Ecole Normale Supérieure de Paris
FIMFA

Introduction au domaine de recherche

Morphismes et diviseurs sur les courbes algébriques Spécificité des courbes elliptiques

Marc Kamal HAIDAR

octobre 2009

Table des matières

1 Curriculum Vitae

Parcours professionnel

2009/2010 Professeur de mathématiques (titulaire) en sections internationales
au lycée Jean-Pierre Vernant de Sèvres (92).
Interrogateur en CPGE (MPSI et MP) au lycée Hoche.
2008/2009 Professeur de mathématiques (TZR) au lycée Agora de Puteaux (92).
Interrogateur en CPGE (MPSI et MP) au lycée Hoche.
Préparateur au Concours Général de Mathématiques pour l'académie de Versailles.
2007/2008 Formation à l'IUFM de Saint-Germain-en-Laye (académie de Versailles).
Professeur de mathématiques stagiaire (IUFM) au lycée Hoche de Versailles (78).
Préparateur au Concours Général de Mathématiques et aux Olympiades Académiques pour le lycée Hoche.
2006/2007 Interrogateur en CPGE (MPSI) aux lycées Hoche et Louis-le-Grand.
2005/2006 Interrogateur en CPGE (MPSI) aux lycées Hoche et Louis-le-Grand.

Parcours étudiant

2007/2009 Master II d'Algèbre Appliquée Mention Très Bien (Université de Versailles)
(validation de la partie informatique en 2009 et de la partie mathématique en 2008).
2006/2007 Agrégation de mathématiques (préparation dans les ENS Cachan et Ulm)
2005/2006 Maîtrise de mathématiques fondamentales (ENS Ulm - Université Paris VII).
2004/2005 Licence de mathématiques Mention Très Bien (Université de Versailles).
2003/2004 MPSI au lycée Hoche.
2003 Baccalauréat Scientifique Mention Bien (Lycée Hoche).

Parcours FIMFA

Master II d'Algèbre Appliquée (sous la direction de Vincent Cossart) :
- Mémoire de Master II sous la direction de Mireille Martin-Deschamps :
"*Classification des courbes elliptiques par la géométrie algébrique et l'analyse complexe*".
- Courbes elliptiques (Mireille Martin-Deschamps)
- Courbes algébriques (Arianne Mézard)
- Algèbre commutative et effectivité (Mireille Martin-Deschamps)
- Algorithmique et langage C I et II (Antoine Joux)
- Algorithmes avancés de la cryptographie - Cryptanalyse (Jacques Patarin)
- Complexité algébrique et cryptographie (Louis Goubin)

Maîtrise de Mathématiques Fondamentales (ENS Ulm) :
- Exposé de Maîtrise sous la direction d'Ariane Mézard : "*Déformations de représentations galoisiennes*"
- Intégration et probabilités (Jean-François Legall)
- Algèbre I (François Loeser)
- Topologie et Analyse Différentielle (Benoît Perthame)
- Analyse Complexe (Georges Skandalis)
- Algèbre II (Marc Rosso)
- Processus aléatoires (Jean-François Legall)
- Analyse fonctionnelle et EDP (Stéphane Mischler)

Groupe de travail : Algèbre et géométrie (Frédéric Paulin).
Russe niveau intermédiaire (Olga Chtcherbakova).

2 Introduction au domaine de recherche

2.1 Introduction

Cette introduction au domaine de recherche se doit d'être replacée dans son contexte, c'est-à-dire celui de mon mémoire de master II. Ce dernier traite de la classification des courbes elliptiques, à l'aide d'outils issus de la géométrie algébrique et de l'analyse complexe (pour les courbes elliptiques définies sur $\mathbb{C}$). L'ouvrage sur lequel s'est effectué principalement tout mon travail est le livre "Algebraic Geometry" de Robin Hartshorne [Har77].
Dans un premier temps, on commencera par définir une notion fondamentale, celle de *courbe algébrique projective*, autour de laquelle s'articule toute la théorie de ce mémoire. Les courbes algébriques projectives sont des objets géométriques remarquables à partir desquels a été élaborée la géométrie algébrique. Les notions de *diviseur algébrique* et de *genre* seront les notions essentielles de cette première partie.
Dans un second temps, on traitera d'une classe particulière de courbes algébriques projectives : *les courbes elliptiques*. Ces courbes possèdent de nombreuses propriétés remarquables, que ce soit de par leur structure ou leurs applications. On peut par exemple citer la conjecture de Shimura-Taniyama-Weil, concernant des courbes elliptiques sur $\mathbb{Q}$, qui a permis à Andrew Wiles de conclure la démonstration du grand théorème de Fermat (on renvoit le lecteur à l'article [Dar99] qui liste les idées-clés de la démonstration) et qui a motivé mon orientation vers la géométrie algébrique. En effet, c'est en travaillant avec Ariane Mézard, qui a dirigé mon mémoire de maîtrise, que s'est réveillé mon engouement pour la géométrie algébrique ainsi que ma volonté de tenter de comprendre le théorème de Fermat.

2.2 Courbes algébriques

On rappelle brièvement la notion de variété algébrique et on renvoit le lecteur vers [Sil86] ou vers [Méz07] pour tout complément sur ce sujet.
Dans toute cette partie, k désigne un corps parfait et $\overline{k}$ sa clôture algébrique.

2.2.1 Définitions

Définition 1. Soit I un idéal homogène de $\overline{k}[X]$ (i.e. engendré par des polynômes homogènes).
On appelle **ensemble (algébrique) projectif** tout ensemble de la forme :

$$V_I = \{P \in \mathbb{P}^n,\ \forall f \in I \text{ homogène},\ f(P) = 0\}$$

Si V est un ensemble projectif, on appelle **idéal homogène de V**, noté $I(V)$, l'idéal engendré par :

$$\{f \in \overline{k}[X] \text{ homogène},\ \forall P \in V,\ f(P) = 0\}$$

On peut alors définir la notion de variété projective :

Définition 2. Un ensemble projectif V est appelé **variété projective** si l'idéal homogène $I(V)$ est premier dans $\overline{k}[X]$.
On dit qu'elle est **définie** sur k si $I(V)$ est engendré par des polynômes à coefficients dans k.

Remarque 1. On peut vérifier que l'intersection d'ensembles projectifs est un ensemble projectif.
On peut alors définir une topologie sur $\mathbb{P}^n$, appelée **topologie de Zariski**, en prenant comme ouverts les complémentaires des ensembles projectifs.
Dans ce cas, les fermés irréductibles sont exactements les variétés projectives définies ci-dessus.

Afin de définir ce qu'est une courbe, il est nécessaire de préciser la notion de dimension d'une variété :

Définition 3. La **dimension** d'une variété projective V de $\mathbb{P}^n$ est le degré de transcendance de $\overline{k}(V)$ sur $\overline{k}$, où $\overline{k}(V)$ désigne :

$$\overline{k}(V) = \{F/G | F, G \in \overline{k}[X_0, \ldots, X_n] \text{ homogènes de même degré, } G \notin I(V)\}/\sim$$

avec $F/G \sim F'/G' \Leftrightarrow FG' - F'G \in I(V)$.
Le corps $\overline{k}(V)$ est appelé **corps de fonctions** de la variété V.

Remarque 2. De la même façon, pour une variété V définie sur k, on pourrait définir le **corps des fonctions** $k(V)$ de V sur k, en remplaçant $\overline{k}$ par k dans les définitions précédentes.

Définition 4. Une **courbe algébrique projective** de $\mathbb{P}^n$ est une variété projective de dimension 1.

Pour utiliser le vocabulaire des catégories, l'objet *courbe projective* étant défini, on peut maintenant définir la notion de *morphisme de courbes.*

Définition 5. Soient C_1 et C_2 deux courbes définies sur k.
Soient $f_0, \ldots, f_m \in k(C_1)$ des fonctions sur C_1 non toutes nulles.
On définit une application ϕ d'une partie de C_1 dans $\mathbb{P}^m$ de la manière suivante :
Soit P un point de C_1. S'il existe $h \in k(C_1)$ tel que les hf_i soient définis et non tous nuls en P, on pose

$$\phi(P) = [hf_0(P), \ldots, hf_m(P)]$$

(on vérifie que cela *ne dépend pas* du choix de h).
On dit que ϕ est une **application rationnelle** (définie sur k) de C_1 dans $\mathbb{P}^m$.
Si $\phi(P)$ est défini pour tout point P de C_1, on dit que ϕ est un **morphisme**.

Mon domaine de recherche ne s'intéressant qu'à des courbes projectives dites *lisses*, il est maintenant question de définir cette notion. On ne cherchera pas à définir la notion de lissité d'une variété projective, mais plutôt à retenir le résultat 7 ci-dessous qui concerne le cas particulier des variétés de dimension 1, i.e. les courbes. Pour cela il nous faut définir ce qu'est un anneau de *valuation discrète.*

Définition 6. On appelle **anneau de valuation discrète**, tout anneau commutatif, unitaire, intègre, principal et possédant un unique idéal premier.

Sur un tel anneau A, il on peut définir une application $v : A \to \mathbb{Z} \cup \{\infty\}$ telle que :

$$\begin{cases} v(x) = \infty \Leftrightarrow x = 0 \\ \forall (x, y) \in A^2,\ v(xy) = v(x) + v(y) \\ \forall (x, y) \in A^2,\ v(x + y) \geq \min(v(x), v(y)) \\ \exists t \in A, v(t) = 1 \end{cases}$$

Proposition 7. *Soit C une courbe projective et soit $P \in C$.*
La courbe C est lisse en P si et seulement si l'anneau local $k[C]_P$ est un anneau de valuation discrète, où :

$$k[C]_P = \{f \in k(C),\ f \text{ est définie en } P\}$$

Si P est un point lisse de C, toute fonction $f \in k(C)^\star$ s'écrit de manière unique $f = ut^n$ où :
• $n \in \mathbb{Z}$,
• $u \in k[C]_P^\star$
• t est une **uniformisante** en P, i.e. un générateur de l'idéal principal $M_P = \{f \in k[C]_P, f(P) = 0\}$.
L'entier n, noté $\mathrm{ord}_P(f)$ est appelé **ordre en P** de f.
On pourra vérifier sans effort que l'application $\mathrm{ord}_P : f \mapsto \mathrm{ord}_P(f)$ est une valuation.

Remarque 3. On ne parlera pas ici de la notion de lissité en un point d'une variété projective V (celle-ci étant liée à celle d'une variété affine V', elle-même définie à partir du rang de la jacobienne en ce point d'une famille de générateurs de l'idéal $I(V')$).

2.2.2 Diviseurs sur une courbe

L'objet de ce paragraphe est d'introduire la notion de diviseur sur une courbe, qui va nous permettre par la suite de définir une arithmétique sur les courbes elliptiques.

Définition 8. On appelle **groupe des diviseurs** d'une courbe lisse C, noté $\mathrm{Div}(C)$, le groupe abélien libre engendré par les points de C.
Le **degré d'un diviseur** $D = \sum_{P \in C} n_P(P)$, où les $n_P \in \mathbb{Z}$ sont presque tous nuls, est $\deg D = \sum_{P \in C} n_P$.
Son **support** est l'ensemble des points $P \in C$ tels que $n_P \neq 0$.

Définition 9. (i) Les diviseurs de degré 0 forment un **sous-groupe** noté $\mathrm{Div}^0(C)$.

(ii) Soit $f \in k(C)$ une fonction non nulle. On lui associe le diviseur :

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$$

(la somme est bien définie car les $\mathrm{ord}_P f$ sont presque tous nuls)
Un tel diviseur est appelé **diviseur principal**.
L'ensemble des diviseurs principaux est un sous-groupe de $\mathrm{Div}(C)$; le quotient de $\mathrm{Div}(C)$ par ce sous-groupe est appelé **groupe de Picard** de C, noté $\mathrm{Pic}(C)$.

Remarque 4. Si $f \notin \overline{k}$, alors $\mathrm{div}(f) \neq 0$.

Définition 10. (i) On dit qu'un diviseur $D = \sum_{P \in C} n_P(P)$ est **effectif**, et on note $D \geq 0$ si :

$$\forall P \in C,\ n_p \geq 0.$$

(ii) On dit que les diviseurs D_1 et D_2 sont **linéairement équivalents**, noté $D_1 \sim D_2$, si le diviseur $D_1 - D_2$ est principal.

2.2.3 Théorème de Riemann-Roch

Ce paragraphe est dédiée au résultat le plus important concernant les diviseurs sur une courbe : le *théorème de Riemann-Roch*, permettant de classer les courbes suivant leur *genre*.
Auparavant, il est nécessaire d'introduire les espaces $\mathcal{L}(D)$ qui interviennent dans le théorème de Riemann-Roch.

Définition 11. Soit C une courbe lisse et soit $D \in \mathrm{Div}(C)$. On lui associe l'ensemble de fonctions :

$$\mathcal{L}(D) = \{f \in \overline{k}(C)^*,\ \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

La proposition suivante résume les propriétés de $\mathcal{L}(D)$:

Proposition 12. *Soit C une courbe lisse et soit $D \in \mathrm{Div}(C)$.*

(i) $\mathcal{L}(D)$ est un espace vectoriel sur k de dimension finie notée $l(D)$.

(ii) Si $\deg D < 0$, $\mathcal{L}(D) = \{0\}$, $l(D) = 0$.

(iii) Si $D,\ D' \in \mathrm{Div}(C)$ sont linéairement équivalents, alors $\mathcal{L}(D)$ et $\mathcal{L}(D')$ sont isomorphes.

(iv) Si $D,\ D' \in \mathrm{Div}(C)$ vérifient $D \leq D'$, alors $\mathcal{L}(D) \subset L(D')$ et :

$$\dim \mathcal{L}(D')/\mathcal{L}(D) \leq \deg D' - \deg D$$

Théorème 13. *<Théorème de Riemann-Roch>*
Soient C une courbe lisse. Alors il existe un diviseur K_C, appelé ***diviseur canonique****, et un entier $g > 0$, appelé* ***genre*** *de C , tel que pour tout diviseur $D \in \mathrm{Div}(C)$ on ait :*

$$l(D) = \deg(D) + 1 - g + l(K_C - D)$$

Remarque 5. On n'explicitera pas ici la notion de diviseur canonique, intimement liée à la notion de différentielle sur une courbe, et on renvoit le lecteur à [Sil86] pour de plus amples informations à ce sujet. On peut cependant déduire du théorème de Riemann-Roch quelques propriétés utiles sur les diviseurs canoniques pour la suite.

Corollaire 14. *Avec les notations précédentes, on a :*

(i) $l(K_C) = g$ *et* $\deg(K_C) = 2g - 2$.

(ii) Si $\deg(D) > 2g - 2$ *alors* $l(D) = \deg(D) + 1 - g$.

2.2.4 Résultats fondamentaux

Bien que ne figurant pas dans cette partie, le théorème de Riemann-Roch y mériterait une place de choix car c'est de loin le résultat le plus important de cette section concernant les courbes algébriques. Sont énoncés ci-dessous quelques résultats qui auront des applications dans la suite de ce document et qui, de par leur "puissance", leur "beauté" ou tout simplement leur simplicité méritent de figurer dans ce paragraphe.
Il s'agit du théorème de Bezout, qui va assurer de pouvoir construire explicitement une arithmétique sur une courbe elliptique (cf 11), ainsi que de quelques résultats concernant l'existence de morphisme d'une courbe dans un espace projectif.

Théorème 15. *< Théorème de Bézout>*
Soient C et D deux courbes projectives planes, sans composante irréductible commune, définies respectivement par deux polynômes homogènes F et G de $\overline{k}[X, Y, T]$, de degrés respectifs m et n.
Alors le nombre de points d'intersection, comptés avec multiplicité, de ces deux courbes est égal à mn.

Le lecteur pourra trouver une démonstration du théorème de Bézout dans l'excellent ouvrage [Per95]. Une démonstration alternative à celle proposée dans cette référence consiste à démontrer le théorème dans le cas affine à l'aide du théorème de structure des modules et d'un peu de combinatoire, puis d'adapter la preuve, sans trop de difficulté au cas projectif.

Considérons désormais l'étude des morphismes d'une courbe algébrique vers un espace projectif. On commence tout d'abord par rappeler qu'un diviseur D fournit $n + 1$ fonctions libres sur une courbe C via l'espace vectoriel $\mathcal{L}(D)$ (cf 13), où $n + 1$ désigne la dimension de $\mathcal{L}(D)$ sur k.
A l'aide de ces $n + 1$ fonctions, on peut ainsi définir une application rationnelle de la courbe vers un espace projectif $\mathbb{P}^n$ (on renvoit à la définition d'une application rationnelle 5). Pour que cette application rationnelle soit un morphisme, c'est-à-dire définie en tout point de la courbe, il faut et il suffit que le diviseur D qu'on s'est fixé vérifie la propriété ci-dessous :

Théorème 16. *Soit C une courbe lisse projective et soit $D \in \mathrm{Div}(C)$.*
Le diviseur D définit un morphisme de la courbe C vers un espace projectif si et seulement si :

$$\forall P \in C,\ l(D - (P)) = l(D) - 1$$

Cette propriété est facilement vérifiable à l'aide du théorème de Riemann-Roch, ce qui permet d'affirmer relativement rapidement si un diviseur définit ou non un morphisme vers un espace projectif. On pourra vérifier que cette propriété est équivalente au fait que l'intersection des supports des diviseurs effectifs linéairement à D est vide.

Si l'on veut affiner les propriétés sur le morphisme ainsi définit, par exemple que ce morphisme sépare les points, il est nécessaire d'ajouter des conditions sur le diviseur D, l'objectif étant de pouvoir *plonger* la courbe dans un espace projectif $\mathbb{P}^n$.

Définition 17. Un **plongement** est une immersion fermée, i.e. un morphisme qui est à la fois une immersion et un homéomorphisme sur son image.

Remarque 6. On admettra qu'un morphisme est un plongement si et seulement s'il sépare les points et les vecteurs tangents.

La séparation des points s'obtient à l'aide de la condition :

$$\forall (P,Q) \in C^2,\ P \neq Q,\ l(D-(P)-(Q)) = l(D) - 2$$

La séparation des vecteurs tangents s'obtient quant à elle grâce à la condition :

$$\forall P \in C,\ l(D-2(P)) = l(D) - 2$$

On en déduit alors le résultat suivant :

Théorème 18. *Un diviseur D définit un plongement vers un espace projectif si et seulement si :*

$$\forall (P,Q) \in C^2,\ l(D-(P)-(Q)) = l(D) - 2$$

Remarque 7. D'après la condition du théorème 16, la condition du théorème ci-dessus implique que le diviseur D définit un morphisme vers un espace projectif.

Dans le cas d'une courbe de genre 1, tout diviseur de degré supérieur ou égal à 3 permet de plonger la courbe dans l'espace projectif $\mathbb{P}^2$ en tant que courbe de degré 3.
Dans le cas d'une courbe de genre supérieur à 1, on ne peut pas toujours plonger la courbe dans $\mathbb{P}^2$. Cependant, et c'est l'objet de cette fin de paragraphe, il est possible de plonger toute courbe dans $\mathbb{P}^3$. Pour cela, on considère un plongement vers un espace projectif défini à partir d'un diviseur (il en existe toujours un, pourvu que le degré du diviseur soit suffisamment grand). Il est maintenant nécessaire de déterminer, pour tout entier n supérieur ou égal à 4, un *"algorithme"* permettant de plonger une courbe d'un espace projectif $\mathbb{P}^n$ quelconque dans un espace projectif $\mathbb{P}^{n-1}$. Pour ce faire, il faut au préalable définir un morphisme de $\mathbb{P}^n$ dans $\mathbb{P}^{n-1}$. En faisant le choix d'un point O de $\mathbb{P}^n$ qui n'appartient pas à la courbe, on peut montrer que la projection de la courbe sur $\mathbb{P}^n$ par rapport au point O définit bien un morphisme de la courbe vers $\mathbb{P}^{n-1}$.
Tous les points O ne vont cependant pas définir un plongement. Le résultat suivant donne une condition nécessaire et suffisante pour que la projection par rapport à O en définisse bien un.

Proposition 19. *Soit C une courbe de $\mathbb{P}^n$ et soit $O \notin C$.*
Soit $\varphi : \mathbb{P}^n \to \mathbb{P}^{n-1}$ le morphisme de projection par rapport à O.
Le morphisme φ est une immersion fermée si et seulement si :

(i) O n'appartient à aucune droite de $\mathbb{P}^n$ passant par deux points de la courbe

(ii) O n'appartient à aucune tangente à la courbe.

Remarque 8. Ces deux conditions sont naturelles pour définir un plongement : la condition (i) traduit bien la séparation des points et la condition (ii) , la séparation des vecteurs tangents.

Il s'agit maintenant de savoir s'il existe toujours un tel point O. Il se trouve qu'à partir de la dimension $n = 4$, l'espace $\mathbb{P}^n$ est topologiquement assez "*grand*" pour en contenir un (et même une infinité !). Ainsi, en appliquant un certain nombre de fois la proposition 19, on peut alors en déduire :

Théorème 20. *Toute courbe peut être plongée dans $\mathbb{P}^3$.*

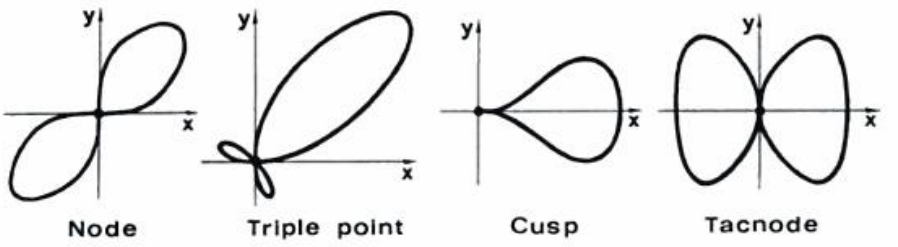

FIGURE 1 – Singularités des courbes non lisses

En règle générale, il n'est pas possible de plonger toute courbe dans $\mathbb{P}^2$. Cependant, en acceptant de perdre la lissité en tout point, il est possible d'établir une application birationnelle de la courbe vers une courbe de $\mathbb{P}^2$:

Proposition 21. *Toute courbe est birationnellement équivalente à une courbe plane dont les singularités sont au plus des "nodes" (noeuds).*

Remarque 9. La figure 1 ci-dessus liste toutes les singularités des courbes non lisses.

2.3 Courbes elliptiques

Les courbes elliptiques sont des courbes particulières, sur lesquelles on peut définir une arithmétique. Elles ont des applications en théorie des nombres ainsi qu'en cryptographie. On propose ici deux approches différentes : dans un premier paragraphe, on considérera les courbes elliptiques comme des objets purement algébriques, puis dans le paragraphe suivant, on prendra le point de vue des équations de Weiertrass, sans oublier de faire le lien entre ces approches.
La suite de cette section concernera l'étude des courbes elliptiques sur les corps finis et leurs applications en cryptographie, ainsi que la classification des courbes elliptiques sur $\mathbb{C}$, par les réseaux du plan complexe. On terminera par une classification des courbes de genre 1 selon un invariant d'isomorphisme, le *j-invariant*.

2.3.1 Définition et loi de groupe sur une courbe elliptique

Les bases ont été posées pour définir la notion de courbe elliptique d'un point de vue purement algébriste.

Définition 22. Une **courbe elliptique** est la donnée d'un couple $(E; O)$ où E désigne une courbe projective lisse de genre 1 et O un point de E, appelé **point de base** ou **origine**.

Remarque 10. On dit qu'une courbe elliptique est une *courbe pointée*.

Le théorème de Riemann-Roch s'écrit plus simplement pour les courbes de genre 1 (donc pour les courbes elliptiques) :

Proposition 23. *Soit E une courbe de genre 1. Alors :*

$$\forall D \in \mathrm{Div}(E),\ l(D) = \deg(D) + l(-D)$$

Sur une courbe elliptique, on peut définir une loi de groupe comme on peut le voir sur la figure 2 ci-après. Cette structure de groupe est souvent suffisamment complexe pour avoir des utilités en cryptographie et notamment dans le problème du logarithme discret.
La loi de groupe d'une courbe elliptique repose sur le résultat suivant :

Proposition 24. *Soit $(E;O)$ une courbe elliptique.*
L'application $E \to \mathrm{Div}^0(E)$ qui, à P associe le diviseur $(P)-(O)$, induit une bijection

$$\kappa : E \to Pic^0(E)$$

Démonstration. Montrons l'injectivité de κ.
Soient P et Q tels que $\kappa(P) = \kappa(Q)$. D'où $(P)-(O) \sim (Q)-(O)$, i.e. $(P) \sim (Q)$.
D'après le théorème de Riemann-Roch, $l((P)) = \deg(P) + l(-(P)) = 1$, donc $\mathcal{L}((P)) = \overline{k}$.
Le seul diviseur positif équivalent à (P) est donc (P) lui-même, et ainsi $P = Q$.
D'où l'injectivité de κ.
Montrons maintenant la surjectivité de κ.
Soient D un diviseur de degré 0 et $D' = D+(O)$. D'après le théorème de Riemann-Roch, on a $l(D') = 1$, donc il existe un diviseur positif D'' équivalent à D'. Un tel diviseur est de degré 1, donc il existe P tel que $D'' = (P)$.
Alors, $D = D' - (O) \sim (P) - (O)$ d'où la surjectivité de κ. □

La bijection ci-dessus permet alors de transporter la structure de groupe vers la courbe E elle-même.

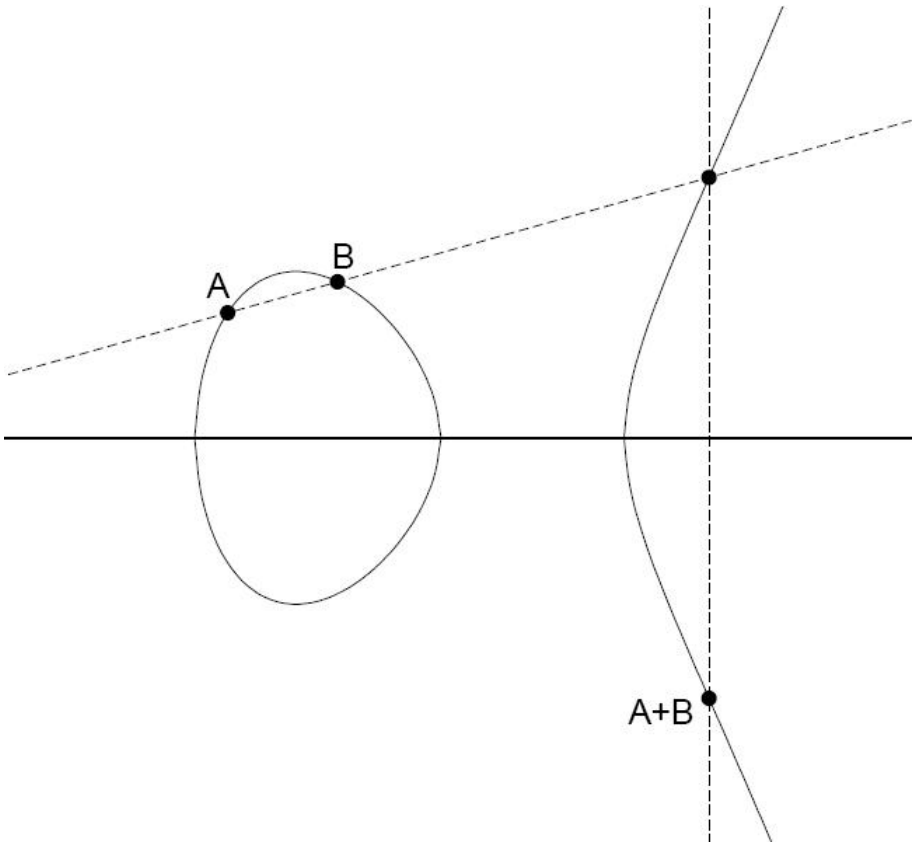

FIGURE 2 – Loi de groupe sur une courbe elliptique

Remarque 11. En appliquant le théorème de Bezout 15, on obtient qu'une droite intersecte une courbe elliptique en 3 points (comptés avec multiplicités), ce que l'on peut remarquer sur la figure 2 ci-dessous. La loi de groupe induite par 24, s'interprète géométriquement grâce à cette figure.
On retiendra le résultat suivant : P, Q et R sont alignés sur E si et seulement si $P+Q+R = 0$, résultat issu de la structure du groupe $\mathrm{Pic}^0(E)$.

Pour déterminer la somme $P+Q$, il faut suivre la procédure suivante :

(i) tracer la droite (PQ) ;

(ii) celle-ci coupe la courbe en un troisième point, non nécessairement distinct des deux précédents ;

(iii) le symétrique de ce point par rapport à l'axe des ordonnées est le point $P + Q$.

Remarque 12. (i)Si la droite (PQ) est verticale, alors $P + Q = O$ où O désigne le point à l'infini.
(ii) Si les points P et Q sont confondus, alors la droite (PQ) devient la tangente à la courbe en P.

2.3.2 Equations de Weierstrass

On peut désormais aborder les courbes elliptiques du point de vue des équations de Weierstrass qui sont présentées ci-dessous.

Définition 25. Soient $a_1, a_2, a_3, a_4, a_6 \in k$.
On appelle **polynôme homogène de Weierstrass** le polynôme :

$$Y^2T + a_1XYT + a_3YT^2 - X^3 - a_2X^2T - a_4XT^2 - a_6T^3$$

Une **équation homogène de Weierstrass** est une équation définie par le polynôme homogène de Weierstrass, de la forme :

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3$$

Une **courbe de Weierstrass** est une courbe définie dans le plan projectif $\mathbb{P}^2$ par une équation homogène de Weiertrass.
Une **équation de Weierstrass affine** s'obtient en prenant $T = 1$:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Remarque 13. (i) Une courbe de Weierstrass n'a qu'un seul point à l'infini, $O = [0; 1; 0]$.
C'est un point lisse et l'espace tangent en ce point est la droite $T = 0$.

(ii) A l'aide d'un changement affine de coordonnées projectives, en caractéristique différente de 2 et de 3, on peut se ramener à une équation de Weierstrass affine de la forme :

$$y^2 = x^3 + a_4x + a_6$$

Le résultat suivant permet de rapprocher la notion de courbe elliptique et celle de courbe de Weierstrass.

Proposition 26. *Toute courbe de Weierstrass lisse munie de son point à l'infini est une courbe elliptique.*

La proposition précédente ainsi que celle ci-dessous mettent en évidence l'équivalence des deux points de vue :

Proposition 27. *Toute courbe elliptique admet une équation de Weierstrass.*

Les courbes elliptiques admettent aussi un autre type d'équation particulière qui nous intéresserons par la suite :

Proposition 28. *En caractéristique différente de* 2*, toute courbe elliptique admet une équation dite de* ***Legendre****, de la forme :*

$$y^2 = x(x - 1)(x - \lambda)$$

où $\lambda \in \overline{k} \setminus \{0, 1\}$.

Les bases sont maintenant posées pour s'intéresser à différentes classifications des courbes elliptiques.

2.3.3 Courbes elliptiques sur quelques corps particuliers

Coubes elliptiques sur les corps finis

Définition 29. Soient (E_1, O_1) et (E_2, O_2) deux courbes elliptiques.
On appelle **isogénie** tout morphisme $\varphi : E_1 \to E_2$ tel que $\varphi(O_1) = O_2$.

La définition ci-dessus ainsi que la proposition ci-dessous existent quelque soit le corps sur lequel sont définies les courbes elliptiques, qu'ils soient finis ou non.
Toute la "force" d'une isogénie tient dans le résultat qui suit :

Proposition 30. *Toute isogénie d'une courbe elliptique vers une autre est un homomorphisme de groupe.*

Définition 31. Soit (E, O) une courbe elliptique.
Pour tout entier $m \in \mathbb{N}^\star$, on définit l'application $[m] : E \to E$ par :

$$\forall P \in E,\ [m]P = \underbrace{P + \ldots + P}_{m \text{ fois}}.$$

Par convention, $[0]$ désignera l'application constante $[0] : P \mapsto O$.

Proposition 32. *Soit (E, O) une courbe elliptique.*
*Pour tout entier $m \in \mathbb{N}$, $[m]$ est une **isogénie** de E dans lui-même.*
*On appelle **sous-groupe des points de m-torsion**, noté $E[m]$, le noyau du morphisme $[m]$.*

Théorème 33. *Soit k un corps de caractéristique $p > 0$ et soit $m \in \mathbb{N}^\star$.*
Soit E une courbe elliptique sur k.

(i) Si l'entier m est premier avec p alors :

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

(ii) Si p divise l'entier m, on a alors l'une des deux possibilités suivantes :

$$a)\ \forall r \in \mathbb{N}^\star,\ E[p^r] \simeq \{O\}$$

$$b)\ \forall r \in \mathbb{N}^\star,\ E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}.$$

Remarque 14. (i) Le point reste vrai en caractéristique nulle.

(ii) La preuve de ce résultat réside dans le fait que $E[m]$ est un groupe abélien dont on sait calculer le cardinal, par des arguments qu'on n'explicitera pas ici.

Le théorème ci-dessous est fondamental : conjecturé par E. Artin puis prouvé par H. Hasse, il permet d'estimer le nombre de points rationnels de la courbe E, c'est-à-dire le nombre de points de la courbe à coordonnée dans k, ou encore le nombre de solutions de l'équation :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

où $(x, y) \in k$.

Théorème 34. *<**Théorème de Hasse (pour les courbes elliptiques)**>*
Soit E une courbe elliptique définie sur un corps fini k à q éléments.
Si $E(k)$ désigne l'ensemble des points rationnels de E sur k, alors :

$$|\#E(k) - q - 1| \leq 2\sqrt{q}.$$

La preuve de ce théorème utilise la version "forme quadratique" de l'inégalité de Cauchy-Schwartz", associée à un résultat de théorie de Galois qui permet d'affirmer que le morphisme de Frobenius (morphisme "d'élévation à la puissance q") fixe les points de $E(K)$, et uniquement ces points.

Les courbes elliptiques sur les corps finis présentent de nombreuses applications, notamment en ce qui concerne la factorisation d'entiers et la cryptographie.
La cryptographie sur les courbes elliptiques est un type de cryptographie à clé publique (le protocole d'échange de clés est celui de Diffie-Hellmann [CFA06]). Cette cryptographie est basée sur la difficulté de la résolution du problème du logarithme discret décrite ci-après.
Etant donné un groupe cyclique G et deux élements x et y, le problème du logarithme discret consiste à déterminer l'entier n tel que $y = x^n$. Pour que ce problème soit réputé difficile, il est clair que l'ordre du groupe G doit être grand. Mais le choix du groupe (et donc de l'arithmétique qui en découle) rentre en compte dans la difficulté du problème. En réalité, la complexité de l'arithmétique sur les courbes elliptiques permet de diviser par 2 la taille des clés sans pour autant diminuer les standards de sécurité informatique.
Cependant, c'est cette même complexité de l'arithmétique ralentit sensiblement les calculs de chiffrement et de déchiffrement, nécessitant d'effectuer un "compromis temps-mémoire", bien connu des informaticiens.

On décrit ci-dessous un exemple simplifié de cryptographie sur courbe elliptique.

Exemple 1. *Imaginons qu'Alice et Bob veuillent s'échanger une clé afin de s'envoyer des messages cryptés. Pour cela, ils se mettent d'accord publiquement sur le choix d'une courbe elliptique* $E(a, b, p) : y^2 = x^3 + ax + b \mod p$ *et d'un point* P *de la courbe.*
Alice choisit de son côté sa clé privée k_A *tandis que Bob fait de même pour* k_B*. Chacun des deux protagonistes publie alors respectivement les points* $[k_A]P$ *et* $[k_B]P$*, puis détermine le point* $[k_A k_B]P$ *qui sera la clé commune.*
Charlie, qui veut mettre la main sur la clé d'Alice et Bob, possède les informations suivantes, en plus de la courbe elliptique : $P, [k_A]P$ *et* $[k_B]P$*. Pour pouvoir déterminer la clé,* $[k_A k_B]P$*, il lui faut par exemple déterminer* k_A *à la simple connaîssance de* P *et de* $[k_A]P$*.*
Cela revient bien à résoudre le problème du logarithme discret décrit plus haut, et réputé difficile pour une courbe elliptique dont le nombre de points est suffisamment grand.

Remarque 15. Actuellement on utilise des courbes sur $\mathbb{F}_q$, où $q \sim 2^{256}$, pour une sécurité de 128 bits (taille de la clé).

Coubes elliptiques sur $\mathbb{C}$

Le corps valué $\mathbb{C}$ ayant des propriétés à la fois algébriques et analytiques, cet ensemble est particulièrement intéressant pour les mathématiciens. Ainsi, sur $\mathbb{C}$, les courbes elliptiques prennent une tournure particulière : on peut les classifier par les réseaux du plan, à l'aide d'outils issus de l'analyse complexe.
La fonction $\mathcal{P}$ de Weierstrass va jouer un rôle tout particulier dans cette classification. Dès lors qu'on se fixe un réseau Λ, la fonction $\mathcal{P}$ de Weierstrass est définie par :

$$\mathcal{P}(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

C'est une fonction méromorphe sur $\mathbb{C}$ qui dont la série converge uniformément sur tout compact de $\mathbb{C} \setminus \Lambda$.
Sa fonction dérivée

$$\mathcal{P}'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$$

vérifie les mêmes propriétés.
On sait même que ces deux fonctions sont elliptiques sur leur réseau associé, et qu'elles engendrent le corps des fonctions elliptiques sur un réseau fixé, mais le résultat va plus loin : il exhibe une relation algébrique entre ces générateurs.

Théorème 35. *Soit Λ un réseau du plan, et soit $\mathcal{P}$ la fonction de Weierstrass associée à ce réseau. Alors :*

$$(\mathcal{P}')^2 = 4\mathcal{P}^3 - g_2\mathcal{P} - g_3$$

$$où \quad g_2 = 60G_2 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4} \quad et \quad g_3 = 140G_4 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$$

Remarque 16. La relation du théorème précédent s'obtient en considérant des séries de Laurent des fonctions $\mathcal{P}$, $\mathcal{P}^3$ et $(\mathcal{P}')^2$.

Avec un peu d'attention, on est tenté de reconnaitre, dans la relation $(\mathcal{P}')^2 = 4\mathcal{P}^3 - g_2\mathcal{P} - g_3$, une équation de Weierstrass (cf 13) d'une courbe elliptique de la forme :

$$y^2 = 4x^3 - g_2x - g_3$$

Dès lors, fixons-nous un réseau Λ du plan complexe.
On peut vérifier qu'une courbe de $\mathbb{P}^2$ dont l'équation est celle ci-dessus est une courbe lisse, donc une courbe elliptique, munie du point à l'infini $(0, 1, 0)$.
On peut même réaliser un isomorphisme de groupes entre $\mathbb{C}/\Lambda$ et la courbe elliptique d'équation

$$y^2 = 4x^3 - g_2x - g_3$$

Pour aller plus loin, on peut étudier les classes d'isomorphisme entre courbes elliptiques sur $\mathbb{C}$. Pour cela, on utilisera le résultat suivant :

Proposition 36. *Soient u et $v \in \mathbb{C}$ tels que $\Delta = u^3 - 27v^3 \neq 0$.*
Alors il existe un unique réseau Λ de $\mathbb{C}$ tels que $g_2(\Lambda) = u$ et $g_3(\Lambda) = v$.

On remarque que la condition $\Delta = u^3 - 27v^3 \neq 0$ signifie que la courbe d'équation $y^2 = 4x^2 - ux - v$ est lisse, i.e. que c'est une courbe elliptique. Ainsi, à toute courbe elliptique sur $\mathbb{C}$, on peut associer un réseau du plan.

On peut alors énoncer le résultat final classifiant entièrement les courbes elliptiques sur $\mathbb{C}$ par les réseaux du plan :

Proposition 37. *L'ensemble des classes d'isomorphismes des courbes elliptiques sur $\mathbb{C}$ est en correspondance bijective avec la classe d'équivalence des réseaux du plan, à homothétie près.*

2.3.4 Classification de courbes elliptiques par le j-invariant

Contrairement à ce qui est annoncé dans le titre de cette partie, il n'est pas question de classifier des courbes elliptiques, mais des courbes lisses de genre 1 en caractéristique différente de deux. En effet, dans cette partie, nous verrons entre autres, l'existence d'un invariant sur les courbes elliptiques, mais aussi que cet invariant ne dépend pas du point de base de ces courbes elliptiques.

On considère une courbe C de genre 1 sur un corps k algébriquement clos de caractéristique différente de 2, ainsi qu'un point P_0 de la courbe.
Vérifions que diviseur $3(P_0)$ répond à la condition du théorème 18 :
Puisque le degré d'un diviseur canonique sur une courbe de genre 1 est égal à 0 ($= 2g - 2$ cf 14), le degré de n'importe quel diviseur de la forme $3(P_0) - (P) - (Q)$ est supérieur au degré d'un diviseur

canonique K_C.
Ainsi, pour tous points P et Q de la courbe, $l(K_C - D) = l(K_C - D + (P) + (Q)) = 0$. Donc, d'après le théorème de Riemann-Roch, $l(D - (P) - (Q)) = \deg(D - (P) - (Q)) = \deg D - 2 = l(D) - 2$. CQFD.
On a alors le résultat suivant :

Proposition 38. *Le diviseur $3(P_0)$ définit alors une immersion fermée de la courbe C vers $\mathbb{P}^2$.*

En appliquant le théorème de Riemann-Roch une fois de plus, on remarque que :

$$\forall n > 0,\ l(n(P_0)) = n.$$

On peut alors aisément montrer qu'il existe une fonction $x \in \mathcal{L}(2(P_0))$ et une fonction $y \in \mathcal{L}(3(P_0))$ telles que $(1, x)$ soit une base de $\mathcal{L}(2(P_0))$ et $(1, x, y)$ soit une base de $\mathcal{L}(3(P_0))$. On remarque alors que les sept fonctions $1,\ x,\ x^2, x^3, y,\ xy$ et y^2 appartiennent à l'espace vectoriel $\mathcal{L}(6(P_0))$ de dimension 6 (on peut s'en convaincre en étudiant les pôles de ces fonctions). Ces fonctions sont donc liées et, par un habile changement de variables affine, on peut se ramener à une relation de la forme voulue :

$$y^2 = x(x-1)(x-\lambda)$$

où λ est un élément de k (on rappelle que k est algébriquement clos).
On a ainsi montré l'existence d'une équation de Legendre pour toute courbe lisse de genre 1.
On définit maintenant la notion de j-invariant :

Définition 39. On appelle **j-invariant** de la courbe C, noté $j(C)$ (ou encore j), l'élément de k :

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (\lambda - 1)^2}.$$

La définition de λ dépend *a-priori* du point P_0. Contrairement à ce à quoi on pourrait s'attendre, le j-invariant ne dépend pas du point choisi.
Pour s'en convaincre, on peut chercher tous les isomorphismes entre deux équations de Legendre (de la même courbe) associées à λ_1 et λ_2. Chacun des ces isomorphismes fixe le point à l'infini. Il s'agit alors de déterminer toutes les applications affines de k dans k qui envoient alors bijectivement l'ensemble $\{0, 1, \lambda_1\}$ vers $\{0, 1, \lambda_2\}$. Des calculs relativement simples montrent que ces applications sont au nombre de 6 et qu'elles sont engendrées par les applications affines qui envoient λ sur $1 - \lambda$ ou sur $\frac{1}{\lambda}$.
On peut immédiatement remarquer que $j(\lambda)$ est invariant par ces deux transformations et donc conclure de l'invariance du j-invariant vis-à-vis du point de base choisi. En ce sens, cette quantité est un invariant géométrique.

On peut alors énoncer le résultat fondamental de ce paragraphe :

Théorème 40. *Soit k un corps algébriquement clos de caractéristique différente de 2. Alors : deux courbes de genre 1 sont isomorphes si et seulement si leurs j-invariants sont égaux.*

Remarque 17. Le fait que le corps de base k soit algébriquement clos nous assure le fait que tout élément de k est le j-invariant d'une courbe elliptique sur k.
On a ainsi une bijection entre les courbes lisses de genre 1, à isomorphisme près, et le corps k : cette bijection est induite par l'application j-invariant qui à une courbe associe son j-invariant.

Bibliographie

Références

[CFA06] Henri Cohen, Gerhard Frey, and Roberto Avanzi. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete mathematics and its applications. CRC Press, 2006. 12

[Dar99] Henri Darmon. *A Proof of the Full Shimura-Taniyama-Weil Conjecture Is Announced*, volume 46. American Mathematical Society, 1999. 3

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977. 3

[Méz07] Ariane Mézard. Courbes algébriques. notes de cours, 2007. 3

[Per95] Daniel Perrin. *Géométrie algébrique : une introduction*. Savoirs actuels. Série Mathématiques. EDP Sciences Editions, 1995. 6

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 1986. 3, 6