

ENS Rennes



Département de Mathématiques

# Configuration hessienne, pinceau hessien et groupes de réflexions associés

Nils Jacquemin

Sous la direction de Jérôme Germoni

2025–2026

## Introduction

Ce mémoire établit un lien entre la configuration hessienne (que l'on peut voir comme le plan affine sur  $\mathbb{F}_3^2$ ) et le pinceau hessien (engendré par la cubique d'équation  $x^3 + y^3 + z^3 = 0$  et sa hessienne, d'équation  $xyz = 0$ ) en réalisant la configuration comme l'ensemble des points d'inflexion de la courbe elliptique associée à l'équation  $x^3 + y^3 + z^3 = 0$ . Cette étude nous amènera à explorer différents pans de la géométrie algébrique, allant de la définition des courbes algébriques planes affines et projectives à des sujets plus poussés comme la topologie de Zariski ou encore le bien connu théorème de Bézout. Nous ferons ensuite porter notre attention sur les courbes elliptiques, dont la structure permet de définir des lois de groupe, et plus particulièrement sur leurs points d'inflexion. L'étude de ces points dans un cas particulier entraînera naturellement un travail autour du pinceau hessien. Enfin, la visualisation de ce pinceau selon différents systèmes de coordonnées fera émerger des potentielles symétries, que l'on recherchera. Au cours de cette recherche, on fera la rencontre du sous-groupe  $G_{26}$  de  $\mathrm{GL}_3(\mathbb{C})$  et de son image par la surjection canonique dans  $\mathrm{PGL}_3(\mathbb{C})$ , elle-même isomorphe au groupe spécial affine de  $\mathbb{F}_3^2$ . Enfin, nous nous concentrerons sur les réflexions de  $G_{26}$  et en exhiberons certaines propriétés à l'aide de célèbres théorèmes liant algèbre commutative et théorie des groupes, comme le théorème de Shephard-Todd/Chevalley-Serre ou les formule de Solomon et Molien.

Une grande partie du travail réalisé, notamment autour du pinceau hessien et de  $G_{26}$ , a été réalisé en parallèle de calculs et tracés sur le logiciel sagemath. Certains scripts utilisés seront ajoutés en annexe.

**Remerciements :** Je tiens à remercier chaleureusement Jérôme Germoni pour son implication durant ce stage et tous ses conseils, qu'ils portent sur les mathématiques ou les lieux à visiter de Lyon. Je ressors plus mûr mathématiquement de ce stage en grande partie grâce à lui.

Merci beaucoup également à Philippe Caldero qui m'a donné l'opportunité de parler du pinceau hessien sur sa chaîne youtube [Phil Caldero](#), d'avoir pris la patience de me filmer et de retirer mes hésitations au montage.

# Table des matières

|          |                                                                           |           |
|----------|---------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Configuration hessienne</b>                                            | <b>1</b>  |
| 1.1      | Définitions générales . . . . .                                           | 1         |
| 1.2      | La configuration hessienne . . . . .                                      | 2         |
| <b>2</b> | <b>Espaces projectifs complexes</b>                                       | <b>3</b>  |
| <b>3</b> | <b>Courbes algébriques</b>                                                | <b>4</b>  |
| 3.1      | Ensembles algébriques affines . . . . .                                   | 4         |
| 3.2      | Courbes algébriques affines . . . . .                                     | 5         |
| 3.2.1    | Points singuliers . . . . .                                               | 7         |
| 3.2.2    | Multiplicité d'intersection . . . . .                                     | 7         |
| 3.2.3    | Points d'inflexion . . . . .                                              | 9         |
| 3.3      | Courbes algébriques projectives . . . . .                                 | 11        |
| 3.4      | Intersections de droites, coniques, cubiques . . . . .                    | 12        |
| 3.5      | Courbes elliptiques . . . . .                                             | 15        |
| <b>4</b> | <b>Pinceau hessien et ses symétries</b>                                   | <b>19</b> |
| 4.1      | Pinceau hessien . . . . .                                                 | 19        |
| 4.2      | Stabilisateur projectif du pinceau . . . . .                              | 24        |
| 4.3      | Un stabilisateur linéaire du pinceau . . . . .                            | 27        |
| <b>5</b> | <b>Groupe de réflexions</b>                                               | <b>28</b> |
| 5.1      | Généralités . . . . .                                                     | 28        |
| 5.2      | Deux méthodes pour trouver les invariants . . . . .                       | 29        |
| 5.2.1    | La méthode « par en-dessous » . . . . .                                   | 29        |
| 5.2.2    | La méthode « par au-dessus » . . . . .                                    | 31        |
| 5.2.3    | Aparté : critère d'indépendance algébrique et formule de Molien . . . . . | 31        |
| 5.2.4    | Algèbre des invariants . . . . .                                          | 32        |

# 1 Configuration hessienne

## 1.1 Définitions générales

Les configurations sont des objets mathématiques permettant d'observer des ensembles et l'organisation de leurs points par la notion d'alignement de ces points. Il faut donc en premier lieu définir cette notion.

**Définition 1.1** — Soit  $\mathcal{E}$  un ensemble appelé ensemble de points et  $\mathcal{D}$  un ensemble appelé ensemble de droites. Un **ensemble d'incidence**  $\mathcal{I}$  est une partie de  $\mathcal{E} \times \mathcal{D}$ . On dit qu'un point  $p$  de  $\mathcal{E}$  **appartient à une droite**  $D$  de  $\mathcal{D}$  (ou que la droite  $D$  passe par le point  $p$ ) et on note  $p \in D$  si et seulement si  $(p, D) \in \mathcal{I}$ .

L'incidence nous permet à présent de définir l'objet de notre étude, les configurations.

**Définition 1.2** — Une **configuration** est la donnée de trois ensembles finis  $\mathcal{E}$  (ensemble de points),  $\mathcal{D}$  (ensemble de droites) et  $\mathcal{I} \subset \mathcal{E} \times \mathcal{D}$  (ensemble d'incidence), tels que par chaque point passe le même nombre de droites et que chaque droite contienne le même nombre de points.

On peut également voir  $\mathcal{D}$  comme une partie de  $\mathcal{P}(\mathcal{E})$  et définir l'appartenance de manière canonique. Ainsi, l'ensemble  $\mathcal{I}$  devient obsolète.

Le type d'une configuration est le quadruplet  $p_k n_l$ , où  $p$  est le nombre de points,  $n$  le nombre de droites,  $k$  le nombre de droites passant par un point et  $l$  le nombre d'éléments d'une droite. Un rapide argument combinatoire permet de montrer que  $pk = nl$  (cette quantité est égale au cardinal de l'ensemble  $\mathcal{I}$ ).

**Définition 1.3** — Un **morphisme de configurations** entre les configurations  $C := (\mathcal{E}, \mathcal{D}, \mathcal{I})$  et  $C' := (\mathcal{E}', \mathcal{D}', \mathcal{I}')$  est la donnée de  $f : \mathcal{E} \rightarrow \mathcal{E}'$  et  $\hat{f} : \mathcal{D} \rightarrow \mathcal{D}'$  telles que pour tout  $(p, D) \in \mathcal{I}$ ,  $(f(p), \hat{f}(D)) \in \mathcal{I}'$ .

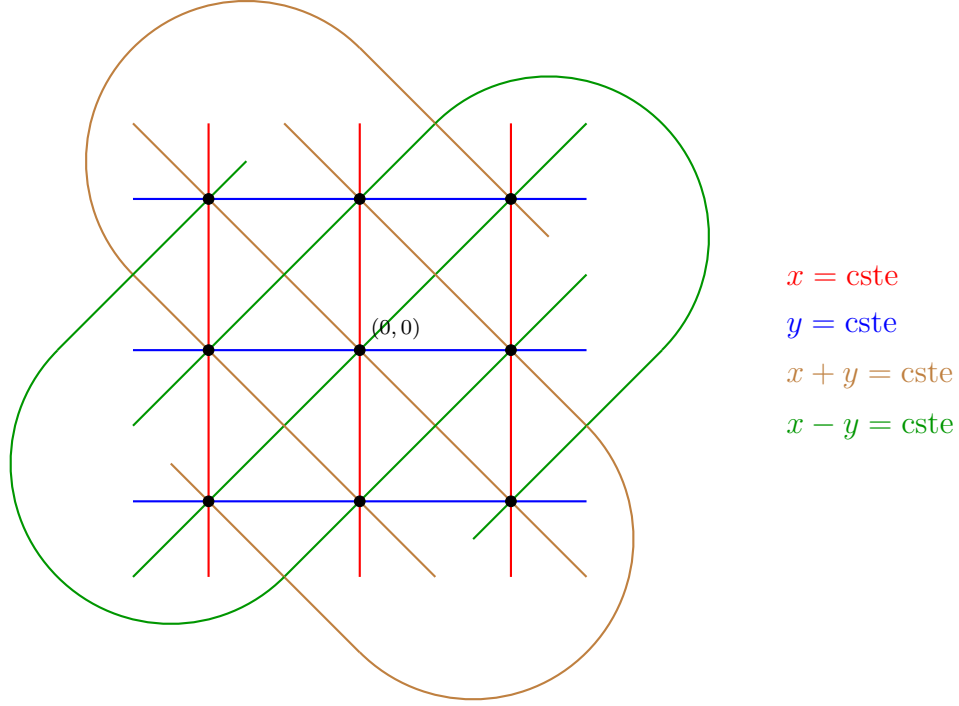
Un **isomorphisme de configurations** entre  $C$  et  $C'$  est la donnée de  $f : \mathcal{E} \rightarrow \mathcal{E}'$  et  $\hat{f} : \mathcal{D} \rightarrow \mathcal{D}'$  bijectives et telles que pour tout  $p \in \mathcal{E}$ , pour tout  $D \in \mathcal{D}$ ,  $p$  appartient à  $D$  si et seulement si  $f(p) \in \hat{f}(D)$ .

Un isomorphisme de  $C$  dans lui-même est appelé **automorphisme**. On note  $\text{Aut}(C)$  l'ensemble de ses automorphismes.

**Remarque :** Il est tentant de penser que deux configuration de même type sont isomorphes, mais ce résultat est faux en général (cf [5, Fig 1.10]).

## 1.2 La configuration hessienne

Nous nous intéresserons en particulier à une configuration : la configuration hessienne, correspondant à l'espace affine  $\text{Aff}_2(\mathbb{F}_3)$  (l'espace  $\mathbb{F}_3^2$  muni de ses droites affines verticales, horizontales et diagonales brisées). Cette configuration est de type  $9_4 12_3$ , et comme elle sera la seule configuration à faire l'objet de notre étude, on la dénotera par abus par son type.



Les neuf points et douze droites de la configuration hessienne

L'objectif de ce mémoire est d'étudier les propriétés de cette configuration, notamment ses symétries (i.e. ses automorphismes), via la théorie des courbes elliptiques. Nous pouvons déjà déterminer son groupe d'automorphismes.

**Proposition 1.1** — *Le groupe d'automorphismes de la configuration hessienne est isomorphe à un produit semi-direct  $\text{GL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ .*

*Démonstration.* Le théorème fondamental de la géométrie affine nous donne que le groupe  $\text{Aut}(9_4 12_3)$  est exactement le groupe affine de cet espace (cf [1, exercice I.67]). Tout élément de ce groupe est de la forme  $\mathbb{F}_3^2 \rightarrow \mathbb{F}_3^2, X \mapsto AX + B$ , avec  $A \in \text{GL}_2(\mathbb{F}_3)$  et  $B \in \mathbb{F}_3^2$ . On remarque qu'une transformation affine  $f_{A,B} : X \mapsto AX + B$  s'identifie à un élément de  $\text{GL}_3(\mathbb{F}_3)$ , qui est  $M_{A,B} = \begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}$ . Un calcul par blocs nous donne, pour  $A, C \in \text{GL}_2(\mathbb{F}_3)$  et  $B, D \in \mathbb{F}_3^2$ ,  $M_{A,B}M_{C,D} = M_{AC, AD+B}$ . En considérant  $\alpha : \text{GL}_2(\mathbb{F}_3) \rightarrow \text{Aut}(\mathbb{F}_3^2)$  l'application envoyant une matrice  $A$  sur l'automorphisme ( $D \mapsto AD$ ), on a bien  $\alpha$  morphisme. Ainsi, le groupe  $\text{Aut}(9_4 12_3)$  est isomorphe au produit semi-direct  $\text{GL}_2(\mathbb{F}_3) \ltimes_{\alpha} \mathbb{F}_3^2$ .  $\square$

Le groupe  $\mathrm{GL}_2(\mathbb{F}_3)$  est d'ordre 48 et  $\mathbb{F}_3^2$  d'ordre 9, donc  $\mathrm{Aut}(9_4 12_3)$  est d'ordre 432.

## 2 Espaces projectifs complexes

**Définition 2.1** — Soit  $n \in \mathbb{N}^*$ . L'espace **projectif complexe de dimension  $n$** , noté  $\mathbb{CP}^n$ , est l'espace des droites vectorielles de  $\mathbb{C}^{n+1}$ , défini par le quotient  $(\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^*$ . L'espace projectif complexe de dimension 1 est appelé la **droite projective complexe**, et celui de dimension 2 le **plan projectif complexe**.

Bien que n'étant pas un  $\mathbb{C}$ -espace vectoriel, cet espace possède un système de coordonnées lié à la base canonique de  $\mathbb{C}^{n+1}$ . Pour  $(x_1, \dots, x_{n+1}) \in \mathbb{C}^{n+1} \setminus \{0\}$ , on note  $[x_1 : \dots : x_{n+1}]$  son image dans  $\mathbb{CP}^n$ , i.e. la droite engendrée par ce vecteur, en gardant en tête que pour tout  $\lambda \in \mathbb{C}^*$ ,  $[\lambda x_1 : \dots : \lambda x_{n+1}] = [x_1 : \dots : x_{n+1}]$ . Cette  $(n+1)$ -liste à scalaire près est appelée « coordonnées homogènes » du point de  $\mathbb{CP}^n$  associé.

Les espaces projectifs possèdent eux aussi leurs transformations.

**Définition 2.2** — Le **groupe projectif linéaire (complexe)** de degré  $n \geq 2$ , noté  $\mathrm{PGL}_n(\mathbb{C})$ , est le quotient de  $\mathrm{GL}_n(\mathbb{C})$  par son centre, réduit à l'ensemble des matrices scalaires. Il agit sur l'espace projectif complexe de dimension  $n-1$ .

La droite projective complexe peut être vue comme  $\hat{\mathbb{C}}$ , la droite  $\mathbb{C}$  à laquelle on a ajouté un point  $\infty$ , en associant à une droite non horizontale  $x = \lambda y$  de  $\mathbb{C}^2$  son abscisse en  $y = 1$  (ici  $\lambda$ ) et à la droite d'équation  $y = 0$  le point  $\infty$ . Deux droites non horizontales se coupant au même point de la droite  $y = 1$  étant égales, on obtient une caractérisation de manière unique des éléments de  $\mathbb{CP}^1$ . Plus précisément, chaque élément de  $\hat{\mathbb{C}}$  possède un et un seul représentant dans  $\mathbb{CP}^1$  de cette manière.

On peut de manière analogue voir le plan projectif complexe comme le plan  $\mathbb{C}^2$  muni d'une droite projective à l'infini en considérant pour toute droite non incluse dans le plan  $z = 0$  les deux premières coordonnées de son point d'intersection avec le plan  $z = 1$ , et pour les droites d'équations  $\lambda x + \mu y = 0$ ,  $z = 0$  le point de  $\mathbb{CP}^1$  défini par  $[\lambda : \mu]$ . De même que précédemment, cette application est une bijection.

Remarquons que le choix de la droite à l'infini pour les droites du plan  $z = 0$  est totalement arbitraire : on considère le plan affine  $z = 1$  (que l'on notera  $\mathbb{A}_{(3)}^2$ ) muni de sa droite à l'infini, tout comme on aurait pu considérer le plan  $x = 1$  (noté  $\mathbb{A}_{(1)}^2$ ) ou  $y = 1$  (noté  $\mathbb{A}_{(2)}^2$ ) ou n'importe quel autre plan affine. On pourra donc utiliser n'importe laquelle de ces visions du plan projectif complexe en fonction des expressions que l'on manipule pour simplifier ces dernières. On parlera dorénavant de la droite à l'infini pour désigner la droite projective  $z = 0$ , et on spécifiera dès que l'on ne se placera pas dans cette visualisation de  $\mathbb{CP}^2$ .

La théorie des espaces projectifs permet d'homogénéiser certaines notions (par exemple confondre les notions de cercles euclidiens et de droites réelles dans la droite projective complexe), ce qui peut s'avérer très utile pour simplifier de nombreux énoncés. Une propriété célèbre du plan projectif est que deux de ses droites se coupent toujours en un unique point. On peut de plus voir la droite à l'infini comme une ligne d'horizon, où l'on verrait deux droites parallèles se couper par effet de perspective.



Une route dans le plan projectif (image pixabay)

De nombreux théorèmes de géométrie se démontrent aisément à l'aide du plan projectif, comme le théorème de Miquel ou celui de Pascal. Nous verrons plus loin en quoi travailler dans le plan projectif complexe est intéressant dans le cadre des courbes algébriques.

## 3 Courbes algébriques

### 3.1 Ensembles algébriques affines

Soit  $n \in \mathbb{N}^*$ . Sauf indication contraire, on travaillera dans cette partie dans  $\mathbb{C}^n$  ou l'algèbre des polynômes à  $n$  coordonnées que l'on identifiera à l'algèbre symétrique associée notée  $\mathcal{S}_n$ .

**Définition 3.1** — *L'ensemble algébrique affine (complexe) associé à un ensemble  $S \subset \mathcal{S}_n$  est le sous-ensemble  $\mathcal{V}(S)$  de  $\mathbb{C}^n$  défini par l'ensemble des points de  $\mathbb{C}^n$  annulant tous les polynômes de  $S$ .*

**Remarque :** Plusieurs sous-ensembles définissent le même ensemble algébrique, comme les ensembles  $\{x\}$  et  $\{x^2\}$  dont l'ensemble algébrique associé dans  $\mathbb{C}^2$  est la droite d'équation  $x = 0$ . Ceci nous permet de caractériser de manière plus précise ces ensembles.

Si  $S$  et  $S'$  deux sous-ensembles de  $\mathcal{S}_n$  telles que  $S'$  est inclus dans  $S$ , annuler tous les polynômes de  $S$  est plus contraignant qu'annuler ceux de  $S'$ , et on a  $\mathcal{V}(S) \subset \mathcal{V}(S')$ .

**Lemme 3.1** — Soit  $S$  une partie de  $\mathcal{S}_n$ . Notons  $I$  l'idéal engendré par  $S$ . Les ensembles algébriques  $\mathcal{V}(S)$ ,  $\mathcal{V}(I)$  et  $\mathcal{V}(\sqrt{I})$  sont égaux.

*Démonstration.* L'inclusion  $\mathcal{V}(\sqrt{I}) \subset \mathcal{V}(I) \subset \mathcal{V}(S)$  est donnée par le fait que  $S$  est inclus dans  $I$  qui est lui-même inclus dans  $\sqrt{I}$ . Réciproquement, si un point  $(y_1, \dots, y_n)$  annule tous les éléments de  $S$ , il annule toutes les sommes finies de produits finis d'éléments de  $S$ , donc tous les éléments de  $I$ . Par intégrité de  $\mathbb{C}$ , il annule également les éléments de  $\sqrt{I}$ .  $\square$

Notons que comme  $\mathbb{C}[x_1, \dots, x_n]$  est noethérien on peut se restreindre à l'étude des lieux d'annulation d'ensembles *finis* de polynômes.

L'ensemble des ensembles algébriques de  $\mathbb{C}[x_1, \dots, x_n]$  (ou  $\mathcal{S}_n$ ) se trouve être stable par certaines opérations, ce qui permet de définir une topologie sur  $\mathbb{C}^n$ .

**Proposition 3.1** — Les ensembles algébriques de  $\mathbb{C}[x_1, \dots, x_n]$  définissent les fermés d'une topologie sur  $\mathbb{C}^n$ . Cette topologie est appelée *topologie de Zariski*.

*Idée de démonstration.* On a déjà  $\emptyset = \mathcal{V}(\mathbb{C}[x_1, \dots, x_n])$  et  $\mathbb{C}^n = \mathcal{V}(0)$ . Il suffit ensuite de montrer que pour  $I, J$  idéaux de  $\mathbb{C}[x_1, \dots, x_n]$ ,  $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$  et que pour  $(I_k)_{k \in \mathbb{N}^*}$  famille d'idéaux,  $\bigcap_{k=0}^{+\infty} \mathcal{V}(I_k) = \mathcal{V}\left(\sum_{k=0}^{+\infty} I_k\right)$  (cf [4, 1.4]).  $\square$

**Remarque :** Les ouverts non vides de cette topologie sont tous denses. En effet, pour  $\mathcal{O}_1, \mathcal{O}_2$  deux ouverts non vides dont les complémentaires sont associés respectivement aux idéaux  $I_1$  et  $I_2$  non nuls,  $\mathcal{O}_1 \cap \mathcal{O}_2 = \mathbb{C}^n \setminus (\mathcal{V}(I_1) \cup \mathcal{V}(I_2)) = \mathbb{C}^n \setminus \mathcal{V}(I_1 \cap I_2)$ . L'intersection de deux idéaux non nuls étant non nulle,  $\mathcal{V}(I_1 \cap I_2) \neq \mathbb{C}^n$ , donc l'intersection de  $\mathcal{O}_1$  et  $\mathcal{O}_2$  est non vide.

## 3.2 Courbes algébriques affines

La plupart des démonstrations de cette partie est inspirée de la section 1 de [6].

On dénotera dans cette partie les indéterminées par  $u$  et  $v$ , les notations  $x, y$  et  $z$  seront utilisées en travaillant dans l'anneau de polynômes (à coefficients complexes) à trois inconnues.

**Définition 3.2** — Une **courbe algébrique plane affine** (complexe) est un ensemble de la forme  $\mathcal{V}(f)$ , où  $f \in \mathbb{C}[u, v]$  est un polynôme non nul. Une courbe  $\mathcal{C}$  est dite **irréductible** s'il existe  $f \in \mathbb{C}[u, v]$  polynôme irréductible tel que  $\mathcal{C} = \mathcal{V}(f)$ .

**Remarque :** De même que précédemment, une telle courbe peut être définie à l'aide de plusieurs polynômes différents.

Dans la suite, on abrégera « courbe algébrique plane affine » en « courbe affine ».

**Proposition 3.2** — Soit  $f \in \mathbb{C}[u, v]$  un polynôme irréductible et  $g \in \mathbb{C}[u, v]$  tel que  $f$  ne divise pas  $g$ . Alors il existe  $a \in \mathbb{C}[u] \setminus \{0\}$  et  $h_1, h_2 \in \mathbb{C}[u, v]$  tels que  $fh_1 + gh_2 = a$ .

*Démonstration.* Comme  $f \in \mathbb{C}[u, v]$ , on peut le voir comme un élément de  $\mathbb{C}(u)[v]$ . On peut montrer que  $f$  reste irréductible et non diviseur de  $g$  dans cet anneau. Ainsi,  $f, g$  sont premiers entre eux dans  $\mathbb{C}(u)[v]$ , qui est un anneau euclidien. On peut donc fixer  $\tilde{h}_1, \tilde{h}_2 \in \mathbb{C}(u)[v]$  tels que  $f\tilde{h}_1 + g\tilde{h}_2 = 1$ . En multipliant cette identité par  $a \in \mathbb{C}[u]$  le dénominateur commun des coefficients de  $\tilde{h}_1$  et  $\tilde{h}_2$  (éléments de  $\mathbb{C}(u)$ ), on obtient  $fh_1 + gh_2 = a$ , avec  $h_1, h_2 \in \mathbb{C}[u, v]$  et  $a \in \mathbb{C}[u]$ .  $\square$

**Remarque :** Ce résultat est toujours vrai si on remplace  $\mathbb{C}$  par un corps quelconque.

**Corollaire 3.1** — Soient  $f, g \in \mathbb{C}[u, v]$  tels que  $f$  est irréductible et ne divise pas  $g$ . Alors  $\mathcal{V}(f) \cap \mathcal{V}(g)$  est fini.

*Démonstration.* D'après ce qui précède on peut fixer  $a \in \mathbb{C}[u]$ ,  $h_1, h_2 \in \mathbb{C}[u, v]$  tels que  $fh_1 + gh_2 = a$ . Ainsi, pour  $\lambda, \mu \in \mathbb{C}$ , si  $f(\lambda, \mu) = g(\lambda, \mu) = 0$  alors  $a(\lambda) = 0$ . Comme  $a \in \mathbb{C}[u]$ , on en déduit que l'égalité est possible uniquement pour un nombre fini de  $\lambda$ . Pour un tel  $\lambda$ , si  $f(\lambda, v)$  admettait une infinité de racines, ce polynôme serait nul et il suivrait que  $f$  est divisible par  $u - \lambda$ , ce qui contredirait l'irréductibilité de  $f$ . À  $\lambda$  fixé,  $f(\lambda, \mu)$  s'annule donc uniquement pour un nombre fini de  $\mu$ . On en déduit que  $\mathcal{V}(f) \cap \mathcal{V}(g)$  est fini.  $\square$

Ainsi, si  $f$  est irréductible, les fermés stricts de  $\mathcal{V}(f)$  pour la topologie de Zariski sont finis. De plus, pour  $P = (u_P, v_P) \in \mathcal{V}(f)$ ,  $\{P\}$  est un fermé de  $\mathcal{V}(f)$  en tant qu'intersection de cette courbe et des deux droites d'équation  $u - u_P = 0$  et  $v - v_P = 0$  (qui ne se coupent qu'en  $P$ ). Par union finie, tous les sous-ensembles finis de  $\mathcal{V}(f)$  en sont des fermés pour la topologie de Zariski. D'après ce qui précède, ces sous-ensembles sont exactement les fermés stricts de  $\mathcal{V}(f)$ . Une union de deux fermés stricts est donc un fermé strict, donc une intersection d'ouverts non vides est un ouvert non vide. On retrouve que tous les ouverts de  $\mathcal{V}(f)$  sont denses.

On peut également remarquer que la réciproque toute application bijective de  $\mathcal{V}(f)$  dans lui même envoie un ensemble fini sur un autre ensemble fini, donc est continue pour la topologie de Zariski.

De plus, si  $f, g \in \mathbb{C}[u, v]$  sont deux polynômes irréductibles non constants, alors  $\mathcal{V}(f)$  et  $\mathcal{V}(g)$  sont infinis (c'est même une équivalence), donc  $\mathcal{V}(f) = \mathcal{V}(g)$  si et seulement si  $\mathcal{V}(f) \cap \mathcal{V}(g)$

est infini, si et seulement si  $(f, g)$  est liée dans  $\mathbb{C}$ . Ainsi, chaque courbe irréductible infinie est déterminée par un unique polynôme irréductible, à un scalaire multiplicatif près. De manière plus générale, toute courbe admet une unique décomposition en union de courbes irréductibles deux à deux sans composante commune. Ceci nous permet de définir le degré d'une courbe.

**Définition 3.3** — Soit  $\mathcal{C}$  une courbe affine. Si  $\mathcal{C}$  est irréductible, on définit son **degré** comme le degré de l'unique  $f \in \mathbb{C}[u, v]$  irréductible tel que  $\mathcal{C} = \mathcal{V}(f)$  (à scalaire près). Si  $\mathcal{C}$  est réductible, écrivons  $\mathcal{C} = \mathcal{C}_1 \cup \dots \cup \mathcal{C}_r$  sa décomposition en irréductibles. Le degré de  $\mathcal{C}$  est la somme des degrés des  $\mathcal{C}_i$ , pour  $1 \leq i \leq r$ . On appelle **droite** une courbe de degré 1, **conique** une courbe de degré 2 et **cubique** une courbe de degré 3.

### 3.2.1 Points singuliers

Nous allons nous concentrer sur les courbes irréductibles. On fixe  $f \in \mathbb{C}[u, v]$  un polynôme non constant, et on note  $\mathcal{C}$  la courbe associée.

**Définition 3.4** — Un **point singulier** (ou **singularité**) de  $\mathcal{C}$  est un point  $P \in \mathcal{C}$  tel que  $f'_u(P) = f'_v(P) = 0$ , où  $f'_u, f'_v$  sont les dérivées directionnelles de  $f$  suivant  $u$  et  $v$ . Un point non singulier est dit **régulier**. Une courbe dont tous les points sont singuliers est dite **lisse**.

On peut montrer sans trop de difficultés, via des arguments de divisibilité qu'une courbe irréductible possède un nombre fini de singularités.

Soit un point  $P = (u_0, v_0)$  de  $\mathcal{C}$ . Si ce point est régulier, on définit la tangente à  $\mathcal{C}$  en  $P$  comme la droite algébrique définie par l'équation  $f'_u(P)(u - u_0) + f'_v(P)(v - v_0) = 0$ . On remarque rapidement que l'on étend de cette manière la notion de tangente à un graphe de fonction aux courbes algébriques.

### 3.2.2 Multiplicité d'intersection

Deux courbes peuvent s'intersecter en un point de façon plus ou moins brutale. La droite  $u = 0$  est orthogonale à la droite  $v = 0$ , et leur intersection en  $(0, 0)$  forme quatre angles droits, tandis que cette dernière droite semble « accompagner » la courbe  $v = u^2$  en  $(0, 0)$ . Ce paragraphe fait l'objet de la formalisation de cette idée. On fixe dans la suite  $\mathcal{C}, \mathcal{C}'$  deux courbes affines associées respectivement à  $f, g \in \mathbb{C}[u, v]$ , sans facteur irréductible commun et s'intersectant en un point  $P$ . On suppose d'abord  $f$  irréductible.

**Proposition 3.3** — En tout point régulier  $Q$  de  $\mathcal{C}$ , il existe une fonction  $t \in \mathbb{C}[u, v]$  s'annulant en  $Q$  et telle que toute fonction rationnelle  $\alpha$  définie, non identiquement nulle sur  $\mathcal{C}$  et s'annulant en  $Q$  s'écrive de la forme  $\alpha = t^k \gamma$ , avec  $k \in \mathbb{Z}$  et  $\gamma$  une fonction régulière ne s'annulant pas en  $Q$ . La fonction  $t$  est appelée **paramètre local** de  $\mathcal{C}$  en  $Q$ .

*Démonstration.* Quitte à faire un changement linéaire de coordonnées, il suffit de démontrer uniquement le résultat pour le point  $Q := (0, 0)$  quand celui-ci est un point régulier de  $\mathcal{C}$ , ce qu'on supposera ici, avec par exemple  $f'_v(Q) \neq 0$ . Montrons que le polynôme  $u$  (qui s'annule en  $Q$ ) est paramètre local de  $\mathcal{C}$  en  $Q$ .

Comme  $(0, 0)$  est un point régulier de  $\mathcal{C}$ , on peut écrire  $f(u, v) = au + bv + h(u, v)$ , avec  $a := f'_u(0, 0)$  et  $b := f'_v(0, 0) \neq 0$ , et  $h \in \mathbb{C}[u, v]$  ne contenant que des monômes de degré  $\geq 2$ . On scinde  $h$  en  $u\varphi \in \mathbb{C}[u], v\psi \in \mathbb{C}[u, v]$  de manière à ce que  $u\varphi$  contienne tous les monômes de  $h$  dans lesquels seul  $u$  intervient. Ainsi, on a  $f(u, v) = u(a + \varphi(u)) + v(b + \psi(u, v))$ . Sur la courbe  $\mathcal{C}$ , on en déduit  $v = -u\beta$ , avec  $\beta := (a + \varphi(u))/(b + \psi(u, v))$  fonction régulière sur  $\mathcal{C}$  qui est en outre régulière en  $Q$  car  $\psi(0, 0) = 0$ .

Soit  $\alpha$  une fonction rationnelle non identiquement nulle sur  $\mathcal{C}$  et telle que  $\alpha(Q) = 0$ , que l'on peut écrire  $\alpha = p/q$ , avec  $p, q \in \mathbb{C}[u, v]$ ,  $p(Q) = 0$  et  $q(Q) \neq 0$ . D'après ce qui précède, on peut écrire  $p(u, v) = p(u, u\beta) = ur$ , avec  $r$  une fonction régulière sur  $\mathcal{C}$  (car  $p(0, 0) = 0$ ). Ainsi,  $\alpha = u\gamma_1$ , avec  $\gamma_1 = r/q$  fonction régulière sur  $\mathcal{C}$  et régulière en  $Q$ . Si  $\gamma_1(Q) = 0$ , on répète donc le processus pour avoir  $\alpha = u^2\gamma_2$  et ainsi de suite. Montrons que ce procédé termine toujours.

On garde les notations  $\alpha = p/q$  précédentes. Fixons  $l \in \mathbb{N}$  et  $\gamma$  fonction régulière sur  $\mathcal{C}$  et régulière en  $Q$  tels que  $p = u^l \gamma$ , et montrons que  $l$  ne peut excéder une certaine valeur.

Comme  $\alpha$  est non nulle,  $p$  ne divise pas  $f$  et est donc premier avec. D'après la proposition 3.2, fixons  $a \in \mathbb{C}[u]$  et  $\gamma_1, \gamma_2 \in \mathbb{C}[u, v]$  tels que  $\gamma_1 p + \gamma_2 f = a$ . Notons  $k$  la multiplicité de 0 en tant que racine de  $a$ , et  $a_0 \in \mathbb{C}[u]$  tel que  $a_0(0) \neq 0$  et  $a = u^k a_0$ . Montrons que  $l \leq k$ .

Par l'absurde, on suppose que  $l > k$ . Sur  $\mathcal{C}$ , on a  $\gamma_1 p = a = u^k a_0$ , donc  $u^k(u^{l-k}\gamma - a_0) = 0$ . En fixant  $b, c \in \mathbb{C}[u, v]$  tels que  $c(Q) = 0$  et  $\gamma = b/c$ , on obtient  $u^k(u^{l-k}b - a_0c) = 0$  sur  $\mathcal{C}$ . Par irréductibilité de  $f$ , par le corollaire 3.1 ce dernier divise  $u^k(u^{l-k}b - a_0c)$ . Comme  $f$  est irréductible et différent de  $u$  (car  $f'_v(Q) \neq 0$ ),  $f$  est premier avec  $u^k$ . Ainsi,  $f$  divise  $u^{l-k}b - a_0c$ . C'est absurde car  $u^{l-k}b$  s'annule en  $Q$ , contrairement à  $a_0c$ .

Le procédé termine donc bien, et il termine en moins de  $k$  étapes. □

**Remarque :** Si  $t$  et  $t'$  sont deux paramètres locaux de  $\mathcal{C}$  en  $P$ , la proposition précédente implique que  $t/t'$  et  $t'/t$  sont des fonctions rationnelles sur  $\mathcal{C}$ , régulières en  $P$ . Ainsi, il existe  $\gamma$  une fonction rationnelle sur  $\mathcal{C}$  régulière et non nulle en  $P$  telle que  $t' = t\gamma$ .

Le polynôme  $g$  associé à  $\mathcal{C}'$  définit une fonction rationnelle sur  $\mathcal{C}$  s'annulant en  $P$  et non identiquement nulle. Par le théorème précédent et la remarque, il existe un unique  $k \in \mathbb{Z}$  (et

même positif car  $g$  est un polynôme) tel que pour tout paramètre local  $t$ , il existe  $\gamma$  fonction rationnelle régulière et non nulle en  $P$  telle que  $g = t^k \gamma$ . Cet entier  $k$  est appelé *multiplicité d'intersection* des courbes  $\mathcal{C}$  et  $\mathcal{C}'$  en  $P$ .

**Exemples :** - Les courbes définies par  $u = 0$  et  $u + v = 0$  s'intersectent en  $(0, 0)$ . Le polynôme  $v$  est un paramètre local en  $(0, 0)$  de la première courbe, et la fonction rationnelle définie par  $u + v$  sur cette dernière est  $v$ . La multiplicité d'intersection entre ces courbes en  $(0, 0)$  est donc 1. On peut vérifier de même qu'en tout autre point du plan, la multiplicité d'intersection de ces deux courbes est 0, ce qui traduit le fait que celles-ci ne s'intersectent qu'en  $(0, 0)$ .

- Les courbes  $u^2 - v = 0$  et  $2u - 1 - v = 0$  s'intersectent en  $(1, 1)$ . Un paramètre local de la seconde courbe en ce point est  $u - 1$ , et sur cette dernière, la fonction  $u^2 - v$  peut s'écrire  $u^2 - 2u + 1 = (u - 1)^2$ . La multiplicité d'intersection entre ces deux courbes en  $(1, 1)$  est donc 2. On retrouve l'idée de « contact d'ordre supérieur » d'une courbe avec sa tangente.

En ne supposant plus forcément  $\mathcal{C}$  irréductible, on peut tout de même définir la multiplicité d'intersection en  $P$  comme la somme des multiplicités d'intersection de  $\mathcal{C}'$  et des facteurs irréductibles de  $\mathcal{C}$  en  $P$ .

### 3.2.3 Points d'inflexion

Nous allons maintenant motiver la définition de point d'inflexion sur une courbe algébrique. On fixe une courbe algébrique  $\mathcal{C}$  associé à un polynôme  $f$ .

Dans le cadre de l'étude des fonctions  $g : \mathbb{R} \rightarrow \mathbb{R}$  de classe  $C^2$ , on définit un point d'inflexion comme étant un point en lequel la tangente au graphe traverse celui-ci, i.e.  $t_0 \in \mathbb{R}$  est point d'inflexion si et seulement si  $g(t) = g(t_0) + g'(t_0)(t - t_0) + c(t - t_0)^3 + o((t - t_0)^3)$  au voisinage de  $t_0$ , avec  $c \neq 0$ . On va ici affaiblir cette définition en ne demandant que  $g(t) - g(t_0) - g'(t_0)(t - t_0) = O((t - t_0)^3)$  : on perd le fait que la tangente traverse la courbe mais on conserve l'idée de « contact d'ordre 3 ou plus ».

Dans le cas des courbes algébriques, une définition analogue serait donc, en regardant un point  $P = (u_0, v_0)$ ,  $f(u_0 + h_1, v_0 + h_2) - f(P) - f'_u(P)h_1 - f'_v(P)h_2 = O(\|(h_1, h_2)\|^3)$ , i.e.  $f''_{uu}(P) = f''_{uv}(P) = f''_{vv}(P) = 0$ , ce qui revient aussi à dire que le contact entre  $\mathcal{C}$  et sa tangente en  $P$  est de multiplicité au moins 3, comme dans le cas précédent. On définit donc un point d'inflexion de  $\mathcal{C}$  comme un point de la courbe vérifiant ces conditions (qui sont équivalentes).

**Définition 3.5** — *Un **point d'inflexion** de  $\mathcal{C}$  est un point  $P$  de  $\mathcal{C}$  régulier et tel que la multiplicité d'intersection de  $\mathcal{C}$  et sa tangente en  $P$  est supérieure ou égale à 3.*

Dans la suite, on suppose que  $f$  s'annule en  $P := (0, 0)$ . On peut toujours se ramener à ce cas via un changement affine de coordonnées.

**Proposition 3.4** — *Le point  $P$  est point d'inflexion de  $\mathcal{C}$  si et seulement si le déterminant  $\begin{vmatrix} f''_{uu} & f''_{uv} & f'_u \\ f''_{uv} & f''_{vv} & f'_v \\ f'_u & f'_v & 0 \end{vmatrix}(P)$  est nul.*

*Démonstration.* On écrit  $f(u, v) = au + bv + cu^2 + duv + ev^2 + h(u, v)$ , avec  $a, b, c, d, e \in \mathbb{C}$  et où  $h \in \mathbb{C}[u, v]$  ne contient que des termes de degrés  $\geq 3$ .

On fixe  $\lambda, \mu \in \mathbb{C}$  tels que la tangente  $\mathcal{T}$  à  $\mathcal{C}$  en  $P$  soit paramétrée par  $u = \lambda t$ ,  $v = \mu t$ , quand  $t$  parcourt  $\mathbb{C}$ . Sur un point  $(\lambda t, \mu t)$  de  $\mathcal{T}$ , on a  $f(\lambda t, \mu t) = t(a\lambda + b\mu) + t^2(c\lambda^2 + d\lambda\mu + e\mu^2) + t^3\varphi(t)$ , avec  $\varphi \in \mathbb{C}[u]$ .  $t$  est la paramétrisation de  $f$  en  $P$  sur  $\mathcal{T}$ . Ainsi on a  $a\lambda + b\mu = 0$  et  $P$  est point d'inflexion si et seulement si  $c\lambda^2 + d\lambda\mu + e\mu^2 = 0$ .

Si  $c\lambda^2 + d\lambda\mu + e\mu^2 = 0$ , comme  $p_1(u, v) := au + bv$  est irréductible dans  $\mathbb{C}[u, v]$  et  $p_2(u, v) := cu^2 + duv + ev^2$  est tel que  $V(p_1) \cap V(p_2)$  est infini (car il contient  $\mathbb{C} \cdot (\lambda, \mu)$  et  $\lambda, \mu$  sont non tous deux nuls car  $P$  est régulier), donc  $p_1$  divise  $p_2$ . Donc  $p_1$  divise  $p_1 + p_2$ , donc la conique associée à  $au + bv + cu^2 + duv + ev^2$ .

Réciproquement, supposons  $q(u, v) := au + bv + cu^2 + duv + ev^2$  réductible. On l'écrit  $q = rs$ , avec  $r, s \in \mathbb{C}[u, v]$  de degré 1. Comme  $q(0, 0) = 0$ , on a  $r(0, 0) = 0$  ou  $s(0, 0) = 0$ . Supposons que  $r(0, 0) = 0$  quitte à intervertir. Ainsi, on peut fixer  $A, B, C, D, E \in \mathbb{C}$  tels que  $r(u, v) = Au + Bv$  et  $s(u, v) = Cu + Dv + E$ . On a donc  $E(Au + Bv) = au + bv$ , donc  $r$  est multiple de  $p_1$ . Ainsi,  $p_1|q = p_1 + p_2$ , donc  $p_1|p_2$ , donc  $c\lambda^2 + d\lambda\mu + e\mu^2 = 0$ .

On a donc montré que  $P$  est point d'inflexion si et seulement si  $q$  est réductible. Le lemme suivant permettra de conclure.

**Lemme 3.2** — *La forme quadratique non nulle sur  $\mathbb{C}^3$  d'équation  $q(x, y, z) = axz + byz + cx^2 + dxy + ey^2$  est irréductible si et seulement si le déterminant  $\begin{vmatrix} 2c & d & a \\ d & 2e & b \\ a & b & 0 \end{vmatrix}$  est non nul.*

*Démonstration.* On a, pour tout  $(x, y, z) \in \mathbb{C}^3$ ,  $q(x, y, z) = \frac{1}{2}(x, y, z)M_q(x, y, z)^\top$ , avec  $M_q$  la matrice de l'énoncé. Ainsi,  $\det(M_q)$  est nul si et seulement si  $q$  est dégénérée, si et seulement s'il existe  $\lambda \in \mathbb{C}$  tel que, dans une base adaptée, on a  $q(\tilde{x}, \tilde{y}, \tilde{z}) = \tilde{x}^2 + \lambda\tilde{y}^2$ , si et seulement s'il existe  $\mu \in \mathbb{C}$  tel que dans cette base,  $q(\tilde{x}, \tilde{y}, \tilde{z}) = (\tilde{x} + i\mu\tilde{y})(\tilde{x} - i\mu\tilde{y})$ . On a ainsi l'équivalence voulue.  $\square$

Comme  $a = f'_u(P)$ ,  $b = f'_v(P)$ ,  $c = \frac{1}{2}f''_{uu}(P)$ ,  $d = f''_{uv}(P)$ ,  $e = f''_{vv}(P)$ , d'après le lemme précédent on a bien  $P$  point d'inflexion de  $\mathcal{C}$  si et seulement si  $\begin{vmatrix} f''_{uu} & f''_{uv} & f'_u \\ f''_{uv} & f''_{vv} & f'_v \\ f'_u & f'_v & 0 \end{vmatrix}(P) = 0$ .  $\square$

### 3.3 Courbes algébriques projectives

Nous allons implémenter dans le cadre projectif les notions introduites pour les courbes affines. Pour plus de simplicité, on se limitera à l'étude de points de  $\mathbb{A}_{(3)}^2$ . Ainsi, dans cette partie, on travaillera dans  $\mathbb{C}[x, y, z]$  et dans  $\mathbb{C}[u, v]$ , avec  $u = x/z$ ,  $v = y/z$ . Ces résultats se transposent de manière analogue à l'étude de points de  $\mathbb{A}_{(1)}^2$  et  $\mathbb{A}_{(2)}^2$ .

Une courbe algébrique plane projective se définit de manière analogue à une courbe affine comme l'ensemble des points du plan projectif  $\mathbb{C}P^2$  dont les coordonnées homogènes annulent un polynôme  $F \in \mathbb{C}[x, y, z]$  homogène non nul. Notons que l'homogénéité de  $F$  est nécessaire car pour une bonne définition de la courbe, on doit avoir  $F(x, y, z) = 0$  si et seulement si pour tout  $\lambda \in \mathbb{C}^*$ ,  $F(\lambda x, \lambda y, \lambda z) = 0$ .

On fixe dans ce paragraphe une courbe projective  $\mathcal{C}$ , associée à un polynôme  $F$ . On considère  $f(u, v) := F(u, v, 1) \in \mathbb{C}[u, v]$  et  $\tilde{\mathcal{C}}$  la courbe associée. On introduit également  $P = [x_P : y_P : z_P] \in \mathbb{A}_{(3)}^2$  (avec donc  $z_P \neq 0$ ), ainsi que  $\tilde{P} := (\lambda, \mu) \in \tilde{\mathcal{C}}$ , où l'on a posé  $\lambda := x_P/z_P$  et  $\mu := y_P/z_P$ . Nous n'étudierons plus dans la suite que des courbes projectives.

Définitions dans le cadre projectif à l'aide du cadre affine :

Le point  $\tilde{P}$  est singulier si et seulement si  $f'_u(\tilde{P}) = f'_v(\tilde{P}) = 0$  i.e. si et seulement si  $F'_u(\lambda, \mu, 1) = F'_v(\lambda, \mu, 1) = 0$ , si et seulement si  $F'_x(P) = F'_y(P) = 0$ . On dit dans ce cas que  $P$  est un point singulier de  $\mathcal{C}$ .

Si  $P$  n'est pas singulier, il est dit régulier. Dans ce cas, la tangente à  $\tilde{\mathcal{C}}$  en  $\tilde{P}$  est d'équation  $f'_u(\tilde{P})(u - \lambda) + f'_v(\tilde{P})(v - \mu) = 0$ , donc d'équation  $F'_u(P)(u - \lambda) + F'_v(P)(v - \mu) = 0$ . En multipliant par  $z$  on obtient

$$F'_x(P)(x - z\lambda) + F'_y(P)(y - z\mu) = 0 \quad (1)$$

Par le théorème d'Euler pour les fonctions homogènes, on a  $F'_x x + F'_y y + F'_z z = nF$ , avec  $n := \deg(F)$ . Comme  $F(P) = 0$ , on a

$$F'_x(P)x_P + F'_y(P)y_P + F'_z(P)z_P = 0 \quad (2)$$

Ainsi,  $z_P \cdot (1) + z \cdot (2)$  donne  $z_P [F'_x(P)x + F'_y(P)y + F'_z(P)z] = 0$ , donc

$$F'_x(P)x + F'_y(P)y + F'_z(P)z = 0 \quad (3)$$

Cette équation définit la tangente à  $\mathcal{C}$  en  $P$ .

Enfin, on dit que le point  $P$  est point d'inflexion de  $\mathcal{C}$  si et seulement si  $\tilde{P}$  est point d'inflexion de  $\tilde{\mathcal{C}}$ . La proposition suivante nous en donne une caractérisation.

**Proposition 3.5** — *On suppose le point  $P$  régulier dans  $\mathcal{C}$ . Alors ce point est point d'inflexion de  $\mathcal{C}$  si et seulement si  $\det(\text{Hess}_F(P)) = 0$ , où  $\text{Hess}_F$  est la matrice Hessienne de  $F$ .*

*Démonstration.* Le point  $P$  est point d'inflexion de  $\mathcal{C}$  si et seulement si  $\tilde{P}$  est point d'inflexion de  $\tilde{\mathcal{C}}$ , donc (d'après la proposition 3.4) si et seulement si  $\begin{vmatrix} f''_{uu} & f''_{uv} & f'_u \\ f''_{uv} & f''_{vv} & f'_v \\ f'_u & f'_v & 0 \end{vmatrix}(\tilde{P}) = 0$ , i.e. si et seulement si  $\begin{vmatrix} F''_{xx} & F''_{xy} & F'_x \\ F''_{xy} & F''_{yy} & F'_y \\ F'_x & F'_y & 0 \end{vmatrix}(P) = 0$ .  
Le théorème d'Euler donne

$$\begin{aligned} F''_{xx}x + F''_{xy}y + F''_{xz}z &= (n-1)F'_x \\ F''_{yx}x + F''_{yy}y + F''_{yz}z &= (n-1)F'_y \\ F'_xx + F'_yy + F'_zz &= nF. \end{aligned}$$

En effectuant les changements de colonnes et de lignes  $C_3 \leftarrow z(n-1)C_3 - xC_1 - yC_2$ , puis  $L_3 \leftarrow z(n-1)L_3 - xL_1 - yL_2$ , où  $C_i$  (resp.  $L_i$ ) est la  $i$ -ième colonne (resp. ligne) de la matrice, on obtient  $P$  point d'inflexion si et seulement si  $z^6 \begin{vmatrix} F''_{xx} & F''_{xy} & F''_{xz} \\ F''_{xy} & F''_{yy} & F''_{yz} \\ F''_{zx} & F''_{zy} & F''_{zz} \end{vmatrix}(P) = 0$ , i.e. si et seulement si  $\det(\text{Hess}_F(P)) = 0$ .  $\square$

**Remarque :** Si  $\deg(F) \geq 2$ , chercher des points d'inflexion de  $\mathcal{C}$  revient donc à chercher points d'intersection de  $\mathcal{C}$  et de sa hessienne, c'est à dire la courbe projective associée à  $\text{Hess}_F = 0$ , qui est un polynôme homogène de degré  $3(n-2)$ .

Les autres résultats de la partie 3.2 se transposent au cadre projectif.

### 3.4 Intersections de droites, coniques, cubiques

Cette partie utilise des résultats et démonstrations de la partie 3.8 de [4].

D'après la partie 3.3, chercher les points d'inflexion d'une courbe projective revient à chercher ses points d'intersection avec sa hessienne. Nous allons donc ici nous pencher sur l'intersection de deux courbes projectives, en particulier de « petit » degré.

Un théorème très important de la théorie des courbes projectives est le théorème de Bézout, portant sur l'intersection de deux courbes.

**Théorème 3.1.** (Théorème de Bézout)

*Soient  $\mathcal{C}_1$ ,  $\mathcal{C}_2$  deux courbes projectives planes de degrés respectifs  $d_1$  et  $d_2$  définies sur  $\mathbb{C}$ , sans composante (irréductible) commune. Alors  $\mathcal{C}_1$  et  $\mathcal{C}_2$  s'intersectent en  $d_1d_2$  points de  $\mathbb{CP}^2$ , comptés avec multiplicité.*

Notre intérêt ne portant que sur les courbes de « bas degré », nous allons démontrer ce théorème dans deux cas particuliers.

**Proposition 3.6** — *Soient  $\mathcal{C}$  une courbe de degré  $d$  et  $\mathcal{L}$  une droite non contenue dans  $\mathcal{C}$ . Alors  $\mathcal{C}$  et  $\mathcal{L}$  s'intersectent en  $d$  points (comptés avec multiplicité).*

*Démonstration.* D'après la proposition 3.1, on sait que ces deux courbes s'intersectent en un nombre fini de points. Il existe donc une droite  $\mathcal{D}$  de  $\mathbb{CP}^2$  ne contenant aucun de ces points. Par changement affine de coordonnées, on peut donc supposer que  $\mathcal{D}$  est la droite à l'infini et que  $\mathcal{L}$  est la droite d'équation  $y = 0$ . En considérant  $F \in \mathbb{C}[x, y, z]$  de degré  $d$  tel que  $\mathcal{C} = V(F)$ , on a  $\mathcal{C} \cap \mathcal{L} = \{[x : 0 : 1] ; x \in \mathbb{C}, F(x, 0, 1) = 0\}$ . Or  $f(x) := F(x, 0, 1) \in \mathbb{C}[x]$  est de degré  $d$  car  $y$  ne divise pas  $F$ . Donc d'après le théorème de d'Alembert-Gauss,  $|\mathcal{C} \cap \mathcal{L}| = d$ .  $\square$

**Remarque :** Cette proposition montre que deux droites de  $\mathbb{CP}^2$  se coupent en exactement un point, comme annoncé dans la section 2.

**Proposition 3.7** — *Soient  $\mathcal{C}$  une courbe de degré  $d$  et  $\Gamma$  une conique sans composante commune avec  $\mathcal{C}$ . Alors  $\mathcal{C}$  et  $\Gamma$  s'intersectent en  $2d$  points (comptés avec multiplicité).*

Ces deux cas particuliers du théorème de Bézout sont utiles pour calculer la dimension d'espaces de courbes passant par des points particuliers.

*Démonstration.* Considérons  $F \in \mathbb{C}[x, y, z]$  le polynôme homogène de degré  $d$  associé à  $\mathcal{C}$ . Si  $\Gamma$  est réductible, elle s'écrit comme réunion de deux droites et on peut appliquer le résultat précédent droite par droite. Supposons maintenant  $\Gamma$  irréductible. L'étude de la théorie des coniques (cf [3], partie 3.2) amène qu'un choix judicieux de repère donne une équation de  $\Gamma$  de la forme  $xy - z^2 = 0$  ainsi, cette conique s'identifie à la droite projective complexe via  $[u : v] \mapsto [u^2 : v^2 : uv]$ . On peut donc étudier  $f(u, v) \mapsto F(u^2, v^2, uv)$  qui est un polynôme homogène à deux variables et de degré  $2d$  par composition. Par homogénéité de  $f$  et comme  $\mathbb{C}$  est algébriquement clos, on peut factoriser  $f(u, v) = \lambda \prod_{k=1}^{2d} (u - a_k v)$ , donc factoriser  $\mathcal{C}$  en union de  $2d$  droites projectives (comptées avec multiplicité). Par la proposition précédente,  $\mathcal{C}$  et  $\Gamma$  ont exactement  $2d$  points d'intersection (avec multiplicité).  $\square$

**Lemme 3.3** — *Soient  $P_1, \dots, P_5$  cinq points distincts de  $\mathbb{CP}^2$ , tels que quatre d'entre eux ne sont jamais alignés. Alors il existe une unique conique contenant tous ces points.*

*Démonstration.* Une conique est définie par une combinaison linéaire de monômes de  $\mathbb{C}[x, y, z]$  de degré 2. Construire un tel monôme revient à choisir les puissances en  $x$ ,  $y$  et  $z$ . Pour ce faire on peut imaginer une rangée de quatre cases dans laquelle on va placer deux taquets. Le nombre de cases vides avant le premier taquet (resp. entre les deux taquets, après le second

taquet) correspond à la puissance associée à  $x$  (resp.  $y, z$ ). L'espace des équations homogènes de degré 2 dans  $\mathbb{C}[x, y, z]$  est donc de dimension  $\binom{4}{2} = 6$ . L'espace des coniques passant par  $P_1, \dots, P_5$  est l'espace d'annulation de cinq formes linéaires (la forme linéaire associée à  $P_i$  étant l'évaluation en  $P_i$ ), donc de dimension  $\geq 1$ .

Par l'absurde, on suppose qu'il existe deux équations linéairement indépendantes définissant deux coniques  $\Gamma_1$  et  $\Gamma_2$  passant par  $P_1, \dots, P_5$ . Par la proposition 3.7, ces coniques possèdent une droite commune  $\mathcal{L}$ . Comme  $\Gamma_1, \Gamma_2$  ne sont pas confondues, elles possèdent chacune une autre droite, notée  $\mathcal{L}_1$  pour  $\Gamma_1$  et  $\mathcal{L}_2$  pour  $\Gamma_2$ . Les droites  $\mathcal{L}_1$  et  $\mathcal{L}_2$  ne sont pas confondues, donc elles possèdent un seul point d'intersection. Les autres points de ces droites ne peuvent pas être dans  $\{P_1, \dots, P_5\}$ . Il y a donc au maximum un de ces points en dehors de  $\mathcal{L}$ , donc au minimum quatre sur cette droite, ce qui est absurde. Il existe bien une unique conique passant par  $P_1, \dots, P_5$ .  $\square$

**Lemme 3.4** — *Soient  $P_1, \dots, P_8$  huit points distincts de  $\mathbb{CP}^2$  tels que quatre d'entre eux ne sont jamais alignés et que sept d'entre eux n'appartiennent jamais à une même conique. Alors l'espace  $V$  des polynômes de  $S^3$  s'annulant en  $P_1, \dots, P_8$  est de dimension 2.*

*Démonstration.* De même que précédemment, l'espace  $S^3$  est de dimension  $\binom{5}{2} = 10$ , donc l'espace des cubiques passant par  $P_1, \dots, P_8$  est de dimension  $\geq 2$ .

Montrons le résultat dans le cas où  $P_1, P_2, P_3$  sont alignés. On fixe un point  $P_9 \in (P_1P_2)$  distinct de  $P_1, P_2, P_3$ . La dimension de l'espace des cubiques passant par  $P_1, \dots, P_9$  est supérieure ou égale à  $\dim(V) - 1$ . Une cubique passant par ces neuf points contient forcément la droite  $(P_1P_2)$  d'après la proposition 3.6. Elle contient donc également une conique passant par  $P_4, \dots, P_8$ . Une telle conique est unique d'après le lemme précédent, donc la cubique passant par  $P_1, \dots, P_9$  l'est également. On en déduit  $\dim(V) \leq 1 + 1 = 2$ . Ce résultat reste valable pour tout autre triplet de points alignés.

On ne suppose plus  $P_1, P_2, P_3$  alignés mais  $P_1, \dots, P_6$  sur une même conique  $\Gamma$ . Les points  $P_7$  et  $P_8$  n'appartiennent pas à  $\Gamma$  par hypothèse. Soit  $P_9$  un point de  $\Gamma$  distinct de  $P_1, \dots, P_6$ . D'après la proposition 3.7, toute cubique passant par  $P_1, \dots, P_9$  contient la conique  $\Gamma$ . Les points  $P_7$  et  $P_8$  étant distincts, une telle cubique contient donc la droite formée par ces points et est donc la seule telle cubique. De même que précédemment, comme la dimension des cubiques passant par  $P_1, \dots, P_9$  est supérieure ou égale à  $\dim(V) - 1$ , on a  $\dim(V) \leq 1 + 1 = 2$ .

Enfin, si trois points ne sont jamais alignés et six points jamais sur une même conique, on suppose par l'absurde que  $\dim(V) > 2$ . Soient  $P_9, P_{10}$  deux points distincts de  $(P_1P_2)$ , distincts de  $P_1$  et  $P_2$ . Comme  $\dim(V) > 2$ , il existe une cubique passant par  $P_1, \dots, P_{10}$ . Elle contient la droite  $(P_1P_2)$  par la proposition 3.6, et donc également une conique. Comme les points  $P_3, \dots, P_8$  ne sont pas sur  $(P_1P_2)$ , ils sont tous sur cette conique, c'est absurde. Donc

$\dim(V) = 2$ .

□

Ces lemmes nous permettent de démontrer le théorème des neuf points.

**Théorème 3.2.** (Théorème des neuf points)

*Soient  $\mathcal{C}_1, \mathcal{C}_2$  deux cubiques s'intersectant en exactement neuf points distincts. On suppose  $\mathcal{C}_1$  irréductible. Toute cubique passant par huit de ces points passe également par le neuvième.*

*Démonstration.* Si la cubique  $\mathcal{C}_1$  contenait quatre points alignés (resp. sept points sur une même conique), elle contiendrait la droite passant par ces points par la proposition 3.6 (resp. la conique passant par ces points par la proposition 3.7), et ne serait pas irréductible. Soient  $P_1, \dots, P_8$  huit des neuf points d'intersection de  $\mathcal{C}_1$  et  $\mathcal{C}_2$ . D'après ce qui précède,  $P_1, \dots, P_8$  vérifient les hypothèses du lemme 3.4, donc la dimension de l'espace des cubiques passant par ces points est 2. Ainsi, toute cubique passant par  $P_1, \dots, P_8$  est combinaison linéaire de  $\mathcal{C}_1$  et  $\mathcal{C}_2$ , donc passe par le neuvième point d'intersection. □

### 3.5 Courbes elliptiques

**Définition 3.6** — Une *courbe elliptique* est une courbe projective lisse irréductible et de degré 3.

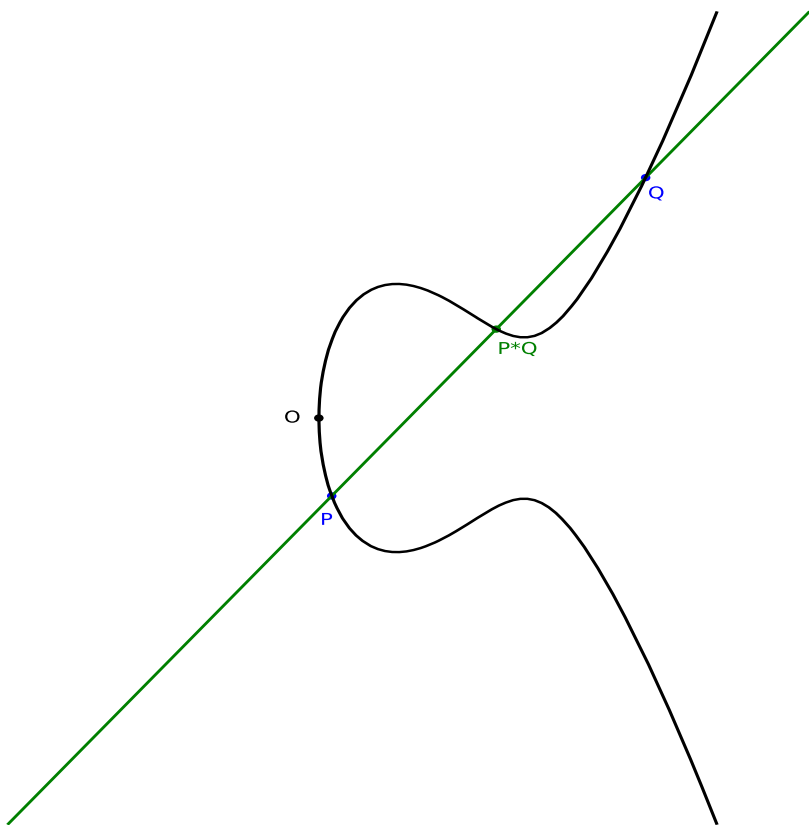
L'étude de ces courbes est très riche et a des applications notamment en théorie des nombres (dans la démonstration du théorème de Fermat-Wiles par exemple) grâce à leur structure particulière qui permet de définir une loi de groupe.

Soit  $\mathcal{C}$  une courbe elliptique et  $O$  un point de cette courbe. D'après la proposition 3.6, comme  $\mathcal{C}$  est de degré 3, elle intersecte toute droite en 3 points (comptés avec multiplicité). Ainsi, pour  $P, Q \in \mathcal{C}$ , on peut définir  $P \star Q$  le troisième point de  $\mathcal{C}$  appartenant à la droite  $(PQ)$  (ou la tangente à  $\mathcal{C}$  en  $P$  si  $P = Q$ ). Si  $P \neq Q$  et  $P$  (resp.  $Q$ ) est point de contact de multiplicité  $\geq 2$  avec la droite on a donc  $P \star Q = P$  (resp.  $P \star Q = Q$ ). On a évidemment  $P \star Q = Q \star P$

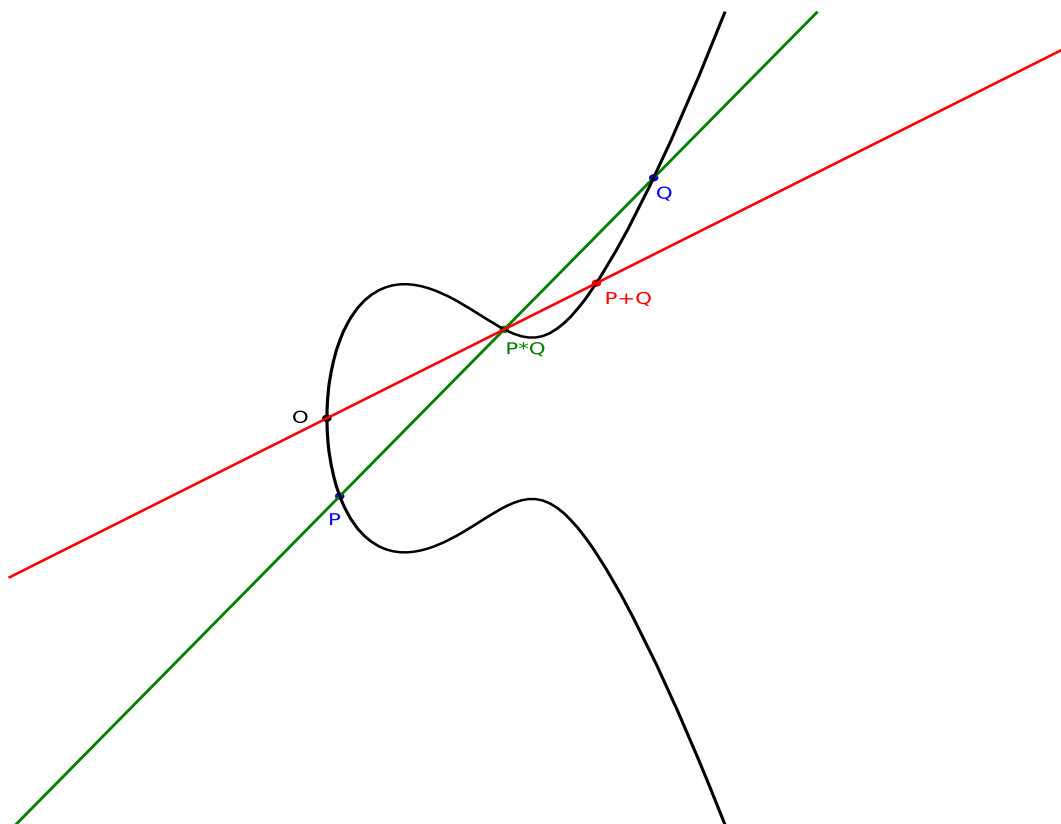
On définit une loi de groupe abélien  $\oplus$  sur  $\mathcal{C}$  de la manière suivante :

- pour  $P, Q \in \mathcal{C}$ , on note  $P \oplus Q := O \star (P \star Q)$  ;
- on pose  $R_O := O \star O$  et pour  $P \in \mathcal{C}$ ,  $\ominus P := P \star R_O$ .

Les figures suivantes illustrent la construction des deux points  $P \star Q$  et  $P \oplus Q$  pour une courbe elliptique et un élément neutre donnés.



construction de  $P * Q$



construction de  $P \oplus Q$

**Remarque :** Pour  $P, Q \in \mathcal{C}$ , on a  $P \oplus Q \oplus (P \star Q) = R_O$ .

La loi  $\oplus$  est commutative par commutativité de  $\star$ .

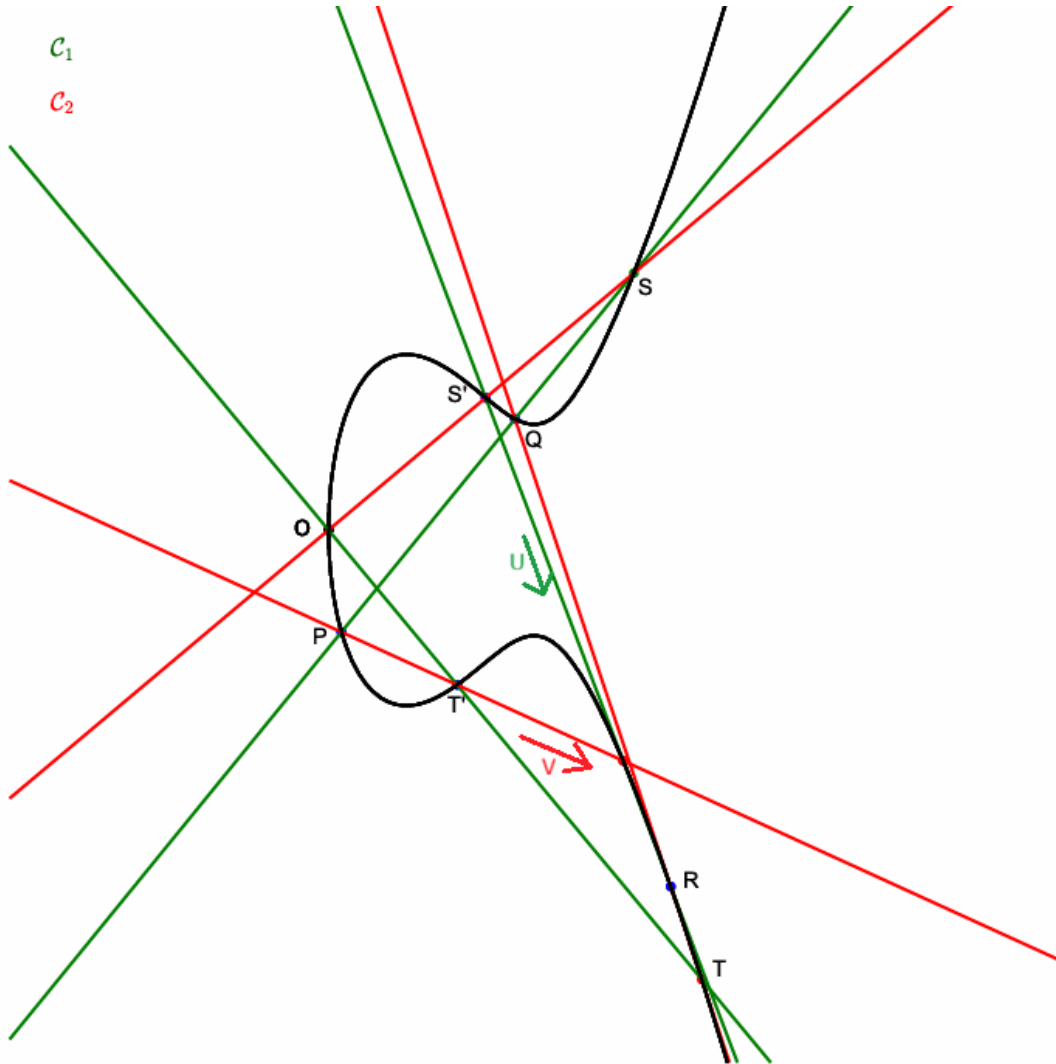
Pour  $P \in \mathcal{C}$ ,  $P \oplus O = O \star (P \star O) = P$ . Ainsi,  $O$  est neutre pour  $\oplus$ .

Pour  $P \in \mathcal{C}$ ,  $P \oplus (\ominus P) = P \oplus (P \star R_O) = O \star (P \star (P \star R_O)) = O \star R_O = O$ . Ainsi,  $\ominus P$  est inverse de  $P$  pour  $\oplus$ .

L'associativité est un peu plus délicate à démontrer. On peut le faire à l'aide du calcul formel en retranscrivant les relations via les coordonnées homogènes des points, mais nous allons ici la démontrer à l'aide du théorème des neuf points.

**Proposition 3.8** — *La loi  $\oplus$  est associative.*

*Démonstration.* Soient  $P, Q, R \in \mathcal{C}$ . On pose  $S := P \star Q$ ,  $S' := P \oplus Q$ ,  $U := R \star S'$ ,  $T := Q \star R$ ,  $T' := P \oplus Q$  et  $V := P \star T'$ . On a  $U = (P \oplus Q) \star R$  et  $V = P \star (Q \oplus R)$  donc montrer que  $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$  revient à montrer que  $U = V$ .



Les points  $P, Q, R, S, S', T, T', U$  et  $V$  et les cubiques  $\mathcal{C}_1$  et  $\mathcal{C}_2$ .

On commence par supposer  $O, P, Q, R, S, S', T, T', U$  deux à deux distincts. On pose  $\mathcal{C}_1 := (PQ) \cup (RS') \cup (OT)$  et  $\mathcal{C}_2 := (QR) \cup (PT') \cup (OS)$ . On a ainsi par le théorème de Bézout « courbe/droite »,  $\mathcal{C}_1 \cap \mathcal{C} = \{O, P, Q, R, S, S', T, T', U\}$  et  $\mathcal{C}_2 \cap \mathcal{C} = \{O, P, Q, R, S, S', T, T', V\}$ . Par le théorème des neuf points, comme  $\mathcal{C}_2$  intersecte  $\mathcal{C}$  en les huit premiers points de  $\mathcal{C}_1 \cap \mathcal{C}$  qui sont deux à deux distincts, elle passe également par le neuvième, qui est  $U$ . Ainsi,  $U \in \mathcal{C}_2 \cap \mathcal{C}$ , donc  $U = V$ .

Supposons maintenant uniquement  $Q, R, T, T', O$  deux à deux distincts. Considérons  $\mathcal{O}$  l'ensemble des points  $P$  de  $\mathcal{C}$  tels que  $P, Q, R, P \star Q, P \oplus Q, Q \star R, Q \oplus R, (P \oplus Q) \star R, O$  sont deux à deux distincts. Pour  $P \in \mathcal{C}$  différent de  $Q$ ,  $P \star Q = -g(1, 0)Q + g(0, 1)P$ , avec  $g(u, v) = \frac{f(uP+vQ)}{uv} \in \mathbb{C}[u, v]$  (cf annexe, addition sur une courbe elliptique). Ainsi,  $P \star Q$  est polynomial en  $P$ . De même pour  $P \oplus Q$  et  $(P \oplus Q) \star R$ . Ainsi, l'égalité de  $P$  et d'un de ces éléments résulte de l'annulation de polynômes sur  $\mathcal{C}$  (de même que l'égalité de  $P$  et  $Q, R, Q \star R, Q \oplus R, O$ ), donc  $\{P \in \mathcal{C} \mid P \in \{Q, R, P \star Q, P \oplus Q, Q \star R, Q \oplus R, (P \oplus Q) \star R, O\}\}$  est un fermé de  $\mathcal{C}$ . De même,  $P \oplus Q$  et  $(P \oplus Q) \star R$  sont polynomiaux en  $P \star Q$  et  $(P \oplus Q) \star R$  est polynomial en  $P \oplus Q$ , donc les ensembles associés sont fermés, puis par union finie on en déduit que  $\mathcal{C} \setminus \mathcal{O}$  est fermé, donc que  $\mathcal{O}$  est ouvert. On remarque que pour chaque fermé décrit précédemment on peut sans trop de difficultés trouver un élément de  $\mathcal{C}$  n'appartenant pas à ce fermé, donc comme les fermés strict de  $\mathcal{C}$  sont ses parties finies et que cet ensemble est infini, leur union n'est pas pleine. Ainsi,  $\mathcal{O}$  est non vide, donc dense. Les applications  $P \mapsto (P \oplus Q) \oplus R$  et  $P \mapsto P \oplus (Q \oplus R)$  sont continues (car des bijections, de réciproques  $P \mapsto (P \ominus R) \ominus Q$  et  $P \mapsto P \ominus (Q \oplus R)$ ) et coïncident sur  $\mathcal{O}$  d'après ce qui précède, donc elles sont égales sur tout  $\mathcal{C}$ .

Si  $R \neq O$ , de même que précédemment l'ensemble  $\{Q \in \mathcal{C} \mid Q \notin \{R, R, Q \star R, Q \oplus R, O\}\}$  est un ouvert dense donc on a l'égalité pour tous  $P, Q$  par continuité, donc si un des trois points n'est pas  $O$  on peut conclure de la même manière, et enfin si  $P = Q = R = O$  on a  $(P \oplus Q) \oplus R = O = P \oplus (Q \oplus R)$ .  $\square$

La loi  $\oplus$  est donc bien une loi de groupe, qui va nous permettre de caractériser les points d'inflexion de  $\mathcal{C}$ . Par la proposition 3.5 et le théorème de Bézout, on sait qu'il y en a  $3 \cdot 3 = 9$ .

**Définition 3.7** — On appelle **point de 3-torsion** (pour la loi  $\oplus$ ) tout point  $P \in \mathcal{C}$  tel que  $P \oplus P \oplus P = O$ .

**Proposition 3.9** — On suppose que  $O$  est point d'inflexion. Alors les points d'inflexions de la courbe  $\mathcal{C}$  sont exactement les points de 3-torsion. On note  $\mathcal{C}[3]$  leur ensemble

*Démonstration.* Le point  $O$  est point d'inflexion si et seulement si  $R_O = O$  par définition de  $R_O$ . On suppose que cette condition est vérifiée dans la suite.

Pour  $P$  un point d'inflexion de  $\mathcal{C}$ , on a  $(P \star P) = P$ , donc on a  $P \oplus P \oplus P = R_O = O$ . Réciproquement, si  $P$  est un point de 3-torsion, on a  $P \oplus P = \ominus P = P \star O$ , ie  $O \star (P \star P) = P \star O$ , donc  $P \star P = P$ , donc  $P$  est point d'inflexion.  $\square$

L'ensemble  $(\mathcal{C}[3], \oplus)$  est un sous-groupe de  $(\mathcal{C}, \oplus)$  (en tant que noyau du morphisme qui à un élément  $P$  renvoie  $P \oplus P \oplus P$ ), qui est abélien et fini, d'ordre 9. D'après le théorème de Kronecker, il est donc isomorphe à  $(\mathbb{Z}/3\mathbb{Z})^2$  ou à  $\mathbb{Z}/9\mathbb{Z}$ . Comme il ne possède pas d'élément d'ordre 9, il est isomorphe à  $(\mathbb{Z}/3\mathbb{Z})^2$  (on utilisera à présent la notation  $\mathbb{F}_3^2$  pour désigner ce groupe).

Si une droite projective passe par deux points de 3-torsion  $P$  et  $Q$ , elle passe par le point  $P \star Q = O \star (P \oplus Q) = \ominus(P \oplus Q) \in \mathcal{C}[3]$ . Ainsi, toute droite passant par deux points de  $\mathcal{C}[3]$  en passe par un troisième. On note  $\mathcal{D}$  l'ensemble des droites projectives passant par trois points de  $\mathcal{C}[3]$ . D'après ce qui précède, pour construire une telle droite il suffit de sélectionner deux éléments de  $\mathcal{C}[3]$  distincts : il y a 72 façons de le faire mais ainsi, on répète chaque droite 6 fois. Il y a donc 12 droites différentes dans  $\mathcal{D}$ . Chaque droite passant par 3 points, et chaque point traversé par 4 droites de  $\mathcal{D}$ , car une droite peut être caractérisée par 2 de ses points). On retrouve ainsi la configuration hessienne  $9_4 12_3$ .

## 4 Pinceau hessien et ses symétries

Dans tout la suite, on note  $\zeta = \exp(2i\pi/3)$ .

### 4.1 Pinceau hessien

La recherche de points d'inflexion d'une courbe elliptique revient à la recherche de ses points d'intersection avec sa hessienne, donc de toute combinaison linéaire non nulle de ces deux courbes. Nous allons étudier ces points dans un cas particulier.

**Définition 4.1** — *Un **pinceau de courbes projectives** est un ensemble de courbes de la forme  $af + bg = 0$ , où  $f, g$  sont des polynômes homogènes.*

On définit le pinceau hessien comme le pinceau engendré par  $x^3 + y^3 + z^3$  et  $xyz$ , c'est-à-dire l'ensemble des courbes projectives de la forme  $f_{a,b} = 0$ , avec  $f_{a,b}(x, y, z) = a(x^3 + y^3 + z^3) + bxyz$ , où  $[a : b] \in \mathbb{C}P^1$ .

On remarque que le pinceau hessien est l'ensemble des courbes d'équation  $af_{1,0} + bH_{f_{1,0}} = 0$ . De plus, un rapide calcul nous donne que la hessienne de toute courbe d'équation  $f_{a,b} = 0$  définit également une courbe du pinceau, d'équation  $f_{-6ab^2, 216a^3+2b^3} = 0$ .

**Proposition 4.1** — Soit  $[a : b] \in \mathbb{CP}^1$ . Le polynôme  $f_{a,b}$  ne possède pas de facteur carré.

*Démonstration.* Si  $a = 0$ , le résultat est évident. Supposons donc  $a \neq 0$ . Par l'absurde, on suppose qu'il existe  $g, h \in \mathbb{C}[x, y, z]$  avec  $g$  non constant tels que  $f_{a,b} = g^2 h$ . Les polynômes  $g$  et  $h$  sont de degré 1 et on a  $3ax^2 + byz = \frac{\partial f_{a,b}}{\partial x} = g \left( \frac{\partial g}{\partial x} h + g \frac{\partial h}{\partial x} \right)$ . Donc  $\frac{\partial g}{\partial x} h + g \frac{\partial h}{\partial x}$  possède un terme en  $x$ . De même en dérivant selon la seconde coordonnée,  $g$  possède un coefficient en  $y$ , donc par produit  $3ax^2 + byz$  possède un terme en  $xy$ . C'est absurde. Ainsi,  $f_{a,b}$  ne possède pas de facteur carré.  $\square$

Ainsi, en vertu du théorème de Bézout, toute courbe lisse du pinceau hessien est irréductible, donc est une courbe elliptique. On cherche donc à savoir quelles courbes du pinceau sont lisses.

Pour  $[a : b] \in \mathbb{CP}^1$ , on notera  $f_\lambda := f_{a,b}$ , avec  $\lambda := \frac{b}{a} \in \hat{\mathbb{C}}$ . On appelle fibre du pinceau une courbe de la forme  $f_\lambda = 0$ , pour  $\lambda \in \hat{\mathbb{C}}$ . Une fibre est dite singulière si elle possède un ou des points singuliers.

**Proposition 4.2** — La courbe  $\mathcal{E}_\lambda$  est singulière si et seulement si le paramètre  $\lambda$  est l'une des quatre valeurs  $\{-3, -3\zeta, -3\zeta^2, \infty\}$ . Les équations de chaque courbe singulière sont données par la table suivante :

$$\begin{aligned} \mathcal{E}_\infty & : & xyz &= 0 ; \\ \mathcal{E}_{-3} & : & (x + y + z)(x + \zeta y + \zeta^2 z)(x + \zeta^2 y + \zeta z) &= 0 ; \\ \mathcal{E}_{-3\zeta} & : & (x + y + \zeta z)(x + \zeta y + z)(x + \zeta^2 y + \zeta^2 z) &= 0 ; \\ \mathcal{E}_{-3\zeta^2} & : & (x + y + \zeta^2 z)(x + \zeta y + \zeta z)(x + \zeta^2 y + z) &= 0. \end{aligned}$$

Les points singuliers de chacune d'entre elles sont donnés par la table suivante :

$$\begin{aligned} \mathcal{E}_\infty & : & [1 : 0 : 0], & [0 : 1 : 0], & [0 : 0 : 1] ; \\ \mathcal{E}_{-3} & : & [1 : 1 : 1], & [1 : \zeta : \zeta^2], & [1 : \zeta^2 : \zeta] ; \\ \mathcal{E}_{-3\zeta} & : & [1 : 1 : \zeta^2], & [1 : \zeta : \zeta], & [1 : \zeta^2 : 1] ; \\ \mathcal{E}_{-3\zeta^2} & : & [1 : 1 : \zeta], & [1 : \zeta : 1], & [1 : \zeta^2 : \zeta^2]. \end{aligned}$$

*Démonstration.*  $\Leftarrow$  On a  $\mathcal{E}_{-3}$  d'équation  $(x + y + z)(x + \zeta y + \zeta^2 z)(x + \zeta^2 y + \zeta z) = 0$ , dont un point singulier est  $[1 : \zeta : \zeta^2]$ .

L'équation de  $\mathcal{E}_{-3\zeta}$  est  $(x + y + \zeta z)(x + \zeta y + z)(x + \zeta^2 y + \zeta^2 z) = 0$ , dont un point singulier est  $[1 : \zeta : \zeta]$ .

L'équation de  $\mathcal{E}_{-3\zeta^2}$  est  $(x + y + \zeta^2 z)(x + \zeta y + \zeta z)(x + \zeta^2 y + z) = 0$ , dont un point singulier est  $[1 : \zeta^2 : \zeta^2]$ .

L'équation de  $\mathcal{E}_\infty$  est  $xyz = 0$ , dont un point singulier est  $[1 : 0 : 0]$ .

$\Rightarrow$  On sait que  $\mathcal{E}_\infty$  est singulière. Soit  $\lambda \in \mathbb{C}$ . On suppose que  $\mathcal{E}_\lambda$  est singulière et on s'en donne  $[x_0, y_0, z_0]$  un point singulier. On a

$$3x_0^2 + \lambda y_0 z_0 = 0 \quad (1)$$

$$3y_0^2 + \lambda x_0 z_0 = 0 \quad (2)$$

$$3z_0^2 + \lambda x_0 y_0 = 0. \quad (3)$$

En faisant  $x_0 \cdot (1)$ ,  $y_0 \cdot (2)$  et  $z_0 \cdot (3)$ , on obtient  $x_0^3 = y_0^3 = z_0^3 = -\frac{\lambda}{3}x_0 y_0 z_0$ . En particulier,  $x_0, y_0, z_0$  sont non nuls. On a  $y_0 = \zeta_1 x_0$ ,  $z_0 = \zeta_2 x_0$ , avec  $\zeta_1, \zeta_2 \in \mathbb{U}_3$ . Donc  $x_0^3 = -\frac{\lambda}{3}\zeta_3 x_0^3$ , avec  $\zeta_3 = \zeta_1 \zeta_2 \in \mathbb{U}_3$ . Ainsi,  $\lambda = -3\zeta_3^{-1} \in -3\mathbb{U}_3$ .

Chaque courbe singulière possède au maximum 3 points singuliers (car ces courbes se factorisent en union de 3 droites).  $[1 : 0 : 0]$ ,  $[0 : 1 : 0]$  et  $[0 : 0 : 1]$  sont des points singuliers de  $\mathcal{E}_\infty$ , donc sont ses point singuliers. De même, on peut trouver 3 points singuliers pour  $\mathcal{E}_{-3}$ ,  $[1 : 1 : 1]$ ,  $[1 : \zeta : \zeta^2]$  et  $[1 : \zeta^2 : \zeta]$  sont les points singuliers. En remarquant que  $f_{-3\zeta}(x, y, z) = f_{-3}(x, y, \zeta z)$  et que  $f_{-3\zeta^2}(x, y, z) = f_{-3}(x, y, \zeta^2 z)$ , on obtient tous les points annoncés par la proposition.  $\square$

On va maintenant s'atteler à la recherche des points d'inflexion des courbes lisses. La proposition suivante implique que l'on en cherche neuf à chaque fois.

**Proposition 4.3** — *Soit  $(a, b) \in \mathbb{C}^2 \setminus \{(0, 0)\}$ . La hessienne de  $f_{a,b}$  est proportionnelle à celle-ci si et seulement si  $\mathcal{E}_{b/a}$  est singulière.*

*Démonstration.* On a vu que la hessienne de  $f_{a,b}$  était  $f_{-6ab^2, 216a^3+2b^3}$ . Si  $a = 0$ ,  $\mathcal{E}_{b/a}$  est singulière et de plus  $H_{f_{0,b}} = f_{0,2b^3}$  qui est proportionnelle à  $f_{0,b}$ . On suppose maintenant  $a$  non nul. Alors  $H_{f_{a,b}}$  est proportionnelle à  $f_{a,b}$  si et seulement s'il existe  $\mu \in \mathbb{C}^*$  tel que  $-6ab^2 = \mu a$  et  $216a^3 + 2b^2 = \mu b$ . Comme  $a$  est non nul, la première inégalité donne  $\mu = -6b^2$ , et en remplaçant dans la seconde on trouve  $-8b^3 = 216a^3$ , i.e.  $\left(\frac{b}{a}\right) = 27$ . Ainsi,  $f_{a,b}$  est proportionnelle à sa hessienne si et seulement si  $\frac{b}{a} \in 3\mathbb{U}_3$ . La proposition 4.2 nous permet de conclure.  $\square$

Déterminons les points d'inflexions des courbes lisses. Ceux de  $\mathcal{E}_0$  sont les points de  $\mathcal{E}_0 \cap \mathcal{E}_\infty$  qui se trouvent facilement : on choisit la coordonnée nulle, on en fixe une autre à 1 et on en déduit la troisième. On trouve ainsi les points  $(P_{j,k})_{0 \leq j,k \leq 3}$  définis ainsi : pour  $0 \leq k \leq 3$ ,

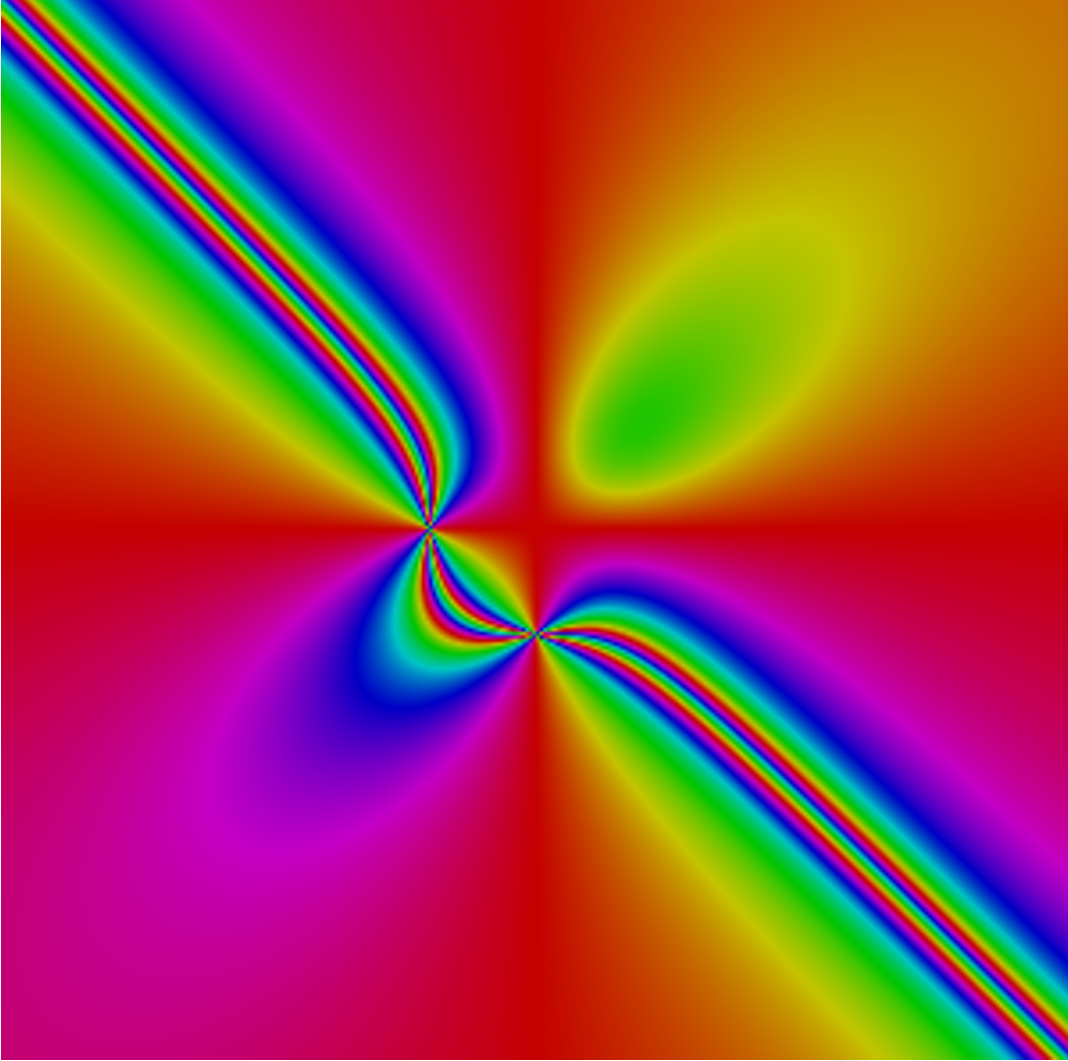
$$P_{0,k} = [0 : 1 : -\zeta^k]$$

$$P_{1,k} = [1 : 0 : -\zeta^k]$$

$$P_{2,k} = [1 : -\zeta^k : 0] .$$

**Proposition 4.4** — *Les  $P_{j,k}$  sont les points d'inflexion de toutes les courbes lisses du pinceau.*

*Démonstration.* D'après la définition du pinceau, la hessienne de toute courbe lisse de ce dernier est encore une courbe du pinceau, donc toute courbe lisse intersecte sa hessienne en ces neuf points exactement.  $\square$

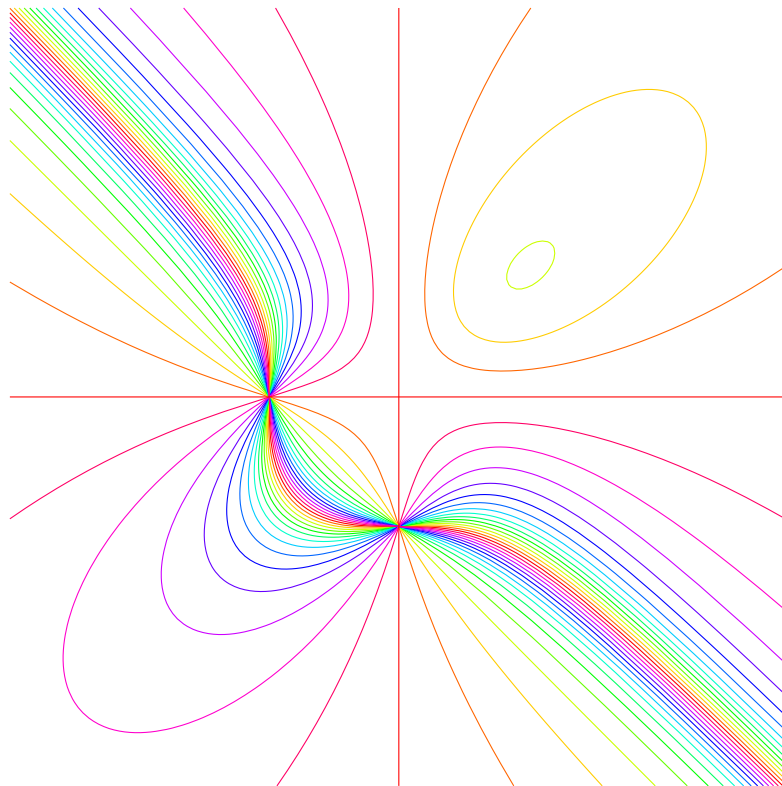


Les courbes du pinceau (de différentes couleurs) s'intersectant en deux points d'inflexion.

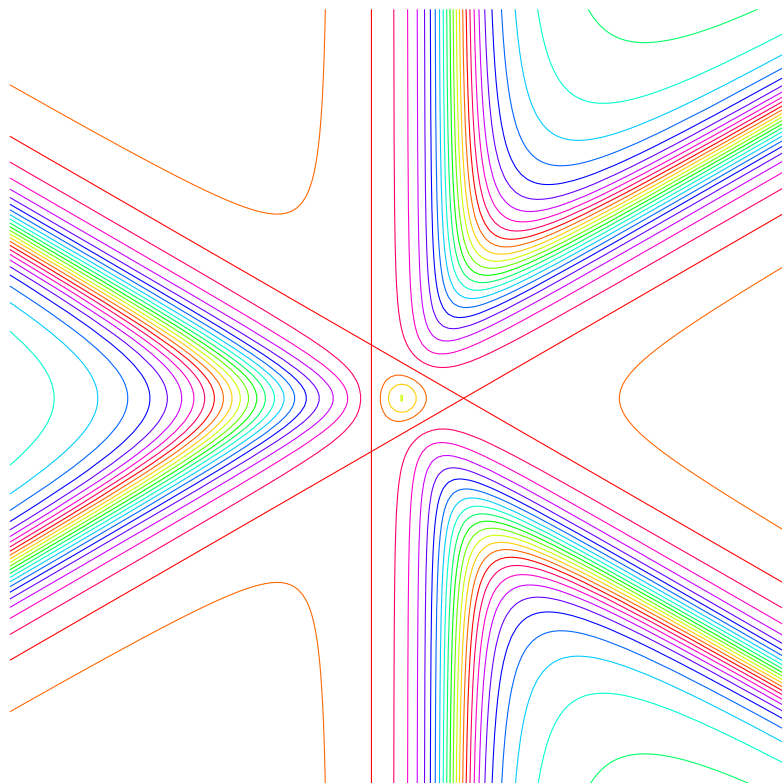
**Remarque :** D'après le théorème des neuf points, les courbes du pinceau hessien sont les seules cubiques à passer par les  $P_{j,k}$ . On peut ainsi définir le pinceau hessien comme l'ensemble des cubiques dont les points d'inflexion sont les  $P_{j,k}$ .

En prenant  $P_{0,0}$  comme neutre, un calcul montre que l'addition sur le lieu de base (sur n'importe quelle courbe elliptique du pinceau) est compatible avec l'addition dans  $\mathbb{F}_3^2$  : pour  $(j, k), (j', k') \in \mathbb{F}_3^2$ ,  $P_{j,k} \oplus P_{j',k'} = P_{j+j',k+k'}$  (voir la page 2 de l'annexe).

La figure suivante correspond à quelques courbes du pinceau hessien, représentées dans le plan  $z = 0$ .



La seconde figure ci-dessous représente les mêmes courbes mais selon des coordonnées différentes.



Ce changement de coordonnées amène à supposer qu'il existe certaines transformations de  $\mathbb{CP}^2$  stabilisant le pinceau. L'étude de telles transformations fait l'objet de la partie suivante.

## 4.2 Stabilisateur projectif du pinceau

Nous allons ici étudier les transformations projectives qui stabilisent le pinceau. On appelle groupe hessien et on note  $\mathbb{H}$  le groupe de ces transformations, c'est-à-dire le plus grand sous-groupe de  $\mathrm{PGL}_3(\mathbb{C})$  tel que pour tout  $\phi \in \mathbb{H}$ , tout  $\lambda \in \hat{\mathbb{C}}$ , il existe  $\mu \in \hat{\mathbb{C}}$  tel que  $\mathcal{V}(f_\mu) = \mathcal{V}(f_\lambda \circ \phi)$ . On peut voir  $\mathbb{H}$  comme le stabilisateur du sous-espace vectoriel engendré par  $x^3 + y^3 + z^3$  et  $xyz$ .

Comme un point de  $\mathcal{E}_0[3]$  appartient à toutes les courbes du pinceau, son image par tout élément de  $\mathbb{H}$  sera aussi un point commun à toutes les courbes du pinceau, donc encore un point de  $\mathcal{E}_0[3]$ . Ainsi,  $\mathbb{H}$  stabilise le lieu de base du pinceau hessien. Ses éléments étant linéaires, ils stabilisent les droites projectives, donc les droites reliant les points d'inflexion. Ainsi,  $\mathbb{H}$  s'identifie à un sous-groupe de  $\mathrm{Aut}(9_4 12_3) \simeq \mathrm{GL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ .

**Proposition 4.5** — *Le groupe  $\mathbb{H}$  stabilise l'ensemble des courbes singulières du pinceau.*

*Démonstration.* Soit  $\phi \in \mathrm{PGL}_3(\mathbb{C})$  et  $\tilde{\phi} \in \mathrm{GL}_3(\mathbb{C})$  tel que  $\tilde{\phi} \cdot \mathbb{C}^* = \phi$ . Soit  $f \in \mathbb{C}[x, y, z]$  telle que la courbe  $\mathcal{C}$  associée dans  $\mathbb{CP}^2$  est singulière en un point  $P \in \mathbb{CP}^2$ , repéré par des coordonnées homogènes  $[x_0 : y_0 : z_0]$ . Montrons que  $\mathcal{C}' := \phi(\mathcal{C})$  est singulière.

La courbe  $\mathcal{C}'$  est définie par  $g(x, y, z) := f(\tilde{\phi}^{-1} \cdot (x, y, z)^\top)$ , et par règle de la chaîne, on obtient  $\nabla g(x, y, z) = (\tilde{\phi}^{-1})^\top \cdot \nabla f(\tilde{\phi}^{-1} \cdot (x, y, z)^\top)$ . En posant  $\tilde{Q} := \tilde{\phi} \cdot (x_0, y_0, z_0)^\top$ , on a  $\nabla g(\tilde{Q}) = (\tilde{\phi}^{-1})^\top \cdot \nabla f(x_0, y_0, z_0) = 0$ . Ainsi,  $\mathcal{C}'$  est singulière en  $\phi(P)$ . On a montré que tout élément de  $\mathrm{PGL}_3(\mathbb{C})$  envoyait une courbe singulière sur une autre courbe singulière. Comme  $\mathrm{PGL}_3(\mathbb{C})$  est un groupe (donc stable par passage à l'inverse), il stabilise l'ensemble des courbes singulières.

Ainsi, un élément de  $\mathbb{H}$  stabilise le pinceau et envoie une courbe singulière sur une autre, donc stabilise l'ensemble des courbes singulières du pinceau.  $\square$

Ainsi,  $\mathbb{H}$  agit sur  $\{\mathcal{E}_\infty, \mathcal{E}_{-3}, \mathcal{E}_{-3\zeta}, \mathcal{E}_{-3\zeta^2}\}$ . Nous pouvons donc scinder  $\mathbb{H}$  en  $\mathbb{H}_{\infty \rightarrow \infty}$ ,  $\mathbb{H}_{\infty \rightarrow -3}$ ,  $\mathbb{H}_{\infty \rightarrow -3\zeta}$  et  $\mathbb{H}_{\infty \rightarrow -3\zeta^2}$  en fonction de l'image de  $\mathcal{E}_\infty$  par un élément de  $\mathbb{H}$ , ces ensembles étant évidemment deux à deux disjoints. Nous commençons par caractériser le groupe  $\mathbb{H}_{\infty \rightarrow \infty}$ , en introduisant un autre groupe.

**Définition 4.2** — Soient  $m, p, n \in \mathbb{N}^*$ , tels que  $p$  divise  $m$ . On définit le **groupe de réflexions complexe monomial**  $G(m, n, p)$  comme le sous-groupe de  $\mathrm{GL}_n(\mathbb{C})$  composé des matrices monomiales dont les coefficients non nuls sont des racines  $m$ -ièmes de l'unité dont le produit est une racine  $m/p$ -ième de l'unité.

Nous nous intéresserons au groupe  $G(3, 1, 3)$ , composé des matrices monomiales  $3 \times 3$  dont les coefficients non nuls sont des racines troisièmes de l'unité. On peut voir  $G(3, 1, 3)$  comme le produit semi-direct de  $\mathfrak{S}_3$  et  $(\mathbb{U}_3)^3$ , où on associe à  $(\sigma, (\zeta^{k_1}, \zeta^{k_2}, \zeta^{k_3})) \in \mathfrak{S}_3 \times (\mathbb{U}_3)^3$  la matrice monomiale associée à  $\sigma$  dont le coefficient non nul de la  $j$ -ième colonne est  $\zeta^{k_j}$  pour  $1 \leq j \leq 3$ . Pour que les opérations entre les deux groupes soient compatibles, le morphisme du produit semi-direct est  $\alpha : \mathfrak{S}_3 \longrightarrow \mathrm{Aut}((\mathbb{U}_3)^3)$ ,  $\sigma \longmapsto ((\omega_1, \omega_2, \omega_3) \mapsto (\omega_{\sigma(1)}, \omega_{\sigma(2)}, \omega_{\sigma(3)}))$ .

**Proposition 4.6** — Le groupe  $\mathbb{H}_{\infty \rightarrow \infty}$  s'identifie à  $(G(3, 1, 3) \cdot \mathbb{C}^*)/\mathbb{C}^*$ .

*Démonstration.* Soit  $\phi \in \mathbb{H}_{\infty \rightarrow \infty}$ . On choisit  $\tilde{\phi}$  tel que précédemment. On a pour  $(x, y, z) \in \mathbb{C}^3$ ,  $\tilde{\phi}(x, y, z) = (ax + by + cz, dx + ey + fz, gx + hy + iz)$ , avec  $a, b, c, d, e, f, g, h, i \in \mathbb{C}$ . Comme  $\phi$  stabilise  $\mathcal{E}_\infty$ ,  $(ax + by + cz)(dx + ey + fz)(gx + hy + iz) = f_\infty(\tilde{\phi}(x, y, z)) = \alpha xyz$ , avec  $\alpha \in \mathbb{C}^*$ . En regardant les degrés en  $x, y, z$  de ces expressions, on en déduit que la matrice de  $\tilde{\phi}$  dans la base canonique est monomiale.

Ainsi,  $\phi$  fixe également  $\mathcal{E}_0$ . En évaluant  $\tilde{\phi}$  en  $(1, -1, 0)$ ,  $(0, 1, -1)$  et  $(-1, 0, 1)$ , on vérifie que  $\tilde{\phi} \in G(3, 1, 3) \cdot \mathbb{C}^*$ . Ainsi,  $\phi \in (G(3, 1, 3) \cdot \mathbb{C}^*)/\mathbb{C}^*$ .

Réciproquement, un élément de  $(G(3, 1, 3) \cdot \mathbb{C}^*)/\mathbb{C}^*$  fixe bien  $\mathcal{E}_\infty$  et fixe également  $\mathcal{E}_0$ , donc est également un élément de  $\mathbb{H}$ .

On a donc bien l'identification voulue.  $\square$

**Remarque :** Le passage au quotient après avoir multiplié par  $\mathbb{C}^*$  permet de regarder uniquement des matrices monomiales dont le coefficient sur la première colonne est 1, les deux autres coefficients non nuls restant des éléments de  $\mathbb{U}_3$  non fixés.

Il est ainsi aisé de dénombrer  $\mathbb{H}_{\infty \rightarrow \infty}$  à l'aide de cette identification. Pour construire un élément de  $(G(3, 1, 3) \cdot \mathbb{C}^*)/\mathbb{C}^*$ , on choisit un couple formé d'une permutation dans  $\mathfrak{S}_3$  (6 choix possibles) et d'un couple dans  $(\mathbb{U}_3)^2$  (9 choix possibles). Ce procédé de construction étant exhaustif et sans redondance,  $|(G(3, 1, 3) \cdot \mathbb{C}^*)/\mathbb{C}^*| = 6 \times 9 = 54$ .

On va montrer que les ensembles  $\mathbb{H}_{\infty \rightarrow -3}$ ,  $\mathbb{H}_{\infty \rightarrow -3\zeta}$  et  $\mathbb{H}_{\infty \rightarrow -3\zeta^2}$  sont du même cardinal. En se ramenant au cas précédent. On se concentre sur les éléments de  $\mathbb{H}$  permettant cela.

**Proposition 4.7** — L'action de  $\mathbb{H}$  sur l'ensemble des courbes singulières du pinceau est transitive.

*Démonstration.* On va d'abord exhiber un élément de  $\mathbb{H}$  permutant  $\mathcal{E}_\infty$  et  $\mathcal{E}_{-3}$ . Pour ce faire, on veut par exemple envoyer le vecteur  $(1, 0, 0)$  (représentant  $x$ ) sur  $(1, 1, 1)$  (représentant  $x + y + z$ ), le vecteur  $(0, 1, 0)$  sur  $(1, \zeta, \zeta^2)$  et  $(0, 0, 1)$  sur  $(1, \zeta^2, \zeta)$ . Il est donc naturel de poser

$$g_0 := \frac{1}{i\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix}, \text{ pour laquelle } g_0^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Une rapide étude des colonnes de  $g_0$  et  $g_0^2$  confirme que le représentant de  $g_0$  dans  $\mathrm{PGL}_3(\mathbb{C})$  permute bien les courbes voulues. En particulier, il stabilise le pinceau et est donc bien un élément de  $\mathbb{H}$ . De plus, le calcul donne que ce représentant envoie  $\mathcal{E}_0$  sur  $\mathcal{E}_6$ .

Ensuite, le représentant de  $\mathrm{diag}(1, 1, \zeta)$ , élément de  $(G(3, 1, 3) \cdot \mathbb{C}^*)/\mathbb{C}^*$ , stabilise  $\mathcal{E}_0$  et  $\mathcal{E}_\infty$  et permute  $\mathcal{E}_{-3}$ ,  $\mathcal{E}_{-3\zeta}$  et  $\mathcal{E}_{-3\zeta^2}$ . En composant ces deux éléments, on peut envoyer  $\mathcal{E}_\infty$  sur n'importe quelle courbe singulière du pinceau.  $\square$

Ainsi,  $\mathrm{diag}(1, 1, \zeta^k) \cdot g_0 \cdot \mathbb{H}_{\infty \rightarrow \infty} \subset \mathbb{H}_{\infty \rightarrow -3\zeta^k}$ , pour  $0 \leq k \leq 2$ . Comme  $g_0 \cdot \mathrm{diag}(1, 1, \zeta^{3-k}) \cdot \mathbb{H}_{\infty \rightarrow -3\zeta^k} \subset \mathbb{H}_{\infty \rightarrow \infty}$ , on trouve par double inégalité  $|\mathbb{H}_{\infty \rightarrow -3\zeta^k}| = |\mathbb{H}_{\infty \rightarrow \infty}| = 54$ .

**Corollaire 4.1** — *Le cardinal de  $\mathbb{H}$  est  $4 \times 54 = 216$ .*

Ainsi, le groupe hessien est isomorphe à un sous-groupe d'indice 2 de  $\mathrm{GL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ .

**Proposition 4.8** — *Le groupe  $\mathbb{H}$  est isomorphe à  $\mathrm{SL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ .*

On peut montrer ce résultat par calcul (voir la page 18 de l'annexe), mais nous en proposons une preuve utilisant l'unicité du déterminant en tant que morphisme non trivial de  $\mathrm{GL}_2(\mathbb{F}_3)$  dans  $\mathbb{F}_3^*$ .

*Démonstration.* Montrons qu'il existe un unique morphisme non trivial de  $\mathrm{GL}_2(\mathbb{F}_3)$  vers  $\mathbb{F}_3^*$ . Tout d'abord, les images des matrices de transvection sont fixées à 1, car ces matrices sont d'ordre 3. Il reste donc à fixer l'image de  $A := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  (car les matrices de transvection et  $A$  engendrent  $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  donc tout le groupe), qui n'est pas contrainte car la matrice est d'ordre 2. En choisissant 1 comme image on obtient l'identité et en choisissant -1 on obtient le déterminant.

D'après le résultat précédent,  $\mathrm{GL}_2(\mathbb{F}_3)$  admet un unique sous-groupe d'indice 2, qui est  $\mathrm{SL}_2(\mathbb{F}_3)$ . Comme  $\mathbb{F}_3^2$  est d'ordre impair,  $\mathrm{GL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$  admet un unique sous-groupe d'ordre 2. Par unicité,  $\mathbb{H}$  est isomorphe à  $\mathrm{SL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ .  $\square$

Ainsi,  $\mathbb{H}$  est le groupe affine spécial  $\mathrm{ASL}_2(\mathbb{F}_3)$  de la configuration hessienne.

### 4.3 Un stabilisateur linéaire du pinceau

Le pinceau hessien est une partie de  $\mathbb{C}P^2$ , mais on peut également le voir comme un ensemble algébrique de  $\mathbb{C}^3$ , et donc étudier les transformations linéaires de  $\mathbb{C}^3$  qui le stabilisent. Les éléments de  $G(3, 1, 3)$  et la matrice  $g_0$  sont de telles transformations car passer de  $\mathbb{C}P^2$  à  $\mathbb{C}^3$  rajoute de l'information uniquement « linéairement » au pinceau (on transforme les points en droites vectorielles). On peut donc étudier un relèvement de  $\mathbb{H}$  dans  $GL_3(\mathbb{C})$ .

**Définition 4.3** — *Le groupe  $G_{26}$  est le sous-groupe de  $GL_3(\mathbb{C})$  engendré par  $G(3, 1, 3)$  et  $g_0$ .*

Les coefficients de  $g_0$  et des éléments de  $G(3, 1, 3)$  appartenant au corps  $\mathbb{Q}(\zeta)$ ,  $G_{26}$  est donc un sous-groupe de  $GL_3(\mathbb{Q}(\zeta))$ . De plus, on a  $\det(g_0) = 1$ . Une transposition de  $G(3, 1, 3)$  est de déterminant -1, et une matrice diagonale de  $G(3, 1, 3)$  est de déterminant appartenant à  $\mathbb{U}_3$ . Ces matrices générant  $G_{26}$ , on en déduit que le déterminant de toute matrice de  $G_{26}$  appartient à  $\mathbb{U}_3 \cup (-\mathbb{U}_3) = \mathbb{U}_6$ .

Le groupe  $G_{26}$  est un relèvement de  $\mathbb{H}$  dans  $GL_3(\mathbb{C})$ , donc on dispose d'un morphisme naturel surjectif  $\Phi : G_{26} \longrightarrow \mathbb{H}$ ,  $h \longmapsto h\mathbb{C}^*$ .

**Proposition 4.9** —  $\ker \Phi = \mathbb{U}_6$  (où l'on identifie  $\mathbb{U}_6$  à  $\mathbb{U}_6 I_3$ ).

*Démonstration.* Le noyau de  $\Phi$  est constitué des matrices scalaires de  $G_{26}$ . Montrons que les scalaires associés sont exactement ceux de  $\mathbb{U}_6$ .

On a  $\mathbb{U}_3 \subset G(3, 1, 3) \subset G_{26}$  et  $-I_3 = g_0^2 \tau \in G_{26}$ , où  $\tau$  est la transposition échangeant les deuxième et troisième colonnes. Par produit,  $-\mathbb{U}_3 \subset G_{26}$ , puis  $\mathbb{U}_6 \subset G_{26}$ .

Réciproquement, on sait déjà qu'une matrice scalaire de  $G_{26}$  appartient à  $\mathbb{Q}(\zeta)$  et que son déterminant est dans  $\mathbb{U}_6$ , donc elle appartient également à  $\mathbb{U}_{18}$ . Le lemme suivant permet de conclure.

**Lemme 4.1** — *L'intersection  $\mathbb{Q}(\zeta) \cap \mathbb{U}_{18}$  est incluse dans  $\mathbb{U}_6$ .*

*Démonstration.* Montrons d'abord que  $\omega := e^{\frac{i\pi}{9}}$  n'appartient pas à  $\mathbb{Q}(\zeta)$ . Soient  $\alpha, \beta \in \mathbb{R}$  tels que  $\alpha\zeta + \beta = \omega$ . On a  $\alpha \frac{\sqrt{3}}{2} = \sin(\frac{\pi}{9})$ , donc  $\frac{\alpha}{2} = \frac{\sin(\frac{\pi}{9})}{\sqrt{3}}$ . Or  $\frac{1}{2} = \cos(\frac{\pi}{3}) = \cos(\frac{2\pi}{9})\cos(\frac{\pi}{9}) - \sin(\frac{2\pi}{9})\sin(\frac{\pi}{9}) = \sqrt{1 - \sin(\frac{\pi}{9})^2}(1 - 4\sin(\frac{\pi}{9})^2)$ . En posant  $X = \sin(\frac{\pi}{9})^2$  et en mettant l'équation au carré, on obtient  $4(1 - X)(1 - 4X)^2 - 1 = 0$ , i.e.  $X$  est racine de  $P = 64T^3 - 96T^2 + 36T - 3$ . Si  $P$  admettait une racine rationnelle sous la forme  $\frac{p}{q}$  avec  $p \in \mathbb{Z}$  et  $q \in \mathbb{N}^*$ , on aurait  $p \mid -3$  et  $q \mid 64$ . Un calcul permet de montrer que pour  $p \in \{1, 3, -1, -3\}$  et  $q \in \{1, 2, 4, 8, 16, 32, 64\}$ ,  $P(\frac{p}{q}) \neq 0$ . Ainsi,  $X \notin \mathbb{Q}$ . En particulier,  $X \notin 3\mathbb{Q}$ , donc  $\sin(\frac{\pi}{9}) \notin \sqrt{3}\mathbb{Q}$ . Il en découle que  $\frac{\alpha}{2} \notin \mathbb{Q}$ , donc  $\alpha \notin \mathbb{Q}$ . Ainsi,  $\omega \notin \mathbb{Q}(\zeta)$ . Pour  $k \in \{2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17\}$ ,  $k \wedge 9 = 1$ ,

donc  $\omega^k$  engendre  $\mathbb{U}_{18}$  et en particulier  $\omega$ . Si  $\omega^k$  était un élément de  $\mathbb{Q}(\zeta)$ , il en découlerait que  $\omega$  également. Donc  $\omega^k \notin \mathbb{Q}(\zeta)$ . L'intersection  $\mathbb{Q}(\zeta) \cap \mathbb{U}_{18}$  est donc incluse dans  $\{1, \omega^3, \omega^6, -1, \omega^{12}, \omega^{15}\} = \mathbb{U}_6$ .  $\square$

On a donc l'égalité voulue par double inclusion.  $\square$

Par le premier théorème d'isomorphisme,  $G_{26}/\mathbb{U}_6$  est donc isomorphe à  $\mathbb{H}$ . Ainsi,  $G_{26}$  est fini et  $|G_{26}| = 6|\mathbb{H}| = 1296$ .

## 5 Groupe de réflexions

### 5.1 Généralités

Dans cette partie on fixe  $V$  un  $\mathbb{C}$ -espace vectoriel de dimension finie  $n$ , et on note  $\mathcal{S}(V)$  son algèbre symétrique. Pour tout sous-espace vectoriel  $W$  de  $V$ , on note  $\text{codim}(W) := \dim(V/W)$  la codimension de  $W$  dans  $V$ .

Une réflexion complexe  $r$  de  $V$  est un élément de  $\text{GL}(V)$  d'ordre fini et tel que  $\text{codim}(\ker(r - \text{id})) = 1$ , c'est-à-dire dont l'ensemble des points fixes est un hyperplan (dans le cas de notre étude, on se concentrera sur les réflexions de  $\mathbb{C}^3$ , qui fixent un plan).

**Définition 5.1** — Soit  $G$  un sous-groupe fini de  $\text{GL}(V)$ . On note  $\text{Ref}(G)$  l'ensemble de ses réflexions. Si  $\text{Ref}(G)$  engendre  $G$ , on dit que  $G$  est un **groupe de réflexions (complexe)**.

Le théorème suivant donne une caractérisation algébrique des groupes de réflexions.

**Théorème 5.1.** (Théorème de Shephard-Todd/Chevalley-Serre)

Soit  $G$  un sous-groupe fini de  $\text{GL}(V)$ . Les assertions suivantes sont équivalentes :

- (i)  $G$  est un groupe de réflexions.
- (ii) L'algèbre  $\mathcal{S}(V)^G$  des invariants de  $\mathcal{S}(V)$  par  $G$  est engendrée par  $n$  polynômes homogènes algébriquement indépendants.

*Démonstration.* cf [2, Théorème 4.1]  $\square$

Dans la suite, on fixe  $G$  un groupe de réflexions de  $V$  et on note  $d_1, \dots, d_n$  les degrés des générateurs de l'algèbre  $\mathcal{S}(V)^G$ .

La formule de Solomon nous donne des informations sur  $G$  à l'aide des  $d_k$ .

**Théorème 5.2.** (Formule de Solomon)

On a l'égalité polynomiale

$$\sum_{g \in G} t^{\text{codim}(V^g)} = \prod_{k=1}^n (1 + t(d_k - 1)) .$$

*Démonstration.* cf [2, Prop 4.47]

□

**Corollaire 5.1** — On a les formules suivantes :

$$1) |G| = d_1 d_2 \dots d_n$$

$$2) |\text{Ref}(G)| = d_1 - 1 + d_2 - 1 + \dots + d_n - 1 .$$

*Démonstration.* En évaluant l'égalité de Solomon en 1, on trouve 1). En dérivant cette égalité et en évaluant en 0, on trouve 2). □

Nous allons montrer que  $G_{26}$  est un groupe de réflexions complexe et lier ses propriétés algébriques (invariants polynomiaux) à la géométrie du pinceau.

De nouveau, une grande majorité de résultats démontrés ci-dessous peuvent être montrés par calcul (voir les pages 17 à 22 de l'annexe).

## 5.2 Deux méthodes pour trouver les invariants

On note dans cette section  $\mathcal{S}$  l'algèbre symétrique de  $\mathbb{C}^3$ , que l'on identifiera à  $\mathbb{C}[x, y, z]$ .

Nous allons chercher les invariants par  $G_{26}$  de deux manières.

### 5.2.1 La méthode « par en-dessous »

**Proposition 5.1** — L'algèbre des invariants par  $G(3, 1, 3)$  est l'algèbre de polynômes  $\mathbb{C}[\tau_1, \tau_2, \tau_3]$ , où  $\tau_1 := x^3 + y^3 + z^3$ ,  $\tau_2 := x^3 y^3 + y^3 z^3 + z^3 x^3$ ,  $\tau_3 := x^3 y^3 z^3$ .

*Démonstration.* L'algèbre des invariants de  $\mathbb{C}[x, y, z]$  par  $(\mathbb{U}_3)^3$  est  $\mathbb{C}[x^3, y^3, z^3]$ . En effet, ce groupe agit linéairement sur les monômes, donc un polynôme invariant par ce groupe est un polynôme dont tous les monômes sont invariants. Un monôme  $x^k y^l z^m$  est invariant pour  $(\zeta, 1, 1)$  si et seulement si  $\zeta^k = 1$ , si et seulement si  $k$  est un multiple de 3. De même, ce monôme est invariant par  $(1, \zeta, 1)$  (resp.  $(1, 1, \zeta)$ ) si et seulement si  $l$  (resp.  $m$ ) est un multiple de 3. Comme ces trois triplets engendrent tout le groupe, les monômes invariants par  $(\mathbb{U}_3)^3$  sont exactement les monômes de la forme  $x^{3k} y^{3l} z^{3m}$ . Ainsi, l'algèbre des invariants par  $(\mathbb{U}_3)^3$  est bien  $\mathbb{C}[x^3, y^3, z^3]$ .

Déterminons maintenant  $\mathbb{C}[x^3, y^3, z^3]^{\mathfrak{S}_3}$ . En posant  $X := x^3$ ,  $Y := y^3$  et  $Z := z^3$ , cela revient à déterminer  $\mathbb{C}[X, Y, Z]^{\mathfrak{S}_3}$ , qui est par le théorème fondamental des fonctions symétriques l'algèbre  $\mathbb{C}[X + Y + Z, XY + YZ + ZX, XYZ]$ . Ainsi,  $\mathbb{C}[x^3, y^3, z^3]^{\mathfrak{S}_3} = \mathbb{C}[\tau_1, \tau_2, \tau_3]$ .

Enfin, un polynôme invariant par  $G(3, 1, 3)$  est un polynôme invariant par  $(\mathbb{U}_3)^3$  (donc dans  $\mathbb{C}[x^3, y^3, z^3]$ ) invariant par  $\mathfrak{S}_3$ , donc  $\mathbb{C}[x, y, z]^{G(3, 1, 3)}$  est une sous-algèbre de  $\mathbb{C}[\tau_1, \tau_2, \tau_3]$ . Un calcul rapide prouve l'inclusion réciproque, et on a bien l'égalité voulue.  $\square$

On note  $\delta_1, \delta_2, \delta_3$  les degrés respectifs de  $\tau_1, \tau_2, \tau_3$ . En utilisant le corollaire 5.1 on retrouve bien  $\delta_1 \delta_2 \delta_3 = 162 = |\mathfrak{S}_3 \ltimes (\mathbb{U}_3)^3|$ . On peut de plus remarquer que ce groupe comporte 15 réflexions (les transpositions dont les deux coefficients transposés sont inverse l'un de l'autre et le troisième est 1 (il y en a 9), et les matrices diagonales dont un seul coefficient est  $\zeta$  ou  $\zeta^2$  (il y en a 6)).

On va chercher les invariants par  $G_{26}$  à partir de  $\tau_1, \tau_2, \tau_3$  (il suffira de montrer qu'un polynôme en  $\tau_1, \tau_2, \tau_3$  est stabilisé par  $g_0$ , puis utiliser le même argument que pour la fin de la preuve précédente). On cherche donc des polynômes homogènes dont le degré est un multiple de 3. Un polynôme de degré impair ne peut pas être invariant par  $G_{26}$  car  $-I_3$  est un élément de ce groupe. On peut ainsi se restreindre à des polynômes dont le degré est un multiple de 6. Pour  $d \in \mathbb{N}$  on note  $(\mathcal{S}^d)^{G_{26}}$  l'espace vectoriel des polynômes homogènes de degré  $d$  invariants par  $G_{26}$ , et on fait de même pour tout autre groupe.

En degré 6, un invariant par  $G(3, 1, 3)$  est forcément combinaison linéaire de  $\tau_1^2$  et  $\tau_2$ . Par calcul,  $g_0 \cdot \tau_1^2 = -\frac{1}{3}\tau_1^2 + v_1$  et  $g_0 \cdot \tau_2 = -\frac{1}{9}\tau_1^2 + \tau_2 + v_2$ , où  $v_1, v_2$  n'ont aucune composante dans l'ensemble des monômes de  $\tau_1^2$  et  $\tau_2$ . On cherche donc une combinaison linéaire  $f := \lambda\tau_1^2 + \mu\tau_2$  vérifiant le système 
$$\begin{cases} -\frac{1}{3}\lambda - \frac{1}{9}\mu = \lambda \\ \mu = \mu \end{cases}$$
. Cette condition est nécessaire pour que  $f$  soit un invariant, mais n'est pas suffisante (si on note  $p$  un projecteur de  $\mathcal{S}^6$  sur  $\text{Vect}(b_1, b_2, b_3, b_4)$ , on sait seulement que  $f$  vérifie  $p \circ g_0 \cdot f = f$ ). Elle permet simplement de réduire la liste des invariants potentiels, mais il faut toujours vérifier que ceux-ci sont de vrais invariants. La résolution du système et cette vérification (cf annexe, pages 23/24) nous donnent un unique invariant (à scalairisation près), qui est  $f_6 := \tau_1^2 - 12\tau_2$ .

On recommence le procédé en dimension supérieure. Un calcul similaire (cf annexe, pages 24/25) indique que l'espace  $(\mathcal{S}^{12})^{G_{26}}$  est de dimension 2. On sait qu'il contient  $f_6^2$ , on en exhibe donc par calcul un linéairement indépendant de celui-ci :  $f_{12} := \tau_1^4 - 216\tau_1\tau_3$ . De même, le calcul (cf annexe, pages 25 à 27) donne  $\dim((\mathcal{S}^{18})^{G_{26}}) = 3$ . Cet espace contient déjà  $f_6^3$  et  $f_6 f_{12}$ . Le polynôme  $f_{18} := \tau_1^6 + 540\tau_1^3\tau_3 + 5832\tau_3^2$  est un invariant complétant cette famille en base.

On montrera dans la partie 5.2.4 que  $f_6, f_{12}$  et  $f_{18}$  engendrent l'algèbre des invariants par  $G_{26}$ .

### 5.2.2 La méthode « par au-dessus »

Cette approche s'appuie sur les caractères de certaines représentations de  $G_{26}$ . On rappelle que si on note  $\chi$  le caractère d'une représentation  $\rho : G_{26} \longrightarrow \text{GL}(V)$ ,  $\mathbb{1}$  le caractère unité et que l'on définit le produit scalaire  $\langle \varphi, \psi \rangle := \frac{1}{|G_{26}|} \sum_{g \in G_{26}} \varphi(g) \overline{\psi(g)}$ , la multiplicité de la représentation triviale dans  $V$  est égale à  $\langle \chi, \mathbb{1} \rangle$ .

Pour  $d \in \mathbb{N}$ , on note  $\rho_d$  la représentation  $G_{26} \longrightarrow \text{GL}(S^d)$ ,  $g \longmapsto (P \mapsto P(g \cdot (x, y, z)^\top))$ , et  $\chi_d$  son caractère. On a ensuite  $\dim((S^d)^{G_{26}}) = \langle \chi_d, \mathbb{1} \rangle = \frac{1}{|G_{26}|} \sum_{g \in G_{26}} \chi_d(g)$ . De cette manière, on peut vérifier de quels degrés sont les invariants. Le calcul (cf annexe, page 28) donne :

|                                    |   |   |    |    |    |    |    |
|------------------------------------|---|---|----|----|----|----|----|
| $d$                                | 0 | 6 | 12 | 18 | 24 | 30 | 36 |
| $\langle \chi, \mathbb{1} \rangle$ | 1 | 1 | 2  | 3  | 4  | 5  | 7  |

Pour un tel  $d$ , on construit  $p := \frac{1}{|G_{26}|} \sum_{g \in G_{26}} \rho_d(g)$ , projecteur sur  $(S^d)^{G_{26}}$ . On retrouve des invariants par  $G_{26}$  en évaluant ces projecteurs.

### 5.2.3 Aparté : critère d'indépendance algébrique et formule de Molien

La propriété ci-dessous permet de montrer que des polynômes sont algébriquement indépendants.

**Proposition 5.2** — Soient  $n \in \mathbb{N}^*$  et  $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$ . S'il existe un point  $X \in \mathbb{C}^n$  tel que le déterminant jacobien  $\det(\text{Jac}(f_1, \dots, f_n))$  est non nul en  $X$ , alors  $f_1, \dots, f_n$  sont algébriquement indépendants.

*Démonstration.* On suppose le déterminant jacobien non nul en un point  $X \in \mathbb{C}^n$ . Soit  $P \in \mathbb{C}[x_1, \dots, x_n]$  tel que  $P(f_1, \dots, f_n) = 0$ . Comme la matrice jacobienne de  $(f_1, \dots, f_n)$  est inversible en  $X$  et comme  $(f_1, \dots, f_n)$  est de classe  $C^1$ , par le théorème d'inversion locale  $(f_1, \dots, f_n)$  réalise un  $C^1$ -difféomorphisme d'un voisinage ouvert  $V$  de  $X$  dans un voisinage ouvert  $W$  de  $(f_1, \dots, f_n)(X)$ , en particulier l'application se surjecte dans ce voisinage. Ainsi,  $P$  s'annule sur  $W$ , un ouvert non vide de  $\mathbb{C}^n$ . Ce polynôme est donc nul. Le seul polynôme annulant  $(f_1, \dots, f_n)$  étant le polynôme nul,  $f_1, \dots, f_n$  sont bien algébriquement indépendants.  $\square$

Enfin, le théorème de Molien s'avère utile pour montrer qu'une famille de polynômes engendre l'algèbre des invariants.

**Théorème 5.3.** (Formule de Molien)

Soit  $V$  un  $\mathbb{C}$ -espace vectoriel de dimension finie  $n$  et  $G$  un sous-espace vectoriel de  $\mathrm{GL}(V)$ . On note, pour  $d \geq 0$ ,  $(\mathcal{S}^d(V))^G$  l'espace vectoriel des invariants nuls ou de degré  $d$ . Alors

$$\sum_{d \geq 0} \dim((\mathcal{S}^d(V))^G) t^d = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - tg)}.$$

*Démonstration.* Comme tout élément  $g$  de  $G$  est d'ordre fini, il est diagonalisable. Notons  $\lambda_1(g), \dots, \lambda_n(g)$  ses valeurs propres. On a

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - tg)} &= \frac{1}{|G|} \sum_{g \in G} \prod_{k=1}^n \frac{1}{1 - \lambda_k(g)t} \\ &= \frac{1}{|G|} \sum_{g \in G} \prod_{k=1}^n \left( \sum_{d \geq 0} (\lambda_k(g)t)^d \right) \\ &= \sum_{d \geq 0} \frac{1}{|G|} \left( \sum_{g \in G} \sum_{a_1 + \dots + a_n = d} \lambda_1(g)^{a_1} \dots \lambda_n(g)^{a_n} \right) t^d. \end{aligned}$$

Soit  $d \geq 0$ , soit  $g \in G$ . En fixant  $\mathcal{B} := (e_1, \dots, e_n)$  une base de  $V$  de valeurs propres de  $g$  telle que pour  $1 \leq k \leq n$ ,  $g(e_i) = \lambda_i(g)e_i$ . Une base de  $\mathcal{S}^d(V)$  est donnée par les produits de  $d$  éléments de  $\mathcal{B}$ , et la trace de  $g$  dans cette base est  $\sum_{a_1 + \dots + a_n = d} \lambda_1(g)^{a_1} \dots \lambda_n(g)^{a_n}$ . En notant  $\chi$  le caractère de la représentation canonique de  $G$  sur  $\mathcal{S}^d(V)$ , on a

$$\frac{1}{|G|} \left( \sum_{g \in G} \sum_{a_1 + \dots + a_n = d} \lambda_1(g)^{a_1} \dots \lambda_n(g)^{a_n} \right) = \frac{1}{|G|} \sum_{g \in G} \chi(g) = \langle \chi, 1 \rangle = \dim((\mathcal{S}^d(V))^G).$$

Par unicité des coefficients d'une série formelle, on a l'égalité voulue.  $\square$

Ces deux résultats combinés permettent de montrer qu'une famille de polynômes engendre bien l'algèbre des invariants.

## 5.2.4 Algèbre des invariants

La méthode « par en-dessous » nous a donné trois invariants explicites :  $f_6$ ,  $f_{12}$  et  $f_{18}$ . On va montrer qu'ils engendrent l'algèbre des invariants

**Proposition 5.3** —  $\mathcal{S}^{G_{26}} = \mathbb{C}[f_6, f_{12}, f_{18}]$

*Démonstration.* L'action d'un élément de  $G_{26}$  étant linéaire et distributive sur le produit de deux polynômes, l'algèbre  $\mathbb{C}[f_6, f_{12}, f_{18}]$  est incluse dans  $\mathcal{S}^{G_{26}}$ . Montrons que l'inclusion réciproque est vérifiée.

Par calcul (cf annexe, page 28), on trouve que le déterminant jacobien de  $(f_6, f_{12}, f_{18})$  est un polynôme non constant. On peut donc trouver un point  $X \in \mathbb{C}^3$  tel que  $\det(\text{Jac}(f_6, f_{12}, f_{18}))(X)$  est non nul. En vertu de la proposition 5.2, les trois polynômes sont algébriquement indépendants.

Ainsi, pour  $d \in \mathbb{N}$ ,  $\text{Vect}(f_6^a f_{12}^b f_{18}^c ; a + b + c = d)$  est un sous-espace vectoriel de dimension  $R(d)$  de  $(\mathcal{S}^d)^{G_{26}}$ , où  $R(d)$  est égal au nombre de triplets d'entiers naturels dont la somme donne  $d$ .

La formule de Molien donne

$$\begin{aligned} \sum_{d \geq 0} \dim((\mathcal{S}^d)^{G_{26}}) t^d &= \frac{1}{|G_{26}|} \sum_{g \in G_{26}} \frac{1}{\det(I_3 - tg)} \\ &= \frac{1}{-t^{36} + t^{30} + t^{24} - t^{12} - t^6 + 1} \\ &= \frac{1}{(1 - t^6)(1 - t^{12})(1 - t^{18})} . \end{aligned}$$

D'autre part,

$$\frac{1}{(1 - t^6)(1 - t^{12})(1 - t^{18})} = \prod_{k=1}^3 \sum_{n \geq 0} t^{6kn} = \sum_{d \geq 0} R(d) t^d .$$

Par unicité de la décomposition en série formelle, pour tout  $d \geq 0$ ,  $\dim((\mathcal{S}^d)^{G_{26}}) = R(d)$ , donc  $(f_6^a f_{12}^b f_{18}^c ; a + b + c = d)$  engendre  $(\mathcal{S}^d)^{G_{26}}$ . Ainsi,  $\mathbb{C}[f_6, f_{12}, f_{18}] = \bigoplus_{d \geq 0} (\mathcal{S}^d)^{G_{26}} = \mathcal{S}^{G_{26}}$ .  $\square$

**Remarque :** Ceci illustre, dans notre cas, le théorème de Shephard-Todd/Chevalley-Serre, ainsi que la formule de Solomon ( $6 \cdot 12 \cdot 18 = 1296$  et  $5 + 11 + 17 = 33$ ).

## Références

- [1] Michèle AUDIN : *Géométrie*. EDP sciences, 2006.
- [2] Michel BROUÉ : *Introduction to complex reflection groups and their braid groups*. Springer, 2010.
- [3] Benoît KLOECKNER : *Un bref aperçu de la géométrie projective*. Calvage & Mounet, 2012.
- [4] Nicolas PERRIN : *Mat 562 : Introduction à la géométrie algébrique et courbes elliptiques*, 2024. Notes de cours, École polytechnique.
- [5] Tomaz PISANSKI et Brigitte SERVATIUS : *Configurations from a graphical viewpoint*. Springer Science & Business Media, 2013.
- [6] Igor R. SHAFAREVICH : *Basic algebraic geometry 1. Varieties in projective space. Translated from the Russian by Miles Reid*. Berlin : Springer, 3rd ed. édition, 2013.

## Addition sur une courbe elliptique

```
[1]: K.<zeta> = CyclotomicField(3)
     A.<a,b,x,y,z,u,v> = PolynomialRing(K,7)
```

### Formules générales

```
[2]: def dic(p):
     return {x:p[0], y:p[1], z:p[2]}
```

Les fonctions ci-dessous permettent respectivement de visualiser un point du plan projectif dans la carte  $z = 1$  si cela est possible, et de vérifier si deux point du plan projectif repérés par des coordonnées homogènes différentes sont égaux.

```
[3]: def normalise_z(p):
     xp,yp,zp = p
     if zp == 0:
         return p
     else:
         return vector([xp/zp,yp/zp,1])

     def egalite(p,q):
         xp,yp,zp = p
         xq,yq,zq = q
         return xp*yq-yp*xq == 0 and xp*zq-zp*xq == 0 and yp*zq-zp*yq == 0
```

La fonction ci-dessous permet de calculer le point  $P * Q$  pour tous points  $P, Q$  donnés.

```
[4]: def troisieme_point(eq,p,q):
     Ap = vector(A,[A(p[0]),A(p[1]),A(p[2])])
     Aq = vector(A,[A(q[0]),A(q[1]),A(q[2])])
     if eq.subs(dic(p)) != 0:
         return "Le premier point n est pas sur la courbe"
     if eq.subs(dic(q)) != 0:
         return "Le second point n est pas sur la courbe"
     if egalite(p,q):
         #si les deux points sont égaux, la droite est la tangente à la courbe en le point
         deq = sum(diff(eq,ww).subs(dic(p))*ww for ww in [x,y,z])
         if deq == 0:
             return "Le point est singulier"
```

```

    r = p.cross_product(vector([diff(eq,ww).subs(dic(p)) for ww in [x,y,z]]))
    Ar = vector(A,[A(r[0]),A(r[1]),A(r[2])])
    f = expand(eq.subs(dic(Ap+u*Ar)))
    alpha = f.coefficient(u**2)
    beta = f.coefficient(u**3)
    s = beta*p-alpha*r
else:
    #si les deux
    ↪ points sont différents, la droite est simplement celle qui les relie
    f = expand(eq.subs(dic(u*Ap+v*Aq)))
    alpha = f.coefficient(u**2*v)
    beta = f.coefficient(v**2*u)
    s = beta*p-alpha*q
return normalise_z(s)

```

On peut maintenant à l'aide de la fonction `troisieme_point` calculer la somme de deux points.

```

[5]: def addition(eq,p0,p,q):
    Ap0 = vector(A,[A(p0[0]),A(p0[1]),A(p0[2])])
    Ap = vector(A,[A(p[0]),A(p[1]),A(p[2])])
    Aq = vector(A,[A(q[0]),A(q[1]),A(q[2])])
    if eq.subs(dic(p0)) != 0:
        return "Le point p0 n est pas sur la courbe"
    if eq.subs(dic(p)) != 0:
        return "Le premier point n est pas sur la courbe"
    if eq.subs(dic(q)) != 0:
        return "Le second point n est pas sur la courbe"
    xp,yp,zp = p
    xq,yq,zq = q
    p_etoile_q = troisieme_point(eq,p,q)
    return normalise_z(troisieme_point(eq,p0,p_etoile_q))

```

## Compatibilité addition dans le lieu de base/addition dans $\mathbb{F}_3^2$

On implémente le pinceau hessien et son lieu de base. Le neutre pour l'addition sera le point de coordonnées homogènes  $[0 : 1 : -1]$  (qui est un point du lieu de base).

```

[6]: pinceau = a*(x**3+y**3+z**3)+b*x*y*z
l0 = [vector([0,1,-zeta^k]) for k in range(3)]
l1 = [vector([-zeta^k,0,1]) for k in range(3)]
l2 = [vector([1,-zeta^k,0]) for k in range(3)]
ldb = [l0,l1,l2]
p0 = ldb[0][0]

```

```

[7]: def add_pinceau(a0,b0,p,q):
    return addition(pinceau.subs({a:a0,b:b0}),p0,p,q)

```

La fonction suivante vérifie si le point  $R$  renseigné est bien la somme des points  $P$  et  $Q$ .

```
[8]: def v_a(a0,b0,p,q,r):
      return egalite(add_pinceau(a0,b0,p,q),r)
```

```
[9]: def add_f3(m,n):
      return (m + n) % 3
```

La fonction suivante vérifie si pour une courbe du pinceau donnée l'addition de deux éléments du lieu de base  $P_{j,k}$  et  $P_{j',k'}$  est compatible avec l'addition dans  $\mathbb{F}_3^2$ , i.e. si pour tous  $(j,k), (j',k') \in \mathbb{F}_3^2$ ,  $P_{j,k} \oplus P_{j',k'} = P_{j+j',k+k'}$ .

```
[10]: def compatibilite(a0,b0):
        verif = True
        L = [(0,0),(1,0),(0,1),(1,1),(2,0),(0,2),(2,1),(1,2),(2,2)]
        i = 0
        while verif and i < 9:
            j = 0
            while verif and j <= i:
                m = (L[i],L[j])
                verif = verif and
→v_a(a0,b0,ldb[m[0][0]][m[0][1]],ldb[m[1][0]][m[1][1]],ldb[add_f3(m[0][0],m[1][0])][add_f3(m[0][1],m[1][1])])
                j += 1
            i += 1
        return verif
```

```
[11]: compatibilite(3,4)
```

```
[11]: True
```

Les additions sont compatibles pour la courbe d'équation  $3(x^3 + y^3 + z^3) + 4xyz = 0$ .

## Outils pour la visualisation de l'addition

Etant donné un point  $P$  fixé et un point  $Q$  (que l'on fera varier), on trace une flèche de  $Q$  à  $P + Q$ .

```
[12]: def trace_fleche(eq,p0,p,q,xmax,ymax):
        vecp = vector([p[0],p[1],1])
        vecq = vector([q[0],q[1],1])
        f = SR(eq.subs({z:1}))
        vecr = addition(eq,p0,vecp,vecq)
        r = (vecr[0],vecr[1])
        fl = arrow(q, r, width = 1, arrowsize = 2, color = "black")
        G = Graphics()
        x0,y0,z0 = p0
        if z0 != 0:
            G += point2d((x0/z0,y0/z0), size = 20)
            G += text("O", (x0/z0-xmax*0.05, y0/z0))
        G += point2d([p], size = 20, color = 'purple')
        G += text("P", (p[0], p[1]-ymax*0.05), color = 'purple')
```

```

if p != q:
    G += point2d([q], size = 20, color = 'red')
    G += text("Q", (q[0], q[1]-ymax*0.05), color = 'red')
G += point2d([r], size = 20, color = 'green')
if p != q:
    G += text("P+Q", (r[0], r[1]-ymax*0.05), color = 'green')
else:
    G += text("2P", (r[0], r[1]-ymax*0.05), color = 'green')
G += fl
G += implicit_plot(f, (x, -xmax, xmax), (y, -ymax, ymax))
G.show()

```

Tracé des multiples d'un point

```

[13]: def multiple(eq,p0,n,p):
    if n == 0:
        return p0
    elif n%2 == 0:
        m_int = multiple(eq,p0,n//2,p)
        return addition(eq,p0,m_int,m_int)
    else:
        m_int = multiple(n//2,p)
        return addition(eq,p0,addition(eq,p0,m_int,m_int),p)

```

```

[14]: def rempliit_multiples(eq,p0,n,p):
    Lm = [(p[0],p[1])]
    po = p
    for i in range(n-1):
        po = addition(eq,p0,po,p)
        Lm.append((po[0],po[1]))
    return Lm

```

```

[15]: def trace_mult_pt(eq,p0,n,p,xmax,ymax):
    Lm = rempliit_multiples(eq,p0,n,p)
    f = SR(eq.subs({z:1}))
    G = Graphics()
    couleurs = [hue(k/n) for k in range(n)]
    for i,q in enumerate(Lm):
        if abs(q[0].n()) < xmax and abs(q[1].n()) < ymax:
            G += point2d([q], color = couleurs[i], size=20)
            G += text(f"${i+1}P$", (q[0], q[1]-ymax*0.05), color = couleurs[i],
↪fontsize = "small")
    G += implicit_plot(f, (x, -xmax, xmax), (y, -ymax, ymax))
    G.show()

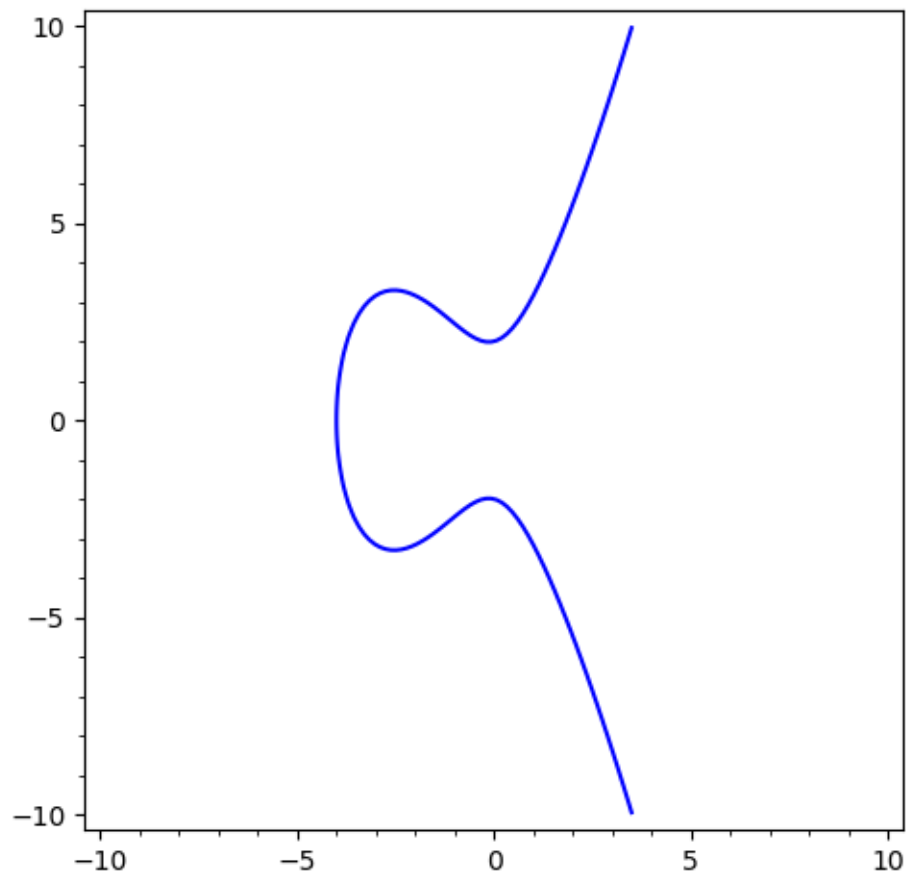
```

## Une première équation

```
[16]: eq1 = y^2*z-(x+4*z)*(x^2+z^2)
      p01 = vector(K,[K(-4),K(0),K(1)])
      p01b = vector(K,[K(0),K(1),K(0)])
```

```
[17]: f1 = SR(eq1.subs({z:1}))
      implicit_plot(f1,(x,-10,10),(y,-10,10))
```

[17]:

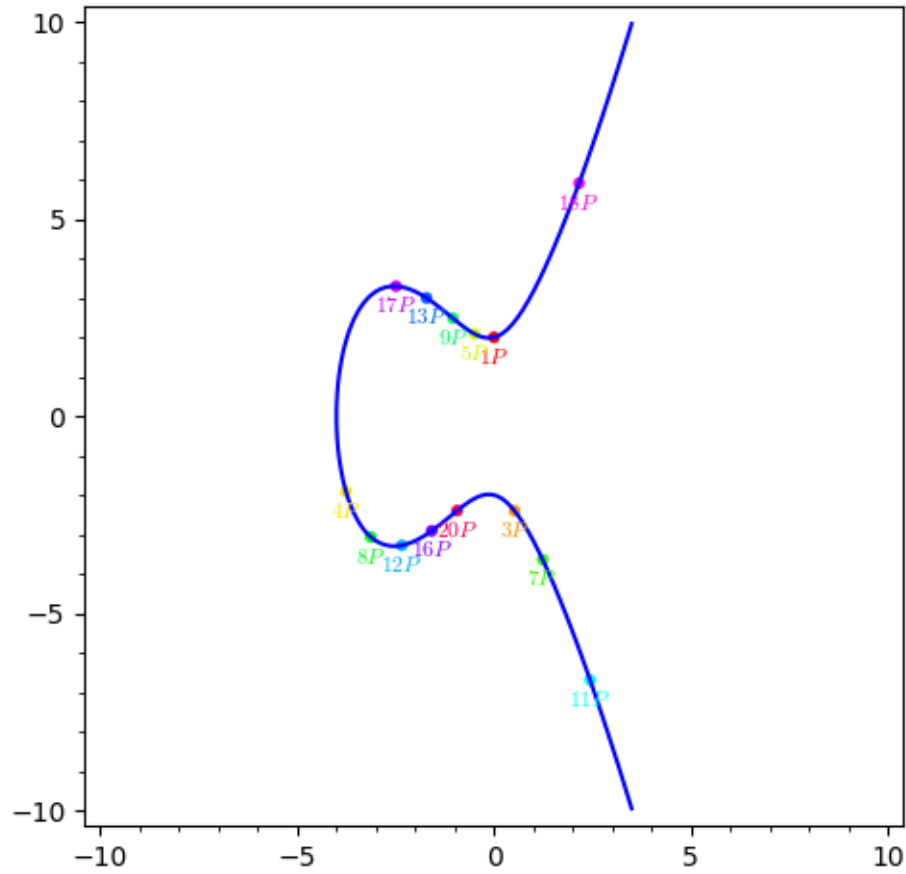


Détermination et traçage de points rationnels

```
[18]: pt1 = vector(K,[K(0),K(2),K(1)])
```

```
[19]: L_mult = rempli_multiples(eq1,p01,20,pt1)
```

```
[20]: trace_mult_pt(eq1,p01,20,pt1,10,10)
```



Nous utiliserons les points  $4P, 8P, 12P, 16P$  et  $20P$  pour visualiser la continuité.

```
[21]: pt_base = L_mult[11]
      L_approch = [L_mult[3], L_mult[7], pt_base, L_mult[15], L_mult[19]]
```

```
[22]: for q in L_approch:
      trace_fleche(eq1, p01, pt_base, q, 10, 10)
```

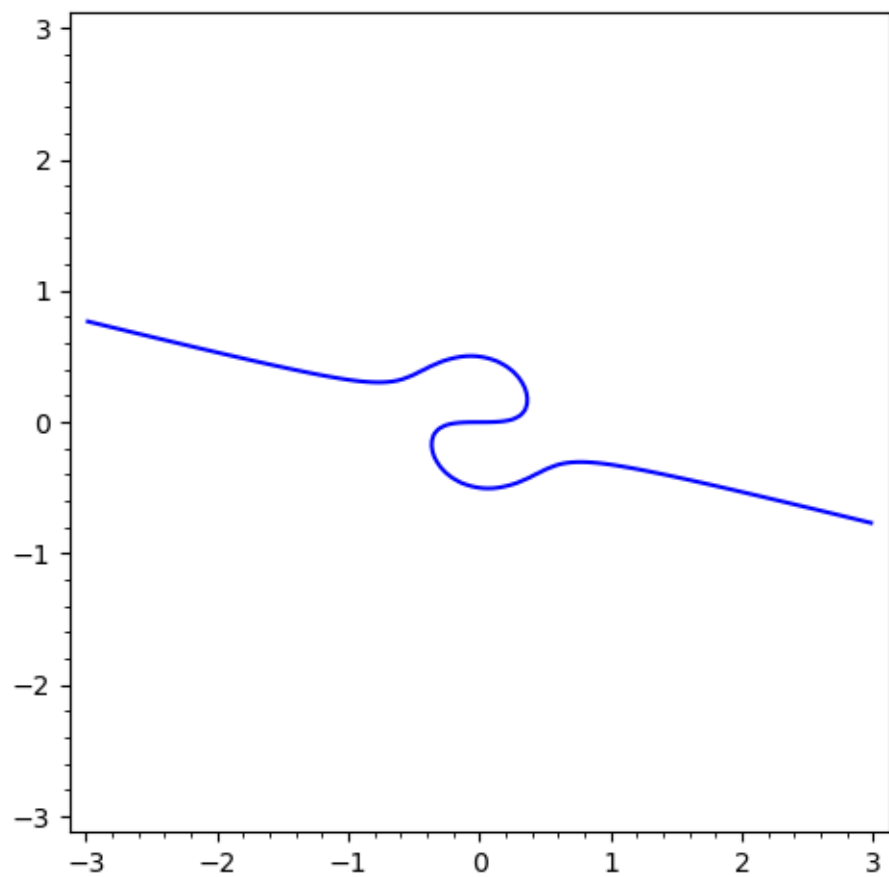
Les quatre premiers graphiques renvoyés sont affichés sur cette page : [\[Voir les figures\]](#)

### Changement de repère

```
[23]: eq2 = z^2*y-(x+4*y)*(x^2+y^2)
      p02 = vector(K, [K(4), K(1), K(0)])
      p02b = vector(K, [K(0), K(0), K(1)])
```

```
[24]: f2 = SR(eq2.subs({z:1}))
      implicit_plot(f2, (x, -3, 3), (y, -3, 3))
```

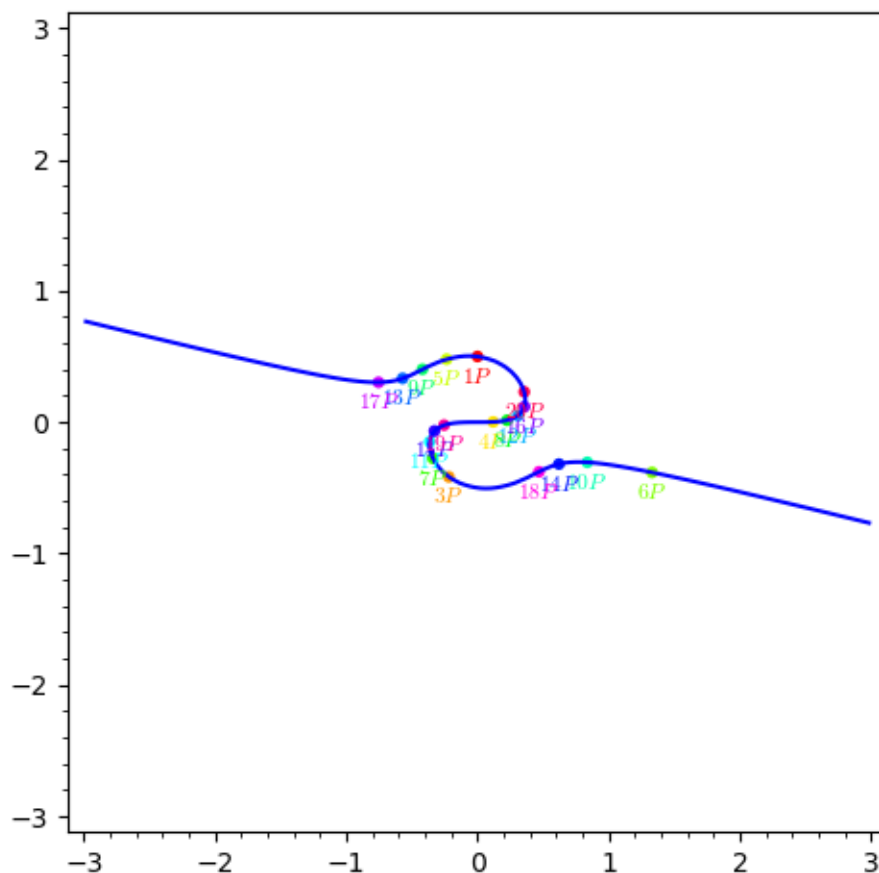
[24]:



```
[25]: pt2 = vector(K,[K(0),K(1/2),K(1)])
```

```
[26]: L_mult2 = rempli_multiples(eq2,p02b,20,pt2)
```

```
[27]: trace_mult_pt(eq2,p02b,20,pt2,3,3)
```



```
[28]: pt_base2 = L_mult2[11]
      L_approch2 = [L_mult2[3],L_mult2[7],pt_base2,L_mult2[15],L_mult2[19]]
```

```
[29]: for q in L_approch2:
      trace_fleche(eq2,p02b,pt_base2,q,1,1)
```

Les quatre premiers graphiques renvoyés sont affichés sur cette page : [\[Voir les figures\]](#)

## Dessins « pédagogiques » sur l'addition

Construction du point  $P + Q$

```
[30]: def droite(eq,p,q):
      ap = p[0]
      op = p[1]
      if p != q:
          alpha = ap-q[0]
          beta = op-q[1]
          return alpha*y-beta*x-(alpha*op-beta*ap)
```

```

    else:
        return (sum(diff(eq,ww).subs({x:ap, y:op, z:1})*ww for ww in [x,y,z])).
        ↪subs({z:1})

def trace_etoile(eq,p0,p2d,q2d,strup = "P",strq = "Q",strpeq = "P*Q",strpep =
    ↪"P*P",cpeq = "green"):
    r = addition(eq,p0,vector([p2d[0],p2d[1],1]),vector([q2d[0],q2d[1],1]))
    sint = troisieme_point(eq,p0,r)
    s = sint/sint[2]
    f = SR(eq.subs({z:1}))
    g = SR(droite(eq,p2d,q2d).subs({z:1}))
    G = implicit_plot(g,(x,-10,10),(y,-10,10), color = cpeq) +
    ↪implicit_plot(f,(x,-10,10),(y,-10,10), color = "black")
    G += point2d([(p0[0],p0[1])], color = "black", size = 20) + text("0",
    ↪(p0[0]-0.5,p0[1]), color = "black")
    if p2d == q2d:
        G += point2d([p2d], size = 20) + text(strp, (p2d[0],p2d[1]-0.5))
        G += point2d([(s[0],s[1])], color = cpeq, size = 20) + text(strpep,
    ↪(s[0],s[1]-0.5), color = cpeq)
    else:
        G += point2d([p2d], size = 20) + text(strp, (p2d[0],p2d[1]-0.5))
        G += point2d([q2d], size = 20) + text(strq, (q2d[0],q2d[1]-0.5))
        G += point2d([(s[0],s[1])], color = cpeq, size = 20) + text(strpeq,
    ↪(s[0],s[1]-0.5), color = cpeq)
    return G
#     G.save("etoile.pdf",figsize = 10, frame = False)

def trace_add(eq,p0,p2d,q2d,strup = "P",strq = "Q",strpeq = "P*Q",strppq =
    ↪"P+Q",strpep = "P*P",strppp = "P+P",cpeq = "green",cppq = "red"):
    r = addition(eq,p0,vector([p2d[0],p2d[1],1]),vector([q2d[0],q2d[1],1]))
    sint = troisieme_point(eq,p0,r)
    s = sint/sint[2]
    f = SR(eq.subs({z:1}))
    g = SR(droite(eq,p2d,q2d).subs({z:1}))
    h = SR(droite(eq,(r[0],r[1]),(p0[0],p0[1])).subs({z:1}))
    G = implicit_plot(g,(x,-10,10),(y,-10,10), color = cpeq) +
    ↪implicit_plot(f,(x,-10,10),(y,-10,10), color = "black") +
    ↪implicit_plot(h,(x,-10,10),(y,-10,10), color = cppq)
    G += point2d([(p0[0],p0[1])], color = "black", size = 20) + text("0",
    ↪(p0[0]-0.5,p0[1]), color = "black")
    if p2d == q2d:
        G += point2d([p2d], size = 20) + text(strp, (p2d[0],p2d[1]-0.5))
        G += point2d([(s[0],s[1])], color = cpeq, size = 20) + text(strp,
    ↪(s[0],s[1]-0.5), color = cpeq)
        G += point2d([(r[0],r[1])], color = cppq, size = 20) + text(strppp,
    ↪(r[0],r[1]-0.5), color = cppq)

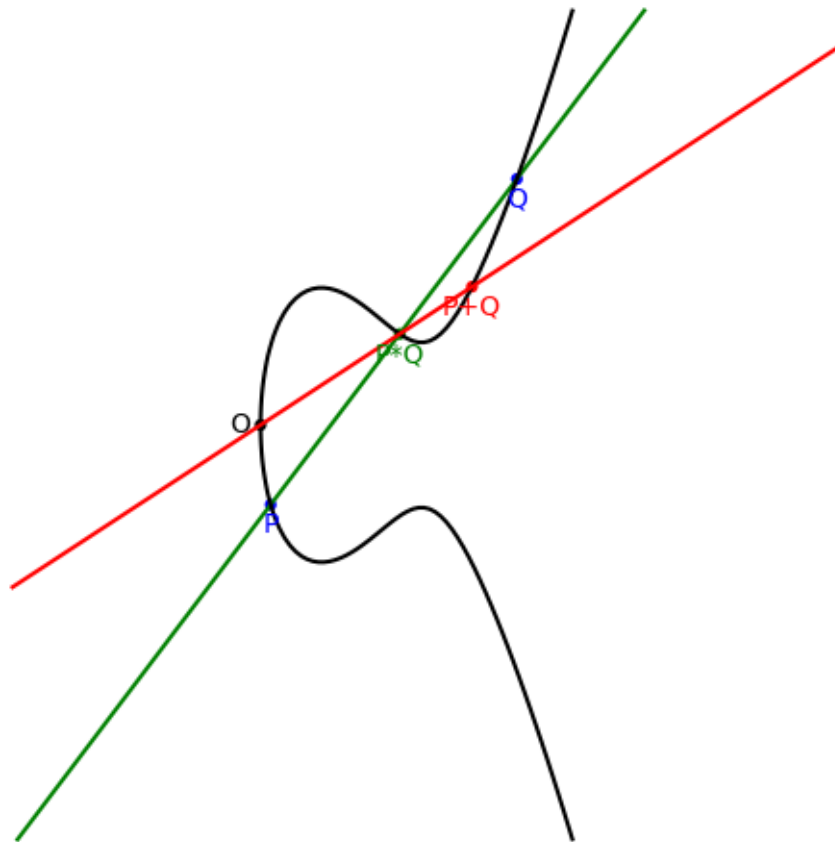
```

```

else:
    G += point2d([p2d], size = 20) + text(strp, (p2d[0],p2d[1]-0.5))
    G += point2d([q2d], size = 20) + text(strq, (q2d[0],q2d[1]-0.5))
    G += point2d([(s[0],s[1])], color = cpeq, size = 20) + text(strpeq,␣
↪(s[0],s[1]-0.5), color = cpeq)
    G += point2d([(r[0],r[1])], color = cppq, size = 20) + text(strppq,␣
↪(r[0],r[1]-0.5), color = cppq)
    return G
#     G.save("plus.pdf", figsize = 10, frame = False)

```

```
[31]: trace_add(eq1,p01,L_mult[3],L_mult[17]).show(frame = False)
```



```
[32]: trace_etoile(eq1,p01,L_mult[3],L_mult[17]).show(frame = False)
```

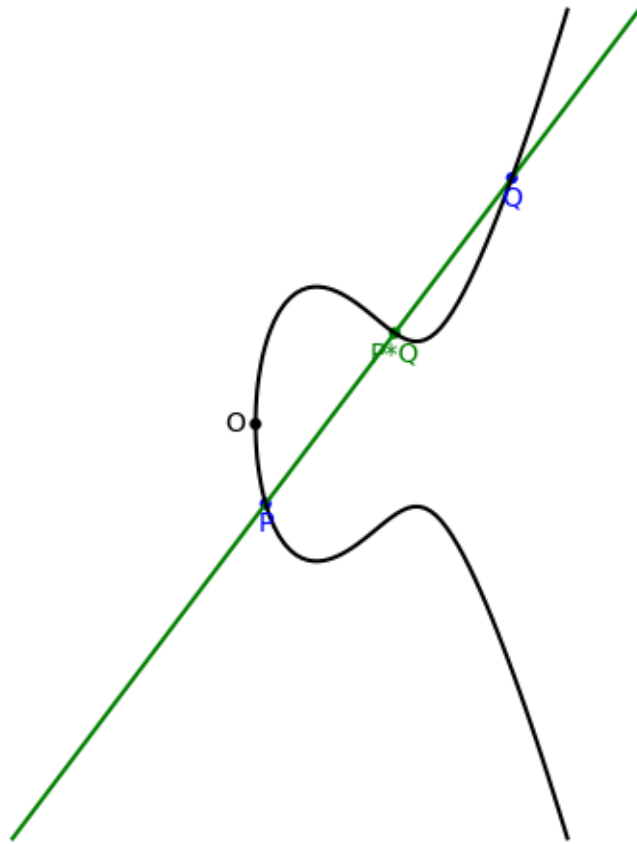
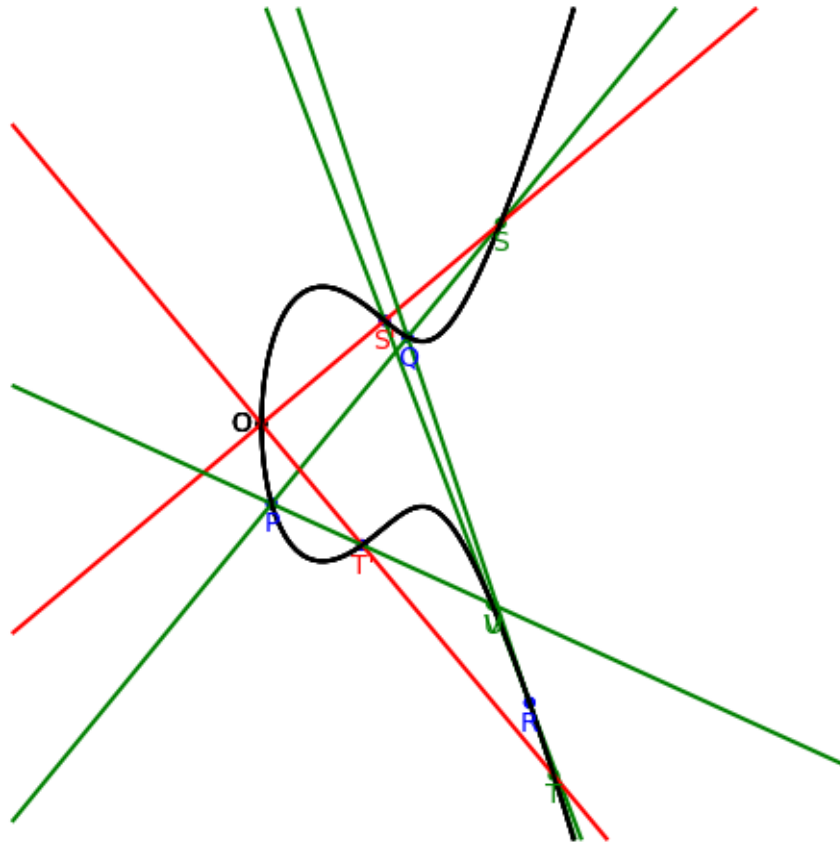


Illustration de l'associativité de l'addition

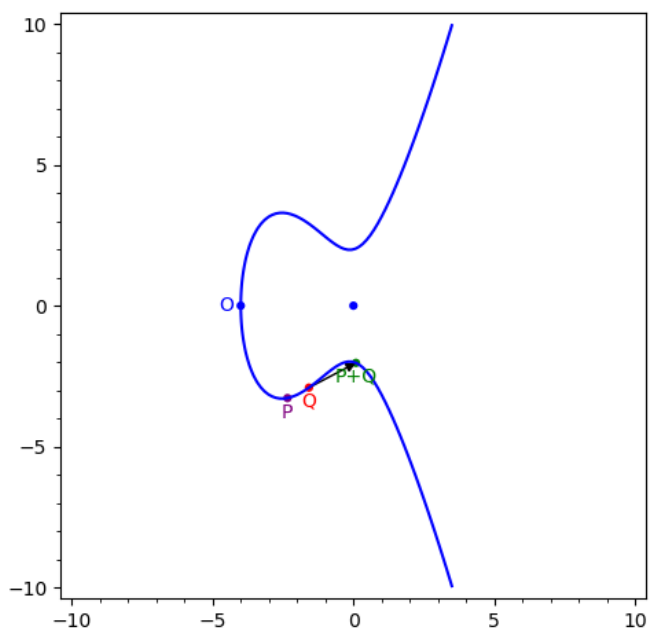
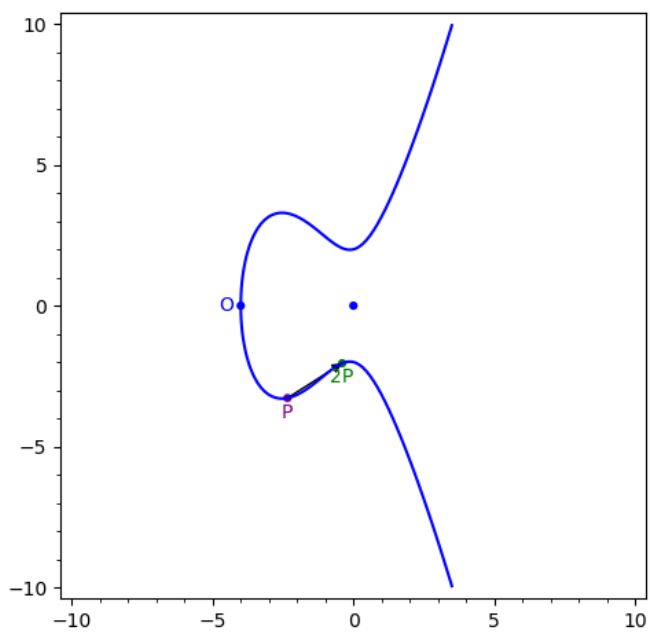
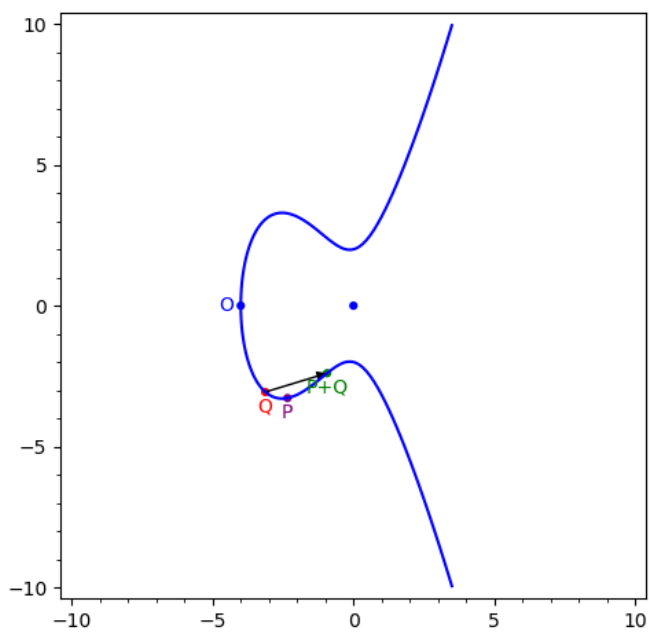
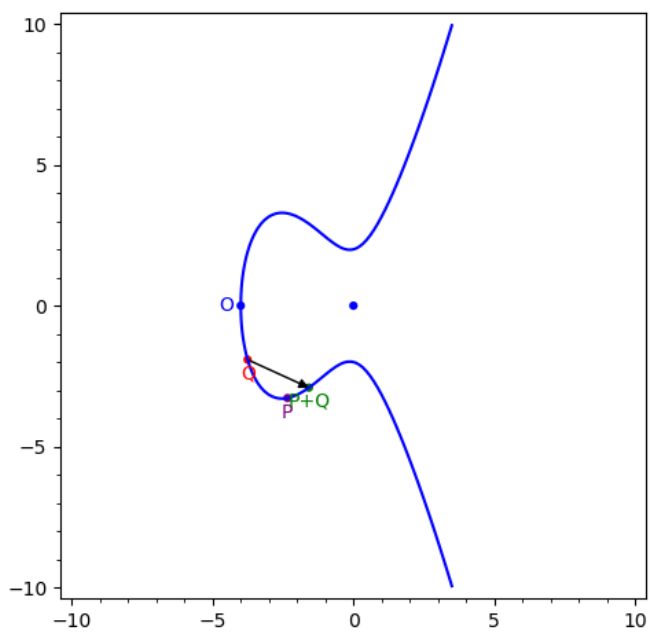
```
[33]: point_p = L_mult[3]
      point_q = L_mult[4]
      point_r = L_mult[10]
      ppqint = ⬅
      ⬅addition(eq1,p01,vector([point_p[0],point_p[1],1]),vector([point_q[0],point_q[1],1]))
      ppq = (ppqint[0],ppqint[1])
      qprint = ⬅
      ⬅addition(eq1,p01,vector([point_q[0],point_q[1],1]),vector([point_r[0],point_r[1],1]))
      qpr = (qprint[0],qprint[1])
```

```
[34]: G_assoc = trace_add(eq1,p01,point_p,point_q,strpeq = "S",strppq = "S'")
      G_assoc += trace_etoile(eq1,p01,ppq,point_r,stri = "",strq = "R",strpeq = "U")
      G_assoc += trace_add(eq1,p01,point_q,point_r,stri = "",strq = "",strpeq = ⬅
      ⬅"T",strppq = "T'")
      G_assoc += trace_etoile(eq1,p01,qpr,point_p,stri = "",strq = "",strpeq = "V")
      G_assoc.show(frame = False)
```

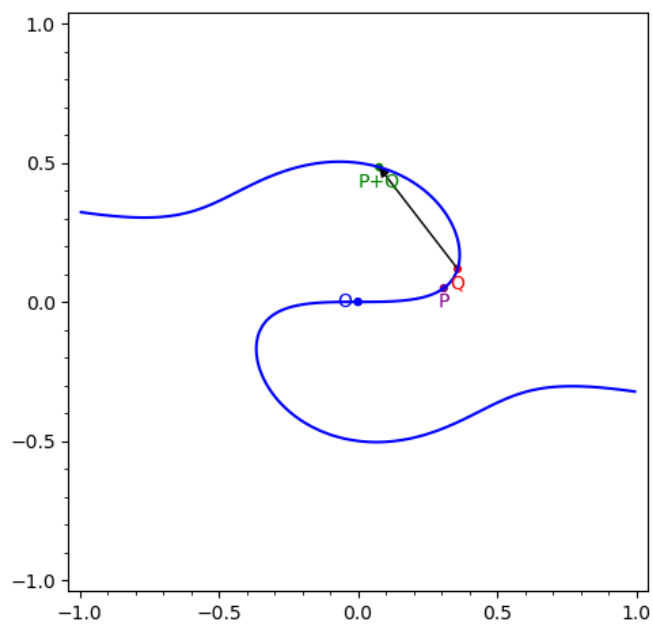
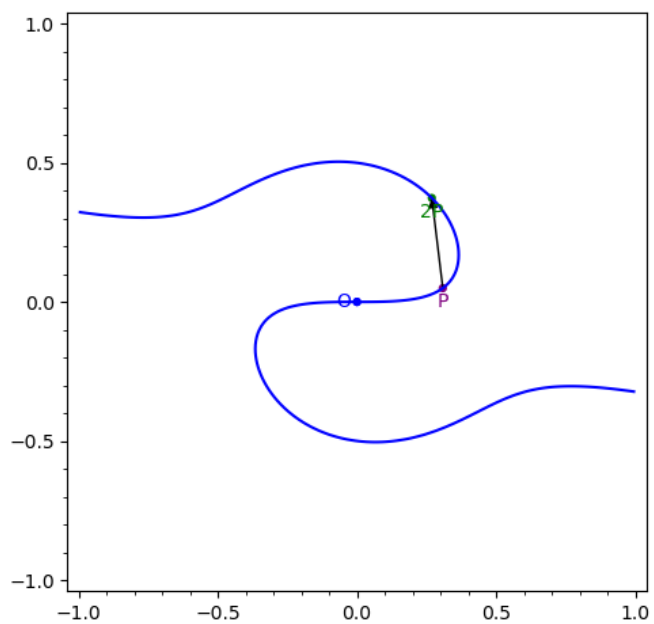
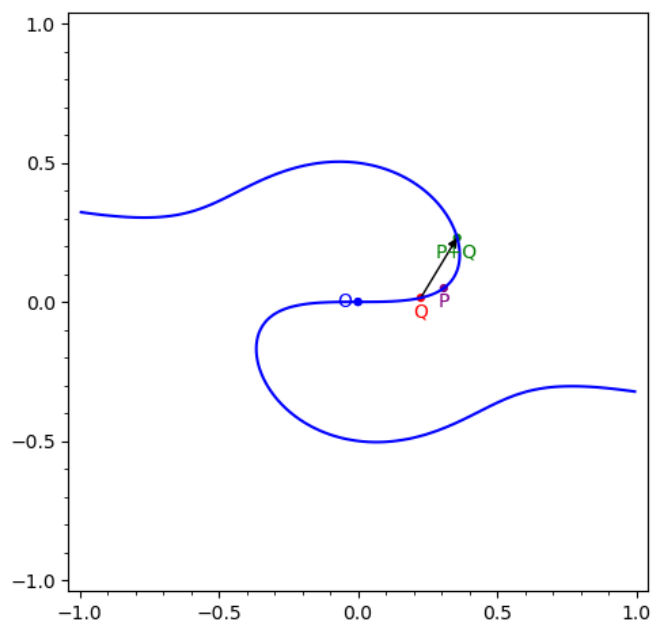
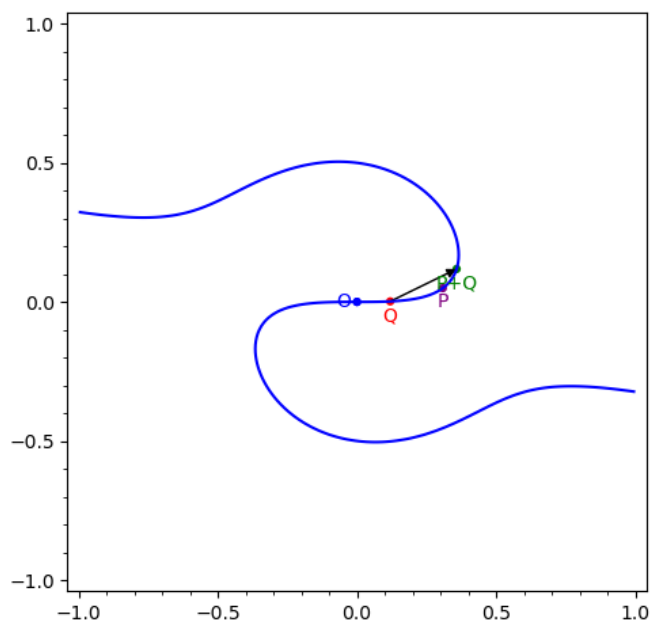


[ ]:

Quatre des graphiques renvoyés par la ligne [22]



Quatre des graphiques renvoyés par la ligne [29]



## Construction du pinceau et du neuvième point induits par huit points (dans le plan affine)

### Construction d'un pinceau à l'aide de 8 points le définissant

```
[1]: A.<x,y,a,b> = PolynomialRing(QQ,4)
monome = vector([x^3,x^2*y,x^2,x*y^2,x*y,x,y^3,y^2,y,1])
```

Résolution d'un système de 8 équations à 10 inconnues pour trouver 2 cubiques qui engendrent le pinceau passant par les 8 points

```
[2]: def ps(p,q):
    n = len(p)
    if n != len(q):
        return 'les vecteurs ne sont pas de la même taille!'
    else:
        c = 0
        for i in range(n):
            c += p[i]*q[i]
        return c
```

```
[3]: def pinceau(L):
    m = matrix(8,10,[[monome[i](L[j][0],L[j][1],0,0) for i in range(10)] for j in range(8)])
    ker = m.right_kernel()
    pf,pg = ker.basis_matrix().rows()
    return (ps(pf,monome),ps(pg,monome))
```

Détermination du neuvième point du pinceau à l'aide des racines du résultant de deux fonctions le générant

```
[4]: def neuvieme_racine(f,L):
    d = f.degree()
    g = f/(f.coefficient(d))
    s = 0
    for i in range(d-1):
        s = s + L[i]
    return -(g.coefficient(d-1)+s)
```

```
[5]: def neuvieme_point(L):
    L_abs = [L[i][0] for i in range(8)]
    L_ord = [L[i][1] for i in range(8)]
    f,g = pinceau(L)
    res_y = f.resultant(g,x)
    ordo = neuvieme_racine(res_y.univariate_polynomial(),L_ord)
    res_x = f.resultant(g,y)
    absc = neuvieme_racine(res_x.univariate_polynomial(),L_abs)
    return vector([absc,ordo])
```

Tracé du pinceau et du neuvième point

```
[6]: def courbe(k, eq, N=30, **args):
    d = {a:cos(pi*k/N), b:sin(pi*k/N)}
    return implicit_plot(eq.subs(d), (x,-7,7), (y,-7,7), color=hue(k/N), **args)

def pinceau_et_points(L, ptvert=False):
    f,g = pinceau(L)
    eq = a*f+b*g
    if not ptvert:
        return add(point(p, size = 50, zorder =1000, color = 'blue') for p in L)
    ↪+ add(courbe(k, eq, 30, linewidth=.7) for k in range(30)) +
    ↪point(neuvieme_point(L), size = 50, zorder = 1000, color = 'red')
    else:
        return add(point(L[i], size = 50, zorder =1000, color = 'blue') for i in
    ↪range(len(L)-1)) + add(courbe(k, eq, 30, linewidth=.7) for k in range(30)) +
    ↪point(neuvieme_point(L), size = 50, zorder = 1000, color = 'red') +
    ↪point(L[len(L)-1], size = 50, zorder = 1000, color = 'lightgreen')

def dessine_pinceau(L):
    pinceau_et_points(L).show(figsize=10, frame=False)

def dessine_complexe(L):
    c1,c2 = pinceau(L)
    def f(z):
        d = {x:z.real(), y:z.imag(), a:1, b:1}
        return (c1.subs(d)+I*c2.subs(d))/sqrt(c1.subs(d)**2+c2.subs(d)**2)
    #G = implicit_plot(c1, (x,-5,5), (y,-5,5)) + implicit_plot(c2, (x,-5,5),
    ↪(y,-5,5))
    (complex_plot(f,(x,-5,5),(y,-5,5), plot_points=150)).show(figsize=10, frame
    ↪= False, axes = False)
```

Pinceau engendré par huit points répartis aléatoirement dans  $[-5,5]$

```
[7]: def approx_decim(x):
    return int(10^10*x)/(10^10)

def randr(M):
```

```

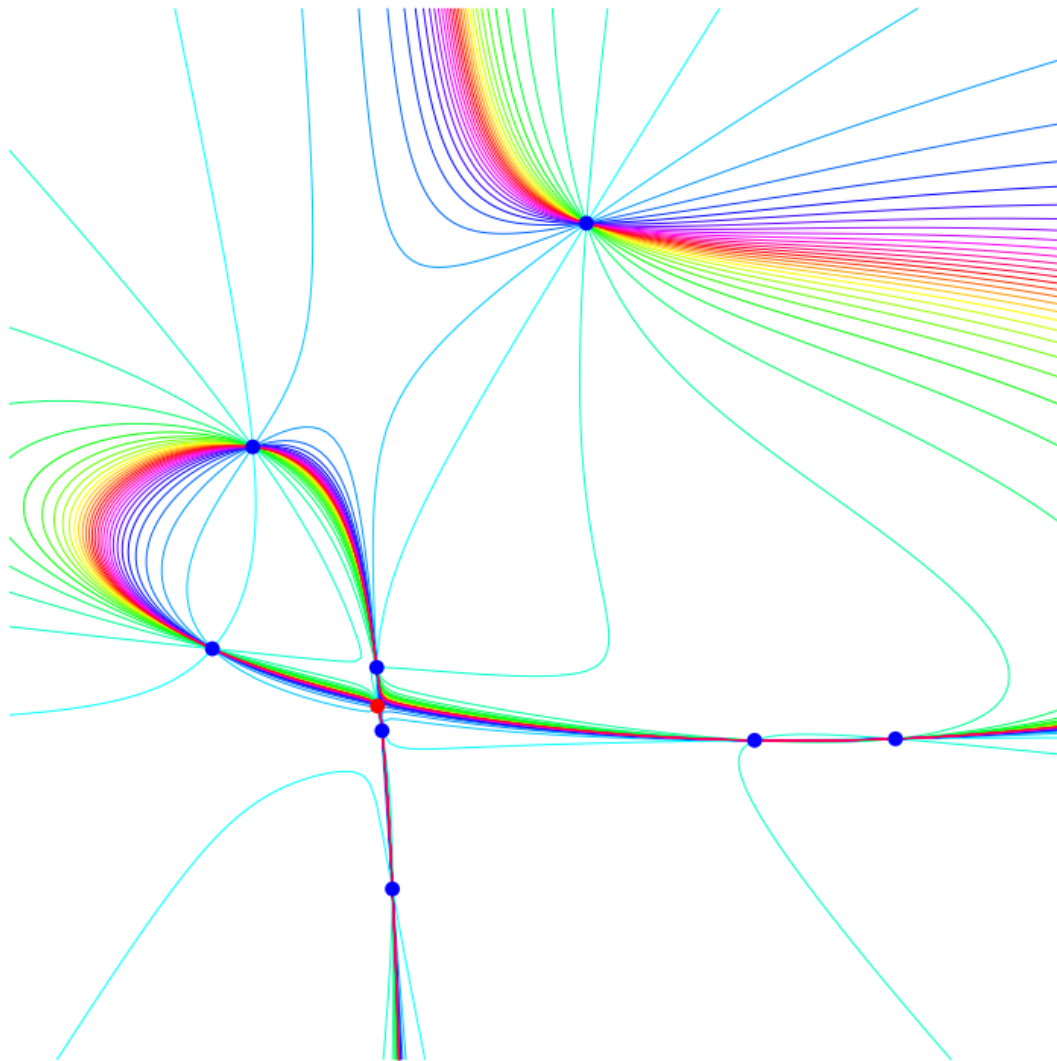
x = approx_decim(random())
return x*2*M-M

def randpoints_r(M,n):
    return [(randr(M),randr(M)) for _ in range(n)]

```

```
[8]: Lr = randpoints_r(5,8)
```

```
[9]: dessine_pinceau(Lr)
```



## « Mouvement » du pinceau en fonction du huitième point

```
[10]: def nouvelle_liste(L,p):  
      L2 = L.copy()  
      L2.append(p)  
      return L2
```

On fait varier le huitième point sur la droite  $y = -\frac{\alpha}{\beta}x$

```
[11]: def construit_gif(L,nbim,alpha = 1,beta = 1):  
      L_gif = []  
      for i in range(-nbim,nbim):  
          p = [i/nbim,-alpha/beta*i/nbim]  
          L_gif.append(pinceau_et_points(nouvelle_liste(L,p),True))  
      return L_gif
```

```
[12]: Lr = randpoints_r(5,7)
```

```
[13]: gif = construit_gif(Lr,25)
```

```
[14]: for i in range(len(gif)):  
      gif[i].save(f"gif1_{i}.png", figsize=10, frame=False, axes=False)
```

```
[15]: for i in range(len(gif)):  
      gif[i].show()
```

Les images renvoyées par le script ci-dessus permettent de générer la vidéo suivante:

[Voir la vidéo](#)

## Implémentation du pinceau hessien, de $\mathbb{H}$ et $G_{26}$ et calcul des invariants polynomiaux par $G_{26}$

### Implémentation des groupes de symétrie du pinceau hessien

```
[1]: L.<zeta9> = CyclotomicField(9)
      K.<zeta> = CyclotomicField(3, embedding = zeta9^3)
      A.<a,b,x,y,z> = PolynomialRing(K,5)
```

```
[2]: eq = a*(x^3+y^3+z^3)+b*x*y*z
```

Pour déterminer le lieu de base du pinceau, on recherche les points d'intersection de  $\mathcal{E}_0$  et  $\mathcal{E}_\infty$ . On les cherche d'abord dans la carte  $z = 1$ .

```
[3]: eq_0 = eq.subs({a:1,b:0,z:1})
      eq_inf = eq.subs({a:0,b:1,z:1})

      res_y = eq_0.resultant(eq_inf,x).univariate_polynomial()
      ord_poss = [racine[0] for racine in res_y.roots()]
      res_x = eq_0.resultant(eq_inf,y).univariate_polynomial()
      abs_poss = [racine[0] for racine in res_x.roots()]

      lieu_de_base = []
      for absc in abs_poss:
          for ordo in ord_poss:
              if eq_0.subs({x:absc,y:ordo}) == 0:
                  lieu_de_base.append(vector([absc,ordo,1]))
```

On cherche les points restants sur la droite à l'infini: elle est contenue dans  $\mathcal{E}_\infty$  donc il suffit de trouver les points de cette droite qui sont sur  $\mathcal{E}_0$ . Pour un tel point, on a  $y \neq 0$  car sinon  $x$  serait également nul. On peut donc fixer  $y$  égal à 1.

```
[4]: eq_0_a_1_inf = eq.subs({a:1,b:0,y:1,z:0}).univariate_polynomial()

      abs_inf = [racine[0] for racine in eq_0_a_1_inf.roots()]
      for absc in abs_inf:
          lieu_de_base.append(vector([absc,1,0]))

      lieu_de_base
```

```
[4]: [(zeta + 1, 0, 1),
      (-zeta, 0, 1),
      (-1, 0, 1),
      (0, zeta + 1, 1),
      (0, -zeta, 1),
      (0, -1, 1),
      (zeta + 1, 1, 0),
      (-zeta, 1, 0),
      (-1, 1, 0)]
```

On recherche ensuite les courbes singulières du pinceau à l'aide de la forme de Weierstrass et du discriminant. On sait déjà que  $\mathcal{E}_\infty$  est singulière. On se concentre maintenant sur  $\mathcal{E}_\lambda$ , pour  $\lambda \in \mathbb{C}$ .

```
[5]: Rl.<lamb> = PolynomialRing(K,1)
Kl = Rl.fraction_field()
Aprim.<xp,yp,zp> = PolynomialRing(Kl,3)

eqprim = (xp^3+yp^3+zp^3)+lamb*xp*yp*zp

wei = EllipticCurve_from_cubic(eqprim, [1,-1,0], morphism=True)
[racine[0] for racine in Rl(wei.codomain().discriminant()).
  ↳univariate_polynomial().roots()]
```

verbose 0 (4167: multi\_polynomial\_ideal.py, groebner\_basis) Warning: falling back to very slow toy implementation.

```
[5]: [3*zeta + 3, -3*zeta, -3]
```

On a ainsi quatre courbes singulières:  $\mathcal{E}_\infty$ ,  $\mathcal{E}_{-3}$ ,  $\mathcal{E}_{-3\zeta}$  et  $\mathcal{E}_{-3\zeta^2}$ .

On (re)définit les éléments du pinceau de manière « commode ».

```
[6]: sing = [eq.subs({a:a0, b:b0}) for (a0,b0) in [(0,1),(-1/3,1),(-1/(3*zeta),1),(1/
  ↳(3*(zeta+1)),1)]]
l0 = [vector([0,1,-zeta^k]) for k in range(3)]
l1 = [vector([-zeta^k,0,1]) for k in range(3)]
l2 = [vector([1,-zeta^k,0]) for k in range(3)]
p = [l0,l1,l2]
ldb = [p[i][j] for i in range(3) for j in range(3)]
```

Définition des groupes  $G(3,1,3)$ ,  $G_{26}$  et  $\mathbb{H}$

```
[7]: def mat_permut(tau,coeff):
      return Matrix(3,3, lambda i,j: coeff[i] if tau[i]==j else 0)
```

```
[8]: transpositions = [[1,0,2],[2,1,0],[0,2,1]]
liste_coeff = [[1,1,zeta^k] for k in range(3)]
```

```
[9]: gen = [mat_permut(tau,coeff) for tau in transpositions for coeff in liste_coeff]
G313 = GL(3,K).subgroup(gen)
```

```
mat_g = 1/(zeta-zeta^2)*matrix(3,3,[[1,1,1],[1,zeta,zeta^2],[1,zeta^2,zeta]])
gen.append(mat_g)
G26 = GL(3,K).subgroup(gen)
oG26 = G26.order()
```

```
[10]: CG26 = G26.conjugacy_classes()
C9 = [c for c in CG26 if len(c) == 9]
c9 = C9[0]
```

```
[11]: lc9 = list(c9)
```

Pour  $h$  dans un système de générateurs de  $G_{26}$ , on calcule la permutation de  $\mathbb{H}$  agissant sur  $c_9$ .

```
[12]: def action_conjugaison(h,L):
      tmp = [L.index(h*L[i]*h^-1)+1 for i in range(len(L))]
      return PermutationGroupElement(tmp)
```

```
[13]: action_conjugaison(gen[7],lc9)
```

```
[13]: (1,7,2,8,9,6)(4,5)
```

```
[14]: Hp = PermutationGroup([action_conjugaison(h,lc9) for h in gen + [mat_g]])
Hp.order()
```

```
[14]: 216
```

```
[15]: F3 = GF(3)
GL33 = GL(3,F3)
gen_aff33 = [matrix(3,3,1).change_ring(F3) for l in
  ↳ [[0,-1,0],[1,0,0],[0,0,1]],[[1,1,0],[0,1,0],[0,0,1]],[[1,0,1],[0,1,0],[0,0,1]],[[1,0,0],[0,1,0],[0,0,1]]]
Aff33 = GL33.subgroup(gen_aff33)
Aff33.is_isomorphic(Hp)
```

```
[15]: True
```

Le groupe  $\mathbb{H}$  est bien isomorphe au groupe affine de  $\mathbb{F}_3^2$ .

Montrons que  $G_{26}$  est un groupe de réflexions complexe et dénombrons ses réflexions.

```
[16]: LG = list(G26)
RefG = [GL(3,K)(g) for g in LG if (g.matrix()-identity_matrix(3)).right_kernel().
  ↳ dimension() == 2]
len(RefG)
```

```
[16]: 33
```

```
[17]: Gprim = GL(3,K).subgroup(RefG)
Gprim.is_isomorphic(G26)
```

[17]: True

Le groupe  $G_{26}$  est bien un groupe de réflexions, qui en comporte 33. Les réflexions sont diagonalisables, ont deux valeurs propres égales à 1 et la troisième est une racine sixième de l'unité. On cherche donc d'abord des réflexions d'ordre 2, puis d'ordre 3 et enfin d'ordre 6.

```
[18]: R_ordre_2 = [r for r in RefG if (r^2).matrix() == identity_matrix(3)]  
len(R_ordre_2)
```

[18]: 9

```
[19]: R_ordre_3 = [r for r in RefG if (r^3).matrix() == identity_matrix(3)]  
len(R_ordre_3)
```

[19]: 24

Comme  $G_{26}$  comporte 33 réflexions, on les a toutes. Cherchons la classe de conjugaison de chaque réflexion selon son ordre.

Une réflexion d'ordre 2 est conjuguée à  $\text{diag}(1, 1, -1)$  dans  $\text{GL}_3(\mathbb{C})$ . Vérifions que ces réflexions sont toujours conjuguées dans  $G_{26}$ .

```
[20]: all(G26.conjugacy_class(r_2) == G26.conjugacy_class(R_ordre_2[0]) for r_2 in  
      ↪ R_ordre_2)
```

[20]: True

Une réflexion d'ordre 3 est conjuguée à  $\text{diag}(1, 1, \zeta)$  ou à  $\text{diag}(1, 1, \zeta^2)$  dans  $\text{GL}_3(\mathbb{C})$ . Vérifions que c'est toujours le cas dans  $G_{26}$ .

```
[21]: czeta = G26.conjugacy_class(R_ordre_3[12])  
czeta2 = G26.conjugacy_class(R_ordre_3[0])  
verif = True  
ind = 0  
while verif and ind < len(R_ordre_3):  
    classe = G26.conjugacy_class(R_ordre_3[ind])  
    verif = classe == czeta or classe == czeta2  
    ind += 1  
verif
```

[21]: True

```
[22]: len(czeta) == len(czeta2)
```

[22]: True

Les réflexions d'ordre 2 sont bien conjuguées deux à deux et les réflexions d'ordre 3 sont bien conjuguées à  $\text{diag}(1, 1, \zeta)$  ou à  $\text{diag}(1, 1, \zeta^2)$  dans  $G_{26}$ . Les deux classes dans le cas d'ordre 3 sont de plus de même cardinal.

```
[23]: hypref_2 = list(set([(r.matrix()-identity_matrix(3)).right_kernel()).basis()
    ↪for r in R_ordre_2]))
len(hypref_2)
```

[23]: 9

Toutes les réflexions d'ordre 2 sont associées à un hyperplan différent.

```
[24]: hypref_3 = list(set([(r.matrix()-identity_matrix(3)).right_kernel()).basis()
    ↪for r in R_ordre_3]))
len(hypref_3)
```

[24]: 12

Pour chaque réflexion  $r_1$  d'ordre 3, il existe une unique réflexion  $r_2$  d'ordre 3 dans l'autre classe de conjugaison telle que  $r_1$  et  $r_2$  stabilisent le même hyperplan.

Listes des axes de réflexion, axes orthogonaux aux hyperplans de réflexion

```
[25]: axeref_2 = [h[0].cross_product(h[1]) for h in hypref_2]
axeref_3 = [h[0].cross_product(h[1]) for h in hypref_3]
```

```
[26]: axeref_2
```

```
[26]: [(zeta, -1, 0),
      (zeta + 1, 0, 1),
      (-zeta, 0, 1),
      (-1, 0, 1),
      (0, -1, 1),
      (1, -1, 0),
      (-zeta - 1, -1, 0),
      (0, -zeta, 1),
      (0, zeta + 1, 1)]
```

```
[27]: axeref_3
```

```
[27]: [(0, 0, 1),
      (zeta, -zeta - 1, 1),
      (1, 0, 0),
      (zeta, 1, 1),
      (-zeta - 1, -zeta - 1, 1),
      (zeta, zeta, 1),
      (-zeta - 1, 1, 1),
      (-zeta - 1, zeta, 1),
      (1, -zeta - 1, 1),
      (0, -1, 0),
      (1, 1, 1),
      (1, zeta, 1)]
```

Les axes des réflexions d'ordre 2 s'identifient aux points du lieu de base et ceux des réflexions d'ordre 3 aux composantes irréductibles des courbes singulières du pinceau. Chaque réflexion d'ordre 2 fixe donc un unique point du lieu de base et chaque hyperplan de réflexion d'ordre 3 est orthogonal à une composante irréductible de courbe singulière.

## Action de $\mathbb{H}$ sur le pinceau

Test de stabilisation par  $\mathbb{H}$  du lieu de base

```
[28]: def egalite(p,q):
      xp,yp,zp = p
      xq,yq,zq = q
      return xp*yq-xq*yp == 0 and xp*zq-xq*zp == 0 and yp*zq-yq*zp == 0
```

```
[29]: def appartient(p,L):
      return any(egalite(p,l) for l in L)
```

```
[30]: all(appartient(h*p,ldb) for h in gen for p in ldb)
```

[30]: True

Implémentation de l'action: La première implémentation s'attarde sur les courbes et ne prend pas en compte une éventuelle multiplication par un scalaire. La seconde se focalise sur les polynômes et prend ce paramètre en compte.

```
[31]: def action_courbe(mat,f):
      [xt,yt,zt] = [x*mat[0][i]+y*mat[1][i]+z*mat[2][i] for i in range(3)]
      g = f.subs({x:xt, y:yt, z:zt})
      coeff_b = g.subs({x:zeta9, y:zeta9^2, z:1})*zeta^2
      if coeff_b != 0:
          return g/coeff_b
      else:
          return x^3+y^3+z^3

      def action_poly(mat,f):
          [xt,yt,zt] = [x*mat[0][i]+y*mat[1][i]+z*mat[2][i] for i in range(3)]
          g = f.subs({x:xt, y:yt, z:zt})
          return g
```

Homographie associée

```
[32]: def hom_associee(mat):
      eqp = action_courbe(mat,eq)
      val_a = eqp.subs({x:0, y:0, z:1})
      val_b = zeta^2*eqp.subs({x:zeta9, y:zeta9^2, z:1})
      dic_a = {b:0, a:1}
      dic_b = {a:0, b:1}
```

```

    return matrix(2,2,[[val_b.subs(dic_b),val_b.subs(dic_a)], [val_a.
↪subs(dic_b),val_a.subs(dic_a)]])

```

```
[33]: hom_associee(mat_g)
```

```
[33]: [ 1 1]
      [-1/3 1/6]
```

Stabilisation des courbes singulières

```
[34]: all(action_courbe(g,f) in sing for g in gen for f in sing)
```

```
[34]: True
```

Permutation des courbes singulières associée à un élément de  $\mathbb{H}$

```
[35]: def permut_sing(mat):
      tmp = [sing.index(action_courbe(mat,sing[i]))+1 for i in range(len(sing))]
      return PermutationGroupElement(tmp)

```

```
[36]: [permut_sing(g) for g in gen]
```

```
[36]: [(), (2,3,4), (2,4,3), (), (2,3,4), (2,4,3), (), (2,3,4), (2,4,3), (1,2)(3,4)]
```

Orbites d'une courbe par l'action de  $G_{26}$

```
[37]: def liste_action_courbe(f):
      L = []
      for g in LG:
          gf = action_courbe(g.matrix(),f)
          if not gf in L:
              L.append(gf)
      return L

      def liste_action_poly(f):
          L = []
          for g in LG:
              gf = action_poly(g.matrix(),f)
              if not gf in L:
                  L.append(gf)
          return L

```

```
[38]: len(liste_action_poly(eq.subs({a:0,b:1})))
```

```
[38]: 24
```

## Méthode « par en-dessous » pour trouver les invariants polynomiaux

Générateurs de l'algèbre des invariants par  $G(3,1,3)$

```
[39]: X,Y,Z = x^3,y^3,z^3
      t1,t2,t3 = X+Y+Z, X*Y+X*Z+Y*Z, X*Y*Z
```

Les degrés des invariants par  $G(3,1,3)$  sont donc des multiples de 3. Il n'y a pas d'invariants de degré impair car  $-I_3$  est un élément de  $G_{26}$ . On recherche donc des invariants par  $G_{26}$  de degré multiple non nul de 6.

Recherche d'invariants de degré 6

On commence par lister les éléments algébriquement indépendants de  $\mathbb{C}[\tau_1, \tau_2, \tau_3]$  (qui est  $S^{G(3,1,3)}$ ). Il y en a deux, que l'on note  $a_1$  et  $a_2$ . On les complète en une base d'un sous-espace vectoriel de  $S^6$  stable par  $g_0$ .

```
[40]: a1 = t1^2
      a2 = t2
```

```
[41]: u = (action_poly(mat_g,a1) - (-1/3*a1))/-4
      u
```

```
[41]: x^4*y*z + x*y^4*z + 3*x^2*y^2*z^2 + x*y*z^4
```

```
[42]: action_poly(mat_g,a2) - (-1/9*a1+a2-u/3)
```

```
[42]: 0
```

```
[43]: action_poly(mat_g,u) - (-2/9*a1+1/3*u)
```

```
[43]: 0
```

L'espace  $\text{Vect}(a_1, a_2, v)$  est un sous-espace vectoriel de  $S^6$  stable par  $g_0$ . Nous allons chercher un éventuel invariant de  $g_0$  à l'aide des éléments propres de sa matrice dans cet espace, qui s'écrit dans la base  $(a_1, a_2, v)$ ,

$$\begin{pmatrix} -1/3 & -1/9 & -2/9 \\ 0 & 1 & 0 \\ -4 & -1/3 & 1/3 \end{pmatrix}$$

.

```
[44]: mat_6 = matrix(3,3,[-1/3,-1/9,-2/9,0,1,0,-4,-1/3,1/3])
      print(mat_6,(mat_6 - identity_matrix(3)).right_kernel())
```

```
[-1/3 -1/9 -2/9]
[  0    1    0]
[-4 -1/3  1/3] Vector space of degree 3 and dimension 2 over Rational Field
Basis matrix:
[  1    0  -6]
[  0    1 -1/2]
```

Pour qu'un élément soit un invariant de  $G_{26}$ , il doit également être invariant par  $G(3,1,3)$ , donc être combinaison linéaire de  $a_1$  et  $a_2$ . À l'aide de la base calculée ci-dessus, on remarque que l'on a bien un invariant de degré 6, qui est  $f_6 := \tau_1^2 - 12\tau_2$ . Le script ci-dessous vérifie que  $f_6$  est invariant par un ensemble de générateurs donc par le groupe tout entier.

```
[45]: invb1 = t1^2-12*t2
      all(action_poly(g,invb1) == invb1 for g in gen)
```

[45]: True

Recherche des invariants de degré 12. Par confort, on ne construira plus dans la suite de base d'un espace stable par  $g_0$  mais on rsoudra simplement un système pour trouver des potentiels invariants.

On trouve quatre éléments algébriquement indépendants de degré 12 dans  $\mathbb{C}[\tau_1, \tau_2, \tau_3]$ .

```
[46]: b1 = t1^4
      b2 = t1^2*t2
      b3 = t2^2
      b4 = t1*t3
```

```
[47]: action_poly(mat_g,b1) - (1/9*b1 + 96*b4)
```

[47]:  $8/3*x^{10}*y*z + 8*x^7*y^4*z + 8*x^4*y^7*z + 8/3*x*y^{10}*z + 24*x^8*y^2*z^2 + 48*x^5*y^5*z^2 + 24*x^2*y^8*z^2 + 8*x^7*y*z^4 + 160*x^4*y^4*z^4 + 8*x*y^7*z^4 + 48*x^5*y^2*z^5 + 48*x^2*y^5*z^5 + 8*x^4*y*z^7 + 8*x*y^4*z^7 + 24*x^2*y^2*z^8 + 8/3*x*y*z^{10}$

```
[48]: action_poly(mat_g,b2) - (1/27*b1 - 1/3*b2 + 8*b4)
```

[48]:  $5/9*x^{10}*y*z - 7/3*x^7*y^4*z - 7/3*x^4*y^7*z + 5/9*x*y^{10}*z + 3*x^8*y^2*z^2 - 6*x^5*y^5*z^2 + 3*x^2*y^8*z^2 - 7/3*x^7*y*z^4 + 10/3*x^4*y^4*z^4 - 7/3*x*y^7*z^4 - 6*x^5*y^2*z^5 - 6*x^2*y^5*z^5 - 7/3*x^4*y*z^7 - 7/3*x*y^4*z^7 + 3*x^2*y^2*z^8 + 5/9*x*y*z^{10}$

```
[49]: action_poly(mat_g,b3) - (1/81*b1 - 2/9*b2 + b3 + 2/3*b4)
```

[49]:  $2/27*x^{10}*y*z - 4/9*x^7*y^4*z - 4/9*x^4*y^7*z + 2/27*x*y^{10}*z + 1/3*x^8*y^2*z^2 - 4/3*x^5*y^5*z^2 + 1/3*x^2*y^8*z^2 - 4/9*x^7*y*z^4 - 5/9*x^4*y^4*z^4 - 4/9*x*y^7*z^4 - 4/3*x^5*y^2*z^5 - 4/3*x^2*y^5*z^5 - 4/9*x^4*y*z^7 - 4/9*x*y^4*z^7 + 1/3*x^2*y^2*z^8 + 2/27*x*y*z^{10}$

```
[50]: action_poly(mat_g,b4) - (1/243*b1 + 5/9*b4)
```

[50]:  $-1/81*x^{10}*y*z - 1/27*x^7*y^4*z - 1/27*x^4*y^7*z - 1/81*x*y^{10}*z - 1/9*x^8*y^2*z^2 - 2/9*x^5*y^5*z^2 - 1/9*x^2*y^8*z^2 - 1/27*x^7*y*z^4 - 20/27*x^4*y^4*z^4 - 1/27*x*y^7*z^4 - 2/9*x^5*y^2*z^5 - 2/9*x^2*y^5*z^5 - 1/27*x^4*y*z^7 - 1/27*x*y^4*z^7 - 1/9*x^2*y^2*z^8 - 1/81*x*y*z^{10}$

Un invariant de  $g_0$  de la forme  $pb_1 + qb_2 + rb_3 + sb_4$  doit nécessairement vérifier le système suivant:

$$\begin{cases} 1/9p + 1/27q + 1/81r + 1/243s = p \\ -1/3q - 2/9r = q \\ 96p + 8q + 2/3r + 5/9s = s \end{cases}$$

(la condition  $r = r$  induite par le fait que  $b_3$  n'apparaît que dans  $g_0 \cdot b_3$  étant inutile).

```
[51]: var('p,q,r,s')
eq1 = 1/9*p + 1/27*q + 1/81*r + 1/243*s == p
eq2 = -1/3*q -2/9*r == q
eq3 = 96*p + 8*q + 2/3*r + 5/9*s == s
solve([eq1,eq2,eq3],p,q,r,s)
```

```
[51]: [[p == 1/216*r1 + 1/144*r2, q == -1/6*r2, r == r2, s == r1]]
```

Les solutions du système ne sont pas forcément des invariants. Si on note  $p_b$  un projecteur de  $S^6$  sur  $\text{Vect}(b_1, b_2, b_3, b_4)$ , on sait seulement qu'une solution  $f_b$  du système vérifie  $p_b \circ g_0 \cdot f_b = f_b$ . Il faut vérifier que  $g_0 \cdot f_b = f_b$ . L'espace des solutions du système est de dimension 2 et on sait déjà que  $b_1 - 24b_2 + 144b_3 = f_6^2$  est invariant par  $G_{26}$ . On peut donc par exemple vérifier que  $b_1 + 216b_4$  l'est aussi.

```
[52]: invb2 = b1+216*b4
all(action_poly(g,invb2) == invb2 for g in gen)
```

```
[52]: True
```

On a bien un autre invariant de degré 12, qui est  $f_{12} := \tau_1^4 + 216\tau_1\tau_3$ .

Recherche d'invariants de degré 18

L'espace  $\mathbb{C}[\tau_1, \tau_2, \tau_3]$  comporte au plus sept polynômes algébriquement indépendants de degré 18, qui sont par exemple ceux ci-dessous.

```
[53]: c1 = t1^6
c2 = t1^4*t2
c3 = t1^3*t3
c4 = t1^2*t2^2
c5 = t1*t2*t3
c6 = t2^3
c7 = t3^2
```

```
[54]: action_poly(mat_g,c1) - (-1/27*c1 - 160*c3 - 1728*c7)
```

```
[54]: -4/3*x^16*y*z - 20/3*x^13*y^4*z - 40/3*x^10*y^7*z - 40/3*x^7*y^10*z -
20/3*x^4*y^13*z - 4/3*x*y^16*z - 20*x^14*y^2*z^2 - 80*x^11*y^5*z^2 -
120*x^8*y^8*z^2 - 80*x^5*y^11*z^2 - 20*x^2*y^14*z^2 - 20/3*x^13*y*z^4 -
2240/3*x^10*y^4*z^4 - 1480*x^7*y^7*z^4 - 2240/3*x^4*y^10*z^4 - 20/3*x*y^13*z^4 -
80*x^11*y^2*z^5 - 1968*x^8*y^5*z^5 - 1968*x^5*y^8*z^5 - 80*x^2*y^11*z^5 -
40/3*x^10*y*z^7 - 1480*x^7*y^4*z^7 - 1480*x^4*y^7*z^7 - 40/3*x*y^10*z^7 -
120*x^8*y^2*z^8 - 1968*x^5*y^5*z^8 - 120*x^2*y^8*z^8 - 40/3*x^7*y*z^10 -
2240/3*x^4*y^4*z^10 - 40/3*x*y^7*z^10 - 80*x^5*y^2*z^11 - 80*x^2*y^5*z^11 -
20/3*x^4*y*z^13 - 20/3*x*y^4*z^13 - 20*x^2*y^2*z^14 - 4/3*x*y*z^16
```

```
[55]: action_poly(mat_g,c2) - (-1/81*c1 + 1/9*c2 - 64/3*c3 + 96*c5 - 144*c7)
```

$$\begin{aligned}
[55]: & -1/3*x^{16}*y*z + x^{13}*y^4*z + 14/3*x^{10}*y^7*z + 14/3*x^7*y^{10}*z + x^4*y^{13}*z - \\
& 1/3*x*y^{16}*z - 11/3*x^{14}*y^2*z^2 + 28/3*x^{11}*y^5*z^2 + 26*x^8*y^8*z^2 + \\
& 28/3*x^5*y^{11}*z^2 - 11/3*x^2*y^{14}*z^2 + x^{13}*y*z^4 - 60*x^{10}*y^4*z^4 + \\
& 22*x^7*y^7*z^4 - 60*x^4*y^{10}*z^4 + x*y^{13}*z^4 + 28/3*x^{11}*y^2*z^5 - \\
& 68*x^8*y^5*z^5 - 68*x^5*y^8*z^5 + 28/3*x^2*y^{11}*z^5 + 14/3*x^{10}*y*z^7 + \\
& 22*x^7*y^4*z^7 + 22*x^4*y^7*z^7 + 14/3*x*y^{10}*z^7 + 26*x^8*y^2*z^8 - \\
& 68*x^5*y^5*z^8 + 26*x^2*y^8*z^8 + 14/3*x^7*y*z^{10} - 60*x^4*y^4*z^{10} + \\
& 14/3*x*y^7*z^{10} + 28/3*x^5*y^2*z^{11} + 28/3*x^2*y^5*z^{11} + x^4*y*z^{13} + \\
& x*y^4*z^{13} - 11/3*x^2*y^2*z^{14} - 1/3*x*y*z^{16}
\end{aligned}$$

$$[56]: \text{action\_poly}(\text{mat\_g}, c3) - (-1/729*c1 + 11/27*c3 + 8*c7)$$

$$\begin{aligned}
[56]: & -1/81*x^{16}*y*z - 5/81*x^{13}*y^4*z - 10/81*x^{10}*y^7*z - 10/81*x^7*y^{10}*z - \\
& 5/81*x^4*y^{13}*z - 1/81*x*y^{16}*z + 1/27*x^{14}*y^2*z^2 + 4/27*x^{11}*y^5*z^2 + \\
& 2/9*x^8*y^8*z^2 + 4/27*x^5*y^{11}*z^2 + 1/27*x^2*y^{14}*z^2 - 5/81*x^{13}*y*z^4 - \\
& 74/81*x^{10}*y^4*z^4 - 46/27*x^7*y^7*z^4 - 74/81*x^4*y^{10}*z^4 - 5/81*x*y^{13}*z^4 + \\
& 4/27*x^{11}*y^2*z^5 - 32/9*x^8*y^5*z^5 - 32/9*x^5*y^8*z^5 + 4/27*x^2*y^{11}*z^5 - \\
& 10/81*x^{10}*y*z^7 - 46/27*x^7*y^4*z^7 - 46/27*x^4*y^7*z^7 - 10/81*x*y^{10}*z^7 + \\
& 2/9*x^8*y^2*z^8 - 32/9*x^5*y^5*z^8 + 2/9*x^2*y^8*z^8 - 10/81*x^7*y*z^{10} - \\
& 74/81*x^4*y^4*z^{10} - 10/81*x*y^7*z^{10} + 4/27*x^5*y^2*z^{11} + 4/27*x^2*y^5*z^{11} - \\
& 5/81*x^4*y*z^{13} - 5/81*x*y^4*z^{13} + 1/27*x^2*y^2*z^{14} - 1/81*x*y*z^{16}
\end{aligned}$$

$$[57]: \text{action\_poly}(\text{mat\_g}, c4) - (-1/243*c1 + 2/27*c2 - 1/3*c4 - 22/9*c3 + 16*c5 - 12*c7)$$

$$\begin{aligned}
[57]: & -2/27*x^{16}*y*z + 20/27*x^{13}*y^4*z - 38/27*x^{10}*y^7*z - 38/27*x^7*y^{10}*z + \\
& 20/27*x^4*y^{13}*z - 2/27*x*y^{16}*z - 5/9*x^{14}*y^2*z^2 + 34/9*x^{11}*y^5*z^2 - \\
& 10/3*x^8*y^8*z^2 + 34/9*x^5*y^{11}*z^2 - 5/9*x^2*y^{14}*z^2 + 20/27*x^{13}*y*z^4 - \\
& 235/27*x^{10}*y^4*z^4 + 10/9*x^7*y^7*z^4 - 235/27*x^4*y^{10}*z^4 + 20/27*x*y^{13}*z^4 + \\
& 34/9*x^{11}*y^2*z^5 - 38/3*x^8*y^5*z^5 - 38/3*x^5*y^8*z^5 + 34/9*x^2*y^{11}*z^5 - \\
& 38/27*x^{10}*y*z^7 + 10/9*x^7*y^4*z^7 + 10/9*x^4*y^7*z^7 - 38/27*x*y^{10}*z^7 - \\
& 10/3*x^8*y^2*z^8 - 38/3*x^5*y^5*z^8 - 10/3*x^2*y^8*z^8 - 38/27*x^7*y*z^{10} - \\
& 235/27*x^4*y^4*z^{10} - 38/27*x*y^7*z^{10} + 34/9*x^5*y^2*z^{11} + 34/9*x^2*y^5*z^{11} + \\
& 20/27*x^4*y*z^{13} + 20/27*x*y^4*z^{13} - 5/9*x^2*y^2*z^{14} - 2/27*x*y*z^{16}
\end{aligned}$$

$$[58]: \text{action\_poly}(\text{mat\_g}, c5) - (-1/2187*c1 + 1/243*c2 - 1/81*c3 + 5/9*c5 + 2/3*c7)$$

$$\begin{aligned}
[58]: & -1/81*x^{13}*y^4*z - 1/27*x^{10}*y^7*z - 1/27*x^7*y^{10}*z - 1/81*x^4*y^{13}*z + \\
& 1/81*x^{14}*y^2*z^2 - 5/81*x^{11}*y^5*z^2 - 4/27*x^8*y^8*z^2 - 5/81*x^5*y^{11}*z^2 + \\
& 1/81*x^2*y^{14}*z^2 - 1/81*x^{13}*y*z^4 - 7/81*x^{10}*y^4*z^4 - 22/27*x^7*y^7*z^4 - \\
& 7/81*x^4*y^{10}*z^4 - 1/81*x*y^{13}*z^4 - 5/81*x^{11}*y^2*z^5 - 20/27*x^8*y^5*z^5 - \\
& 20/27*x^5*y^8*z^5 - 5/81*x^2*y^{11}*z^5 - 1/27*x^{10}*y*z^7 - 22/27*x^7*y^4*z^7 - \\
& 22/27*x^4*y^7*z^7 - 1/27*x*y^{10}*z^7 - 4/27*x^8*y^2*z^8 - 20/27*x^5*y^5*z^8 - \\
& 4/27*x^2*y^8*z^8 - 1/27*x^7*y*z^{10} - 7/81*x^4*y^4*z^{10} - 1/27*x*y^7*z^{10} - \\
& 5/81*x^5*y^2*z^{11} - 5/81*x^2*y^5*z^{11} - 1/81*x^4*y*z^{13} - 1/81*x*y^4*z^{13} + \\
& 1/81*x^2*y^2*z^{14}
\end{aligned}$$

$$[59]: \text{action\_poly}(\text{mat\_g}, c6) - (-1/729*c1 + 1/27*c2 - 1/3*c4 + c6 - 7/27*c3 + 2*c5 - c7)$$

```
[59]: -1/81*x^16*y*z + 13/81*x^13*y^4*z - 37/81*x^10*y^7*z - 37/81*x^7*y^10*z +
13/81*x^4*y^13*z - 1/81*x*y^16*z - 2/27*x^14*y^2*z^2 + 19/27*x^11*y^5*z^2 -
13/9*x^8*y^8*z^2 + 19/27*x^5*y^11*z^2 - 2/27*x^2*y^14*z^2 + 13/81*x^13*y*z^4 -
110/81*x^10*y^4*z^4 - 28/27*x^7*y^7*z^4 - 110/81*x^4*y^10*z^4 + 13/81*x*y^13*z^4
+ 19/27*x^11*y^2*z^5 - 26/9*x^8*y^5*z^5 - 26/9*x^5*y^8*z^5 + 19/27*x^2*y^11*z^5
- 37/81*x^10*y*z^7 - 28/27*x^7*y^4*z^7 - 28/27*x^4*y^7*z^7 - 37/81*x*y^10*z^7 -
13/9*x^8*y^2*z^8 - 26/9*x^5*y^5*z^8 - 13/9*x^2*y^8*z^8 - 37/81*x^7*y*z^10 -
110/81*x^4*y^4*z^10 - 37/81*x*y^7*z^10 + 19/27*x^5*y^2*z^11 + 19/27*x^2*y^5*z^11
+ 13/81*x^4*y*z^13 + 13/81*x*y^4*z^13 - 2/27*x^2*y^2*z^14 - 1/81*x*y*z^16
```

```
[60]: action_poly(mat_g,c7) - (-1/19683*c1 + 20/729*c3 -1/27*c7)
```

```
[60]: 2/2187*x^16*y*z + 10/2187*x^13*y^4*z + 20/2187*x^10*y^7*z + 20/2187*x^7*y^10*z +
10/2187*x^4*y^13*z + 2/2187*x*y^16*z - 5/729*x^14*y^2*z^2 - 20/729*x^11*y^5*z^2
- 10/243*x^8*y^8*z^2 - 20/729*x^5*y^11*z^2 - 5/729*x^2*y^14*z^2 +
10/2187*x^13*y*z^4 - 95/2187*x^10*y^4*z^4 - 70/729*x^7*y^7*z^4 -
95/2187*x^4*y^10*z^4 + 10/2187*x*y^13*z^4 - 20/729*x^11*y^2*z^5 -
2/243*x^8*y^5*z^5 - 2/243*x^5*y^8*z^5 - 20/729*x^2*y^11*z^5 + 20/2187*x^10*y*z^7
- 70/729*x^7*y^4*z^7 - 70/729*x^4*y^7*z^7 + 20/2187*x*y^10*z^7 -
10/243*x^8*y^2*z^8 - 2/243*x^5*y^5*z^8 - 10/243*x^2*y^8*z^8 + 20/2187*x^7*y*z^10
- 95/2187*x^4*y^4*z^10 + 20/2187*x*y^7*z^10 - 20/729*x^5*y^2*z^11 -
20/729*x^2*y^5*z^11 + 10/2187*x^4*y*z^13 + 10/2187*x*y^4*z^13 -
5/729*x^2*y^2*z^14 + 2/2187*x*y*z^16
```

On réapplique la méthode du degré 12 pour trouver des invariants.

```
[61]: var('p,q,r,s,t,v,w')
eq1 = -1/27*p - 1/81*q - 1/729*r - 1/243*s - 1/2187*t - 1/729*v - 1/19683*w == p
eq2 = 1/9*q + 2/27*s + 1/243*t + 1/27*v == q
eq3 = -160*p - 64/3*q + 11/27*r - 22/9*s - 1/81*t - 7/27*v + 20/729*w == r
eq4 = -1/3*s - 1/3*v == s
eq5 = 96*q + 16*s + 5/9*t + 2*v == t
eq6 = -1728*p - 144*q + 8*r - 12*s + 2/3*t - v - 1/27*w == w
solve([eq1,eq2,eq3,eq4,eq5,eq6],p,q,r,s,t,v,w)
```

```
[61]: [[p == -1/5832*r3 - 1/1728*r4 - 1/2592*r5,
q == 1/48*r4 + 1/216*r5,
r == 5/54*r3 - 1/12*r5,
s == -1/4*r4,
t == r5,
v == r4,
w == r3]]
```

L'espace des solutions du système est de dimension 3 et comme précédemment on sait que les polynômes donnés par les ctriplets (0, 1, 0) et (0, 0, 1) sont des invariants. On peut donc vérifier que celui donné par le triplet (1, 0, 0) (ou  $(-5832, 0, 0)$ ) est un invariant.

```
[62]: invb3 = -1/5832*c1+5/54*c3+c7
      all(action_poly(g,invb3) == invb3 for g in gen)
```

[62]: True

On a bien trouvé un troisième invariant, qui est  $f_{18} := \tau_1^6 - 540\tau_1^3\tau_3 - 5832\tau_3^2$ .

Si on arrive à montrer que  $f_6$ ,  $f_{12}$  et  $f_{18}$  sont algébriquement indépendants et qu'ils engendrent bien l'ensemble  $S^{G_{26}}$ , on aura montré grâce au théorème de Shephard-Todd/Chevalley-Serre que  $G_{26}$  est un groupe de réflexions.

## Méthode « Par au-dessus » pour trouver les invariants polynomiaux

```
[63]: def calcule_carac(h,n):
      trace = 0
      for i in range(n+1):
          for j in range(n+1-i):
              P = action_poly(h,x**i*y**j*z**(n-i-j))
              trace += P.coefficient(x**i*y**j*z**(n-i-j))
      return trace
```

```
[64]: def deg_inv(n):
      deg = 0
      for c in CG26:
          deg += calcule_carac(c[0].matrix(),n)*len(c)
      return deg/oG26
```

```
[65]: [deg_inv(3*n) for n in range(7)]
```

[65]: [1, 0, 1, 0, 2, 0, 3]

```
[66]: sum(i for i in range(3))
```

[66]: 3

```
[67]: def projecteur(f):
      return sum(action_poly(l.matrix(),f) for l in LG)/oG26
```

```
[68]: invh1 = projecteur(x^6+y^6+z^6)
      invh2 = projecteur(x^12+y^12+z^12)
      invh3 = projecteur(x^18+y^18+z^18)
```

## Vérification de l'indépendance algébrique

```
[69]: def jac(L):
      return matrix(3,3,[[diff(l,ww) for l in L] for ww in [x,y,z]])
```

```
[70]: jac([invb1,invb2,invb3]).det() != 0
```

```
[70]: True
```

```
[71]: jac([invh1,invh2,invh3]).det() != 0
```

```
[71]: True
```

Les invariants trouvés avec les deux méthodes sont bien algébriquement indépendants.

## Utilisation de la formule de Molien pour montrer que les invariants de degré 6, 12 et 18 engendrent $S^{G_{26}}$

```
[72]: molien = 0
      for c in CG26:
          molien += len(c)/(identity_matrix(3)-x*c[0]).det()
      molien/oG26 == 1/((1-x^6)*(1-x^12)*(1-x^18))
```

```
[72]: True
```

Les polynômes trouvés avec les deux méthodes engendrent donc bien  $S^{G_{26}}$ . Comme ceux-ci sont algébriquement indépendants, par le théorème de Shephard-Todd/Chevalley-Serre,  $G_{26}$  est bien un groupe de réflexions.