, $a_1, a_2, a_3 \in k$ passe par p si et seulement si $a_1 = -a_2a - a_3b$. On note $L_{a_3,-a_2} = (-a_2a - a_3b)X_1 + a_2X_2 + a_3X_3$ une droite quelconque passant par p. Un point $(1 \colon x \colon y) \in L_{a_3,-a_2}$ si et seulement s'il existe $t \in k$ tels que

$$x = a + a_3t \text{ et } y = b - a_2t.$$

En effet, si $(1, x, y) \in L_{a_3,-a_2}$,alors $a_2(x-a)+a_3(y-b)=0$. On a soit $a_2 \neq 0$, soit $a_3 \neq 0$. Si $a_2 \neq 0$, alors $x = a + a_3(\frac{-1}{a_2}(y-b))$. On choisit $t = \frac{-1}{a_2}(y-b)$, alors on a bien $x = a + a_3 t$ et $y = b - a_2 t$. Si $a_3 \neq 0$, alors $y = b - a_2(\frac{1}{a_3}(x-a))$. Si on choisit $t = \frac{1}{a_3}(x-a)$, on a $x = a + a_3 t$ et $y = b - a_2 t$. Dans l'autre sens, c'est évident. On pose $\lambda = a_3$ et $\mu = -a_2$.

Lemme 2.1.4 *La multiplicité de l'intersection p de C avec $L_{\lambda,\mu}$ est la multiplicité de la racine $t = 0$ du polynôme $g(t) = C(1, a + \lambda t, b + \mu t)$.*

Preuve : Soit $\varphi \in \mathsf{GL}_3(k)$ tel que $L_{\lambda,\mu} \circ \varphi = X_3$ et $X_1 \circ \varphi = X_1$. On pose

$$\varphi = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Puisque $X_1 \circ \varphi = X_1$, alors $a_{11} = 1$, $a_{12} = 0$ et $a_{13} = 0$. Ainsi

$$\varphi = \begin{pmatrix} 1 & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Et $L_{\lambda,\mu} \circ \varphi = X_3$ implique

$$\begin{cases} (\mu a - \lambda b).(1) - \mu a_{21} + \lambda a_{31} = 0 \\ (\mu a - \lambda b).(0) - \mu a_{22} + \lambda a_{32} = 0 \\ (\mu a - \lambda b).(0) - \mu a_{23} + \lambda a_{33} = 1 \end{cases} \Longleftrightarrow \begin{cases} \lambda(a_{31} - b) = \mu(a_{21} - a) \\ \lambda a_{32} = \mu a_{22} \\ \lambda a_{33} = 1 + \mu a_{23} \end{cases}.$$

Par définition, si $L_{\lambda,\mu}$ divise C, alors $m_p(C, L_{\lambda,\mu}) = \infty$ et si $L_{\lambda,\mu}$ ne divise pas C,

$$C \circ \varphi(X_1, X_2, 0) = \alpha \prod_{i=1}^{n} (\alpha_1 X_2 - \beta_i X_1),$$

pour certains $\alpha_i, \beta_i \in \overline{k}$, $\alpha \in k$, $\alpha \neq 0$, $p = \underline{\varphi}(1{:}\,c{:}\,0)$, $c \in k$, alors

$$m_p(C, L_{\lambda,\mu}) = \Big| \{ i \mid (\alpha_i{:}\,\beta_i{:}\,0) = (1{:}\,c{:}\,0) \text{ dans } \mathbb{P}^2(\overline{k}) \} \Big|.$$

On pose $f(X) = C \circ \varphi(1, X, 0)$. Si $L_{\lambda,\mu}$ ne divise pas C,

$$f(X) = \alpha \prod_{i=1}^{n} (\alpha_i X - \beta_i)$$

et

$$(\alpha_i{:}\,\beta_i{:}\,0) = (1{:}\,c{:}\,0) \Longleftrightarrow \exists d \in k \text{ tel que } \alpha_i = d \text{ et } \beta_i = dc \Longleftrightarrow \beta_i = c\alpha_i.$$

Alors, puisque $f(X) = 0$ si et seulement si $L_{\lambda,\mu}$ divise C, $m_p(C, L_{\lambda,\mu})$ est égal à la multiplicité de la racine c du polynôme $f(X)$. On va voir que

$$f(X) = C(1, a + \lambda \cdot t(X), b + \mu \cdot t(X))$$

pour un certain polynôme $t(X) \in k[X]$ de degré 1. Si $\mu \neq 0$, $a_{21} = a + \frac{\lambda}{\mu}(a_{31} - b)$ et $a_{22} = \frac{\lambda}{\mu} a_{32}$. Ainsi

$$a_{21} + a_{22}X = a + \lambda\Big(\frac{1}{\mu}(a_{31} - b + a_{32}X)\Big).$$

On pose $t(X) = \frac{1}{\mu} a_{32} X + \frac{1}{\mu}(a_{31} - b)$. Alors

$$\begin{cases} a_{21} + a_{22}X = a + \lambda \cdot t(X) \\ a_{31} + a_{32}X = b + \mu \cdot t(X) \end{cases}$$

et $t(X) = \alpha X + \beta$ avec $\alpha \neq 0$ (en effet, si $a_{32} = 0$, puisque $\lambda a_{32} = \mu a_{22}$, alors $a_{22} = 0$, ce qui impliquerait $\det \varphi = 0$). Si $\lambda \neq 0$, $a_{31} = b + \frac{\mu}{\lambda}(a_{21} - a)$ et $a_{32} = \frac{\mu}{\lambda} a_{22}$. Ainsi

$$a_{31} + a_{32}X = b + \mu\Big(\frac{1}{\lambda}(a_{21} - a) + a_{22}X)\Big).$$

On pose $t(X) = \frac{1}{\lambda} a_{22} X + \frac{1}{\lambda}(a_{21} - a)$. Alors

$$\begin{cases} a_{21} + a_{22}X = a + \lambda \cdot t(X) \\ a_{31} + a_{32}X = b + \mu \cdot t(X) \end{cases}$$

et $t(X) = \alpha X + \beta$ avec $\alpha \neq 0$ (car $a_{22} \neq 0$). Ainsi

$$f(X) = C \circ \varphi(1, X, 0) = C(1, a + \lambda \cdot t(X), b + \mu \cdot t(X)) = g \circ t(X).$$

$$\varphi(1, c, 0) = (1, a, b) \Rightarrow \begin{cases} a_{21} + a_{22}c = a \\ a_{31} + a_{32}c = b \end{cases}.$$

Si $\mu \neq 0$ (alors $a_{32} \neq 0$),

$$t(c) = \frac{1}{\mu} a_{32} \frac{b - a_{31}}{a_{32}} + \frac{1}{\mu}(a_{31} - b) = 0$$

et si $\lambda \neq 0$ (alors $a_{22} \neq 0$),

$$t(c) = \frac{1}{\lambda} a_{22} \frac{a - a_{21}}{a_{22}} + \frac{1}{\lambda}(a_{21} - a) = 0.$$

Dans tous les cas, $t(X) = \alpha(X - c)$. Soit

$$g(t) = g(0) + g'(0)t + \ldots + \frac{g^{(n)}(0)}{n!} t^n$$

le développement de Taylor de g en $t = 0$. Alors

$$f(X) = g \circ t(X) = g(0) + \alpha g'(0)(X - c) + \ldots + \alpha^n \frac{g^{(n)}(0)}{n!}(X - c)^n.$$

Ainsi la multiplicité de la racine c du polynôme $f(X)$ et égale à celle de la racine $t = 0$ du polynôme $g(t)$. $\square$

Définition 2.1.5 *Soit C une courbe et $p = (a_1 \colon a_2 \colon a_3)$ un point de C. On définit la multiplicité de C en p, notée $m_p(C)$, comme étant l'entier m tel que pour tout $l < m$, $i_1, \ldots, i_l \in \{1, 2, 3\}$,*

$$\partial^l_{i_1 \ldots i_l} C(a_1, a_2, a_3) = 0$$

et tel qu'il existe $i_1, \ldots, i_m \in \{1, 2, 3\}$ avec $\partial^m_{i_1 \ldots i_m} C(a_1, a_2, a_3) \neq 0$.

Soit C une courbe et $p = (a_1 \colon a_2 \colon a_3)$ un point de C. On pose $m = m_p(C)$. Soit $\varphi \in \mathsf{GL}_3(k)$ tel que $p = \underline{\varphi}(1 \colon a \colon b)$ pour certains $a, b \in k$. Alors pour tout $l < m$, $j = 0, \ldots, l$,

$$\frac{\partial^l (C \circ \varphi)}{\partial X_2^j \partial X_3^{l-j}}(1, a, b) = 0.$$

En effet, si

$$\varphi = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

par induction, on prouve que, pour tout entier $l = 0, \ldots, \deg C$, $i_1, \ldots, i_l \in \{1, 2, 3\}$,

$$\partial^l_{i_1 \ldots i_l}(C \circ \varphi) = \sum_{j_1, \ldots, j_l = 1}^{3} a_{j_1 i_1} \ldots a_{j_l i_l} \left(\partial^l_{j_1 \ldots j_l} C \right) \circ \varphi.$$

Et, il existe $j \in \{0, \ldots, m\}$ tel que

$$\frac{\partial^m (C \circ \varphi)}{\partial X_2^j \partial X_3^{m-j}}(1, a, b) \neq 0.$$

En effet, si pour tout $i_1, \ldots, i_m \in \{1, 2, 3\}$,

$$\frac{\partial^m (C \circ \varphi)}{\partial X_2^j \partial X_3^{m-j}}(1, a, b) = 0,$$

alors pour tout $j = 0, \ldots, m-1$, si on pose

$$f = \frac{\partial^{m-1} (C \circ \varphi)}{\partial X_2^j \partial X_3^{m-1-j}},$$

par la formule d'Euler, on a

$$\partial_1 f(1, a, b) + a \partial_2 f(1, a, b) + b \partial_3 f(1, a, b) = \deg f \cdot f(1, a, b).$$

Or $\partial_2 f(1, a, b) = \partial_3 f(1, a, b) = f(1, a, b) = 0$, d'où

$$\frac{\partial^m (C \circ \varphi)}{\partial X_1 \partial X_2^j \partial X_3^{m-1-j}}(1, a, b) = \partial_1 f(1, a, b) = 0.$$

En procédant de la même manière avec

$$f = \frac{\partial^m (C \circ \varphi)}{\partial X_1 \partial X_2^j \partial X_3^{m-2-j}},$$

on obtient

$$\frac{\partial^m (C \circ \varphi)}{\partial X_1^2 \partial X_2^j \partial X_3^{m-2-j}}(1, a, b) = 0.$$

On continue jusqu'à obtenir, pour tout $i_1, \ldots, i_m \in \{1, 2, 3\}$,

$$\partial^m_{i_1,\ldots,i_m}(C \circ \varphi)(1, a, b) = 0.$$

Mais en utilisant cette fois-ci

$$\varphi^{-1} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix},$$

on obtient pour tout $l = 0, \ldots, \deg C$ et pour tout $i_1, \ldots, i_l \in \{1, 2, 3\}$,

$$\left(\partial^l_{i_1 \ldots i_l} C\right) \circ \varphi \quad = \quad \sum_{j_1, \ldots, j_l = 1}^{3} b_{j_1 i_1} \ldots b_{j_l i_l} \partial^l_{j_1 \ldots j_l}(C \circ \varphi). \qquad (2.1)$$

Ainsi pour tout $i_1, \ldots, i_m \in \{1, 2, 3\}$, $\partial^m_{i_1 \ldots i_m} C \circ \varphi(1, a, b) = 0$ et ceci contredit le fait que $m_p(C) = m$. Soit $\lambda, \mu \in k$ non tous nuls. On considère le développement de Taylor du polynôme $C \circ \varphi(1, X, Y)$ en $(X, Y) = (a, b)$:

$$C \circ \varphi(1, X, Y) = \sum_{l=0}^{n} \frac{1}{l!} \sum_{i=0}^{l} \begin{pmatrix} l \\ i \end{pmatrix} \frac{\partial^l (C \circ \varphi)}{\partial X_2^i \partial X_3^{l-i}}(1, a, b)(X - a)^i (Y - b)^{l-i}.$$

Alors

$$C \circ \varphi(1, a + \lambda t, b + \mu t) = \sum_{l=0}^{n} \Big(\frac{1}{l!} \sum_{i=0}^{l} \begin{pmatrix} l \\ i \end{pmatrix} \frac{\partial^l (C \circ \varphi)}{\partial X_2^i \partial X_3^{l-i}}(1, a, b) \lambda^i \mu^{l-i}\Big) t^l.$$

Donc la multiplicité de la racine $t = 0$ du polynôme $C \circ \varphi(1, a + \lambda t, b + \mu t)$ est supérieure ou égale à $m_p(C)$. Ainsi toutes les droites passant par p coupent C avec une multiplicité supérieure ou égale à $m_p(C)$. Les droites passant par p qui coupent C avec une multiplicité strictement supérieure à $m_p(C)$ sont les droites $L_{\lambda,\mu} \circ \varphi^{-1}$ telles que (λ, μ) soit racine du polynôme des variables X, Y

$$g(X, Y) = \sum_{i=1}^{m} \begin{pmatrix} m \\ i \end{pmatrix} \frac{\partial^m (C \circ \varphi)}{\partial X_2^i \partial X_3^{m-i}}(1, a, b) X^i Y^{m-i}.$$

Il y en a au plus m.

Définition 2.1.6 *Les m droites $L_{\lambda,\mu} \circ \varphi^{-1}$ (comptées avec la multiplicité de la racine $(X,Y) = (\lambda,\mu)$ du polynôme $g(X,Y)$) qui coupent C en p avec une multiplicité strictement supérieure à m sont appelées tangentes à C en p.*

Si $m_p(C) = 1$, il existe une unique tangente à C en p. C'est la droite $L_{\lambda,\mu}$ avec (λ,μ) racine du polynôme $\partial_2(C \circ \varphi)(1,a,b)X + \partial_3(C \circ \varphi)(1,a,b)Y$, c'est-à-dire

$$(\lambda{:}\, \mu) = \Big(\partial_3(C \circ \varphi)(1,a,b){:} -\partial_2(C \circ \varphi)(1,a,b)\Big).$$

Alors $\mu a - \lambda b = -\partial_2(C \circ \varphi)(1,a,b)a - \partial_3(C \circ \varphi)(1,a,b)b$. Ainsi, par le Théorème d'Euler, $\mu a - \lambda b = \partial_1(C \circ \varphi)(1,a,b)$. Alors la tangente T à C en p est la droite

$$\Big(\partial_1(C\circ\varphi)(1,a,b)X_1 + \partial_2(C\circ\varphi)(1,a,b)X_2 + \partial_3(C\circ\varphi)(1,a,b)X_3\Big) \circ \varphi^{-1}(X_1,X_2,X_3).$$

Par la relation (1.2), on trouve que

$$T(X_1,X_2,X_3) = \partial_1 C(a_1,a_2,a_3)X_1 + \partial_2 C(a_1,a_2,a_3)X_2 + \partial_3 C(a_1,a_2,a_3)X_3.$$

2.2 Cubiques

Soit k un corps.

Définition 2.2.1 *Une cubique en 3 variables à coefficients dans k est une courbe projective à coefficients dans k de degré 3.*

Pour simplifier, on dira cubique pour cubique en 3 variables. On note $C_{3,3}(k)$ l'ensemble des cubiques à coefficients dans k. On a une action de $\mathsf{GL}_3(k)$ sur $C_{3,3}(k)$ de la manière suivante : si $C \in C_{3,3}(k)$ et $\varphi \in \mathsf{GL}_3(k)$, alors on définit $\varphi(C)$ comme étant $C \circ \varphi$. On remarque que par cette action les matrices scalaires laissent les cubiques invariantes.

Définition 2.2.2 *Une cubique $C \in C_{3,3}(k)$ est dite singulière si elle possède un point singulier, c'est-à-dire un point $(a_1{:}\, a_2{:}\, a_3) \in \mathbb{P}^2(\overline{k})$, où $\overline{k}$ désigne la clôture algébrique de k, tel que $C(a_1,a_2,a_3) = 0$ et $\forall i \in \{1,2,3\}$, $\partial_i C(a_1,a_2,a_3) = 0$ (un point singulier est donc un point de C tel que la multiplicité de C en ce point est strictement supérieure à 1).*

Si la caractéristique de k est différente de 3, alors il n'est pas utile de préciser que $C(a_1,a_2,a_3) = 0$ dans la définition de point singulier, car si $\partial_i C(a_1,a_2,a_3) = 0$ pour tout i, on déduit par le Théorème d'Euler que $C(a_1,a_2,a_3) = 0$.

On note $C^-_{3,3}(k)$ l'ensemble des cubiques singulières et $C^+_{3,3}(k)$ l'ensemble des cubiques non singulières. L'action de $\mathsf{GL}_3(k)$ se restreint à $C^+_{3,3}(k)$ et à $C^-_{3,3}(k)$, en effet si $\varphi \in \mathsf{GL}_3(k), C, C' \in C_{3,3}(k)$ tels que $C' \circ \varphi(X_1,X_2,X_3) = C(X_1,X_2,X_3)$, on écrit $\varphi(X_1,X_2,X_3) = (Y_1,Y_2,Y_3)$ où $Y_i = \sum_{j=1}^3 a_{ij}X_j$ et $det(a_{ij}) \neq 0$; alors

$$\partial_i C(X_1,X_2,X_3) = \partial_i(C' \circ \varphi)(X_1,X_2,X_3) = \sum_{j=1}^{3} a_{ji}\partial_j C'(\varphi(X_1,X_2,X_3))$$

et donc $(a_1\colon a_2\colon a_3)$ est un point singulier de C si et seulement si $\underline{\varphi}(a_1\colon a_2\colon a_3)$ est un point singulier de C'.

Lemme 2.2.3 *Si C est une cubique à coefficients dans k non singulière, alors C est irréductible en tant qu'élément de $\overline{k}[X_1, X_2, X_3]$.*

Preuve : Supposons que C soit réductible dans $\overline{k}[X_1, X_2, X_3]$, alors il existe une droite d et une courbe Q de degré 2 à coefficients dans $\overline{k}$ telles que $C = d \cdot Q$. On peut supposer que $d = X_1$, car il existe $\varphi \in \mathsf{GL}_3(\overline{k})$ tel que $d \circ \varphi = X_1$ et alors $C \circ \varphi = d \circ \varphi \cdot Q \circ \varphi = X_1 \cdot Q \circ \varphi$. Alors les dérivées partielles sont :

$$\begin{aligned} \partial_1 C &= Q + X_1 \partial_1 Q \\ \partial_2 C &= X_1 \partial_2 Q \\ \partial_3 C &= X_1 \partial_3 Q. \end{aligned}$$

Or on a soit $Q(0, X_2, X_3) = 0$, soit $Q(0, X_2, X_3)$ est un polynôme homogène non nul de degré 2 en 2 variables. Dans tous les cas, il existe $b, c \in \overline{k}$, non tous nuls, tels que $Q(0, b, c) = 0$. Alors $(0\colon b\colon c)$ est un point singulier de C. $\square$

Les points singuliers d'une cubique à coefficients dans k ne sont par forcément dans $\mathbb{P}^2(k)$. En effet, la cubique $X_1^3 + X_2^3 + X_3^3 - 3X_1X_2X_3$ est à coefficients dans $\mathbb{Q}$ et pourtant $(\epsilon\colon \epsilon^2\colon 1)$ et $(\epsilon^2\colon \epsilon\colon 1)$ sont des points singuliers de C, où $\epsilon \notin \mathbb{Q}$ est une racine cubique primitive de l'unité.

Définition 2.2.4 *On dit que les cubiques C et C' sont équivalentes et on écrit $C \sim C'$, si elles sont dans la même orbite sous l'action de $\mathsf{GL}_3(k)$.*

Ceci définit une relation d'équivalence sur les cubiques. On note $[C]$ la classe d'équivalence de la cubique C. On note $\mathsf{Cub}_3(k)$, respectivement $\mathsf{Cub}_3^+(k)$ et $\mathsf{Cub}_3^-(k)$, l'ensemble $C_{3,3}(k)$,respectivement $C_{3,3}^+(k)$ et $C_{3,3}^-(k)$, quotienté par cette relation d'équivalence.

3

Propriétés des cubiques

Dans ce chapitre, nous allons voir que toute cubique non singulière à coefficients dans un corps k séparablement clos est équivalente à une forme particulière appelée forme normale, et qu'elle possède 9 points d'inflexion dans $\mathbb{P}^2(k)$. Ensuite, on introduira un invariant sur les cubiques non singulières, on parlera de pinceaux canoniques et on étudiera un cas particulier de cubiques non singulières. Enfin, on discutera les différentes classes d'équivalence de cubiques singulières.

3.1 Points d'inflexion d'une cubique

Définition 3.1.1 *Soit C une cubique. Un point $p \in C$ non singulier est appelé point d'inflexion de C si la tangente à C en p intersecte C en p avec une multiplicité supérieure ou égale à 3.*

La définition de multiplicité d'intersection d'une courbe avec une droite étant définie à un changement de variables linéaire près, on a que, pour tout $\varphi \in \mathsf{GL}_3(k)$, p est un point d'inflexion d'une cubique C, si et seulement si $\underline{\varphi}^{-1}(p)$ est un point d'inflexion de $C \circ \varphi$.

Définition 3.1.2 *Soit C une cubique. Le hessien de C, noté H_C, est la courbe projective définie par $H_C = \det(\partial^2_{ij}C)$.*

Il faut voir que le hessien H_C ne dépend pas du choix du polynôme représentant la cubique C. Ceci est vrai car si f et g sont des polynômes représentant C, alors il existe $\alpha \in k^\times$ tel que $g = \alpha f$. Or $\det(\partial^2_{ij}g) = \alpha^3 \det(\partial^2_{ij}f)$, donc $\det(\partial^2_{ij}g)$ et $\det(\partial^2_{ij}f)$ représentent la même courbe. On vérifie que H_C est une cubique, puisque les dérivées partielles secondes $\partial^2_{ij}C$ sont des polynômes homogènes de degré 1 et $\det(\partial^2_{ij}C)$ est une somme de produits de 3 tels polynômes.

Proposition 3.1.3 *Si C est une cubique et $\varphi \in \mathsf{GL}_3(k)$, alors*

$$H_{C\circ\varphi} = (\det \varphi)^2 H_C \circ \varphi.$$

Preuve : On écrit $\varphi(X_1, X_2, X_3) = (Y_1, Y_2, Y_3)$ où $Y_i = \sum_{j=1}^{3} a_{ij} X_j$. Alors

$$\partial^2_{ij}(C \circ \varphi) = \sum_{k=1}^{3} \sum_{l=1}^{3} a_{kj} a_{li} (\partial^2_{lk} C) \circ \varphi.$$

D'où

$$\begin{aligned} H_{C\circ\varphi} &= \det\Big(\partial^2_{ij}(C \circ \varphi)\Big) \\ &= \det\Big((a_{ji}) \cdot (\partial^2_{ij} C) \circ \varphi \cdot (a_{ij})\Big) \\ &= (\det\varphi)^2 \cdot det(\partial^2_{ij} C) \circ \varphi \\ &= (\det\varphi)^2 H_C \circ \varphi. \end{aligned}$$

□

Grâce à cette proposition, on voit qu'on peut définir le hessien pour une classe d'équivalence de cubiques.

Exemple 3.1.4 *Si* $C(X_1, X_2, X_3) = X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1 X_2 X_3$, *alors*

$$H_C(X_1, X_2, X_3) = -54\lambda^2(X_1^3 + X_2^3 + X_3^3) + (216 - 54\lambda^3) X_1 X_2 X_3.$$

On peut voir que les points singuliers d'une cubique C sont des points de H_C. En effet, d'après le Théorème d'Euler, si $(a_1 \colon a_2 \colon a_3)$ est un point singulier de C, alors

$$0 = 2\partial_i C(a_1, a_2, a_3) = \sum_{j=1}^{3} \partial^2_{ij} C(a_1, a_2, a_3) a_j, \quad i = 1, 2, 3.$$

Ainsi les colonnes de la matrice $(\partial^2_{ij} C(a_1, a_2, a_3))$ sont linéairement dépendantes et alors $\det(\partial^2_{ij} C(a_1, a_2, a_3)) = 0$.

Théorème 3.1.5 *Un point non singulier d'une cubique C à coefficients dans un corps k de caractéristique différente de 2 est un point d'inflexion de C si et seulement s'il est un point d'intersection de C avec son hessien.*

Preuve : Soit p un point non singulier de C. On peut supposer que $p = (1\colon 0\colon 0)$ et l'équation de la tangente T à C en p soit $T(X_1, X_2, X_3) = X_3$. En effet, pour tout $\varphi \in \mathsf{GL}_3(\overline{k})$, p est un point d'inflexion de C si et seulement si $\underline{\varphi}^{-1}(p)$ est un point d'inflexion de $C \circ \varphi$ et p est un point de H_C si et seulement si $\underline{\varphi}^{-1}(p)$ est un point de $H_{C\circ\varphi} = \det(\varphi)^2 H_C \circ \varphi$. Si X_3 divise C, alors il existe un polynôme homogène Q de degré 2 en 3 variables tel que $C(X_1, X_2, X_3) = X_3 Q(X_1, X_2, X_3)$. Alors

$$H_C(X_1, X_2, X_3) = \det \begin{pmatrix} X_3\partial^2_{11}Q & X_3\partial^2_{12}Q & X_3\partial^2_{13}Q + \partial_1 Q \\ X_3\partial^2_{12}Q & X_3\partial^2_{22}Q & X_3\partial^2_{23}Q + \partial_2 Q \\ X_3\partial^2_{13}Q + \partial_1 Q & X_3\partial^2_{23}Q + \partial_2 Q & X_3\partial^2_{33}Q + 2\partial_3 Q \end{pmatrix}.$$

Ainsi X_3 divise aussi H_C. Donc p est un point de H_C et p est un point d'inflexion de C. Supposons maintenant que X_3 ne divise pas C. Si la multiplicité de l'intersection de C avec T vaut $r+2$, avec $r=0$ ou $r=1$, alors

$$C(X_1,X_2,0) = X_2^{r+2}\cdot a\prod_{i=r+3}^{3}(a_iX_2-b_iX_1),$$

pour certains $a_i, b_i \in k$ tels que $(a_i\colon b_i)\neq(1\colon 0)$. Alors on peut écrire

$$C(X_1,X_2,0)=X_2^{r+2}G(X_1,X_2),$$

où G est un polynôme homogène de degré $3-r-2$ en 2 variables tel que $G(1,0)\neq 0$ et donc $C(X_1,X_2,X_3)=X_3\cdot U(X_1,X_2,X_3)+X_2^{r+2}\cdot G(X_1,X_2)$ où U est un polynôme homogène de degré 2 en 3 variables. En général, la tangente T à C en un point non singulier $q=(q_1\colon q_2\colon q_3)$ est donnée par

$$T(X_1,X_2,X_3)=\partial_1C(q_1,q_2,q_3)X_1+\partial_2C(q_1,q_2,q_3)X_2+\partial_3C(q_1,q_2,q_3)X_3.$$

Donc $\partial_3C(1,0,0)\neq 0$. Or $\partial_3C(X_1,X_2,X_3)=U(X_1,X_2,X_3)+X_2\cdot\partial_3U(X_1,X_2,X_3)$, donc $U(1,0,0)\neq 0$. On peut voir aussi que $\partial_1U(1,0,0)\neq 0$. Pour cela, on écrit $C(X_1,X_2,X_3)=\sum_{i_1+i_2+i_3=3}\lambda_{i_1,i_2,i_3}X_1^{i_1}X_2^{i_2}X_3^{i_3}$. Alors

$$U(X_1,X_2,X_3)=\sum_{i_1+i_2+i_3=3,i_3\geq 1}\lambda_{i_1,i_2,i_3}X_1^{i_1}X_2^{i_2}X_3^{i_3-1}.$$

D'où

$$\partial_1U(X_1,X_2,X_3)=\sum_{i_1+i_2+i_3=3,i_1,i_3\geq 1}\lambda_{i_1,i_2,i_3}i_1X_1^{i_1-1}X_2^{i_2}X_3^{i_3-1}$$

et

$$\partial_1U(1,0,0)=\sum_{i_1+i_2+i_3=3,i_2=0=i_3-1}\lambda_{i_1,i_2,i_3}i_1 1^{i_1-1}0^{i_2}0^{i_3-1}=2\lambda_{2,0,1}.$$

Or

$$U(1,0,0)=\sum_{i_1+i_2+i_3=3,i_2=0=i_3-1}\lambda_{i_1,i_2,i_3}X_1^{i_1}X_2^{i_2}X_3^{i_3-1}=\lambda_{2,0,1}\neq 0.$$

Donc $\partial_1U(1,0,0)\neq 0$. On veut calculer H_C, pour cela on a besoin des dérivées partielles secondes de C.

$$\begin{array}{rcl}
\partial_1C &=& X_3\cdot\partial_1U+X_2^{r+2}\cdot\partial_1G\\
\partial_{11}^2C &=& X_3\cdot\partial_{11}^2U+X_2^{r+2}\cdot\partial_{11}^2G\\
\partial_{12}^2C &=& X_3\cdot\partial_{12}^2U+(r+2)X_2^{r+1}\cdot\partial_1G+X_2^{r+2}\cdot\partial_{12}^2G\\
\partial_{13}^2C &=& \partial_1U+X_3\cdot\partial_{13}^2U\\
\partial_2C &=& X_3\cdot\partial_2U+(r+2)X_2^{r+1}\cdot G+X_2^{r+2}\cdot\partial_2G\\
\partial_{22}^2C &=& X_3\cdot\partial_{22}^2U+(r+2)(r+1)X_2^{r}\cdot G+2(r+2)X_2^{r+1}\cdot\partial_2G+X_2^{r+2}\cdot\partial_{22}^2G\\
\partial_{23}^2C &=& \partial_2U+X_3\cdot\partial_{23}^2U\\
\partial_3C &=& U+X_3\cdot\partial_3U\\
\partial_{33}^2C &=& 2\partial_3U+X_3\cdot\partial_{33}^2U.
\end{array}$$

Alors $H_C(X_1, X_2, 0)$ vaut le déterminant de

$$\begin{pmatrix} X_2^{r+2} \cdot \partial_{11}^2 G & \kappa X_2^{r+1} \cdot \partial_1 G + X_2^{r+2} \cdot \partial_{12}^2 G & \partial_1 U \\ \kappa X_2^{r+1} \cdot \partial_1 G + X_2^{r+2} \cdot \partial_{12}^2 G & \kappa' X_2^r \cdot G + \kappa'' X_2^{r+1} \cdot \partial_2 G + X_2^{r+2} \cdot \partial_{22}^2 G & \partial_2 U \\ \partial_1 U & \partial_2 U & 2\partial_2 U \end{pmatrix},$$

où $\kappa = r + 2$, $\kappa' = (r + 2)(r + 1)$ et $\kappa'' = 2(r + 2)$. Ainsi

$$H_C(X_1, X_2, 0) = X_2^r \cdot H(X_1, X_2),$$

où H est un polynôme homogène de degré $3 - r$ en 2 variables et

$$H(1, 0) = (r + 2)(r + 1) \cdot G(1, 0)(\partial_1 U(1, 0, 0))^2 \neq 0.$$

Ainsi, $H_C(1, 0, 0) = 0$ si et seulement si $r > 0$ et donc $(1{:}\,0{:}\,0)$ est un point d'intersection de C avec H_C si et seulement si $(1{:}\,0{:}\,0)$ est un point d'inflexion de la cubique C. □

Théorème 3.1.6 *Toute cubique non singulière en 3 variables à coefficients dans un corps algébriquement clos de caractéristique différente de 2 et de 3 possède au moins 2 points d'inflexion.*

Preuve : Soit k un corps algébriquement clos, $\mathsf{car}(k) \neq 2, 3$ et C une cubique non singulière en 3 variables à coefficients dans k. On cherche un premier point d'inflexion, c'est-à-dire un point d'intersection de C avec H_C. Il existe au moins un point qui n'appartient ni à C ni à H_C. On fait un changement de coordonnées pour que ce point soit $(0{:}\,0{:}\,1)$. Alors C et H_C sont tous les deux des polynômes de degré 3 en la variable X_3. On considère le résultant $R(X_1, X_2)$ de C et H_C par rapport à X_3. On sait alors que soit $R = 0$, soit R est un polynôme homogène de degré 9. Si $R = 0$, alors C et H_C ont un facteur commun non constant $F(X_1, X_2, X_3) \in k[X_1, X_2][X_3]$. On peut écrire

$$F(X_1, X_2, X_3) = F_r(X_1, X_2)X_3^r + \ldots + F_1(X_1, X_2)X_3 + F_0(X_1, X_2),$$

où les $F_i(X_1, X_2)$ sont des polynômes homogènes en 2 variables à coefficients dans k et $F_r(X_1, X_2) \neq 0$, $r > 0$. Alors, comme k est infini, il existe $\alpha_1, \alpha_2 \in k$ tels que $F_r(\alpha_1, \alpha_2) \neq 0$. Ainsi $F(\alpha_1, \alpha_2, X_3)$ est un polynôme à une seule variable de degré non nul. Puisque k est algébriquement clos, $F(\alpha_1, \alpha_2, X_3)$ possède une racine α_3 dans k. On obtient ainsi un point d'inflexion $(\alpha_1{:}\,\alpha_2{:}\,\alpha_3)$. Dans le cas où R est un polynôme homogène de degré 9, on peut alors écrire

$$R(X_1, X_2) = \alpha \prod_{i=1}^{9} (\alpha_i X_2 - \beta_i X_1)$$

avec $\alpha, \alpha_i, \beta_i \in k$ et $\alpha \neq 0$. Ainsi $R(\alpha_1, \beta_1) = 0$, ce qui veut dire que les polynômes $C(\alpha_1, \beta_1, X_3)$ et $H_C(\alpha_1, \beta_1, X_3)$ ont un facteur commun non constant et donc une racine commune γ_1 dans k. On trouve aussi un point d'inflexion $(\alpha_1 : \beta_1 : \gamma_1)$. On note p le premier point d'inflexion. Il faut maintenant trouver un autre point d'inflexion. On choisit des coordonnées homogènes telles que $p = (0:0:1)$ et l'équation de la tangente à C en p soit $X_2 = 0$. Par le travail effectué dans la démonstration du théorème 3.1.5, on sait qu'on peut écrire $C(X_1, X_2, X_3) = X_1^3 + X_2 U(X_1, X_2, X_3)$ avec U un polynôme homogène de degré 2 en 3 variables tel que $U(0,0,1) \neq 0$. On écrit

$$U(X_1, X_2, X_3) = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2 + b_1 X_2 X_3 + b_2 X_1 X_3 + b_3 X_1 X_2$$

et on a la condition $a_3 \neq 0$. Alors

$$C(X_1, X_2, X_3) = X_1^3 + a_1 X_1^2 X_2 + a_2 X_2^3 + a_3 X_2 X_3^2 + b_1 X_2^2 X_3 + b_2 X_1 X_2 X_3 + b_3 X_1 X_2^2$$

et H_C est le déterminant de la matrice

$$\begin{pmatrix} 6X_1 + 2a_1 X_2 & 2a_1 X_1 + b_2 X_3 + 2b_3 X_2 & b_2 X_2 \\ 2a_1 X_1 + b_2 X_3 + 2b_3 X_2 & 6a_2 X_2 + 2b_1 X_3 + 2b_3 X_1 & 2a_3 X_3 + 2b_1 X_2 + b_2 X_1 \\ b_2 X_2 & 2a_3 X_3 + 2b_1 X_2 + b_2 X_1 & 2a_3 X_2 \end{pmatrix}.$$

On choisit les coordonnées affines $X = \frac{X_1}{X_2}$ et $Y = \frac{X_3}{X_2}$ (la tangente à C en p est ainsi la droite à l'infini). Alors

$$C(X, 1, Y) = X^3 + a_1 X^2 + b_3 X + a_3 Y^2 + b_1 Y + b_2 XY + a_2.$$

Si on fait le changement de coordonnées $X' = X - \frac{a_1}{3}$ et $Y' = Y$, alors

$$C(X, 1, Y) = X'^3 + (\frac{a_1^2}{3} + b_3) X' + a_3 Y'^2 + (b_1 - \frac{a_1 b_2}{3}) Y' + b_2 X' Y' + \frac{2a_1^3}{27} - \frac{a_1 b_3}{3} + a_2.$$

On peut donc supposer que $a_1 = 0$ et on obtient ainsi

$$C(X, 1, Y) = A_3(Y) X^3 + A_2(Y) X^2 + A_1(Y) X + A_0(Y),$$

où $A_3(Y) = 1$, $A_2(Y) = 0$, $A_1(Y) = b_2 Y + b_3$ et $A_0(Y) = a_3 Y^2 + b_1 Y + a_2$ et

$$H_C(X, 1, Y) = \det \begin{pmatrix} 6X & b_2 Y + 2b_3 & b_2 \\ b_2 Y + 2b_3 & 6a_2 + 2b_1 Y + 2b_3 X & 2a_3 Y + 2b_1 + b_2 X \\ b_2 & 2a_3 Y + 2b_1 + b_2 X & 2a_3 \end{pmatrix}.$$

En calculant le déterminant, on trouve $H_C(X, 1, Y) = B_3 X^3 + B_2 X^2 + B_1 X + B_0$ où

$$\begin{aligned} B_3(Y) &= -6b_2^2 \\ B_2(Y) &= -24a_3 b_2 Y + 24a_3 b_3 - 24b_1 b_2 \\ B_1(Y) &= -24a_3^2 Y^2 + (-24a_3 b_1 + 2b_2^3) Y + 72a_2 a_3 + 2b_2^2 b_3 - 24b_1^2 \\ B_0(Y) &= 2a_3 b_2^2 Y^2 + 2b_1 b_2^2 Y + 8b_1 b_2 b_3 - 6a_2 b_2^2 - 8a_3 b_3^2. \end{aligned}$$

On pose $f(X,Y)=C(X,1,Y)$ et $g(X,Y)=H_C(X,1,Y)$. Si $b_2\neq 0$, alors le résultant $R_{f,g}(Y)$ de f et g par rapport à X est donné par

$$R_{f,g}(Y)=\det\begin{pmatrix} A_0(Y) & 0 & 0 & B_0(Y) & 0 & 0\\ A_1(Y) & A_0(Y) & 0 & B_1(Y) & B_0(Y) & 0\\ A_2(Y) & A_1(Y) & A_0(Y) & B_2(Y) & B_1(Y) & B_0(Y)\\ A_3(Y) & A_2(Y) & A_1(Y) & B_3(Y) & B_2(Y) & B_1(Y)\\ 0 & A_3(Y) & A_2(Y) & 0 & B_3(Y) & B_2(Y)\\ 0 & 0 & A_3(Y) & 0 & 0 & B_3(Y)\end{pmatrix}.$$

Si on note C_i la $i$ème colonne de la matrice dont on calcule le déterminant, en remplaçant C_i par $C_i-2b_2^2C_{i-3}$ pour $i=4,5,6$, les B_i deviennent

$$\begin{array}{rcl} B_0(Y) &=& 8b_1b_2b_3-8a_3b_3^2-8a_2b_2^2\\ B_1(Y) &=& -24a_3^2Y^2-24a_3b_1Y+72a_2a_3-24b_1^2\\ B_2(Y) &=& -24a_3b_2Y+24a_3b_3-24b_1b_2\\ B_3(Y) &=& -8b_2^2. \end{array}$$

Si maintentant on remplace C_i par $\frac{C_i}{-8}$ pour $i=4,5,6$, alors

$$R_{f,g}(Y)=(-8)^3\det\begin{pmatrix} A_0(Y) & 0 & 0 & B_0(Y) & 0 & 0\\ A_1(Y) & A_0(Y) & 0 & B_1(Y) & B_0(Y) & 0\\ A_2(Y) & A_1(Y) & A_0(Y) & B_2(Y) & B_1(Y) & B_0(Y)\\ A_3(Y) & A_2(Y) & A_1(Y) & B_3(Y) & B_2(Y) & B_1(Y)\\ 0 & A_3(Y) & A_2(Y) & 0 & B_3(Y) & B_2(Y)\\ 0 & 0 & A_3(Y) & 0 & 0 & B_3(Y)\end{pmatrix},$$

où les B_i sont changés en

$$\begin{array}{rcl} B_0(Y) &=& a_3b_3^2+a_2b_2^2-b_1b_2b_3\\ B_1(Y) &=& 3a_3^2Y^2+3a_3b_1Y+3b_1^2-9a_2a_3\\ B_2(Y) &=& 3a_3b_2Y+3b_1b_2-3a_3b_3\\ B_3(Y) &=& b_2^2. \end{array}$$

On remplace ensuite C_i par $C_i-3a_3C_{i-2}$ pour $i=4,5$, alors le résultant vaut

$$(-8)^3\det\begin{pmatrix} A_0 & 0 & 0 & a_3b_3^2+a_2b_2^2-b_1b_2b_3 & 0 & 0\\ A_1 & A_0 & 0 & 3b_1^2-12a_2a_3 & a_3b_3^2+a_2b_2^2-b_1b_2b_3 & 0\\ A_2 & A_1 & A_0 & 3b_1b_2-6a_3b_3 & 3b_1^2-12a_2a_3 & B_0\\ A_3 & A_2 & A_1 & b_2^2 & 3b_1b_2-6a_3b_3 & B_1\\ 0 & A_3 & A_2 & -3a_3 & b_2^2 & B_2\\ 0 & 0 & A_3 & 0 & -3a_3 & B_3\end{pmatrix}.$$

On voit ainsi que le coefficient devant Y^8 (la plus haute puissance de Y que l'on puisse obtenir) est $3^3(-8)^3a_3^7\neq 0$. Si maintenant $b_2=0$ et $b_3\neq 0$ alors H_C est un polynôme de degré 2 en la variable X et donc

$$R_{f,g}(Y) = \det \begin{pmatrix} A_0(Y) & 0 & B_0(Y) & 0 & 0 \\ A_1(Y) & A_0(Y) & B_1(Y) & B_0(Y) & 0 \\ A_2(Y) & A_1(Y) & B_2(Y) & B_1(Y) & B_0(Y) \\ A_3(Y) & A_2(Y) & 0 & B_2(Y) & B_1(Y) \\ 0 & A_3(Y) & 0 & 0 & B_2(Y) \end{pmatrix},$$

où

$$\begin{aligned} A_3(Y) &= 1 \\ A_2(Y) &= 0 \\ A_1(Y) &= b_3 \\ A_0(Y) &= a_3Y^2 + b_1Y + a_2 \end{aligned} \qquad \begin{aligned} B_2(Y) &= 24a_3b_3 \\ B_1(Y) &= -24a_3^2Y^2 - 24a_3b_1Y + 72a_2a_3 - 24b_1^2 \\ B_0(Y) &= -8a_3b_3^2. \end{aligned}$$

Si on remplace C_3 par $C_3 + 24a_3C_2$, on obtient

$$R_{f,g} = det \begin{pmatrix} A_3(Y) & 0 & B_2(Y) & 0 & 24a_3 \\ A_2(Y) & A_3(Y) & B_1(Y) & B_2(Y) & 0 \\ A_1(Y) & A_2(Y) & B_0(Y) & B_1(Y) & 48a_3b_3 \\ A_0(Y) & A_1(Y) & 0 & B_0(Y) & 96a_2a_3 - 24b_1^2 \\ 0 & A_0(Y) & 0 & 0 & -8a_3b_3^2 \end{pmatrix}.$$

Le coefficient devant Y^8 est donc $(24)^3a_3^7 \neq 0$. Dans les deux cas, $R_{f,g}$ est un polynôme non constant et possède une racine y_0 dans k. Ainsi les polynômes $f(X, y_0)$ et $g(X, y_0)$ ont un facteur commun non constant et donc une racine commune x_0. On a obtenu un deuxième point d'inflexion $(x_0 \colon 1 \colon y_0)$. Si $b_2, b_3 = 0$,

$$\begin{aligned} C(X,1,Y) &= X^3 + a_3Y^2 + b_1Y + a_2 \\ H_C(X,1,Y) &= (-24a_3^2Y^2 - 24a_3b_1Y + 72a_2a_3 - 24b_1^2)X. \end{aligned}$$

Alors, si y_0 est une racine de $a_3Y^2 + b_1Y + a_2$, $(0 \colon 1 \colon y_0)$ est un point d'inflexion de C. □

3.2 Forme normale

Dans cette section, k est un corps de caractéristique différente de 2 et de 3. On note ϵ une racine cubique primitive de l'unité.

Définition 3.2.1 *Une cubique C à coefficients dans k est une forme normale s'il existe $\lambda \in k$ tel que*

$$C(X_1, X_2, X_3) = X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3$$

ou si

$$C(X_1, X_2, X_3) = X_1X_2X_3.$$

On note C_λ, respectivement C_∞, la cubique $X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3$, respectivement $X_1X_2X_3$.

Proposition 3.2.2 *La cubique C_∞ est singulière. Pour $\lambda \in k$, la cubique C_λ est non singulière si et seulement si $\lambda^3 \neq 1$.*

Preuve : Supposons que $(a\colon b\colon c)$ soit un point singulier de C_λ. On calcule les dérivées partielles de C_λ :

$$\begin{aligned} \partial_1 C_\lambda &= 3X_1^2 - 3\lambda X_2X_3, \\ \partial_2 C_\lambda &= 3X_2^2 - 3\lambda X_1X_3, \\ \partial_3 C_\lambda &= 3X_3^2 - 3\lambda X_1X_2. \end{aligned}$$

On a donc que $a^2 = \lambda bc$, $b^2 = \lambda ac$ et $c^2 = \lambda ab$. Si $a = 0$, alors $b = 0$ et $c = 0$. Donc $a \neq 0$. On trouve

$$a^4 = \lambda^2 b^2 c^2 = \lambda^2(\lambda ac)(\lambda ab) = \lambda^3 a^2(\lambda bc) = \lambda^3 a^4$$

et puisque $a \neq 0$, $\lambda^3 = 1$. Inversement, si $\lambda^3 = 1$, alors $(1\colon 1\colon \frac{1}{\lambda})$ est un point singulier. Pour la forme normale C_∞, $\partial_1 C_\infty = X_2X_3$, $\partial_2 C_\infty = X_1X_3$ et $\partial_3 C_\infty = X_1X_2$. Alors $(1\colon 0\colon 0)$ est un point singulier de C_∞. □

Remarque 3.2.3 *Soit $\lambda \in k$. Si $\lambda^3 \neq 1$, on sait que C_λ est irréductible dans $\overline{k}[X_1, X_2, X_3]$, puisque C_λ est non singulière. Et si $\lambda^3 = 1$, alors C_λ est un produit de 3 droites :*

$$\begin{aligned} C_1(X_1,X_2,X_3) &= (X_1 + X_2 + X_3)(X_1 + \epsilon X_2 + \epsilon^2 X_3)(X_1 + \epsilon^2 X_2 + \epsilon X_3) \\ C_\epsilon(X_1,X_2,X_3) &= (X_1 + \epsilon X_2 + X_3)(X_1 + \epsilon^2 X_2 + \epsilon^2 X_3)(X_1 + X_2 + \epsilon X_3) \\ C_{\epsilon^2}(X_1,X_2,X_3) &= (X_1 + \epsilon^2 X_2 + X_3)(X_1 + \epsilon X_2 + \epsilon X_3)(X_1 + X_2 + \epsilon^2 X_3). \end{aligned}$$

Clairement, la dernière forme normale singulière C_∞ est aussi un produit de 3 droites.

Remarque 3.2.4 *Pour $\lambda \in k$, $H_{C_\lambda} = C_\lambda$ si et seulement si $\lambda^3 = 1$.*

Preuve : On sait que

$$H_{C_\lambda}(X_1,X_2,X_3) = -54\lambda^2(X_1^3 + X_2^3 + X_3^3) + (216 - 54\lambda^3)X_1X_2X_3.$$

Ainsi, si $\lambda \neq 0$, $H_{C_\lambda} = C_{\frac{4-\lambda^3}{3\lambda^2}}$ et si $\lambda = 0$, $H_{C_\lambda} = C_\infty$. Or

$$\frac{4-\lambda^3}{3\lambda^2} = \lambda \iff 4 - \lambda^3 = 3\lambda^3 \iff \lambda^3 = 1.$$

Donc $H_{C_\lambda} = C_\lambda \iff \lambda^3 = 1$. □

Théorème 3.2.5 *Si k est un corps algébriquement clos et C est une cubique non singulière à coefficients dans k, alors C est équivalente à une forme normale.*

Preuve : Par le théorème 3.1.6, on sait que C possède 2 points d'inflexion qu'on appelle p et q. Il existe $\varphi \in \mathsf{GL}_3(k)$ tel que $\underline{\varphi}(p) = (0{:}\,0{:}\,1)$, $\underline{\varphi}(q) = (0{:}\,1{:}\,0)$ et les tangentes à C en p et en q sont $X_2 \circ \varphi$ et $X_3 \circ \varphi$ respectivement. En effet, les tangentes à C en p et q sont distinctes car alors on aurait une droite possédant plus de 3 points d'intersection, en comptant la multiplicité, avec une cubique. Ceci n'est possible que si la droite divise la cubique. Or C est irréductible, puisqu'elle est non singulière. On choisit alors $\varphi \in \mathsf{GL}_3(k)$ tel que $\underline{\varphi}$ soit l'homographie envoyant les points p, q sur les points $(0{:}\,0{:}\,1), (0{:}\,1{:}\,0)$ et le point d'intersection des tangentes sur $(1{:}\,0{:}\,0)$. On peut ainsi supposer que $p = (0{:}\,0{:}\,1)$, $q = (0{:}\,1{:}\,0)$, les tangentes à C en p et en q sont X_2 et X_3 respectivement. En utilisant à nouveau le travail effectué dans la démonstration du théorème 3.1.5, on peut écrire

$$C(X_1, X_2, X_3) = X_2 U(X_1, X_2, X_3) + aX_1^3,$$

où U est un polynôme homogène de degré 2 en 3 variables tel que $U(0,0,1) \neq 0$ et $a \in k$, $a \neq 0$. D'où $C(X_1, 0, X_3) = aX_1^3$. De même, en utilisant le point d'inflexion q, on trouve

$$C(X_1, X_2, X_3) = X_3 V(X_1, X_2, X_3) + a' X_1^3,$$

où V est un polynôme homogène de degré 2 en 3 variables tel que $V(0,1,0) \neq 0$, $a' \in k$, $a' \neq 0$. Alors $C(X_1, X_2, 0) = a' X_1^3$. Ainsi $X_2 X_3$ divise tous les termes de $C(X_1, X_2, X_3)$ sauf aX_1^3. On peut donc écrire

$$C(X_1, X_2, X_3) = a_1 X_1 X_2 X_3 + a_2 X_2^2 X_3 + a_3 X_2 X_3^2 + aX_1^3$$

avec les conditions $a_2 \neq 0$ et $a_3 \neq 0$ (car $U(0,0,1) \neq 0$ et $V(0,1,0) \neq 0$). On fait le changement de variables suivant

$$\begin{aligned} X_1 &= Y_1 \\ a_2 X_2 &= -\frac{a_1}{3} Y_1 + \epsilon Y_2 + \epsilon^2 Y_3 \\ a_3 X_3 &= -\frac{a_1}{3} Y_1 + \epsilon^2 Y_2 + \epsilon Y_3. \end{aligned}$$

Alors

$$\begin{aligned} -(a_1 X_1 + a_2 X_2 + a_3 X_3) &= -\frac{a_1}{3} X_1 - (\epsilon + \epsilon^2) Y_2 - (\epsilon + \epsilon^2) Y_3 \\ &= -\frac{a_1}{3} Y_1 + Y_2 + Y_3, \end{aligned}$$

puisque $\epsilon^2 + \epsilon + 1 = 0$. Alors

$$\begin{aligned} &-a_2 a_3 C(X_1, X_2, X_3) \\ &= -a_2 a_3 X_2 X_3 (a_1 X_1 + a_2 X_2 + a_3 X_3) - a a_2 a_3 X_1^3 \\ &= (-\frac{a_1}{3} Y_1 + \epsilon Y_2 + \epsilon^2 Y_3)(-\frac{a_1}{3} Y_1 + \epsilon^2 Y_2 + \epsilon Y_3)(-\frac{a_1}{3} Y_1 + Y_2 + Y_3) - a a_2 a_3 Y_1^3 \\ &= -(\frac{a_1^3}{27} + a a_2 a_3) Y_1^3 + Y_2^3 + Y_3^3 + a_1 Y_1 Y_2 Y_3. \end{aligned}$$

Donc C est équivalente à

$$C'(Y_1, Y_2, Y_3) = -\Big(\frac{a_1^3}{27} + aa_2a_3\Big)Y_1^3 + Y_2^3 + Y_3^3 + a_1Y_1Y_2Y_3.$$

On doit avoir $\frac{a_1^3}{27} + aa_2a_3 \neq 0$, car sinon $(1\colon 0\colon 0)$ est un point singulier de C'. On fait maintenant le changement de variable

$$\begin{aligned} Z_1 &= \Big(-\frac{a_1^3}{27} - aa_2a_3\Big)^{\frac{1}{3}} Y_1 \\ Z_2 &= Y_2 \\ Z_3 &= Y_3. \end{aligned}$$

Alors C' est équivalente à $C''(Z_1, Z_2, Z_3) = Z_1^3 + Z_2^3 + Z_3^3 - 3\lambda Z_1Z_2Z_3$, où

$$\lambda = \frac{a_1}{3\Big(\frac{a_1^3}{27} + aa_2a_3\Big)^{\frac{1}{3}}}.$$

□

Ce résultat est intéressant car il permet de déduire un grand nombre de propriétés sur les cubiques non singulières.

Remarque 3.2.6 *Les formes normales non singulières à coefficients dans k possèdent exactement 9 points d'inflexion sur $k(\epsilon)$.*

Preuve : Soit $\lambda \in k$ tel que $\lambda^3 \neq 1$. Les points d'inflexion de C_λ sont les points communs à C_λ et H_{C_λ}. On doit ainsi résoudre le système

$$\begin{cases} X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3 = 0 \\ -54\lambda^2(X_1^3 + X_2^3 + X_3^3) + (216 - 54\lambda^3)X_1X_2X_3 = 0 \end{cases}.$$

Si $\lambda = 0$, le système est équivalent à

$$\begin{cases} X_1^3 + X_2^3 + X_3^3 = 0 \\ X_1X_2X_3 = 0 \end{cases}.$$

Et si $\lambda \neq 0$, le système est équivalent à

$$\begin{cases} X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3 = 0 \\ X_1^3 + X_2^3 + X_3^3 + (\lambda - 4\lambda^{-2})X_1X_2X_3 = 0 \end{cases}$$

$$\Longleftrightarrow \begin{cases} X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3 = 0 \\ 4\lambda^{-2}(\lambda^3 - 1)X_1X_2X_3 = 0 \end{cases}$$

$$\Longleftrightarrow \begin{cases} X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3 = 0 \\ X_1X_2X_3 = 0 \end{cases}.$$

Dans tous les cas, on est réduit à résoudre le système

$$\begin{cases} X_1^3 + X_2^3 + X_3^3 = 0 \\ X_1X_2X_3 = 0 \end{cases}$$

$$\iff \left(\begin{array}{l} X_1 = 0 \\ X_2^3 = -X_3^3 \end{array} \right) \text{ ou } \left(\begin{array}{l} X_2 = 0 \\ X_3^3 = -X_1^3 \end{array} \right) \text{ ou } \left(\begin{array}{l} X_3 = 0 \\ X_1^3 = -X_2^3 \end{array} \right).$$

On trouve exactement 9 solutions. Ainsi C_λ possède exactement 9 points d'inflexion :

$$\begin{array}{lll} x_{00} = (0\colon -1\colon 1) & x_{01} = (0\colon -\epsilon\colon 1) & x_{02} = (0\colon -\epsilon^2\colon 1) \\ x_{10} = (1\colon 0\colon -1) & x_{11} = (1\colon 0\colon -\epsilon) & x_{12} = (1\colon 0\colon -\epsilon^2) \\ x_{20} = (-1\colon 1\colon 0) & x_{21} = (-\epsilon\colon 1\colon 0) & x_{22} = (-\epsilon^2\colon 1\colon 0). \end{array}$$

□

Les points $x_{00}, \ldots, x_{22}$ ont une configuration particulière. On remarque que les formes normales non singulières C_1, C_ϵ, C_{ϵ^2} et C_∞ sont des produits de 3 droites passant par 3 de ces points. On obtient ainsi 12 droites et 9 points, chaque droite passant par 3 points et chaque point appartenant à 4 droites. Cette configuration est isomorphe à celle des 9 points et des 12 droites du plan affine $\mathbb{F}_3^2$. En faisant correspondre à un point d'inflexion x_{ab} le point (a, b) du plan affine, l'image de l'ensemble des points se trouvant sur une droite d'une forme normale singulière est une droite de $\mathbb{F}_2^3$. On remarque en particulier qu'une droite passant par 2 points d'inflexion rencontre un troisième point d'inflexion.

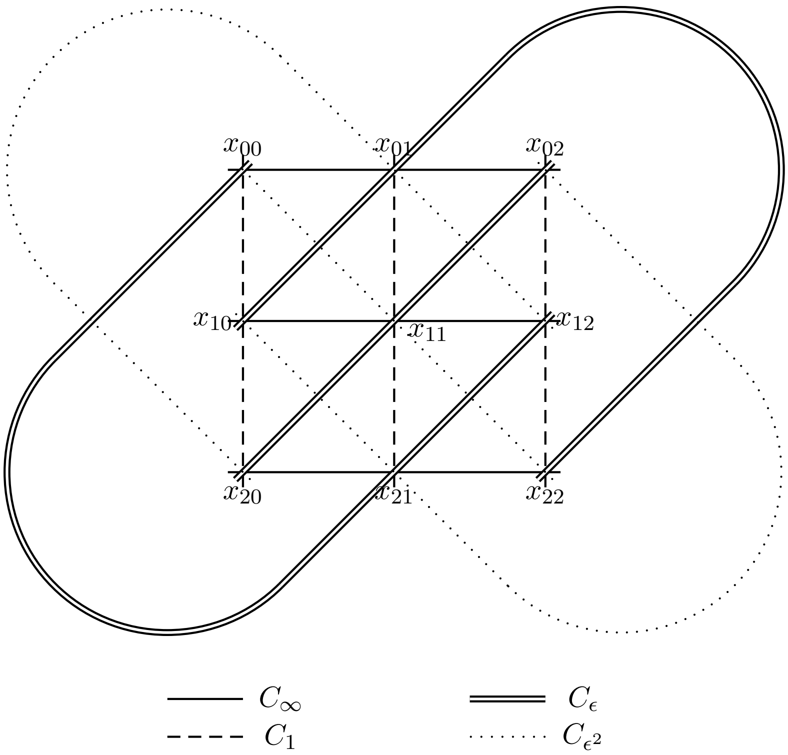
Les points d'inflexion des formes normales singulières sont tous les points non singuliers de ces cubiques. En effet, soit C une forme normale non singulière, alors $C = d_1d_2d_3$, où d_1, d_2, d_3 sont des droites distinctes du plan projectif. Alors, si p est un point non singulier de C, $p \in d_i$, pour un certain $i = 1, 2, 3$, la multiplicité du point d'intersection p de C avec d_i vaut l'infini. Donc p est un point d'inflexion de C. On peut même préciser que les points singuliers de C sont exactement les points d'intersection des droites d_1, d_2, d_3. En effet, par un changement linéaire de coordonnée, on peut revenir au cas où $C = X_1X_2X_3$. Alors

$$\begin{aligned} \partial_1 C &= X_2X_3 \\ \partial_2 C &= X_1X_3 \\ \partial_3 C &= X_1X_2. \end{aligned}$$

Ainsi, les points singuliers sont les points $(1\colon 0\colon 0), (0\colon 1\colon 0), (0\colon 0\colon 1)$ qui sont les points d'intersection des droites X_1, X_2, X_3.

Proposition 3.2.7 *Si k est algébriquement clos, toute cubique non singulière possède exactement 9 points d'inflexion.*

Preuve : Soit C une cubique à coefficients dans k. Par le théorème 3.2.5, on sait que C est équivalente à une forme normale C_λ, pour un certain $\lambda \in k$. Alors, il existe



Configuration des points d'inflexion des formes normales non singulières

$a \in k$, $a \neq 0$ et $\varphi \in \mathsf{GL}_3(k)$ tel que $aC_\lambda = C \circ \varphi$. Alors les points d'inflexion de C sont exactement les $\varphi(x_{ij})$, $i,j = 0,1,2$. □

De plus, la configuration des points d'inflexion d'une cubique non singulière et des droites passant par ces points est aussi isomorphe à celle des 9 points et des 12 droites du plan affine $\mathbb{F}_3^2$.

Remarque 3.2.8 *Si C est une cubique non singulière, alors $H_C \neq 0$.*

Preuve : Soit C une cubique non singulière à coefficients dans k. Alors il existe $a \in k$, $a \neq 0$ et $\varphi \in \mathsf{GL}_3(\overline{k})$ et $\lambda \in \overline{k}$ tels que $C \circ \varphi = aC_\lambda$. Or

$$H_{C_\lambda} = -54\lambda^2(X_1^3 + X_2^3 + X_3^3) + (216 - 54\lambda^3)X_1X_2X_3$$

n'est pas nul, car si $\lambda = 0$, alors $216 - 54\lambda^3 \neq 0$. Donc

$$H_C = (\det \varphi)^{-2} a^3 H_{C_\lambda} \circ \varphi^{-1}$$

est aussi non nul. □

Proposition 3.2.9 *Si k est un corps infini et C est une cubique non singulière à coefficients dans k, alors les 9 points d'inflexion de C dans $\mathbb{P}^2(\overline{k})$ sont en fait dans $\mathbb{P}^2(k_s)$.*

Preuve : On sait qu'il existe $a \in \overline{k}$, $a \neq 0$ et $\varphi \in \mathsf{GL}_3(\overline{k})$ tel que $C_\lambda = aC \circ \varphi$. Alors les $\varphi(x_{ij}) \in \mathbb{P}^2(\overline{k})$, $i,j = 0,1,2$, sont les points d'inflexion de C. On les note $p_1, \ldots, p_9$. Soit $q \in \mathbb{P}^2(k)$ tel que q ne soit pas un point d'inflexion de C. On considère les droites passant par q. Puisque k est infini, il en existe une ne passant pas par un point d'inflexion. On peut supposer que cette droite est $d(X_1, X_2, X_3) = X_3$. On passe en coordonnées affines en prenant d pour droite à l'infini :

$$X = \frac{X_1}{X_3} \text{ et } Y = \frac{X_2}{X_3}.$$

On note $(a_1, b_1), \ldots, (a_9, b_9)$ les coordonnées affines des points d'inflexion. On peut supposer que $a_i \neq a_j$ pour $i \neq j$. En effet, le polynôme

$$p(t) = \prod_{i<j} \Big((a_i - tb_i) - (a_j - tb_j) \Big) = \prod_{i<j} \Big((a_i - a_j) - t(b_i - b_j) \Big) \in \overline{k}[t]$$

est un polynôme non nul (si $i < j$, soit $a_i \neq a_j$, soit $b_i \neq b_j$). Alors il possède un nombre fini de racines. Donc il existe $c \in k$ tel que $p(c) \neq 0$. Alors l'isomorphisme d'espaces affines $(X, Y) \mapsto (X - cY, Y)$ envoie les points d'inflexion sur $(a'_1, b'_1), \ldots, (a'_9, b'_9)$ avec $a'_i \neq a'_j$, pour $i \neq j$. On pose R le résultant des polynômes $C(X, Y, 1)$ et $H_C(X, Y, 1)$ par rapport à Y. On peut parler de ce résultant car $C(X, Y, 1)$ n'est pas un polynôme constant en Y et $H_C(X, Y, 1)$ n'est pas nul. En effet, sinon C ne dépend que de X_1 et de X_3 et alors C est réductible sur $\overline{k}$

(par le théorème 1.2.3, les polynômes homogènes en 2 variables de degré strictement supérieur à 1 sont réductibles) ce qui n'est pas possible car C est non singulière. On veut voir que $R \neq 0$ et $R(a_i) = 0$ pour tout $i = 1, \ldots, 9$. On écrit

$$\begin{aligned} C(X, Y, 1) &= \alpha_r(X)Y^r + \ldots + \alpha_0(X) \\ H_C(X, Y, 1) &= \beta_s(X)Y^s + \ldots + \beta_0(X), \end{aligned}$$

avec les $\alpha_i, \beta_j \in k[X]$, $r \geq 1$ et $s \geq 0$. Si $s = 0$, alors $R(X) = \beta_0(X)^r$. Ainsi $R \neq 0$ car sinon $\beta_0(X) = 0$ et $H_C = 0$. D'autre part, $R(a_i) = \beta_0(a_i)^r = H_C(a_i, b_i, 1)^r = 0$ (on remarque que dans ce cas le degré de $\beta_0(X)$ doit être strictement supérieur à 0). Maintenant, si $s \neq 0$, alors $R \neq 0$. En effet, sinon $C(X, Y, 1)$ et $H_C(X, Y, 1)$ ont un facteur commun non constant $p(Y)$ dans $k[Y]$ et alors si $b \in \overline{k}$ est racine de $p(Y)$, pour tout $a \in \overline{k}$, $C(a, b, 1) = 0$ et $H_C(a, b, 1) = 0$. On obtient une infinité de points d'inflexion dans $\mathbb{P}_2(\overline{k})$ ce qui n'est pas possible car C possède exactement 9 points d'inflexion. Soit $i \in \{1, \ldots, 9\}$. Si $C(a_i, Y, 1)$ est un polynôme constant, alors cette constante est nulle puisque $C(a_i, b_i, 1) = 0$. On a alors

$$R(a_i) = \det \begin{pmatrix} \alpha_0(a_i) & \ldots & \ldots & \alpha_r(a_i) & & \\ & \ddots & & & \ddots & \\ & & \alpha_0(a_i) & \ldots & \ldots & \alpha_r(a_i) \\ \beta_0(a_i) & \ldots & \ldots & \beta_s(a_i) & & \\ & \ddots & & & \ddots & \\ & & \beta_0(a_i) & \ldots & \ldots & \beta_s(a_i) \end{pmatrix},$$

avec $\alpha_j(a_i) = 0$ pour tout $j = 0, \ldots, r$. Donc $R(a_i) = 0$. De même, si $H_C(a_i, Y, 1)$ est constant, alors $R(a_i) = 0$. Supposons maintenant que $C(a_i, Y, 1)$ et $H_C(a_i, Y, 1)$ ne soient pas constants. Alors $R(a_i) = \pm\alpha_r(a_i)^{s-p}\beta_s(a_i)^{r-l}R_i(a_i)$ où l (respectivement p) est le premier entier en partant de r (resp. s) tel que $\alpha_l(a_i) \neq 0$ (resp. $\beta_p(a_i) \neq 0$) et R_i est le résultant des polynômes $C(a_i, Y, 1)$ et $H_C(a_i, Y, 1)$. Mais puisque b_i est une racine commune de $C(a_i, Y, 1)$ et $H_C(a_i, Y, 1)$, $Y - b_i$ est un facteur commun de ces deux polynômes et donc $R_i = 0$. Ainsi $R(a_i) = 0$. On a $R(X) = R_{C,H_C}(X, 1)$ où $R_{C,H_C}(X_1, X_3)$ est le résultant de C et H_C par rapport à X_2. Si $s \geq 1$, comme C et H_C sont de polynômes homogènes de degré r et s respectivement par rapport à la variable X_2, soit $R_{C,H_C} = 0$, soit R_{C,H_C} est un polynôme homogène de degré rs. Ainsi, soit $R(X) = 0$, soit $R(X)$ est un polynôme de degré au plus rs, donc au plus 9. Si $s = 0$, $R(X)$ est un polynôme non nul de degré $r \cdot (\deg \beta_0)$, donc aussi de degré plus petit que 9. Or R possède 9 racines distinctes, les a_i, $i = 1, \ldots, 9$, donc le degré de R est 9 et R possède toutes ses racines simples. Comme $R(X) \in k[X]$, a_i est séparable sur k, pour tout $i \in \{1, \ldots, 9\}$. Reste à voir que les b_i sont aussi dans k_s. Soit $i \in \{1, \ldots, 9\}$. Si $C(a_i, Y, 1)$ et $H_C(a_i, Y, 1)$ ne sont pas constants, comme $R_i(a_i) = 0$, les polynômes $C(a_i, Y, 1)$ et $H_C(a_i, Y, 1)$ de $k_s[Y]$ ont un facteur commun non constant $f(Y)$ dans $k_s[Y]$. Ce facteur doit être une puissance de $Y - b_i$ (car sinon ce facteur possèderait une autre racine b_i' et on obtiendrait un dixième point d'inflexion

$(a_i\colon b_i'\colon 1))$. Si $f(Y) = Y - b_i$, alors on a directement $b_i \in k_s$. Si $f(Y) = (Y - b_i)^2$, alors $Y^2 - 2b_iY + b_i^2 \in k_s[Y]$ et on a encore $b_i \in k_s$. Finalement, si $f(Y) = (Y - b_i)^3$, $Y^3 - 3b_iY^2 + 3b_i^2Y - b_i^3 \in k_s[Y]$ et donc $b_i \in k_s$. Si $C(a_i, Y, 1)$ est constant, alors $C(a_i, Y, 1) = 0$ et donc $H_C(a_i, Y, 1)$ est une puissance de $Y - b_i$ (en effet, si b est une racine de $H_C(a_i, Y, 1)$ distincte de b_i, alors $C(a_i, b, 1) = 0$ et $H_C(a_i, b, 1) = 0$, on obtient donc un dixième point d'inflexion). Comme $H_C(a_i, Y, 1) \in k_s[Y]$, on obtient que b_i est dans k_s. De même, on prouve que $b_i \in k_s$ si $H_C(a_i, Y, 1)$ est constant. □

Théorème 3.2.10 *Toute cubique non singulière à coefficients dans un corps k infini et séparablement clos est équivalente à une forme normale.*

Preuve : Toute la démonstration du théorème 3.2.5 reste valable sur k puisque que l'on sait maintenant qu'une cubique non singulière à coefficients dans un corps k infini et séparablement clos possède 9 points d'inflexion dans $\mathbb{P}^2(k)$. □

3.3 j-Invariant

Dans cette section, k est un corps infini de caractéristique différente de 2 et 3. Si C est une cubique à coefficients dans k, on sait alors que C est équivalente sur k_s à une forme normale C_λ, $\lambda \in k_s$, $\lambda^3 \neq 1$. On définit le j-invariant de C, noté $j(C)$, par

$$j(C) = \frac{\lambda^3(\lambda^3 + 8)^3}{(\lambda^3 - 1)^3}.$$

Nous allons voir que le j-invariant est bien défini. Il faut en fait vérifier que pour $\lambda, \mu \in k_s$, si C_λ est équivalente à $C\mu$, alors

$$\frac{\lambda^3(\lambda^3 + 8)^3}{(\lambda^3 - 1)^3} = \frac{\mu^3(\mu^3 + 8)^3}{(\mu^3 - 1)^3}.$$

Pour cela, on considère le groupe $\mathfrak{G}$ des éléments de $\mathsf{PGL}_3(k_s) = \mathsf{GL}_3(k_s)/k^\times \mathsf{Id}_{k_s^3}$ (rappelons que cet ensemble correspond aux homographies de $\mathbb{P}^2(k_s)$ dans lui-même) qui permutent les points d'inflexion d'une forme normale non singulière. On a vu que ces points et les droites formées par ces points ont une configuration isomorphe à celle des points du plan affine $\mathbb{F}_3^2$. Alors les éléments de $\mathsf{PGL}_3(k_s)$ qui permutent les points $x_{00}, \ldots, x_{22}$ vont correspondre à des applications bijectives du plan affine sur lui-même qui conservent la colinéarité et l'incidence. Ces applications du plan affine sont exactement les automorphismes affines. On note $\mathsf{A}_2(\mathbb{F}_3)$ le groupe des automorphismes affines de $\mathbb{F}_3^2$. Il est engendré par les translations (qui sont au nombre de 9) et les automorphismes linéaires de $\mathsf{GL}_2(\mathbb{F}_3)$ (qui sont au nombre de 48). Le cardinal de $\mathsf{A}_2(\mathbb{F}_3)$ est donc 432. Le groupe des affinités spéciales $\mathsf{SA}_2(\mathbb{F}_3)$, engendré par les translations et les éléments de $\mathsf{SL}_2(\mathbb{F}_3)$ (les automorphimses linéaires de $\mathbb{F}_3^2$ de déterminant 1) est un sous-groupe de $\mathsf{A}_2(\mathbb{F}_3)$ d'indice 2. $\mathsf{SL}_2(\mathbb{F}_3)$ est engendré par

$U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $V = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$. On pose $W = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. On a alors

$$\mathsf{A}_2(\mathbb{F}_3) = \mathsf{SA}_2(\mathbb{F}_3) \cup W \cdot \mathsf{SA}_2(\mathbb{F}_3),$$

où la réunion est disjointe. On définit une application

$$\Theta\colon \mathfrak{G} \to \mathsf{A}_2(\mathbb{F}_3)\colon \underline{\varphi} \mapsto f,$$

telle que pour tout $(a, b) \in \mathbb{F}_3^2$, $f(a, b) = (c, d)$ si $\underline{\varphi}(x_{ab}) = x_{cd}$. L'application Θ est un homomorphisme injectif de groupes. En effet, si $\underline{\varphi}, \underline{\psi} \in \mathfrak{G}$ et $\Theta(\underline{\varphi}) = \Theta(\underline{\psi})$, alors les images de x_{00}, x_{01}, x_{10} et x_{11} sont les mêmes par $\underline{\varphi}$ et par $\underline{\psi}$. Mais puisque les points x_{00}, x_{01}, x_{10} et x_{11} forment un repère de $\mathbb{P}^2(k_s)$, on a $\underline{\varphi} = \underline{\psi}$. Soit G_{216} le sous-groupe de $\mathsf{PGL}_3(k_s)$ engendré par $\underline{A}$, $\underline{C}$, $\underline{D}$ et $\underline{E}$ avec

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix},$$

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon \end{pmatrix} \text{ et } E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \epsilon & \epsilon^2 \\ 1 & \epsilon^2 & \epsilon \end{pmatrix}$$

(l'image de x_{ab} étant obtenu par multiplication à gauche par x_{ab}, puisque l'on travaille avec des vecteurs lignes). Un calcul montre que $\underline{A}$,$\underline{C}$,$\underline{D}$ et $\underline{E}$ sont dans $\mathfrak{G}$ et que $\Theta(\underline{A})$ est la translation de vecteur $(2, 0)$, $\Theta(\underline{C})$ la translation de vecteur $(0, 2)$, $\Theta(\underline{D}) = U$ et $\Theta(\underline{E}) = V$. Le groupe G_{216} a ainsi le même cardinal que $\mathsf{SA}_2(\mathbb{F}_3)$, c'est-à-dire 216. On va voir que l'image de Θ est $\mathsf{SA}_2(\mathbb{F}_3)$. D'abord, on voit que W n'est pas dans l'image. En effet, puisque

$$W \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, W \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix},$$

$$W \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } W \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix},$$

on cherche l'unique élément de $\mathsf{PGL}_3(k_s)$ qui envoie x_{00} sur lui-même, x_{01} sur x_{02}, x_{10} sur lui-même et x_{11} sur x_{12}. On trouve $\underline{F}$ où $F = \begin{pmatrix} 1 & 0 & \epsilon \\ 0 & \epsilon & 1 \\ 0 & 0 & -\epsilon^2 \end{pmatrix}$. On a alors $\underline{F}(0\colon -\epsilon^2\colon 1) = (0\colon -\epsilon\colon -2)$ et $(0\colon -\epsilon\colon -2) \notin \{x_{00}, \ldots, x_{22}\}$. Alors, si $\underline{\varphi} \in \mathfrak{G}$ est tel que $\Theta(\underline{\varphi}) \in W \cdot \mathsf{SA}_2(\mathbb{F}_3)$, il existe $f \in \mathsf{SA}_2(\mathbb{F}_3)$ tel que $\Theta(\underline{\varphi}) = W \circ f$. Par définition de G_{216}, il existe $\underline{\psi} \in G_{216}$ tel que $\Theta(\underline{\psi}) = f$. Alors $\underline{\varphi \circ \psi^{-1}} \in \mathfrak{G}$ et $\Theta(\underline{\varphi \circ \psi^{-1}}) = W$. C'est impossible, on prouve ainsi que $\mathsf{Im}(\Theta) = \mathsf{SA}_2(\mathbb{F}_3)$. On obtient le résultat suivant :

Proposition 3.3.1 *Le groupe $\mathfrak{G}$ des éléments de $\mathsf{PGL}_3(k_s)$ qui permutent les points $x_{00}, \ldots, x_{22}$ est engendré par les automorphismes $\underline{A}, \underline{C}, \underline{D}, \underline{E}$ de $\mathbb{P}^2(k_s)$, où*

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix}, D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon \end{pmatrix}, E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \epsilon & \epsilon^2 \\ 1 & \epsilon^2 & \epsilon \end{pmatrix}.$$

$\mathfrak{G}$ est en fait un sous-groupe de $\mathsf{PGL}_3(k(\epsilon))$.

Proposition 3.3.2 *Soient $\varphi \in \mathsf{GL}_3(k_s)$ et $\lambda \in k_s$, $\lambda^3 \neq 1$. Alors $C_\lambda \circ \varphi$ est une forme normale si et seulement $\underline{\varphi} \in \mathfrak{G}$.*

Preuve : Si $C_\lambda \circ \varphi$ est une forme normale, en particulier, p est un point d'inflexion de $C_\lambda \circ \varphi$ si et seulement si $\underline{\varphi}(p)$ est un point d'inflexion de C_λ. Donc $\underline{\varphi}$ permute les points $x_{00}, \ldots, x_{22}$ et $\varphi \in \mathfrak{G}$. Maintenant, si $\underline{\varphi} \in \mathfrak{G}$, on sait qu'il existe $\alpha \in k_s$ tel que $\alpha \mathsf{Id}_{k_s^3} \circ \varphi$ est dans le groupe engendré par

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 & 1 \\ 1 & \epsilon & \epsilon^2 \\ 1 & \epsilon^2 & \epsilon \end{pmatrix}.$$

Puisque les cubiques sont inchangées sous l'action des matrices scalaires, on peut supposer que $\alpha = 1$. Or les cubiques que l'on peut obtenir par changement de variables engendré par ces matrices sont toutes des formes normales C_μ avec μ dans l'ensemble

$$N_\lambda = \left\{\lambda, \epsilon\lambda, \epsilon^2\lambda, \tfrac{\lambda+2}{\lambda-1}, \tfrac{\lambda+2}{\epsilon\lambda-\epsilon}, \tfrac{\lambda+2}{\epsilon^2\lambda-\epsilon^2}, \tfrac{\lambda+2\epsilon}{\lambda-\epsilon}, \tfrac{\lambda+2\epsilon}{\epsilon\lambda-\epsilon^2}, \tfrac{\lambda+2\epsilon}{\epsilon^2\lambda-1}, \tfrac{\lambda+2\epsilon^2}{\lambda-\epsilon^2}, \tfrac{\lambda+2\epsilon^2}{\epsilon\lambda-1}, \tfrac{\lambda+2\epsilon^2}{\epsilon^2\lambda-\epsilon}\right\}.$$

□

Soit J l'application définie par

$$J\colon k_s \setminus \{1, \epsilon, \epsilon^2\} \to k_s\colon \lambda \mapsto \frac{\lambda^3(\lambda^3+8)^3}{(\lambda^3-1)^3}.$$

Proposition 3.3.3 *Pour $\lambda, \mu \in k_s$, C_λ est équivalente à C_μ sur k_s si et seulement si $J(\lambda) = J(\mu)$.*

Preuve : Supposons que C_λ soit équivalente à C_μ. Alors $\mu \in N_\lambda$. On vérifie par un calcul que les valeurs $\nu \in N_\lambda$ vérifient toutes $J(\nu) = J(\lambda)$. Inversement, si $J(\lambda) = J(\mu)$, alors μ est racine du polynôme

$$p_\lambda(t) = (\lambda^3-1)^3 \cdot t^3(t^3+8)^3 - \lambda^3(\lambda^3+8)^3 \cdot (t^3-1)^3.$$

Ce polynôme a au plus 12 racines puisqu'il est non nul et de degré 12. Or si $\lambda \notin N$, où

$$N = \left\{0, -2, -2\epsilon, -2\epsilon^2, 1+\sqrt{3}, \epsilon(1+\sqrt{3}), \epsilon^2(1+\sqrt{3}), 1-\sqrt{3}, \epsilon(1-\sqrt{3}), \epsilon^2(1-\sqrt{3})\right\},$$

on remarque que les 12 valeurs de l'ensemble N_λ sont toutes distinctes. Comme elles sont racines du polynôme $p_\lambda(t)$, $\mu \in N_\lambda$ et on sait alors que C_λ est équivalente C_μ. Si $\lambda = 0, -2, -2\epsilon$ ou $-2\epsilon^2$, alors les racines de $p_\lambda(t) = (\lambda^3-1)^3 \cdot t^3(t^3+8)^3$ sont $0, -2, -2\epsilon, -2\epsilon^2$ qui forment l'ensemble N_0. On pose $A_\lambda(t) = (\lambda^3-1)(t^4+8t)$ et $B_\lambda(t) = \lambda(\lambda^3+8)(t^3-1)$. Alors

$$p_\lambda(t) = \Big(A_\lambda(t) - B_\lambda(t)\Big) \cdot \Big(A_\lambda(t) - \epsilon B_\lambda(t)\Big) \cdot \Big(A_\lambda(t) - \epsilon^2 B_\lambda(t)\Big).$$

Si $\lambda = 1+\sqrt{3}, \epsilon(1+\sqrt{3}), \epsilon^2(1+\sqrt{3}), 1-\sqrt{3}, \epsilon(1-\sqrt{3})$ ou $\epsilon^2(1-\sqrt{3})$,

$$\begin{aligned} p_\lambda(t) &= (\lambda^3-1)^3(t^4-4t^3+8t+4)(t^4-4\epsilon t^3+8t+4\epsilon)(t^4-4\epsilon^2t^3+8t+4\epsilon^2) \\ &= (\lambda^3-1)^3\Big((t-\lambda)(t-\epsilon\lambda)(t-\epsilon^2\lambda)(t-\overline{\lambda})(t-\epsilon\overline{\lambda})(t-\epsilon^2\overline{\lambda})\Big)^2, \end{aligned}$$

où on écrit $\overline{1+\sqrt{3}}$ pour $1-\sqrt{3}$, $\overline{\epsilon(1+\sqrt{3})}$ pour $\epsilon(1-\sqrt{3})$, etc.. On trouve encore que les racines de $p_\lambda(t)$ forment l'ensemble N_λ. □

Ce résultat montre en particulier que le j-invariant est bien défini. Si C est une cubique non singulière, $j(C) = \frac{\lambda^3(\lambda^3+8)^3}{(\lambda^3-1)^3}$, avec $\lambda \in k_s$, $\lambda^3 \neq 1$, tel que C est équivalente à C_λ sur k_s. Donc a priori, $j(C)$ est dans k_s.

Proposition 3.3.4 *Pour une cubique non singulière C, $j(C) \in k$.*

Preuve : Nous allons voir que pour tout $\gamma \in \mathsf{Gal}(k_s/k)$, $\gamma(j(C)) = j(C)$. Il existe $a \in k$, $a \neq 0$, $\varphi \in \mathsf{GL}_3(k_s)$ et $\lambda \in k_s$, $\lambda^3 \neq 1$, tels que $C \circ \varphi = aC_\lambda$. On écrit $\varphi = (a_{ij})$, avec les $a_{ij} \in k_s$ tels que $\det(a_{ij}) \neq 0$. Soit $\gamma \in \mathsf{Gal}(k_s/k)$. On définit $\gamma(\varphi) \in \mathsf{GL}_3(k_s)$ par

$$\gamma(\varphi) = (\gamma(a_{ij}))$$

$(\det(\gamma(a_{ij})) = \gamma(\det(a_{ij})) \neq 0)$. $\mathsf{Gal}(k_s/k)$ agit sur les cubiques à coefficients dans k_s de la manière suivante : si C' est une cubique à coefficients dans k_s et $\gamma \in \mathsf{Gal}(k_s/k)$,

$$C'(X_1, X_2, X_3) = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3},$$

où la somme varie sur les indices i_1, i_2, i_3 tels que $i_1 + i_2 + i_3 = 3$ et $\lambda_{i_1,i_2,i_3} \in k_s$, alors

$$\gamma \star C'(X_1, X_2, X_3) = \sum \gamma(\lambda_{i_1,i_2,i_3}) X_1^{i_1} X_2^{i_2} X_3^{i_3}.$$

Puisque les coefficients de C sont dans k, on a

$$C \circ \gamma(\varphi) = \gamma \star (C \circ \varphi) = \gamma \star (aC_\lambda) = \gamma(a) C_{\gamma(\lambda)}.$$

Donc C_λ est équivalente à $C_{\gamma(\lambda)}$. Ainsi

$$j(C) = \frac{\lambda^3(\lambda^3+8)^3}{(\lambda^3-1)^3} = \frac{\gamma(\lambda)^3\Big(\gamma(\lambda)^3+8\Big)^3}{\Big(\gamma(\lambda)^3-1\Big)^3} = \gamma\left(\frac{\lambda^3(\lambda^3+8)^3}{(\lambda^3-1)^3}\right) = \gamma(j(C)).$$

□

On vérifie facilement le résultat suivant :

Lemme 3.3.5 *Si k est séparablement clos et $\lambda \in k \setminus (N \cup \{1, \epsilon, \epsilon^2\}$, en posant $B = E^2$, pour tout $\varphi \in \mathsf{GL}_3(k_s)$, $C_\lambda \circ \varphi = C_\lambda$ si et seulement si $\underline{\varphi}$ est dans le groupe H engendré par $\underline{A}$, $\underline{B}$ et $\underline{C}$.*

3.4 Pinceaux canoniques de cubiques

On suppose encore que k est un corps infini de caractéristique différente de 2 et de 3.

Définition 3.4.1 *Soit C une cubique à coefficients dans k. Le pinceau canonique associé à C, noté $\mathcal{F}_C$, est l'ensemble des cubiques de la forme $\alpha C + \beta H_C$, pour $\alpha, \beta \in k$.*

$\mathcal{F}_C$ ne dépend pas du choix du polynôme représentant C. En effet, si f et g représentent C, alors il existe $\lambda \in k^\times$ tel que $g = \lambda f$. Or, si $\alpha, \beta \in k$,

$$\alpha g + \beta \det(\partial^2_{ij} g) = \alpha\lambda f + \beta\lambda^3 \det(\partial^2_{ij} f) = \alpha' f + \beta' \det(\partial^2_{ij} f),$$

pour certains $\alpha', \beta' \in k$ et

$$\alpha f + \beta \det(\partial^2_{ij} f) = \alpha\lambda^{-1} g + \beta\lambda^{-3} \det(\partial^2_{ij} g) = \alpha'' g + \beta'' \det(\partial^2_{ij} g),$$

pour certains $\alpha'', \beta'' \in k$.

Si p est un point d'inflexion de la cubique C, alors toute cubique de l'ensemble $\mathcal{F}_C$ passe par p. En effet, $p = (a\colon b\colon c)$ est un point non singulier de C appartenant à H_C et donc si $\alpha C + \beta H_C \in \mathcal{F}_C$,

$$(\alpha C + \beta H_C)(a, b, c) = \alpha C(a, b, c) + \beta H_C(a, b, c) = 0.$$

Maintenant, si C est non singulière et p est un point d'inflexion de C, alors p est un point d'inflexion de toute cubique de $\mathcal{F}_C$. En effet, il existe $a \in k_s$, $a \neq 0$, $\varphi \in \mathsf{GL}_3(k_s)$ et $\lambda \in k_s$ tels que $C \circ \varphi = aC_\lambda$. Alors, pour toute cubique $\alpha C + \beta H_C$,

$$\begin{aligned}(\alpha C + \beta H_C) \circ \varphi &= \alpha C \circ \varphi + \beta H_C \circ \varphi \\ &= \alpha a C_\lambda + \beta (\det \varphi)^{-2} a^3 H_{C_\lambda}.\end{aligned}$$

Puisque H_{C_λ} est une forme normale, on remarque que $(\alpha C + \beta H_C) \circ \varphi$ est aussi une forme normale. Comme p est un point d'inflexion de C, $\underline{\varphi}^{-1}(p)$ est un point d'inflexion de C_λ et donc p est un point d'inflexion de $\alpha C + \beta H_C$.

On va voir que si C est une cubique non singulière, alors $\mathcal{F}_C$ est l'ensemble des cubiques passant par les 9 points d'inflexion de C.

Lemme 3.4.2 *Pour tout $\lambda \in k$, $\lambda^3 \neq 1$, $\mathcal{F}_{C_\lambda}$ est l'ensemble des formes normales (singulières ou non), c'est-à-dire*

$$\mathcal{F}_{C_\lambda} = \Big\{ C_\mu \mid \mu \in k \cup \{\infty\} \Big\}.$$

Preuve : Soit $\lambda \in k$, $\lambda^3 \neq 1$. Puisque

$$H_{C_\lambda} = -54\lambda^2(X_1^3 + X_2^3 + X_3^3) + (216 - 54\lambda^3)X_1X_2X_3,$$

alors on a

$$\alpha C_\lambda + \beta H_{C_\lambda} = (\alpha - 54\lambda^2\beta)(X_1^3 + X_2^3 + X_3^3) - 3(\lambda\alpha + 18\lambda^3\beta - 72\beta)X_1X_2X_3.$$

Pour tout $\mu \in k \cup \{\infty\}$, on voudrait trouver $\alpha, \beta \in k$ tels que $\alpha C_\lambda + \beta H_{C_\lambda} = C_\mu$. Soit $\mu \in k$. On cherche $\alpha, \beta \in k$ tels que

$$\left\{\begin{array}{l} \alpha - 54\lambda^2\beta = 1 \\ \lambda\alpha + 18\lambda^3\beta - 72\beta = \mu \end{array}\right. \iff \left\{\begin{array}{l} \alpha = 1 + 54\lambda^2\beta \\ \lambda + 72\lambda^3\beta - 72\beta = \mu \end{array}\right. .$$

Alors

$$\alpha = \frac{\lambda^3 + 3\lambda^2\mu - 4}{4(\lambda^3 - 1)} \text{ et } \beta = \frac{\mu - \lambda}{72(\lambda^3 - 1)}$$

conviennent. Maintenant, si $\mu = \infty$, on cherche $\alpha, \beta \in k$ tels que

$$\left\{\begin{array}{l} \alpha - 54\lambda^2\beta = 0 \\ -3(\lambda\alpha + 18\lambda^3\beta - 72\beta) = 1 \end{array}\right. \iff \left\{\begin{array}{l} \alpha = 54\lambda^2\beta \\ -216\beta\lambda^3 + 216\beta = 1 \end{array}\right. .$$

Ainsi on peut choisir

$$\alpha = \frac{-\lambda^2}{4(\lambda^3 - 1)} \text{ et } \beta = \frac{-1}{216(\lambda^3 - 1)}.$$

$\square$

Lemme 3.4.3 *Les cubiques passant par les points $x_{00}, \ldots, x_{22}$ sont exactement les formes normales.*

Preuve : Soit C une cubique à coefficients dans k, passant par les points $x_{00}, \ldots, x_{22}$. On écrit

$$C(X_1, X_2, X_3) = \sum_{i_1+i_2+i_3=3} \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3},$$

pour certains $\lambda_{i_1,i_2,i_3} \in k$. Alors les λ_{i_1,i_2,i_3} vérifient les 9 équations :

$$\left\{\begin{array}{l} -\lambda_{0,3,0} + \lambda_{0,0,3} + \lambda_{0,2,1} - \lambda_{0,1,2} = 0 \\ -\lambda_{0,3,0} + \lambda_{0,0,3} + \epsilon^2\lambda_{0,2,1} - \epsilon\lambda_{0,1,2} = 0 \\ -\lambda_{0,3,0} + \lambda_{0,0,3} + \epsilon\lambda_{0,2,1} - \epsilon^2\lambda_{0,1,2} = 0 \\ +\lambda_{3,0,0} - \lambda_{0,0,3} + \lambda_{1,0,2} - \lambda_{2,0,1} = 0 \\ +\lambda_{3,0,0} - \lambda_{0,0,3} + \epsilon^2\lambda_{1,0,2} - \epsilon\lambda_{2,0,1} = 0 \\ +\lambda_{3,0,0} - \lambda_{0,0,3} + \epsilon\lambda_{1,0,2} - \epsilon^2\lambda_{2,0,1} = 0 \\ -\lambda_{3,0,0} + \lambda_{0,3,0} + \lambda_{2,1,0} - \lambda_{1,2,0} = 0 \\ -\lambda_{3,0,0} + \lambda_{0,3,0} + \epsilon^2\lambda_{2,1,0} - \epsilon\lambda_{1,2,0} = 0 \\ -\lambda_{3,0,0} + \lambda_{0,3,0} + \epsilon\lambda_{2,1,0} - \epsilon^2\lambda_{1,2,0} = 0 \end{array}\right.$$

$$\Rightarrow \left\{ \begin{array}{l} \lambda_{3,0,0} = \lambda_{0,3,0} = \lambda_{0,0,3} \\ \lambda_{2,1,0} = \lambda_{1,2,0} = \lambda_{2,0,1} = \lambda_{1,0,2} = \lambda_{0,2,1} = \lambda_{0,1,2} = 0 \end{array} \right. .$$

Ainsi,

$$C(X_1, X_2, X_3) = \lambda_{3,0,0}(X_1^3 + X_2^3 + X_3^3) + \lambda_{1,1,1}X_1X_2X_3$$

est une forme normale. □

Grâce à ces deux lemmes, on obtient le résultat annoncé :

Proposition 3.4.4 *Si C est une cubique non singulière, alors $\mathcal{F}_C$ est l'ensemble des cubiques passant par les 9 points d'inflexion de C.*

Preuve : Soit C une cubique non singulière à coefficients dans k. On a déjà vu que toute cubique de $\mathcal{F}_C$ passe par les 9 points d'inflexion de C. Maintenant, soit C' une cubique à coefficients dans k passant par les 9 points d'inflexion de C. Il existe $a \in k_s$, $\varphi \in \mathsf{GL}_3(k_s)$ et $\lambda \in k_s$ tel que $C \circ \varphi = aC_\lambda$. Alors $C' \circ \varphi$ passe par les points $x_{00}, \ldots, x_{22}$ (en effet, comme $C \circ \varphi = aC_\lambda$, les points d'inflexion de C sont $\underline{\varphi}(x_{00}), \ldots, \underline{\varphi}(x_{22})$). Par le lemme 3.4.3, on sait que $C' \circ \varphi$ est une forme normale et donc, par le lemme 3.4.2, il existe $\alpha, \beta \in k_s$ tels que $C' \circ \varphi = \alpha C_\lambda + \beta H_{C_\lambda}$ (les coefficients de $C' \circ \varphi$ sont a priori dans k_s). Ainsi,

$$\begin{aligned} C' &= \alpha C_\lambda \circ \varphi^{-1} + \beta H_{C_\lambda} \circ \varphi^{-1} \\ &= \alpha a^{-1} C + \beta (\det \varphi)^2 a^{-3} H_C \\ &= \alpha' C + \beta' H_C, \end{aligned}$$

pour certains $\alpha', \beta' \in k_s$. Pour montrer que $\alpha', \beta' \in k$, on utilise une nouvelle fois l'action du groupe de Galois $\mathsf{Gal}(k_s/k)$ sur les cubiques à coefficients dans k_s. Soit $\gamma \in \mathsf{Gal}(k_s/k)$. Puisque C et C' sont des cubiques à coefficients dans k, $\gamma \star C' = C'$ et $\gamma \star (\alpha' C + \beta' H_C) = \gamma(\alpha')C + \gamma(\beta')H_C$. Ainsi $(\alpha' - \gamma(\alpha'))C + (\beta' - \gamma(\beta'))H_C = 0$. Supposons que $\alpha' - \gamma(\alpha') \neq 0$, alors

$$C = -\frac{\beta' - \gamma(\beta')}{\alpha' - \gamma(\alpha')} H_C$$

et alors C et H_C sont les mêmes cubiques. Ceci ne peut être vrai car C_λ et H_{C_λ} ne sont pas les mêmes cubiques ($\lambda^3 \neq 1$). De même, si $\beta' - \gamma(\beta') = 0$, alors C et H_C sont les mêmes cubiques. Donc $\alpha' = \gamma(\alpha')$ et $\beta' = \gamma(\beta')$ et ainsi, $\alpha', \beta' \in k$. □

On a donc que les cubiques du pinceau associé à une cubique non singulière C sont les cubiques passant par les points d'inflexion de C et de plus que les points d'inflexion de C sont aussi des points d'inflexion pour les cubiques du pinceau. Ce sont les seuls points d'inflexion sauf dans le cas où la cubique du pinceau est singulière (alors cette cubique est un produit de 3 droites et tous les points de la cubique sont des points d'inflexion sauf les points d'intersection des droites). On remarque que, dans le cas où une cubique du pinceau est singulière, alors son hessien est la même cubique. En effet, une cubique singulière du pinceau est un produit de 3 droites, on peut alors considérer le cas où cette cubique est $X_1X_2X_3$ et on vérifie alors que le hessien est aussi $X_1X_2X_3$. Ainsi, les cubiques du pinceau sont singulières si et seulement si elles sont égales à leur hessien.

On note $\mathfrak{P}(k)$ (resp. $\mathfrak{P}^+(k)$) l'ensemble des pinceaux canoniques associés aux cubiques (resp. cubiques non singulières) à coefficients dans k. $\mathsf{GL}_3(k)$ agit sur $\mathfrak{P}(k)$ de la manière suivante : si $\mathcal{F}_C \in \mathfrak{P}(k)$ et $\varphi \in \mathsf{GL}_3(k)$, $\varphi(\mathcal{F}_C) = \mathcal{F}_{\varphi(C)}$. Il faut voir que $\varphi(\mathcal{F}_C)$ est bien défini. Si $\mathcal{F}_C = \mathcal{F}_{C'}$, alors soit $\alpha\varphi(C) + \beta H_{\varphi(C)} \in \mathcal{F}_{\varphi(C)}$. On a

$$\begin{aligned}\alpha\varphi(C) + \beta H_{\varphi(C)} &= \alpha C \circ \varphi + \beta(\det\varphi)^2 H_C \circ \varphi \\ &= (\alpha C + \beta(\det\varphi)^2 H_C) \circ \varphi.\end{aligned}$$

Or $\alpha C + \beta(\det\varphi)^2 H_C \in \mathcal{F}_C = \mathcal{F}_{C'}$, donc $\alpha C + \beta(\det\varphi)^2 H_C = \alpha' C' + \beta' H_{C'}$, pour certains $\alpha', \beta' \in k$. Ainsi,

$$\begin{aligned}\alpha\varphi(C) + \beta H_{\varphi(C)} &= (\alpha' C' + \beta' H_{C'}) \circ \varphi \\ &= \alpha' C' \circ \varphi + \beta'(\det\varphi)^{-2} H_{C\circ\varphi'} \\ &= \alpha'\varphi(C') + \beta'(\det\varphi)^{-2} H_{\varphi(C')} \in \mathcal{F}_{\varphi(C')}.\end{aligned}$$

On vérifie de même que $\mathcal{F}_{\varphi(C')} \subset \mathcal{F}_{\varphi(C)}$.

On dit que $\mathcal{F}_C$ et $\mathcal{F}_{C'}$ sont isomorphes sur k s'ils sont dans la même orbite sous l'action de $\mathsf{GL}_3(k)$. Ceci définit une relation d'équivalence sur $\mathfrak{P}(k)$. On note $\mathsf{Pen}_3(k)$ le quotient de $\mathfrak{P}(k)$ par cette relation d'équivalence et $[\mathcal{F}_C]$ la classe d'équivalence du pinceau $\mathcal{F}_C$. Il est clair que l'action de $\mathsf{GL}_3(k)$ se restreint à $\mathfrak{P}^+(k)$. On note $\mathsf{Pen}^+(k)$ le quotient de $\mathfrak{P}^+(k)$ par la relation d'équivalence.

3.5 Etude de cubiques particulières

Dans cette section, on s'intéresse aux cubiques de la forme

$$a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3.$$

Cette forme est plus générale que la forme normale et vérifie une propriété intéressante. Soit k un corps de caractéristique différente de 2 et de 3.

Lemme 3.5.1 *Une cubique $a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3$, $a_1, a_2, a_3, b \in k$ est non singulière si et seulement si $a_1, a_2, a_3 \neq 0$ et $b^3 \neq a_1a_2a_3$.*

Preuve : Soit C la cubique définie par $C = a_1X_1^2 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3$. Si $a_1 = 0$, alors $(1:0:0)$ est un point singulier de C. De même, si $a_2 = 0$ ou $a_3 = 0$, alors C est singulière. Supposons maintenant que $a_1, a_2, a_3 \neq 0$. Supposons que $b^3 = a_1a_2a_3$. On note α une racine cubique de $\frac{a_1}{a_2}$ et β une racine cubique de $\frac{a_1}{a_3}$ telles que $b = \frac{a_1}{\alpha\beta}$, alors on vérifie que $(1{:}\,\alpha{:}\,\beta)$ est un point singulier de C. Supposons que la cubique C soit singulière. Alors, il existe $(x_1{:}\,x_2{:}\,x_3) \in \mathbb{P}^2(\overline{k})$ tel que

$$\begin{aligned} 3a_1x_1^2 - 3bx_2x_3 &= 0 \\ 3a_2x_2^2 - 3bx_1x_3 &= 0 \\ 3a_3x_3^2 - 3bx_1x_2 &= 0. \end{aligned}$$

Si $x_1 = 0$, alors $x_2 = 0$ et $x_3 = 0$. Donc $x_1 \neq 0$. On a

$$a_2a_3a_1^2x_1^4 = a_2a_3b^2x_2^2x_3^2 = b^4x_1^2x_2x_3 = b^3a_1x_1^4.$$

Ainsi, $b^3 = a_1a_2a_3$. □

Lemme 3.5.2 *Soit $a_1, a_2, a_3, b \in k$. Si $C = a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3$ est non singulière, alors les 9 points d'inflexion de C sont sur les droites X_1, X_2 et X_3 et ne dépendent pas de b.*

Preuve : On calcule le hessien de C.

$$\begin{aligned} H_C &= 3^3 \det \begin{pmatrix} 2a_1X_1 & -bX_3 & -bX_2 \\ -bX_3 & 2a_2X_2 & -bX_1 \\ -bX_2 & -bX_1 & 2a_3X_3 \end{pmatrix} \\ &= 3^3\Big(-2b^2(a_1X_1^3 + a_2X_2^3 + a_3X_3^3) + (8a_1a_2a_3 - 2b^3)X_1X_2X_3\Big). \end{aligned}$$

Ainsi, pour trouver les points d'inflexion, il faut résoudre le système

$$\left\{ \begin{array}{l} a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3 = 0 \\ -2b^2(a_1X_1^3 + a_2X_2^3 + a_3X_3^3) + (8a_1a_2a_3 - 2b^3)X_1X_2X_3 = 0. \end{array} \right. .$$

Ce système est équivalent à

$$\left\{ \begin{array}{l} a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3 = 0 \\ (8a_1a_2a_3 - 8b^3)X_1X_2X_3 = 0 \end{array} \right. .$$

Puisque C est régulière, $b^3 - a_1a_2a_3 \neq 0$ et ainsi il suffit de résoudre le système

$$\left\{ \begin{array}{l} a_1X_1^3 + a_2X_2^3 + a_3X_3^3 = 0 \\ X_1X_2X_3 = 0 \end{array} \right. .$$

On obtient donc que les points d'inflexion sont sur les droites X_1, X_2 et X_3. On note α_{32}, respectivement α_{13} et α_{21}, une racine cubique de $\frac{a_3}{a_2}$, respectivement $\frac{a_1}{a_3}$ et $\frac{a_2}{a_3}$. Alors les points d'inflexion sont

$$p_{00} = (0{:}\, -\alpha_{32}{:}\, 1), p_{01} = (0{:}\, -\epsilon\alpha_{32}{:}\, 1), p_{02} = (0{:}\, -\epsilon^2\alpha_{32}{:}\, 1)$$

$$p_{10} = (1{:}\, 0{:}\, -\alpha_{13}), p_{11} = (1{:}\, 0{:}\, -\epsilon\alpha_{13}), p_{12} = (1{:}\, 0{:}\, -\epsilon^2\alpha_{13})$$

$$p_{20} = (-\alpha_{21}{:}\, 1{:}\, 0), p_{21} = (-\epsilon\alpha_{21}{:}\, 1{:}\, 0), p_{22} = (-\epsilon^2\alpha_{21}{:}\, 1{:}\, 0).$$

□

Proposition 3.5.3 *Si une cubique non singulière à coefficients dans k possède tous ses points d'inflexion sur les droites X_1, X_2 et X_3, alors elle est de la forme $a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3$, pour certains $a_1, a_2, a_3, b \in k$.*

Preuve : Soit C une cubique non singulière à coefficients dans k avec tous ses points d'inflexion sur les droites X_1, X_2 et X_3. La configuration des points d'inflexion d'une cubique non singulière et des droites passant par ces points impose que les droites X_i passent chacune par 3 points d'inflexion et que les points d'inflexion ne se trouvent pas à l'intersection de 2 droites X_i et X_j. Soient p_1, p_2, p_3 les points d'inflexion de C sur la droite X_1. On a $p_1 = (0{:}\,\alpha_1{:}\,1)$, $p_2 = (0{:}\,\alpha_2{:}\,1)$, $p_3 = (0{:}\,\alpha_3{:}\,1)$, pour certains $\alpha_1, \alpha_2, \alpha_3 \in k_s^\times$. On va voir que $\alpha_1^3 = \alpha_2^3 = \alpha_3^3$. Soit p_4 un point d'inflexion de C sur la droite X_2, $p_4 = (1{:}\,0{:}\,\beta_1)$, $\beta_1 \in k_s^\times$. On peut déduire les autres points d'inflexion de C à partir de ces 4 premiers. On utilise le fait que C est équivalente à une forme normale. Ceci implique que la configuration des points d'inflexion de C est identique à celle des points $x_{00}, \ldots, x_{22}$. Ainsi, si une droite passe par deux points d'inflexion de C, alors elle rencontre un troisième point d'inflexion. Si p et q sont 2 points de $\mathbb{P}^2(k)$, on note (pq) la droite passant par p et q. Si d et d' sont deux doites, on note $d \cap d'$ le point d'intersection de ces 2 droites. Soit p_7 le point d'intersection de la droite (p_1p_4) avec la droite X_3. Alors $p_7 = (s{:}\,r\alpha_1{:}\,r + s\beta_1)$ où $r, s \in k$ vérifient $r + s\beta_1 = 0$. D'où $p_7 = (1{:}\,-\beta_1\alpha_1{:}\,0)$. Soit p_8 le point d'intersection des droites (p_2p_4) et X_3. Alors $p_8 = (s{:}\,r\alpha_2{:}\,r + s\beta_1)$ où $r + s\beta_1 = 0$. Ainsi, $p_8 = (1{:}\,-\beta_1\alpha_2{:}\,0)$. Soit p_9 le point d'intersection des droites (p_3p_4) et X_3, alors $p_9 = (1{:}\,-\beta_1\alpha_3{:}\,0)$. Les points p_7, p_8, p_9 sont les points d'inflexion de C sur la droite X_3. Soit $p_5 = (p_1p_8) \cap X_2$, alors $p_5 = (s{:}\,r\alpha_1 - s\beta_1\alpha_2{:}\,r)$, où $r\alpha_1 - s\beta_1\alpha_2 = 0$, donc $p_5 = (\alpha_1{:}\,0{:}\,\beta_1\alpha_2)$. Soit $p_6 = p_1p_9 \cap X_2$, alors $p_6 = (\alpha_1{:}\,0{:}\,\beta_1\alpha_3)$. Or, les points $p_2p_7 \cap X_2$ et $p_2p_9 \cap X_2$ sont 2 points d'inflexion de C sur la droite X_2 distincts de p_4. Donc, on a soit $p_2p_7 \cap X_2 = p_5$ et $p_2p_9 \cap X_2 = p_6$, soit $p_2p_7 \cap X_2 = p_6$ et $p_2p_9 \cap X_2 = p_5$. Dans le premier cas, puisque $p_2p_7 \cap X_2 = (\alpha_2{:}\,0{:}\,\beta_1\alpha_1)$ et $p_2p_9 \cap X_2 = (\alpha_2{:}\,0{:}\,\beta_1\alpha_3)$, on devrait avoir $\alpha_1 = \alpha_2$ et c'est impossible. Donc

$$\frac{\beta_1\alpha_1}{\alpha_2} = \frac{\beta_1\alpha_3}{\alpha_1} \text{ et } \frac{\beta_1\alpha_3}{\alpha_2} = \frac{\beta_1\alpha_2}{\alpha_1}.$$

Ainsi, on a $\frac{\alpha_1}{\alpha_2} = \frac{\alpha_3}{\alpha_1} = \frac{\alpha_2}{\alpha_3}$ (si on utilise le fait que $(p_3p_7) \cap X_2$ et $(p_3p_8) \cap X_2$ sont des points d'inflexion sur la droite X_2 distincts de p_4, on obtient encore la même condition sur les α_i). Alors $\alpha_1^2 = \alpha_2\alpha_3$, $\alpha_2^2 = \alpha_1\alpha_3$ et $\alpha_3^2 = \alpha_1\alpha_2$. Ainsi $\alpha_1^3 = \alpha_2^3 = \alpha_3^3 = \alpha_1\alpha_2\alpha_3$. Or, p_1, p_2, p_3 sont des points d'intersection de C avec la droite X_1. Si on écrit

$$C = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3},$$

où la somme varie sur les indices i_1, i_2, i_3 tels que $i_1 + i_2 + i_3 = 3$, alors

$$C(0, X_2, X_3) = \lambda_{0,3,0}X_2^3 + \lambda_{0,2,1}X_2^2X_3 + \lambda_{0,1,2}X_2X_3^2 + \lambda_{0,0,3}X_3^3.$$

Donc les α_i sont racines du polynôme de la variable t

$$\lambda_{0,3,0}t^3 + \lambda_{0,2,1}t^2 + \lambda_{0,1,2}t + \lambda_{0,0,3}.$$

Mais puisque les α_i sont aussi racines du polynôme $t^3 - \alpha_1\alpha_2\alpha_3$, alors on a

$$\lambda_{0,3,0}t^3 + \lambda_{0,2,1}t^2 + \lambda_{0,1,2}t + \lambda_{0,0,3} = \lambda_{0,3,0}(t^3 - \alpha_1\alpha_2\alpha_3).$$

D'où, $\lambda_{0,2,1} = \lambda_{0,1,2} = 0$. En échangeant le rôle des variables et en faisant le même travail, on obtient aussi que $\lambda_{2,1,0} = \lambda_{1,2,0} = \lambda_{2,0,1} = \lambda_{1,0,2} = 0$. Ainsi,

$$C = \lambda_{3,0,0}X_1^3 + \lambda_{0,3,0}X_2^2 + \lambda_{0,0,3}X_3^3 + \lambda_{1,1,1}X_1X_2X_3.$$

$\square$

Grâce à ce résultat, on déduit une borne sur la dimension d'une extension de k telle qu'une cubique non singulière soit équivalente sur cette extension à une cubique de la forme $a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3$.

Proposition 3.5.4 *Si k est un corps infini et C est une cubique non singulière à coefficients dans k, alors il existe une sous-extension L/k de k_s/k de dimension inférieure ou égale à 24 telle que C est équivalente sur L à une forme $a_1X_1^3+a_2X_2^3+a_3X_3^3 - 3bX_1X_2X_3$, pour certains $a_i, b \in L$.*

Preuve : On sait que les cubiques $\alpha C + \beta H_C$ décrivent les cubiques passant par les points d'inflexion de C et qu'il en existe exactement 4 singulières qui sont des produits de 3 droites. Ainsi, il existe 4 valeurs de $\lambda \in k_s$ telles que $\lambda C + H_C$ soit un produit de 3 droites (C n'est pas un produit de droites, puisque C est non singulière). Or $H_{\lambda C+H_C} = A(\lambda)C + B(\lambda)H_C$, où $A, B \in k[X]$ et $\deg A, \deg B \leq 3$. De plus, $\lambda C + H_C$ est un produit de droites si et seulement s'il existe $\alpha \in k(\lambda)$ tel que $\alpha(\lambda C + H_C) = A(\lambda)C + B(\lambda)H_C$, c'est-à-dire $\lambda B(\lambda) - A(\lambda) = 0$. Donc $XB(X) - A(X)$ est un polynôme à coefficients dans k de degré 4 possédant toutes ses racines simples. Soit $\lambda_0 \in k_s$ une racine de $XB(X) - A(X)$, alors $\lambda_0 C + H_C$ est un produit de droites et $[k(\lambda_0) : k] \leq 4$. On pose $k' = k(\lambda_0)$. Soit L/k' la plus petite sous-extension galoisienne de k_s/k' telle que $\lambda_0 C + H_C = d_1d_2d_3$ et $d_i \in L[X_1X_2X_3]$ pour tout i. On a que L est une extension finie de k', donc $[L : k'] = |\mathsf{Gal}(L/k')|$. On a une action de $\mathsf{Gal}(L/k')$ sur les courbes projectives à coefficients dans k_s. Pour tout $\gamma \in \mathsf{Gal}(L/k')$, $\gamma \star C = C$, ainsi il existe une permutation σ de $\{1, 2, 3\}$ telle que pour tout $i = 1, 2, 3$, il existe $\lambda_i \in L$ tel que $\gamma \star d_i = \lambda_i d_{\sigma(i)}$. On note $\mathsf{Sym}(d_1, d_2, d_3)$ l'ensemble des permutations des droites d_1, d_2, d_3. Alors on a un homomorphisme de groupes

$$\mathsf{Gal}(L/k') \to \mathsf{Sym}(d_1, d_2, d_3).$$

Nous allons voir que cet homomorphisme est injectif. Pour cela, on considère le sous-groupe $H = \ker(\mathsf{Gal}(L/k') \to \mathsf{Sym}(d_1, d_2, d_3))$. Alors H est un sous-groupe normal de $\mathsf{Gal}(L/k')$. Par le théorème fondamental de la théorie de Galois, $M = \mathcal{F}(H)$ est une extension galoisienne de k' et $\mathsf{Gal}(M/k') \cong \mathsf{Gal}(L/k')/H$. Alors on a un homomorphisme de groupe injectif de

$$\mathsf{Gal}(M/k') \cong \mathsf{Gal}(L/k')/M \to \mathsf{Sym}(d_1, d_2, d_3).$$

Nous allons voir que C est un produit de 3 droites à coefficients dans M. D'abord, on voit que si d est une droite à coefficients dans L telle que pour tout $\gamma \in H$, il existe $\lambda_\gamma \in L$ avec $\gamma \star d = \lambda_\gamma d$, alors il existe une droite d' à coefficients dans M et $a \in L$ tels que $d = ad'$. En effet, $d = a_1X_1 + a_2X_2 + a_3X_3$, où $a_1, a_2, a_3 \in L$ sont non tous nuls. On peut supposer que $a_1 \neq 0$. Alors $d = a_1d'$ avec $d' = X_1 + \frac{a_2}{a_1}X_2 + \frac{a_3}{a_1}X_3$. Alors pour tout $\gamma \in H$, il existe $\lambda'_\sigma \in L$ tel que $\gamma \star d' = \lambda'_\sigma d'$. On doit avoir $\lambda'_\sigma = 1$, puisque $\gamma(1) = 1$. Donc $d' \in M[X_1, X_2, X_3]$ et $d = a_1d'$. Alors $d_1 = a_1d'_1$, $d_2 = a_2d'_2$ et $d_3 = a_3d'_3$, pour certains $a_1, a_2, a_3 \in L$ et des droites d'_1, d'_2, d'_3 à coefficients dans M. Comme $C = d_1d_2d_3 = a_1a_2a_3d'_1d'_2d'_3$, C est à coefficients dans $k' \subset M$ et $d'_1d'_2d'_3$ est à coefficients dans M, alors $a_1a_2a_3 \in M$ et dans $C = d''_1d''_2d''_3$, pour certaines droites d''_1, d''_2, d''_3 à coefficients dans M. Ainsi M/k' est une sous-extension de L/k' telle que C est un produit de 3 droites à coefficients dans M. Alors $L = M$ et l'homomorphisme de groupes $\mathsf{Gal}(L/k') \to \mathsf{Sym}(d_1, d_2, d_3)$ est injectif. Or $|\mathsf{Sym}(d_1, d_2, d_3)| = 6$, donc $|\mathsf{Gal}(L/k')| \leq 6$. Puisque L/k' est galoisienne, $[L \colon k'] = |\mathsf{Gal}(L/k')| \leq 6$. Donc, L est une extension de k, $[L \colon k] \leq 24$ et les points d'inflexion de C sont sur des droites d_i, avec $d_i \in L[X_1, X_2, X_3]$. Alors il existe $\varphi \in \mathsf{GL}_3(L)$ tel que $d_1 \circ \varphi = X_1$, $d_2 \circ \varphi = X_2$ et $d_3 \circ \varphi = X_3$. Ainsi $C \circ \varphi$ est de la forme $a_1X_1^3 + a_2X_2^3 + a_3X_3^3 - 3bX_1X_2X_3$, pour certains $a_i, b \in L$. □

On remarque que l'on peut aussi trouver une borne sur la dimension d'une extension de k contenant les points d'inflexion d'une cubique non singulière. Soit k un corps infini et C une cubique non singulière à coefficients dans k. On sait qu'il existe une extension L/k de dimension inférieure ou égale à 24 telle que les points d'inflexion de C se trouvent sur des droites d_1, d_2, d_3 à coefficients dans L. Alors il existe $\varphi \in \mathsf{GL}_3(L)$ tel que $d_1 \circ \varphi = X_1$, $d_2 \circ \varphi = X_2$ et $d_3 \circ \varphi = X_3$. On note $(0 \colon a_1 \colon 1)$, $(0 \colon a_2 \colon 1)$ et $(0 \colon a_3 \colon 1)$, pour certains $a_i \in k_s$, les points d'inflexion de $C \circ \varphi$ se trouvant sur la droite X_1. Les a_i sont racines du polynôme $C \circ \varphi(0, X, 1)$, donc $[L(a_1) \colon L] \leq 3$. Or $(X - a_2)(X - a_3) \in L(a_1)[X]$, donc $[L(a_1, a_2) \colon L(a_2)] \leq 2$. Ainsi, $[L(a_1, a_2) \colon k] \leq 144$ et les points d'inflexion de $C \circ \varphi$ de trouvant sur la droite X_1 sont dans $\mathbb{P}^2(L(a_1, a_2))$. Ensuite, un point d'inflexion de $C \circ \varphi$ se trouvant sur la droite X_2 est $(1 \colon 0 \colon b_1)$, avec b_1 racine de $C(1, X, 0) \in L(a_1, a_2)[X]$. On trouve que $[L(a_1, a_2, b_1) \colon L(a_1, a_2)] \leq 3$. On pose $E = L(a_1, a_2, b_1)$, alors

$$(0 \colon a_1 \colon 1), (0 \colon a_2 \colon 1), (0 \colon a_3 \colon 1), (1 \colon 0 \colon b_1) \in \mathbb{P}^2(E).$$

On remarque, qu'à partir de ces 4 points, on peut obtenir tous les autres points d'inflexion de $C \circ \varphi$ dans $\mathbb{P}^2(E)$ (en faisant des intersections de droites passant par 2 points d'inflexion, on obtient un nouveau point d'inflexion). Alors $[E \colon k] \leq 432$ et les points d'inflexion de C sont dans $\mathbb{P}^2(E)$.

3.6 Cubiques singulières

Dans cette section, nous allons classifier les différents types de cubiques singulières. Soit k un corps algébriquement clos de caractéristique différente de 2 et de 3. Nous allons voir qu'il y a 9 classes d'équivalences de cubiques singulières à coefficients dans k (où la relation d'équivalence est celle induite par l'action de $\mathsf{GL}_3(k)$). Parmi les cubiques singulières, on peut déjà distinguer les cas des cubiques réductibles et des cubiques irréductibles.

Soit C une cubique à coefficients dans k réductible. Deux cas se présentent : soit C est le produit de 3 droites, soit C est le produit d'une droite avec un polynôme homogène de degré 2 irréductible(on appelera conique une courbe projective de degré 2). Si C est un produit de 3 droites, alors soit C est le produit de 3 droites identiques, soit C est le produit de 2 droites identiques et d'une troisième distincte, soit C est le produit de 3 droites distinctes concourantes (c'est-à-dire, les 3 droites ont un unique point d'intersection), soit C est le produit de 3 droites non concourantes. Ceci définit 4 classes d'équivalence de cubiques singulières dont on donne un représentant :

$$\begin{array}{ll} (1) & X_1^3 \\ (2) & X_1^2X_2 \\ (3) & X_1X_2(X_1+X_2) \\ (4) & X_1X_2X_3 \end{array}$$

Il n'est pas difficile de voir qu'on peut trouver $\varphi \in \mathsf{GL}_3(k)$ tel que $C \circ \varphi$ soit l'une des cubiques ci-dessus, il suffit de choisir un bon repère. Par exemple, dans le cas où les 3 droites sont distinctes non concourantes, on choisit pour repère les 3 points d'intersection formés par les droites et on choisit un quatrième point qui n'appartient à aucune des 3 droites. Et on envoie ce repère sur $(1{:}0{:}0)$, $(0{:}1{:}0)$, $(0{:}0{:}1)$, $(1{:}1{:}1)$. Maintentant, si C est le produit d'une conique irréductible Q avec une droite d, alors soit d coupe Q en un point double (on dit que d est tangente à Q), soit d coupe Q en 2 points distincts.

Lemme 3.6.1 *Soit C une cubique à coefficients dans k. Si $C = Qd$, où Q est une conique irréductible et d est une droite tangente à Q, alors C est équivalente à $(X_2^2 - X_1X_3)X_3$.*

Preuve : Soit p le point d'intersection de Q avec d. On peut supposer que $p = (1{:}0{:}0)$ et que $d = X_3$. On écrit

$$Q = a_1X_1^2 + a_2X_2^2 + a_3X_3 + b_1X_2X_3 + b_2X_1X_3 + b_3X_1X_2,$$

où les $a_i, b_j \in k$. Puisque $m_p(Q, d) = 2$,

$$\begin{aligned} Q(X_1, X_2, 0) &= \alpha(1 \cdot X_2 - 0 \cdot X_1)^2 \\ &= \alpha X_2^2, \end{aligned}$$

pour un certain $\alpha \in k$. Or $Q(X_1, X_2, 0) = a_1X_1^2 + a_2X_2^2 + b_3X_1X_2$, donc $a_2 \neq 0$ et $a_1, b_3 = 0$. Ainsi,

$$Q(X_1, X_2, X_3) = a_2X_2^2 + a_3X_3^2 + b_1X_2X_3 + b_2X_1X_3.$$

On doit avoir $b_2 \neq 0$, car sinon Q n'est pas irréductible. En faisant le changement de variables linéaire

$$\begin{array}{rcl} X_1 & = & Y_1 - \frac{b_1}{b_2} Y_2 - \frac{a_3}{b_2} Y_3 \\ X_2 & = & Y_2 \\ X_3 & = & Y_3, \end{array}$$

on obtient $C = a_2 Y_2^2 Y_3 + b_2 Y_1 Y_3^2$. Enfin, par le changement de variables

$$\begin{array}{rcl} Z_1 & = & -\frac{b_2}{a_2} Y_1 \\ Z_2 & = & Y_2 \\ Z_3 & = & Y_3, \end{array}$$

on trouve $C = a_2(Z_2^2 - Z_1 Z_3) Z_3$. □

Lemme 3.6.2 *Soit C une cubique à coefficients dans k. Si $C = Qd$, où Q est une conique irréductible et d une droite coupant Q en 2 points distincts, alors C est équivalente à $(X_3^2 - X_1 X_2) X_3$.*

Preuve : Soient p et q les 2 points d'intersection de Q avec d. On peut supposer que $p = (1{:}\,0{:}\,0)$, $q = (0{:}\,1{:}\,0)$ et $d = X_3$. On écrit

$$Q = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2 + b_1 X_2 X_3 + b_2 X_1 X_3 + b_3 X_1 X_2.$$

Comme p et q sont des points de Q, on a $a_1 = a_2 = 0$. Ainsi,

$$Q = a_3 X_3^2 + b_1 X_2 X_3 + b_2 X_1 X_3 + b_3 X_1 X_2.$$

On doit avoir $b_3 \neq 0$ car sinon Q n'est pas irréductible. En faisant le changement de variables

$$\begin{array}{rcl} X_1 & = & Y_1 - \frac{b_1}{b_3} Y_3 \\ X_2 & = & Y_2 - \frac{b_2}{b_3} Y_3 \\ X_3 & = & Y_3, \end{array}$$

on obtient $C = (a_3' Y_3^2 + b_3' Y_1 Y_2) Y_3$, où $a_3' = a_3 - \frac{b_1 b_2}{b_3}$ et $b_3' = b_3$. Alors $a_3', b_3' \neq 0$ car sinon, Q ne serait pas irréductible. Finalement, on fait le changement de variables

$$\begin{array}{rcl} Z_1 & = & -\frac{b_3'}{a_3'} Y_1 \\ Z_2 & = & Y_2 \\ Z_3 & = & Y_3 \end{array}$$

et on obtient $C = a_3'(Z_3^2 - Z_1 Z_2) Z_3$. □

Ces deux lemmes permettent de voir que les cubiques qui sont des produits d'une conique irréductible et une droite, nous donnent deux nouvelles classes d'équivalence :

$$\begin{array}{ll}(5) & (X_2^2 - X_1X_3)X_3 \\ (6) & (X_3^2 - X_1X_2)X_3.\end{array}$$

Etudions maintenant le cas des cubiques singulières irréductibles.

Lemme 3.6.3 *Soit C une cubique singulière irréductible. Alors C possède un unique point singulier et la multiplicité de C en ce point vaut 2.*

Preuve : Supposons d'abord que C possède un point singulier p avec $m_p(C) \geq 3$. On écrit

$$C = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3},$$

où la somme se fait sur les indices i_1, i_2, i_3 tels que $i_1 + i_2 + i_3 = 3$. On peut supposer que $p = (1{:}\,0{:}\,0)$. Puisque $m_p(C) \geq 3$, C et les dérivées partielles premières et secondes de C s'annulent en $(1, 0, 0)$. Ainsi

$$\lambda_{3,0,0} = \lambda_{2,1,0} = \lambda_{2,0,1} = \lambda_{1,2,0} = \lambda_{1,1,1} = \lambda_{1,0,2} = 0.$$

Alors $C = \lambda_{0,3,0}X_2^3 + \lambda_{0,0,3}X_3^3 + \lambda_{0,2,1}X_2^2X_3 + \lambda_{0,1,2}X_2X_3^2$ n'est pas irréductible (par le théorème 1.2.3). Maintenant, supposons que C possède 2 points singuliers p et q, la multiplicité de C en ces points étant égale à 2. On peut supposer que $p = (1{:}\,0{:}\,0)$ et $q = (0{:}\,1{:}\,0)$. On écrit encore $C = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3}$. Alors

$$\lambda_{3,0,0} = \lambda_{0,3,0} = \lambda_{1,2,0} = \lambda_{2,1,0} = \lambda_{2,0,1} = \lambda_{0,2,1} = 0.$$

Ainsi, $C = \lambda_{0,0,3}X_3^3 + \lambda_{1,0,2}X_1X_3^2 + \lambda_{0,2,1}X_2^2X_3 + \lambda_{1,1,1}X_1X_2X_3$. Alors X_3 diviserait C. Ceci contredit l'irréductibilité de C. □

Si C est une cubique singulière irréductible, alors C possède une unique point singulier avec la multiplicité de C en ce point égale à 2. On a encore deux possibilités : soit le point singulier possède une tangente double, soit il possède 2 tangentes distinctes.

Lemme 3.6.4 *Soient C une cubique singulière irréductible et p un point singulier, $m_p(C) = 2$. Supposons que C possède une tangente double en p, alors C est équivalente à $X_3^3 - X_1X_2^2$.*

Preuve : On peut supposer que $p = (1{:}\,0{:}\,0)$ et la tangente double soit X_2. On écrit $C = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3}$, où la somme se fait sur les indices i_1, i_2, i_3 tels que $i_1 + i_2 + i_3 = 3$. Alors, comme la multiplicité de C en p est égale à 2, on a $\lambda_{3,0,0} = \lambda_{2,1,0} = \lambda_{2,0,1} = 0$. Dans la section"Courbes projectives", on a vu que si

$q = (q_1 \colon q_2 \colon q_3)$ est une point de C et $m_q(C) = 2$, alors les tangentes à C en q sont les droites $L_{\lambda,\mu}$ avec (λ, μ) racine de

$$\partial_{22}^2 C(q_1, q_2, q_3)X^2 + 2\partial_{23}^2 C(q_1, q_2, q_3)XY + \partial_{33}^2 C(q_1, q_2, q_3)Y^2.$$

Puisque p possède une tangente double $L_{0,1} = X_2$, on doit avoir

$$\partial_{23}^2 C(1,0,0) = \partial_{33}^2 C(1,0,0) = 0 \text{ et } \partial_{22}^2 C(1,0,0) \neq 0.$$

Ainsi, $\lambda_{1,1,1} = \lambda_{1,0,2} = 0$ et $\lambda_{1,2,0} \neq 0$. Donc

$$C = \lambda_{0,3,0}X_2^3 + \lambda_{0,0,3}X_3^3 + \lambda_{1,2,0}X_1X_2^2 + \lambda_{0,2,1}X_2^2X_3 + \lambda_{0,1,2}X_2X_3^2.$$

Remarquons qu'on doit avoir aussi $\lambda_{0,0,3} \neq 0$ car sinon C ne serait pas irréductible. On peut voir que C possède un unique point d'inflexion. Pour cela, on calcule le hessien de C : celui-ci vaut

$$(2\lambda_{1,2,0}X_2)^2(2\lambda_{0,1,2}X_2 + 6\lambda_{0,0,3}X_3).$$

Supposons que $q = (x_1 \colon x_2 \colon x_3)$ soit un point d'inflexion. Alors q est un point d'intersection de C avec H_C. Ainsi, on a soit $x_2 = 0$, soit $x_3 = -\frac{\lambda_{0,1,2}}{3\lambda_{0,0,3}}x_2$. Si $x_2 = 0$, comme p est un point de C, on aurait $x_3 = 0$. Ce n'est pas possible car le point $(1 \colon 0 \colon 0)$ est singulier. Si $x_3 = -\frac{\lambda_{0,1,2}}{3\lambda_{0,0,3}}x_2$, alors $C(x_1, x_2, x_3) = 0$ implique

$$\lambda_{0,3,0}x_2^3 - \frac{\lambda_{0,1,2}^3}{27\lambda_{0,0,3}^2}x_2^3 + \lambda_{1,2,0}x_1x_2^2 - \frac{\lambda_{0,2,1}\lambda_{0,1,2}}{3\lambda_{0,0,3}}x_2^3 + \frac{\lambda_{0,1,2}^3}{9\lambda_{0,0,3}^2}x_2^3 = 0,$$

d'où $\alpha x_2 + \lambda_{1,2,0}x_1 = 0$, avec $\alpha = \lambda_{0,3,0} + \frac{2\lambda_{0,1,2}^3}{27\lambda_{0,0,3}^2} - \frac{\lambda_{0,2,1}\lambda_{0,1,2}}{3\lambda_{0,0,3}}$. Ainsi on obtient un unique point d'inflexion, le point $(\alpha \colon -\lambda_{1,2,0} \colon \frac{\lambda_{1,2,0}\lambda_{0,1,2}}{3\lambda_{0,0,3}})$. On remarque que le point d'inflexion ne se trouve pas sur la tangente double puisque $\lambda_{1,2,0} \neq 0$. On peut supposer que $q = (0 \colon 1 \colon 0)$ et la tangente à C en q est X_1. C'est possible parce que la tangente à C en q ne passe pas par p car sinon elle aurait 4 intersections avec C en comptant la multiplicité. Aussi, il existe $\varphi \in \mathsf{GL}_3(k)$ tel que $\underline{\varphi}$ envoie p sur p, q sur $(0 \colon 1 \colon 0)$ et le point d'intersection des tangentes à C en p et q sur $(0 \colon 0 \colon 1)$, puisque ces points ne sont pas alignés. Alors d'après la démonstration du théorème 3.1.5, $C = aX_3^3 + X_1Q$, pour un certain $a \in k$, $a \neq 0$ et un polynôme homogène Q de degré 2. Donc $C = \lambda_{0,0,3}X_3^3 + \lambda_{1,2,0}X_1X_2^2$. Le changement de variable

$$\begin{aligned} Y_1 &= -\frac{\lambda_{1,2,0}}{\lambda_{0,0,3}} \\ Y_2 &= X_2 \\ Y_3 &= X_3 \end{aligned}$$

permet d'obtenir $C = \lambda_{0,0,3}(Y_3^3 - Y_1Y_2^2)$. □

Dans cette démonstration, on a vu en particulier que si C est singulière irréductible avec une tangente double au point singulier, alors C possède un unique point d'inflexion.

Lemme 3.6.5 *Soient C une cubique singulière irréductible et p un point singulier de C, $m_p(C) = 2$. Supposons que les tangentes à C en p soient distinctes, alors C est équivalente à $X_3^3 + X_1X_3^2 - X_1X_2^2$.*

Preuve : On peut supposer que $p = (1\colon 0\colon 0)$ et les tangentes à C en p soient $X_2 - X_3$ et X_2+X_3. On écrit $C = \sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3}$. Comme la multiplicité de C en p vaut 2, on a $\lambda_{3,0,0} = \lambda_{2,1,0} = \lambda_{2,0,1} = 0$. On utilise maintenant les fait que $L_{1,1} = X_2 - X_3$ et $L_{1,-1} = X_2 + X_3$ sont les tangentes à C en p. Alors on doit avoir

$$\begin{aligned} \partial_{22}^2 C(1,0,0)X^2 + 2\partial_{23}^2 C(1,0,0)XY + \partial_{33}^2 C(1,0,0)Y^2 &= \alpha(Y - X)(Y + X) \\ &= \alpha(Y^2 - X^2), \end{aligned}$$

pour un certain $\alpha \in k$. Ainsi, on a $\lambda_{1,1,1} = 0$, $\lambda_{1,2,0} = -\lambda_{1,0,2}$, $\lambda_{1,2,0} \neq 0$. D'où

$$C = \lambda_{0,3,0}X_2^3 + \lambda_{0,0,3}X_3^3 + \lambda_{1,2,0}X_1X_2^2 - \lambda_{1,2,0}X_1X_3^2 + \lambda_{0,2,1}X_2^2X_3 + \lambda_{0,1,2}X_2X_3^2.$$

Nous allons voir si C possède des points d'inflexion. On calcule le hessien de C :

$$\begin{aligned} H_C = 8\lambda_{1,2,0}^2\Big(&\lambda_{0,1,2}X_2^3 + \lambda_{0,2,1}X_3^3 - \lambda_{1,2,0}X_1X_2^2 + \lambda_{1,2,0}X_1X_3^2 \\ &+(2\lambda_{0,2,1} + 3\lambda_{0,0,3})X_2^2X_3 + (2\lambda_{0,1,2} + 3\lambda_{0,0,3})X_2X_3^2\Big). \end{aligned}$$

Si $(x_1\colon x_2\colon x_3)$ est un point d'inflexion de C, alors $(8\lambda_{1,2,0}^2 C - H_C)(x_1, x_2, x_3) = 0$. Donc,

$$(\lambda_{0,3,0}+\lambda_{0,1,2})x_2^3+(\lambda_{0,0,3}+\lambda_{0,2,1})x_3^3+3(\lambda_{0,0,3}+\lambda_{0,2,1})x_2^2x_3+3(\lambda_{0,3,0}+\lambda_{0,1,2})x_2x_3^2 = 0.$$

Si $\lambda_{0,3,0} + \lambda_{0,1,2} = 0$ et $\lambda_{0,0,3} + \lambda_{0,2,1} = 0$, alors

$$\begin{aligned} C &= \lambda_{0,3,0}X_2^3 + \lambda_{0,0,3}X_3^3 + \lambda_{1,2,0}X_1X_2^2 - \lambda_{1,2,0}X_1X_3^2 + \lambda_{0,0,3}X_2^2X_3 - \lambda_{0,3,0}X_2X_3^2 \\ &= (\lambda_{1,2,0}X_1 + \lambda_{0,3,0}X_2 - \lambda_{0,0,3}X_3)(X_2^2 - X_3^2). \end{aligned}$$

Donc, l'un des deux est non nul. On suppose que $\lambda_{0,3,0} + \lambda_{0,1,2} \neq 0$ (dans le cas contraire, on permute les rôles de X_2 et de X_3). On pose $\alpha = \frac{\lambda_{0,0,3}+\lambda_{0,2,1}}{\lambda_{0,3,0}+\lambda_{0,1,2}}$. Alors, si $(x_1\colon x_2\colon x_3)$ est un point d'inflexion de C,

$$x_2^3 + \alpha x_3^3 + 3\alpha x_2^2x_3 + 3x_2x_3^2 = 0.$$

Si $\alpha = 1$, $X_2^3 + \alpha X_3^3 + 3\alpha X_2^2X_3 + 3X_2X_3^2 = (X_2 + X_3)^2$. Alors $(x_1\colon 1\colon -1)$ est un point d'inflexion si et seulement si $C(x_1, 1, -1) = 0$, ce qui revient à $\lambda_{0,3,0} + \lambda_{0,1,2} = \lambda_{0,0,3} + \lambda_{0,2,1}$. On obtient une contradiction car alors la droite $X_2 + X_3$ a plus de 3 points d'intersection avec C (le point p et les points $(x_1\colon 1\colon -1)$ pour $x_1 = 0, 1, 2$) et donc on a $X_2 + X_3$ divise C. Et si $(x_1\colon x_2\colon x_3)$ est un point d'inflexion se trouvant sur la droite $X_2 + X_3$, alors $H_C(x_1, x_2, x_3) = 0$ implique $\alpha = 1$ (on ne peut avoir $x_2 = 0$ ou $x_3 = 0$ car sinon on obtient le point $(1\colon 0\colon 0)$ qui est un point singulier). Donc C ne possède pas de points d'inflexion sur le droite $X_2 + X_3$. Si $\alpha = -1$,

$$X_2^3 + \alpha X_3^3 + 3\alpha X_2^2X_3 + 3X_2X_3^2 = (X_2 - X_3)^3.$$

Alors $(x_1{:}\,1{:}\,1)$ est un point d'inflexion si et seulement $C(x_1,1,1)=0$, ce qui revient à $\lambda_{0,3,0}+\lambda_{0,0,3}+\lambda_{0,2,1}+\lambda_{0,1,2}=0$. On obtient une contradiction car alors la droite X_2-X_3 a plus de 3 points d'intersection avec C. Et si $(x_1{:}\,x_2{:}\,x_3)$ est un point d'inflexion de C sur la droite X_2-X_3, $H_C(x_1,x_2,x_3)=0$ implique $\alpha=-1$. Donc, C ne possède pas de points d'inflexion sur la droite X_2-X_3. Soit $q=(x_1{:}\,x_2{:}\,x_3)$ avec

$$x_2^3+\alpha x_3^3+3\alpha x_2^2x_3+3x_2x_3^2,$$

x_2,x_3 non tous nuls et

$$x_1=\frac{1}{\lambda_{1,2,0}(x_2^2-x_3^2)}(-\lambda_{0,3,0}x_2^3-\lambda_{0,0,3}x_3^3-\lambda_{0,2,1}x_2^2x_3-\lambda_{0,1,2}x_2x_3^2).$$

Alors q est un point d'inflexion. On peut supposer que $q=(0{:}\,1{:}\,0)$ et la tangente à C en q est X_1. En effet, il existe $\varphi\in\mathsf{GL}_3(k)$ tel que $\underline{\varphi}$ envoie p sur p, q sur $(0{:}\,1{:}\,0)$, le point d'intersection de X_2-X_3 avec la tangente à C en q sur $(0{:}\,1{:}\,1)$ et un point de la droite X_2+X_3 distinct de p et q sur $(1{:}\,1{:}\,-1)$. Alors $C=aX_3^3+X_1Q$, pour un certain $a\in k$, $a\neq 0$ et un polynôme homogène Q de degré 2. Ainsi $\lambda_{0,3,0}=\lambda_{0,2,1}=\lambda_{0,1,2}=0$. Donc $C=\lambda_{0,0,3}X_3^3+\lambda_{1,2,0}X_1X_2^2-\lambda_{1,2,0}X_1X_3^2$ et $\lambda_{0,0,3},\lambda_{1,2,0}\neq 0$. En faisant le changement de variables

$$\begin{array}{rcl} Y_1 & = & -\dfrac{\lambda_{1,2,0}}{\lambda_{0,0,3}}X_1 \\ Y_2 & = & X_2 \\ Y_3 & = & X_3, \end{array}$$

on obtient $C=\lambda_{0,0,3}(Y_3^3+Y_1Y_3^2-Y_1Y_2^2)$. □

Remarquons que la cubique $C=X_3^3+X_1X_3^2-X_1X_2^2$ possède exactement 3 points d'inflexion et ces points sont alignés. En effet,

$$H_C=8(X_1X_3^2-3X_2^2X_3-X_1X_2^2).$$

Donc, si $(x_1{:}\,x_2{:}\,x_3)$ est un point d'inflexion, alors

$$\begin{cases} x_3^3+x_1x_3^2-x_1x_2^2=0 \\ x_1x_3^2-3x_2^2x_3-x_1x_2^2=0 \end{cases}.$$

D'où, $-3x_2^2x_3-x_3^3=0$. Ainsi, soit $x_3=0$, soit $-3x_2^2-x_3^2=0$. Si $x_3=0$, alors soit $x_1=0$, soit $x_2=0$. Mais si $x_2=0$, $(x_1{:}\,x_2{:}\,x_3)$ est le point $(1{:}\,0{:}\,0)$ qui est singulier. Donc $(0{:}\,1{:}\,0)$ est le seul point d'inflexion sur la droite X_3. Si $-3x_2^2-x_3^2=0$, on note α une racine carrée de -3. Alors soit $x_3=\alpha x_2$, soit $x_3=-\alpha x_2$. Dans le premier cas, $x_1=-\frac{3\alpha}{4}x_2$ et dans le second cas, $x_1=\frac{3\alpha}{4}x_2$. Donc les points d'inflexion de C sont les points :

$$(0{:}\,1{:}\,0),(-\frac{3\alpha}{4}{:}\,1{:}\,\alpha),(\frac{3\alpha}{4}{:}\,1{:}\,-\alpha)$$

et ces points sont sur la droite $4X_1 + 3X_3$. Ainsi, les deux dernières classes d'équivalence de cubiques singulières sont :

$$\begin{array}{ll} (7) & X_3^3 - X_1X_2^2 \\ (8) & X_3^3 + X_1X_3^2 - X_1X_2^2 \end{array}$$

3.7 Quelques jolis dessins

Pour des cubiques à coefficients dans $\mathbb{R}$, on voudrait essayer de représenter sur un dessin les points de cette cubique. Le problème est que les points d'une cubique C à coefficients dans $\mathbb{R}$ sont dans le plan projectif $\mathbb{P}(\mathbb{C})$... et il est difficile de dessiner dans ce plan projectif ! On a donc besoin de cartes affines : on choisit une droite appelée droite à l'infini et on représente les points de C qui se trouvent dans le complémentaire de la droite à l'infini. Le complémentaire dans $\mathbb{P}(\mathbb{C})$ d'une droite possèdant une structure d'espace affine, on se retrouve à dessiner dans un plan affine complexe. Biensûr, on ne peut représenter seulement les points réels de C. Ces points ne constituent certainement pas tous les points de C. Ainsi, les dessins de cette section serviront simplement à représenter des points singuliers, des tangentes et des points d'inflexion et à vérifier comment les définitions algébriques de ces notions concordent avec les dessins.

Remarquons qu'en générale une droite possède 3 points d'intersection (en comptant la multiplicité) avec une cubique. Pour ne pas perdre encore trop d'information sur la cubique que l'on veut dessiner, on essaie donc de choisir pour droite à l'infini, une droite qui possède 2 intersections complexes, non réelles avec la cubique. Dans ce cas, la cubique possède une unique intersection réelle avec cette droite à l'infini.

Dans un premier temps, on dessine des formes normales C_λ, pour quelques valeurs de λ réelles. Celles-ci sont représentées dans les deux premiers tableaux des figures (1) à (16). Dans le premier tableau, on a dans l'ordre les formes normales C_λ, pour λ valant -8, -4, -2, -1, -0.5, 0, 0.5, 1. Elles sont dessinées dans le plan affine avec pour droite à l'infini, la droite $-X_1 + X_3$. Cette droite ne passe par aucun des points d'inflexion réels et ne possède qu'une intersection réelle avec les cubiques C_λ, pour les valeurs de λ ci-dessus, sauf pour $\lambda = 1$. Les courbes ne sont pas fermées parce qu'il reste toujours un point réel de chaque cubique sur la droite à l'infini. Pour $\lambda > 1$, C_λ possède 3 intersections avec $-X_1 + X_3$. Ainsi, pour représenter ces cubiques, on prend une autre droite à l'infini. Dans le deuxième tableau, il se trouve dans l'ordre les formes normales C_λ pour λ valant 0, 0.5, 1, 1.1, 2, 4, 8, 16, dessinées dans le plan affine avec $2X_1 + X_3$ pour droite à l'infini.

On connait déjà les points d'inflexion d'une forme normale non singulière. Il y en a exactement 3 réels. Dans le cas où la forme normale est non singulière, on repère les points d'inflexion aux endroits où la courbe change de courbure. Dans le cas de la forme normale singulière C_1, seule la droite $X_1 + X_2 + X_3$ est représentée, les points des 2 autres droites étant non réels (en fait, si un point des droites $X_1 + \epsilon X_2 + \epsilon^2 X_3$ et

$X_1+\epsilon^2 X_2+\epsilon X_3$ est réel, alors il est isolé et n'est donc pas visible sur le dessin). Tous les points dessinés de la droite $X_1+X_2+X_3$ sont des points d'inflexion, puisque les points singuliers de C_1 se trouvant sur cette droite, sont non réels (ce sont les points d'intersection de $X_1+X_2+X_3$ avec les droites $X_1+\epsilon X_2+\epsilon^2 X_3$ et $X_1+\epsilon^2 X_2+\epsilon X_3$, c'est-à-dire $(1{:}\,\epsilon{:}\,\epsilon^2)$ et $(1{:}\,\epsilon^2{:}\,\epsilon)$). On remarque une continuité des représentations des formes normales C_λ quand on fait varier λ. Le passage de C_1 à $C_{1.1}$ fait apparaitre une petite courbe fermée, qui n'existe pas dans C_1. Cela vient du fait que le point $(1{:}\,1{:}\,1)$ de C_1, placé au point $(\frac{1}{3}, \frac{1}{3})$ sur le plan affine (avec $2X_1+X_3$ comme droite à l'infini) est isolé, les points proches de celui-ci étant non réels). Quand λ augmente, ce point se transforme en une courbe fermée.

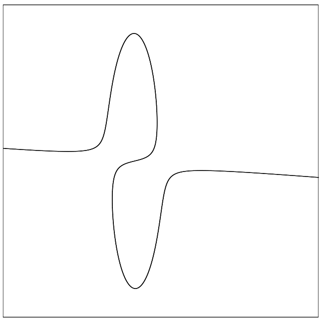
On s'intéresse maintenant aux dessins des représentants des classes d'équivalence de cubiques singulières, présentés dans la section précédente. Les dessins se trouvent dans le troisième tableau.

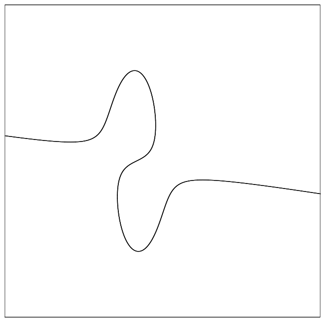
Les figures (17), (18) et (19) représentent respectivement les cubiques X_1^3, $X_1^2X_2$ et $X_1X_2(X_1+X_2)$ dans le plan affine avec X_3 comme droite à l'infini. Sur le dessin, on ne fait pas la différence entre la droite triple X_1^3 et la droite simple X_1. De même, sur le dessin de la cubique $X_1^2X_2$, on ne distingue pas la droite double de la droite simple.

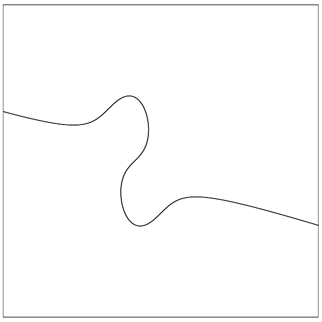
La figure (20) est le dessin de la cubique $X_1X_2X_3$ formée de droites non concourantes, la figure (21) est celui de la cubique $(X_2^2-X_1X_3)X_3$ (conique non dégénérée et droite tangente) et la figure (22) est celui de $(X_3^2-X_1X_2)X_3$ (conique non dégénérée et droite coupant la conique en 2 points). Pour ces 3 cubiques, on choisit $X_1+X_2+X_3$ comme droite à l'infini, car celle-ci ne passe pas par des points particuliers tels que des points d'intersection de 3 droites dans le cas de $X_1X_2X_3$ ou des points réels de la conique dans les deux autres cas.

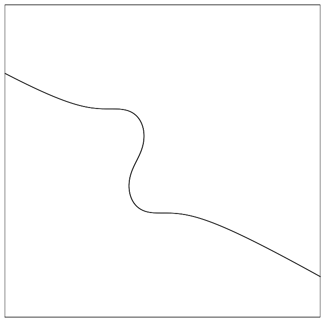
Les deux dernières figures représentent les cubiques singulières irréductibles $X_3^3-X_1X_2^2$ et $X_3^3+X_1X_3^2-X_1X_2^2$ avec X_1+X_2 pour droite à l'infini, cette droite ne passant pas par des points singuliers ou des points d'inflexion réels de ces 2 cubiques.

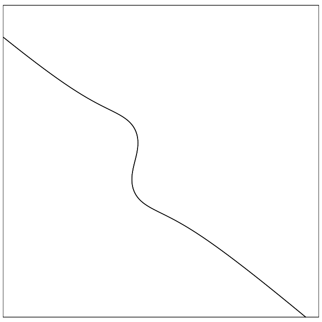
On repère les points singuliers de toutes ces cubiques aux endroits où la cubique passe deux fois. Par exemple, sur les figures (19), (20), (21) et (22), les points singuliers sont des points d'intersection de droites. Pour la figure (24), la cubique passe deux fois par le même point en faisant une boucle. Pour la figure (23), la courbe fait un rebroussement au point singulier. Par contre, pour les figures (17) et (18), les points singuliers sont moins visibles, ce sont les points se trouvant sur la droite triple et sur la droite double. Les points d'inflexion des six premières cubiques singulières sont tous les points des droites simples qui ne sont pas des points d'intersection avec les autres droites de la cubique. Sur les dessin des deux dernières cubiques, les tangentes aux points d'inflexion sont tracées en pointillés et la courbe passe de part et d'autre de la tangente. On remarque que la dernière cubique singulière possède 3 points d'inflexion mais un seul est réel.

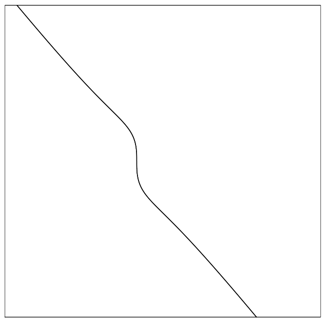

(1)

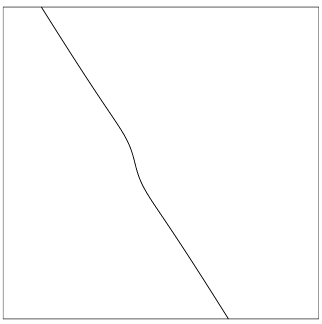

(2)

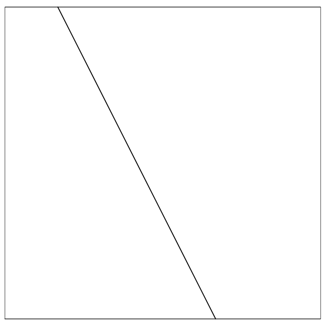

(3)


(4)

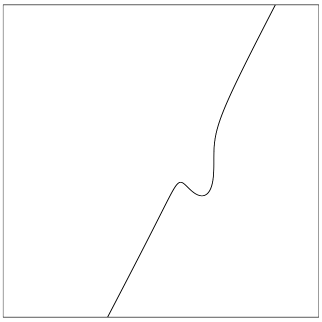

(5)

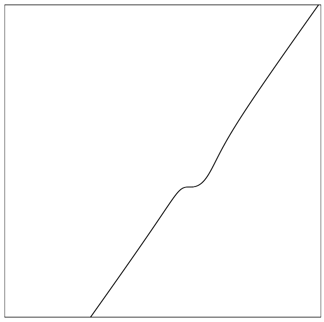

(6)

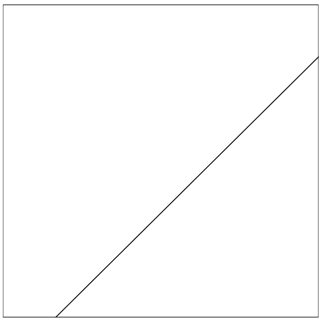

(7)

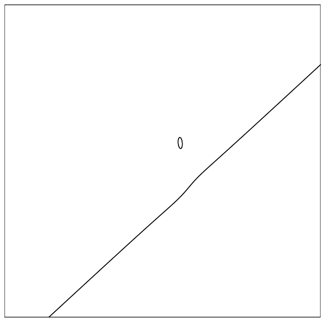

(8)

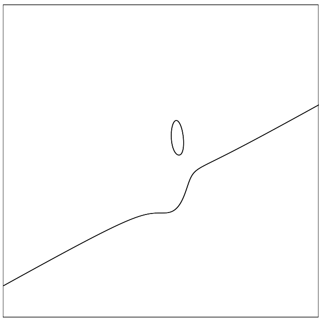
Représentations de formes normales dans le plan affine
avec $-X_1 + X_3$ comme droite à l'infini

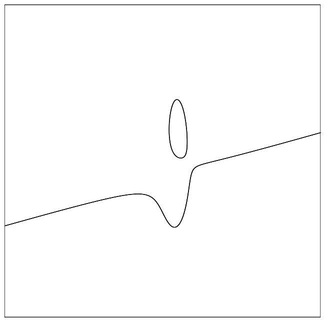

(9)

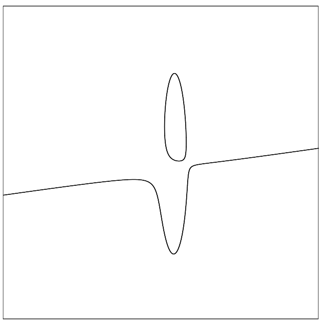

(10)

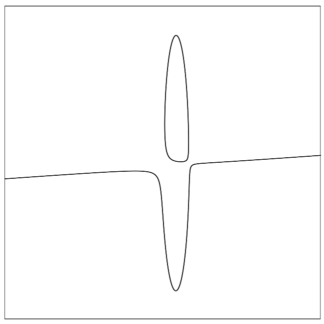

(11)


(12)

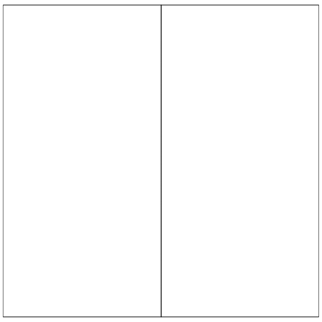

(13)


(14)

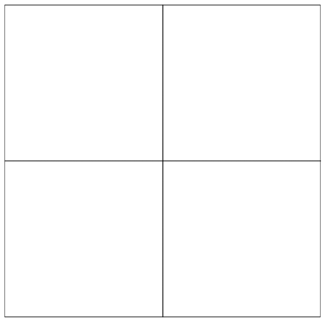

(15)


(16)

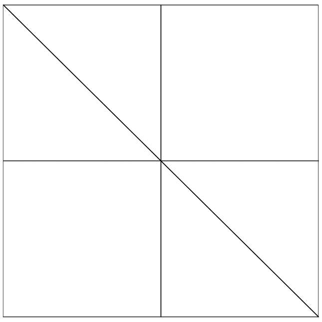
Représentation de formes normales dans le plan affine
avec $2X_1 - X_3$ comme droite à l'infini



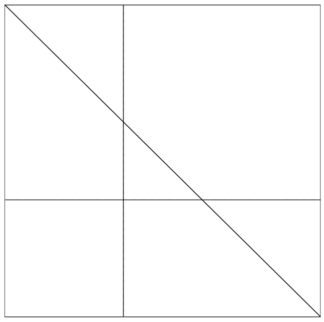
(17)



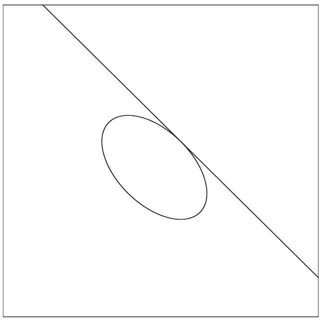
(18)



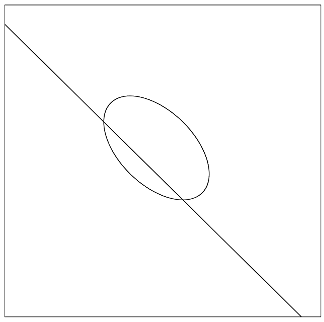
(19)



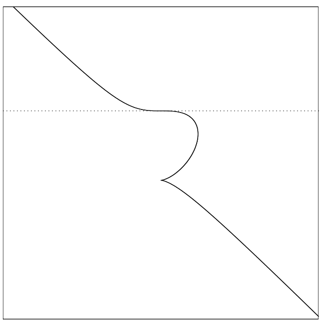
(20)



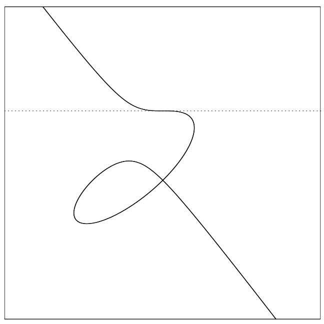
(21)



(22)



(23)



(24)

Les 8 types de cubiques singulières

4

Dimension essentielle des cubiques

Dans ce chapitre, nous allons parler à titre informatif d'une notion à la mode : "la dimension essentielle". A travers l'article [Berhuy et Favi, 2004], nous allons voir que la dimension essentielle des cubiques sur un corps infini de caractéristique différente de 2 et de 3, vaut 3. Il ne sera donné qu'un plan de la démonstration du calcul, ce sujet sortant du cadre de nos recherches et on peut se référer à l'article pour la démonstration complète.

4.1 Notions élémentaires de la théorie des catégories

Une catégorie $\mathcal{C}$ est constituée des données suivantes :
(1) une classe $\mid \mathcal{C} \mid$, dont les éléments sont appelés objets de la catégorie ;
(2) pour toute paire d'objets A, B, un ensemble $\mathcal{C}(A, B)$, dont les éléments sont appelés morphismes ou flèches de A vers B ;
(3) pour tout triplet d'objets A, B, C, une loi de composition

$$\mathcal{C}(A, B) \times \mathcal{C}(B, C) \longrightarrow \mathcal{C}(A, C);$$

la composée de la paire (f, g) est notée $g \circ f$ ou simplement gf ;
(4) pour tout objet A, un morphisme $1_A \in \mathcal{C}(A, A)$, appelé l'identité de A.
Ces données vérifient certains axiomes.
(1) Axiome d'associativité : étant donnés des morphismes $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$, $h \in \mathcal{C}(C, D)$, on a l'égalité suivante

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(2) Axiome d'identité : étant donnés des morphismes $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$, on a les égalités suivantes

$$1_B \circ f = f, \quad g \circ 1_B = g.$$

Un morphisme $f \in \mathcal{C}(A, B)$ sera souvent représenté par la notation $f \colon A \to B$.

Un foncteur F de la catégorie $\mathcal{A}$ vers la catégorie $\mathcal{B}$ est constitué des données suivantes :
(1) une application

$$\mid \mathcal{A} \mid \longrightarrow \mid \mathcal{B} \mid$$

entre les classes d'objets $\mathcal{A}$ et $\mathcal{B}$; l'image de $A \in \mathcal{A}$ est notée $F(A)$ ou simplement FA ;
(2) pour toute paire d'objets A, A' de $\mathcal{A}$, une application

$$\mathcal{A}(A, A') \longrightarrow \mathcal{B}(FA, FA') :$$

l'image de $f \in \mathcal{A}(A, A')$ est notée $F(f)$ ou simplement Ff.
Ces données vérifient les propriétés suivantes :
(1) pour toute paire de morphismes $f \in \mathcal{A}(A, A')$, $g \in \mathcal{A}(A', A'')$,

$$F(g \circ f) = F(g) \circ F(f);$$

(2) pour tout objet $A \in \mathcal{A}$,

$$F(1_A) = 1_{FA}.$$

Etant donnés deux foncteurs $F: \mathcal{A} \to \mathcal{B}$ et $G: \mathcal{B} \to \mathcal{C}$, la composition point par point nous donne un nouveau foncteur $G \circ F: \mathcal{A} \to \mathcal{C}$. Cette loi de composition est associative. Le foncteur identité sur la catégorie $\mathcal{A}$ (c'est-à-dire les deux applications définissant le foncteur sont l'identité) est l'identité pour cette loi de composition.

Soit deux foncteurs F et G d'une catégorie $\mathcal{A}$ vers une catégorie $\mathcal{B}$. Une transformation naturelle $\alpha: F \Rightarrow G$ de F vers G est une classe de morphismes

$$(\alpha_A: FA \to GA)_{A \in \mathcal{A}}$$

de $\mathcal{B}$ indexée par les objets de $\mathcal{A}$, telle que pour tout morphisme $f: A \to A'$ de $\mathcal{A}$,

$$\alpha_{A'} \circ F(f) = G(f) \circ \alpha_A.$$

Si F, G, H sont des foncteurs de $\mathcal{A}$ vers $\mathcal{B}$ et $\alpha: F \Rightarrow G$, $\beta: G \Rightarrow H$ sont des transformations naturelles, alors $\beta \circ \alpha: F \Rightarrow H$ avec $(\beta \circ \alpha)_A = \beta_A \circ \alpha_A$, définit une nouvelle transformation naturelle. Cette loi de composition est associative et possède une unité en tout foncteur F, c'est juste la transformation naturelle 1_F avec $(1_F)_A = 1_{FA}$.

4.2 Définition de la dimension essentielle et exemples

Dans cette section, des notions vont être évoquées sans être approfondies. Pour plus de précisions, on pourra consulter e.g. [Knus *et. al.*, 1998]. On pose, pour k un corps, $\Gamma = \mathsf{Gal}(k_s/k)$ et pour L une extension de k, $\Gamma_L = \mathsf{Gal}(L_s/L)$. Avant de définir la dimension essentielle, on a besoin de la définition du degré de transcendance d'une extension de corps.

Soit L/k une extension de corps. Pour $r > 0$, des éléments $a_1, \ldots, a_r \in L$ sont dits algébriquement indépendants sur k si, pour tout polynôme $f \in k[X_1, \ldots, X_r]$ non nul, $f(a_1, \ldots, a_r) \neq 0$. On définit le degré de transcendance de L sur k, noté $\mathsf{trdeg}(L: k)$, comme étant le supremum de l'ensemble des entiers r tels qu'il existe des éléments $a_1, \ldots, a_r \in L$ algébriquement indépendants sur k.

La catégorie des extensions du corps k, notée $\mathfrak{C}_k$, est la catégorie dont les objets sont les extensions du corps k et les morphismes sont les k-homomorphismes, définis dans les préliminaires. La catégorie des ensembles, notée Ens, est celle dont les objets sont les ensembles et les morphismes sont les applications. Si F est un foncteur de $\mathfrak{C}_k$ vers Ens et $K/k \to L/k$ est un morphisme dans $\mathfrak{C}_k$, pour tout $a \in F(K/k)$, son image par l'application $F(K/k) \to F(L/k)$ sera notée a_L. Quand il n'y aura pas de confusion possible, on écrira $F(K)$ à la place de $F(K/k)$.

Définition 4.2.1 *Soient F un foncteur de $\mathfrak{C}_k$ vers Ens, K/k une extension de corps et $a \in F(K)$. Pour tout $n \in \mathbb{N}$, on dit que la dimension essentielle de a est inférieure ou égale à n et on écrit $\mathsf{ed}(a) \leq n$, s'il existe une sous-extension E/k de K/k telle que*
(i) $\mathsf{trdeg}(E{:}\, k) \leq n$,
(ii) l'élément a est dans l'image de l'application $F(E) \to F(K)$.
On dit que $\mathsf{ed}(a) = n$ si $\mathsf{ed}(a) \leq n$ et $\mathsf{ed}(a) \nleq n-1$. La dimension essentielle de F, notée $\mathsf{ed}_k(F)$, est le supremum des $\mathsf{ed}(a)$, pour tout $a \in F(K)$ et pour toute extension K/k.

La dimension essentielle est en quelque sorte le nombre de paramètres algébriquement indépendants caractérisant un élément quelconque de $F(K)$, pour toute extension K de k.

Exemple 4.2.2 *Pour chaque extension K de k, on choisit arbitrairement un élément $a_K \in K$. On définit le foncteur constant*

$$*{:}\, \mathfrak{C}_k \to \mathsf{Ens}{:}\, K \mapsto \{a_K\}$$

et pour tout k-homomorphisme $f{:}\, K \to L$, $*(f)$ est l'application

$$*(K) \to *(L){:}\, a_K \mapsto a_L.$$

Alors $\mathsf{ed}_k(*) = 0$.

Preuve : Soient $K/k \in \mathfrak{C}_k$ et $a \in *(K)$ (cela veut dire exactement que $*(K) = a$). On a que $\mathsf{ed}(a) \leq 0$. En effet, k/k est une sous-extension de K/k telle que $\mathsf{trdeg}(k{:}\, k) = 0$ et a est dans l'image de l'application $*(k) \to *(K)$ car l'application $*(k) \to *(K)$ est celle qui envoie a_k sur a. Ainsi, $\mathsf{ed}(a) = 0$ et donc $\mathsf{ed}_k(*) = 0$.

Exemple 4.2.3 *On définit le foncteur d'oubli*

$$\mathsf{O}{:}\, \mathfrak{C}_k \to \mathsf{Ens}{:}\, K \mapsto K, \text{ vu en tant qu'ensemble}$$

et pour tout k-homomorphisme $f{:}\, K \to L$, $\mathsf{O}(f)$ est l'application ensembliste f sous-jacente. Alors $\mathsf{ed}_k(\mathsf{O}) = 1$.

Preuve : Soient K/k une extension et $a \in \mathsf{O}(K) = K$. On a alors que $k(a)/k$ est une sous-extension de K/k telle que $\mathsf{trdeg}(k(a)\colon k)$ vaut 0, si a est algébrique sur k et 1, si a est transcendant sur k. Ainsi, $\mathsf{trdeg}(k(a)\colon k) \leq 1$ et a est dans l'image de l'application $\mathsf{O}(k(a)) \to \mathsf{O}(K)$ qui est l'application entre ensembles $k(a) \to K$. Ainsi, $\mathsf{ed}(a) \leq 1$. Or, il existe une extension K de k qui n'est pas algébrique sur k. Alors il existe un élément $a \in K$ transcendant sur k. Ainsi, pour toute sous-extension E/k de K/k telle que a est dans l'image de $E \to K$, il existe $b \in E$ tel que l'image de b par l'application $E \to K$ soit a. Alors b est transcendant sur k est donc $\mathsf{trdeg}(E\colon k) \geq 1$. D'où $\mathsf{ed}(a) \nleq 0$ et donc $\mathsf{ed}_k(\mathsf{O}) = 1$.

Exemple 4.2.4 *Soient k un corps de caractéristique différente de 2 et $n \geq 1$. On définit le foncteur $\mathsf{Q}_n\colon \mathfrak{C}_k \to \mathsf{Ens}$ par, pour toute extension K/k, Q_n est l'ensemble des classes d'isomorphismes de formes quadratiques non dégénérees de dimension n sur K. Alors $\mathsf{ed}(\mathsf{Q}_n) = n$.*

On sait que toute matrice symétrique est diagonalisable. De manière intuitive, on comprend donc que n paramètres suffisent pour déterminer une forme quadratique non dégénérée de dimension n. La démonstration est moins évidente et on peut la retrouver dans [Berhuy et Favi, 2003].

Avant de donner un autre exemple, il nous faut définir la notion de schéma en groupe et pour cela on définit d'abord les algèbres de Hopf.

Définition 4.2.5 *Soient k un corps et A une k-algèbre commutative (associative avec unité) avec multiplication $m\colon A \otimes_F A \to A$. Supposons qu'on ait des homomorphismes de k-algèbres*

$$c\colon A \to A \otimes_k A \text{ (appelé co-multiplication)},$$

$$i\colon A \to A \text{ (appelé co-inverse)},$$

$$u\colon A \to k \text{ (appelé co-unité)}$$

satisfaisant
(i) $(c \otimes \mathsf{Id}_A) \circ c = (\mathsf{Id}_A \otimes c) \circ c$,
(ii) $(u \otimes \mathsf{Id}_A) \circ c = \mathsf{Id}_A$,
(iii) $m \circ (i \otimes \mathsf{Id}_A) \circ c = (\cdot 1_A) \circ u$, *où* $\cdot 1_A$ *désigne l'application* $k \to A\colon \lambda \mapsto \lambda \cdot 1_A$, *alors A est une algèbre de Hopf sur k.*

Si A et B sont des algèbres de Hopf sur k, un homomorphisme de k-algèbres $f\colon A \to B$ est un homomorphisme d'algèbres de Hopf sur k si $(f \otimes f) \circ c_A = c_B \circ f$, $f \circ i_A = i_B \circ f$ et $u_A = u_B \circ f$.

Soit A une algèbre de Hopf sur k et R une k-algèbre. On note $\mathsf{G}^A(R)$ l'ensemble des homomorphismes de k-algèbres entre A et R. Sur $\mathsf{G}^A(R)$, on définit un produit : si f et g sont des homomorphismes de k-algèbres de A dans R,

$$fg = m_R \circ (f \otimes g) \circ c,$$

où $m_R\colon R\otimes_k R \to R$ est la multiplication dans R. On vérifie que le produit est associatif avec une identité à gauche donnée par la composée $(\cdot 1_R)\circ u$ et un inverse à gauche donné, pour f un homomorphisme de k-algèbres de A dans R, par $f^{-1} = f\circ i$. Ainsi, $\mathsf{G}^A(R)$ est un groupe (en considérant que les groupes sont les ensembles munis d'une opération interne associative possédant une identité à gauche et un inverse à gauche). Pour tout homomorphisme de k-algèbres $f\colon R\to S$, on a un homomorphisme de groupes

$$\mathsf{G}^A(f)\colon \mathsf{G}^A(R)\to \mathsf{G}^A(S)\colon g\to f\circ g.$$

On note Grp la catégorie dont les objets sont les groupes et les morphismes sont les homomorphismes de groupes et Alg_k la catégorie dont les objets sont les k-algèbres et les morphismes sont les homomorphismes de k-algèbres. Alors on obtient un foncteur

$$\mathsf{G}^A\colon \mathsf{Alg}_k\to \mathsf{Grp}.$$

Un homomorphisme $A\to B$ d'algèbres de Hopf sur k induit une transformation naturelle $\mathsf{G}^B\to\mathsf{G}^A$.

Définition 4.2.6 *Un schéma en groupe G sur k est un foncteur $G\colon \mathsf{Alg}_k\to\mathsf{Grp}$ isomorphe à G^A pour une certaine algèbre de Hopf A sur k, c'est-à-dire, il existe une transformation naturelle $\rho\colon G\Rightarrow \mathsf{G}^A$ telle que pour toute k-algèbre R, $\rho_R\colon G(R)\to \mathsf{G}^A(R)$ est un isomorphisme.*

Un résultat montre que l'algèbre de Hopf A est uniquement déterminée (à isomorphisme près) par G et on note $A = k[G]$. Un homomorphisme de schémas en groupe $\rho\colon G\Rightarrow H$ est une transformation naturelle. On montre encore que ρ est complètement déterminé par l'unique homomorphisme d'algèbres de Hopf $\rho^*\colon k[H]\to k[G]$ tel que, pour toute k-algèbre R et tout $g\in G(R)$, $\rho_R(g) = g\circ\rho^*$. Un schéma en groupe G sur k est dit de type fini si la k-algèbre $k[G]$ est finiment engendrée.

Un exemple de schéma en groupe de type fini est le foncteur

$$\mathsf{GL}_n(k)\colon \mathsf{Alg}_k\to\mathsf{Grp}\colon R\mapsto \mathsf{GL}_n(R).$$

On vérifie alors que $k[\mathsf{GL}_n(k)]$ est l'algèbre $k[X_{ij}, Y]$ quotientée par l'idéal engendré par $(\det X)Y-1$, où $\det X = \sum_{\sigma\in S_n}\mathsf{sgn}(\sigma)X_{1\sigma(1)}\ldots X_{n\sigma(n)}$, S_n étant l'ensemble des permutations de $\{1,\ldots,n\}$ et $\mathsf{sgn}(\sigma)$ la signature de σ.

Si H est un groupe fini muni d'une Γ-action continue par automorphismes de groupes, alors on a une Γ-action sur la k_s-algèbre $\mathsf{Map}(H,k_s)$. On définit H_{et} comme étant le schéma en groupe représenté par l'algèbre de Hopf

$$\mathsf{Map}(H,k_s)^\Gamma = \{f\in\mathsf{Map}(H,k_s)\mid \forall\gamma\in\Gamma, \gamma\star f = f\}.$$

On introduit une notation : si G est un sous-schéma en groupe de PGL_3, alors $\tilde{G}\colon\mathsf{Alg}_k\to\mathsf{Grp}$ est le foncteur défini par, pour toute k-algèbre R,

$$\tilde{G}(R) = \pi_R^{-1}(G(R)),$$

où $\pi_R\colon \mathsf{GL}_3(R) \to \mathsf{PGL}_3(R)$ est la projection canonique. Alors $\tilde{G}$ est un schéma en groupe.

Rappelons que, pour k un corps, si A est un groupe sur lequel Γ agit continûment par automorphismes de groupe, alors on définit un 1-cocycle de Γ à valeurs dans A comme étant une application continue (les topologies sont la topologie de Krull pour Γ et la topologie discrète pour A) $\alpha\colon \Gamma \to A$ telle que, si on note α_σ l'image de $\sigma \in \Gamma$ dans A, on a

$$\alpha_{\sigma\tau} = \alpha_\sigma \cdot \sigma \star \alpha_\tau, \text{ pour tout } \sigma, \tau \in \Gamma.$$

On définit une relation d'équivalence sur les 1-cocycles : α est équivalent à α' s'il existe $a \in A$ tel que pour tout $\sigma \in \Gamma$,

$$\alpha'_\sigma = a \cdot \alpha_\sigma \cdot \sigma \star (a^{-1}).$$

On note $H^1(\Gamma, A)$ le quotient de l'ensemble des 1-cocyles de Γ à valeurs dans A par cette relation d'équivalence. Cet ensemble possède un élément distingué : la classe du 1-cocycle $\mathbf{1}\colon \Gamma \to A$ avec $\mathbf{1}_\sigma = 1$ pour tout $\sigma \in \Gamma$.

Pour un schéma en groupe de type fini G sur k, on peut considérer, pour toute extension L de k, $H^1(L, G) = H^1(\Gamma_L, G(L_s))$, car le fait que G soit un schéma en groupe représenté par une algèbre de Hopf finiment engendrée implique que Γ_L agit continûment par automorphismes de groupes sur $G(L_s)$. On note $\mathsf{ed}_k(G)$ la dimension essentielle du foncteur $H^1(-, G)$. Un exemple est celui des schémas en groupe est $\widetilde{H_{et}}$ et $\widetilde{\mathfrak{G}_{et}}$, où H est le sous-groupe de $\mathsf{PGL}_3(k_s)$ défini dans le lemme 3.3.5, $\mathfrak{G}$ est le groupe défini dans la section sur le j-invariant. Alors, on trouve que, si k est un corps de caractéristique différente de 2 et de 3, $\mathsf{ed}_k(\widetilde{H_{et}}) = 2$ et $\mathsf{ed}_k(\widetilde{\mathfrak{G}_{et}}) = 2$. On ne donne pas de démonstrations de ces résultats (e.g. [Berhuy et Favi, 2003]).

Le dernier exemple est celui des cubiques. On définit le foncteur

$$\mathsf{Cub}_3\colon \mathfrak{C}_k \to \mathsf{Ens}\colon L \mapsto \mathsf{Cub}_3(L)$$

tel que pour tout k-homomorphisme $f\colon K \to L$, $\mathsf{Cub}_3(f)\colon \mathsf{Cub}_3(K) \to \mathsf{Cub}_3(L)$ est l'application telle que

$$\mathsf{Cub}_3(f)\Big(\Big[\sum \lambda_{i_1,i_2,i_3} X_1^{i_1} X_2^{i_2} X_3^{i_3}\Big]\Big) = \Big[\sum f(\lambda_{i_1,i_2,i_3}) X_1^{i_1} X_2^{i_2} X_3^{i_3}\Big].$$

Le reste du chapitre s'interessera au calcul de la dimension essentielle de Cub_3 et sans donner les détails de la démonstration, on verra que, si k est un corps infini de caractéristique différente de 2 et de 3, $\mathsf{ed}_k(\mathsf{Cub}_3) = 3$.

4.3 Esquisse du calcul de la dimension essentielle des cubiques

Si F et G sont des foncteurs de $\mathfrak{C}_k$ vers Ens, alors on définit le foncteur coproduit de F et G, noté $F \coprod G$, de $\mathfrak{C}_k$ vers Ens : pour toute extension K de k,

$$(F \coprod G)(K) = F(K) \coprod G(K)$$

(qui est la réunion disjointe des ensembles $F(K)$ et $G(K)$) et pour tout k-homomorphisme $f\colon K \to L$,

$$(F \coprod G)(f)\colon (F \coprod G)(K) \to (F \coprod G)(L)$$

est l'application qui envoie $x \in (F \coprod G)(K)$ sur $F(f)(x)$, si $x \in F(K)$ et sur $G(f)(x)$, si $x \in G(K)$.

Lemme 4.3.1 *Si F et G sont des foncteurs de $\mathfrak{C}_k$ vers Ens, alors*

$$\mathsf{ed}_k(F \coprod G) = \max\{\mathsf{ed}_k(F), \mathsf{ed}_k(G)\}.$$

Preuve : Soient K/k une extension et $a \in (F \coprod G)(K)$. Si $a \in F(K)$, alors il existe une sous-extension E/K de K/k telle que $\mathsf{trdeg}(E\colon k) \leq \mathsf{ed}_k(F)$ et a est dans l'image de $F(E) \to F(K)$. Alors, a est dans l'image de $(F \coprod G)(E) \to (F \coprod G)(K)$. D'où, $\mathsf{ed}(a) \leq \mathsf{ed}_k(F)$ et $\mathsf{ed}_k(F \coprod G) \leq \mathsf{ed}_k(F)$. De même, on trouve $\mathsf{ed}_k(F \coprod G) \leq \mathsf{ed}_k(G)$, donc $\mathsf{ed}_k(F \coprod G) \leq \max\{\mathsf{ed}_k(F), \mathsf{ed}_k(G)\}$. Maintenant, soient K/k une extension et $a \in F(K)$. Alors $a \in (F \coprod G)(K)$, donc il existe une sous-extension E/k de K/k et $b \in (F \coprod G)(E)$ tels que $\mathsf{trdeg}(E\colon k) \leq \mathsf{ed}_k(F \coprod G)$ et $a = b_K$. Mais si $b_K = a$, alors $b_K \in F(K)$ et donc $b \in F(E)$. Ainsi, a est dans l'image de $F(E) \to F(K)$ et $\mathsf{ed}(a) \leq \mathsf{ed}_k(F \coprod G)$. Donc, $\mathsf{ed}_k(F) \leq \mathsf{ed}_k(F \coprod G)$. De même, $\mathsf{ed}_k(G) \leq \mathsf{ed}_k(F \coprod G)$, donc $\max\{\mathsf{ed}_k(F), \mathsf{ed}_k(G)\} \leq \mathsf{ed}_k(F \coprod G)$. □

On définit le foncteur des cubiques non singulières

$$\mathsf{Cub}_3^+\colon \mathfrak{C}_k \to \mathsf{Ens}\colon K \mapsto \mathsf{Cub}_3^+(K)$$

et le foncteur des cubiques singulières

$$\mathsf{Cub}_3^-\colon \mathfrak{C}_k \to \mathsf{Ens}\colon K \mapsto \mathsf{Cub}_3^-(K).$$

Alors $\mathsf{Cub}_3 = \mathsf{Cub}_3^+ \coprod \mathsf{Cub}_3^-$. Le lemme 4.3.1 montre que

$$\mathsf{ed}_k(\mathsf{Cub}_3) = \max\{\mathsf{ed}_k(\mathsf{Cub}_3^+), \mathsf{ed}_k(\mathsf{Cub}_3^-)\}.$$

Ainsi, pour calculer la dimension essentielle des cubiques, on voit qu'on peut traiter séparément le cas des cubiques non singulières et celui des cubiques singulières.

On définit le foncteur $\mathsf{Pen}_3^+\colon \mathfrak{C}_k \to \mathsf{Ens}\colon K \mapsto \mathsf{Pen}_3^+(K)$ tel que pour tout k-homomorphisme $f\colon K \to L$,

$$\mathsf{Pen}_3^+(f)\colon \mathsf{Pen}_3^+(K) \to \mathsf{Pen}_3^+(L)\colon [\mathcal{F}_C] \mapsto [\mathcal{F}_{C'}],$$

où $[C'] = \mathsf{Cub}_3^+(f)([C])$.

Lemme 4.3.2 *Soient K/k une extension et $[C] \in \mathsf{Cub}_3^+(K)$. Alors*

$$\mathsf{ed}([\mathcal{F}_C]) \leq \mathsf{ed}([C]) \leq \mathsf{ed}([\mathcal{F}_C]) + 1.$$

Preuve : Soit E/k une sous-extension de K/k telle que $[C]$ soit défini sur E et $\mathsf{trdeg}(E\colon k) = \mathsf{ed}([C])$. Alors clairement $[\mathcal{F}_C]$ est aussi défini sur E, ainsi $\mathsf{ed}([\mathcal{F}_C]) \leq \mathsf{ed}([C])$. Supposons maintenant que $\mathsf{ed}([\mathcal{F}_C]) = n$. Alors il existe une sous-extension L/K de E/K et $[C'] \in \mathsf{Cub}_3^+(L)$ tels que $\mathsf{trdeg}(L\colon k) = n$ et $[\mathcal{F}_C] = [\mathcal{F}_{C'_E}]$. Par définition, il existe $\varphi \in \mathsf{GL}_3(E)$ tel que $\mathcal{F}_{\varphi(C)} = \mathcal{F}_{C'_E}$. En particulier, il existe $\alpha, \beta \in E$ tels que $C \circ \varphi = \alpha C' + \beta H_{C'}$. Ainsi $[C] = [\alpha C' + \beta H_{C'}]$ (dans $\mathsf{Cub}_3(E)$). Puisque α et β ne sont pas tous les deux nuls, $[C]$ est défini soit sur $L(\frac{\alpha}{\beta})$, soit sur $L(\frac{\beta}{\alpha})$. Ainsi, $[C]$ est défini sur un corps de degré de transcendance sur k au plus égal à $n+1$. □

Grâce à ce résultat, on obtient que $\mathsf{ed}_k(\mathsf{Cub}_3^+) \leq \mathsf{ed}_k(\mathsf{Pen}_3^+) + 1$. Pour le calcul de $\mathsf{ed}_k(\mathsf{Pen}_3^+)$, $\mathsf{ed}(\mathsf{Cub}_3^+)$ et de $\mathsf{ed}(\mathsf{Cub}_3^-)$, l'article [Berhuy et Favi, 2004] utilise un lemme de descente galoisienne. Nous ne donnerons ni l'énoncé, ni la démonstration de ce résultat. Nous ne dirons que les implications obtenues sur le calcul de la dimension essentielle des différents foncteurs utilisés.

Soit k un corps infini de caractéristique différente de 2 et de 3 (dans l'article, il n'est pas supposé que k soit infini). Pour $\lambda \in k$, $\lambda^3 \neq 1$, on sait que

$$\mathcal{F}_C = \{C_\mu \mid \mu \in k \cup \{\infty\}\}.$$

Ainsi, pour toute extension L de k, si C, C' sont des cubiques non singulières à coefficients dans L, alors $\mathcal{F}_C$ est équivalente à $\mathcal{F}_{C'}$ sur L_s. En effet, C et C' sont toutes les deux équivalentes à des formes normales non singulières sur L_s. Or, les pinceaux des formes normales non singulières sont identiques, donc $[\mathcal{F}_C] = [\mathcal{F}_{C_\lambda}] = [\mathcal{F}_{C'}]$ dans $\mathsf{Pen}_3^+(L_s)$. On pose, pour $\lambda \in k$, $(\mathsf{Pen}_3^+)_{C_\lambda}\colon \mathfrak{C}_k \to \mathsf{Ens}$ le foncteur défini par, pour L/k une extension,

$$(\mathsf{Pen}_3^+)_{C_\lambda}(L) = \{[\mathcal{F}_C] \mid [\mathcal{F}_C] = [\mathcal{F}_{C_\lambda}] \text{ dans } \mathsf{Pen}_3^+(L_s)\}.$$

Alors, $\mathsf{Pen}_3^+ = (\mathsf{Pen}_3^+)_{C_\lambda}$. Or, par le lemme de descente galoisienne, on a que

$$(\mathsf{Pen}_3^+)_{C_\lambda} \simeq H^1(-, \widetilde{\mathfrak{G}_{et}}),$$

donc $\mathsf{Pen}_3^+ \simeq H^1(-, \widetilde{\mathfrak{G}_{et}})$. Ainsi, $\mathsf{ed}_k(\mathsf{Pen}_3^+) = \mathsf{ed}_k(\widetilde{\mathfrak{G}_{et}}) = 2$. On en déduit que $\mathsf{ed}(\mathsf{Cub}_3^+) \leq 3$.

Soit k'/k une extension et $\lambda \in k' \setminus (N \cup \{1, \epsilon, \epsilon^2\})$ où N est l'ensemble défini dans la section sur le j-invariant. On pose $(\mathsf{Cub}_3^+)_{C_\lambda}\colon \mathfrak{C}_{k'} \to \mathsf{Ens}$ le foncteur défini par, pour toute extension L/k',

$$(\mathsf{Cub}_3^+)_{C_\lambda}(L) = \{[C] \in \mathsf{Cub}_3^+(L) \mid [C] = [C_\lambda] \text{ dans } \mathsf{Cub}_3^+(L_s)\}.$$

Alors par le lemme de descente galoisienne, $(\mathsf{Cub}_3^+)_{C_\lambda} \simeq H^1(-, \widetilde{H_{et}})$. D'où,

$$\mathsf{ed}_{k'}((\mathsf{Cub}_3^+)_{C_\lambda}) = \mathsf{ed}_{k'}(\widetilde{H_{et}}) = 2.$$

Remarquons que les classes d'équivalence de cubiques de $(\mathsf{Cub}_3^+)_{C_\lambda}$ ont toutes le même j-invariant. Donc les cubiques non singulières avec un j-invariant fixé peuvent être décrites avec deux paramètres. On choisit une variable t sur k et $\lambda \in \overline{k(t)}$ tel que $j(C_\lambda) = t$. Comme $\mathsf{ed}_{\overline{k(t)}}((\mathsf{Cub}_3^+)_{C_\lambda}) = 2$, il existe une extension $L/\overline{k(t)}$ et une cubique $[C] \in \mathsf{Cub}_3^+(L)$ tels que $\mathsf{trdeg}(L\colon \overline{k(t)}) \leq 2$, et $[C]$ ne soit pas défini sur une extension $K/\overline{k(t)}$ de degré de transcendance sur $\overline{k(t)}$ strictement inférieur à 2. Alors pour $[C] \in \mathsf{Cub}_3^+(L/k)$, $\mathsf{ed}([C]) = 3$ sur k. Ainsi $\mathsf{ed}_k(\mathsf{Cub}_3^+) \geq 3$ et donc $\mathsf{ed}_k(\mathsf{Cub}_3^+) = 3$.

Pour le cas des cubiques non singulières, le problème est encore divisé. On sait que l'on a, sur $\overline{k}$, 8 classes d'équivalence de cubiques non singulières. Pour $1 \leq i \leq 8$, on note C_i un représentant de la $i$ème classe d'équivalence de cubiques non singulières présentée dans le chapitre propriétés des cubiques. Alors, par le lemme de descente galoisienne,

$$\mathsf{Cub}_3^- \simeq \coprod_{1 \leq i \leq 8} H^1(-, \mathsf{Stab}(C_i)),$$

où $\mathsf{Stab}(C_i)\colon \mathsf{Alg}_k \to \mathsf{Grp}$ est le foncteur défini par

$$\mathsf{Stab}(C_i) = \{\varphi \in GL_3(R) \mid C_i \circ \varphi = C_i\}$$

(en fait, $\mathsf{Stab}(C_i)$ est un schéma en groupe). D'où

$$\mathsf{ed}_k(\mathsf{Cub}_3^-) = \max_{1 \leq i \leq 8} \mathsf{ed}_k(\mathsf{Stab}(C_i)).$$

Or $\mathsf{ed}_k(\mathsf{Stab}(C_6)) = 2$ et pour tout $1 \leq i \leq 8$, $\mathsf{ed}_k(\mathsf{Stab}(C_i)) \leq 2$, donc $\mathsf{ed}_k(\mathsf{Cub}_3^-) = 2$ et on conclut que $\mathsf{ed}_k(\mathsf{Cub}_3) = 3$.

Bibliographie

[1] [Berger, Marcel, 1977], *Géométrie Vol. 1, Actions de groupes, espaces affines et projectifs*, CEDIC, Paris.

[2] [Berhuy, Grégory et Favi, Giordano, 2003] Essential dimension : a functorial point of view (after A. Merkurjev), *Documenta Mathematica*, **8**, pp. 279–330 (electronic).

[3] [Berhuy, Grégory et Favi, Giordano, 2004] Essential dimension of cubics, *Journal of Algebra* **278**, pp. 199–216.

[4] [Brieskorn, Egbert et Knörrer, Horst, 1986] *Plane algebraic curves*, Birkhäuser Verlag, Basel.

[5] [Knus, Max-Albert, Merkurjev, Alexander, Rost, Markus et Tignol, Jean-Pierre, 1998] *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI.

[6] [Miller, George A., Bliechfeld, Hans F., Dickson, Leonard E., 1916] *Theory and applications of finite groups*, John Wiley & Sons, New York

[7] [Morandi, Patrick, 1996] *Field and Galois theory*, Graduate Texts in Mathematics **167**, Springer-Verlag, New York.

[8] [Salmon, George, 1884] *Traité de géométrie analytique*, Gauthier-Villars, Paris.

[9] [Serret, Joseph-Alfred, 1866] *Cours d'algèbre supérieure. Tome II*, Gauthier-Villars, Paris.

[10] [Walker, Robert J., 1950] *Algebraic Curves*, Princeton Mathematical Series, vol. 13, Princeton University Press, Princeton, N. J.

[11] [Weber, Heinrich, 1896] *Lehrbuch der Algebra*, Vieweg und Sohn, Braunschweig.