MAT 562 : Introduction à la géométrie algébrique et courbes elliptiques

Table des matières

Chapitre 1

Variétés algébriques affines

Dans ce chapitre, la lettre k désigne un corps algébriquement clos.

1.1 Parties algébriques et idéaux

Soit $P \in k[X_1, \ldots, X_n]$ un polynôme multivarié. On note $V(P)$ l'ensemble des solutions de l'équation $P(x_1, \ldots, x_n) = 0$ dans k^n. Ainsi

$$V(P) \coloneqq \{(x_1, \ldots, x_n) \in k^n \mid P(x_1, \ldots, x_n) = 0\}.$$

Plus généralement, on peut considérer l'ensemble des solutions d'un système de telles équations polynomiales. Si A est une partie de $k[X_1, \ldots, X_n]$, on note

$$V(A) \coloneqq \{x \in k^n \mid \forall P \in A,\, P(x) = 0\} = \bigcap_{P \in A} V(P).$$

Une partie de k^n de la forme $V(A)$ est appelée *partie algébrique de* k^n.

Exemple 1.1. (i) Les ensembles suivants sont des parties algébriques :

$$\{(x, y) \in k^2 \mid y = x^2\}, \quad \{(x, y) \in k^2 \mid xy = 1\}, \quad \{(x, y, z) \in k^3 \mid z = xy,\, x^2 + y^3 + z^4 = 0\}.$$

(ii) Pour $a_1, ..., a_n \in k$, on a $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\}$.

(iii) Les parties algébriques de k sont les parties finies de k et k tout entier.

Rappelons que si $(A, +, \cdot)$ est un anneau commutatif, un *idéal* de A est une partie I de A telle que $(I, +)$ est un sous-groupe de $(A, +)$ et qui est de plus stable par multiplication par tout élément de A, autrement dit, pour tous $a \in A$ et $x \in I$, on a $ax \in I$.

Si B et C sont des parties de A telles que $B \subset C$, on a $V(C) \subset V(B)$. De plus, si $P_1, \ldots, P_m$ sont des éléments de B, pour tout m-uplet $(Q_1, \ldots, Q_m)$ de polynômes

de $k[X_1, \ldots, X_n]$, le polynôme $Q_1P_1 + \cdots + Q_mP_m$ s'annule sur $V(B)$. Ainsi, si I désigne l'idéal de $k[X_1, \ldots, X_n]$ engendré par B, on a $V(B) \subset V(I)$ et donc $V(A) = V(I)$ (puisque $V(I) \subset V(B)$ par $B \subset I$). On ne perd donc pas de généralité à considérer uniquement les parties algébriques de k^n de la forme $V(I)$ où I est un *idéal* de $k[X_1, \ldots, X_n]$.

Les idéaux de $k[X_1, \ldots, X_n]$ vont être des objets particulièrement utiles pour décrire les parties algébriques de k^n.

1.2 Quelques rappels sur les anneaux et les idéaux

1.2.1 Rappels sur les idéaux

a) Exemples classiques

Soit A un anneau commutatif et soit I un idéal de A. Comme $(I, +)$ est un sous-groupe de $(A, +)$, I contient l'élément neutre pour l'addition, c'est-à-dire 0. En particulier I est une partie non vide de A et contient toujours 0.

Exemple 1.2.

a) L'ensemble $\{0\}$ est un idéal appelé idéal nul. Il est souvent noté simplement 0.

b) L'ensemble A tout entier est lui aussi un idéal de A.

c) Si $x \in A$, on note (x) ou Ax l'ensemble $\{ax \mid a \in A\}$ des multiples de x. Il s'agit d'un idéal de A. Les idéaux de cette forme sont dits *principaux*.

d) Si $x_1, ..., x_n \in A$, on note $(x_1, ..., x_n)$ ou $Ax_1 + ... + Ax_n$ l'ensemble $\{a_1x_1 + ... + a_nx_n \mid a_1, ..., a_n \in A\}$. Il s'agit d'un idéal de A. Les idéaux de cette forme sont dits *finiment engendrés* ou *de type fini*.

e) Si I et J sont des idéaux de A, l'ensemble $I \cap J$ est un idéal de A.

f) Si I et J sont des idéaux de A, on définit $I + J$ par

$$I + J = \{x + y \mid x \in I,\, y \in J\},$$

il s'agit d'un idéal de A.

g) Si I et J sont des idéaux de A, on veut définir l'idéal produit de I et J, c'est-à-dire une partie de A qui est un idéal et qui contient tous les produits d'éléments de I par des éléments de J. Il est naturel de définir

$$IJ = \left\{ \sum_i x_i y_i \mid x_i \in I,\, y_i \in J \right\}.$$

L'ensemble IJ est alors un idéal de A et $IJ \subset I \cap J$. Il faut prendre garde au fait que cette inclusion n'est en général pas une égalité. Lorsque $I = (x_1, ..., x_n)$ et $J = (y_1, ..., y_m)$, on a $IJ = (x_i y_j, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m)$.

h) Si f est un morphisme d'anneaux $A \to B$, le noyau $\operatorname{Ker} f$ de f est toujours un idéal de A.

b) Anneau quotient

Soit I un idéal de A. On définit une relation d'équivalence sur A en posant $x \sim_I y$ si et seulement si $x - y \in I$. On note A/I l'ensemble des classes d'équivalence pour la relation $\sim_I$. Si $x \in A$, on note $[x]$ la classe de x, autrement dit l'ensemble $x + I$. On peut munir l'ensemble A/I d'une structure d'anneau en posant $[x] + [y] = [x + y]$ et $[x][y] = [xy]$. Il est important de vérifier que cette définition est cohérente, c'est-à-dire que les classes $[x + y]$ et $[xy]$ sont indépendantes des choix faits pour les représentants x et y des classes $[x]$ et $[y]$. Cette vérification est laissée au lecteur, de même que la preuve de la proposition suivante.

Proposition 1.3. *(i) L'application $p_I : x \mapsto [x]$ est un morphisme surjectif d'anneaux de A vers A/I dont le noyau est égal à l'idéal I.*

(ii) (Propriété universelle) *Soit $f : A \to B$ un morphisme d'anneaux. On a $I \subset \mathrm{Ker}(f)$ si, et seulement si, il existe un morphisme $\hat{f} : A/I \to B$ tel que $f = \hat{f} \circ p_I$. Le morphisme $\hat{f}$ est alors unique et on a :*

$$\mathrm{Ker}(\hat{f}) = p_I(\mathrm{Ker}(f)), \quad \mathrm{im}(\hat{f}) = (f).$$

Le corollaire suivant est très utile pour calculer des quotients :

Corollaire 1.4. *Soit $f : A \to B$ un morphisme d'anneaux. Il induit alors un isomorphisme $A/\mathrm{Ker}(f) \cong \mathrm{im}(f)$.*

Démonstration. D'après la propriété universelle, f induit un morphisme $\hat{f} : A/\mathrm{Ker}(f) \to \mathrm{im}(f)$. Comme $\mathrm{Ker}(\hat{f}) = p_{\mathrm{Ker}(f)}(\mathrm{Ker}(f)) = 0$ et $\mathrm{im}(\hat{f}) = \mathrm{im}(f)$, on déduit que $\hat{f}$ est un isomorphisme. □

Remarque 1.5. La construction de la relation d'équivalence $\sim_I$ est une généralisation de la notion de congruence. En effet, si on considère l'anneau $A = \mathbb{Z}$ et l'idéal $I = \mathbb{Z}n$ alors la relation d'équivalence $\sim_I$ est exactement la relation de congruence modulo n et l'anneau quotient A/I est l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exemple 1.6. Soit k un corps et soit A l'anneau $k[X, Y]$ des polynômes en deux variables à coefficients dans k. On considère I l'idéal des multiples de Y. L'anneau A/I est alors isomorphe à l'anneau $k[X]$ des polynômes en une variable. Il suffit en effet de considérer le morphisme envoyant un polynôme $P(X, Y)$ sur le polynôme $P(X, 0)$ en une variable puis d'appliquer la propriété universelle.

Exemple 1.7. L'anneau $\mathbb{R}[X]/(X^2 + 1)$ est isomorphe à $\mathbb{C}$. Pour le voir, il suffit d'appliquer la propriété universelle au morphisme $\mathbb{R}[X] \to \mathbb{C}$ envoyant P sur $P(i)$.

c) Idéaux premiers et maximaux

1.2.2 Quelques classes d'anneaux

Il existe existe bien sûr des idéaux qui ne sont pas de type fini. Cependant ces idéaux n'apparaîtront pas naturellement dans notre étude de la géométrie algébrique. Les anneaux commutatifs dont tous les idéaux sont de type fini ont des propriétés algébriques très agréables, on les appelle des *anneaux noethériens*. Ces anneaux sont d'autant plus utiles qu'ils sont loin d'être rares, la plupart des anneaux rencontrés en géométrie algébrique élémentaire sont noethériens. C'est une conséquence du théorème suivant, dû à Hilbert.

Théorème 1.8 (Théorème de la base finie)**.** *Soit k un corps. Tout idéal de $k[X_1, \ldots, X_n]$ est de type fini.*

Remarque 1.9. Lorsque $n = 1$, c'est une conséquence immédiate du fait que l'anneau $k[X]$ est principal. Tout idéal de $k[X]$ est de la forme (P), c'est-à-dire engendré par un élément. Dès que $n \geqslant 2$, il existe dans $k[X_1, \ldots, X_n]$ des idéaux non principaux.

Une démonstration de ce théorème est donnée dans l'appendice 8.3.

Comme tout idéal de $k[X_1, \ldots, X_n]$ est de type fini, si I est un idéal de $k[X_1, \ldots, X_n]$, il existe des éléments $P_1, \ldots, P_m$ dans $k[X_1, \ldots, X_n]$ tels que $I = (P_1, \ldots, P_m)$. On a alors

$$V(I) = \{(x_1, \ldots, x_n) \in k^n \mid P_1(x_1, \ldots, x_n) = \cdots = P_m(x_1, \ldots, x_n) = 0\}.$$

Ainsi toute partie algébrique de k^n est un ensemble de solutions d'un système *fini* d'équations polynomiales en n variables.

1.3 Opérations élémentaires sur les parties algébriques

Soient I et J des idéaux de $k[X_1, \ldots, X_n]$.

a) On a $V(0) = k^n$ et $V(k[X_1, \ldots, X_n]) = \emptyset$.

b) Si $I \subset J$, on a $V(J) \subset V(I)$.

c) On a $V(I + J) = V(I) \cap V(J)$.

d) On a $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

e) Tout idéal de $k[X]$ est principal. Si $P \in k[X] \smallsetminus \{0\}$, l'ensemble $V(P)$ est l'ensemble des racines de k. Ainsi les parties algébriques de k sont k et les parties finies de k.

f) Si $(a_1, \ldots, a_n) \in k^n$, on a $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$.

Si I et J sont deux idéaux de $k[X_1, \ldots, X_n]$, l'idéal $I \cap J$ n'est pas si facile à déterminer. En effet, on sait qu'il est de type fini en vertu du théorème 1.8 mais il n'est pas évident de déterminer une famille génératrice finie de $I \cap J$ si l'on connaît des familles génératrices finies de I et J. En revanche, il est plus simple de déterminer

une famille génératrice de IJ. En effet si $I = (P_1, \ldots, P_r)$ et $J = (Q_1, \ldots, Q_s)$, alors $IJ = (P_i Q_j; 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s)$.

Si $n \geqslant 0$, la variété algébrique affine k^n est aussi notée $\mathbb{A}^n_k$.

1.4 La topologie de Zariski

Si X est un ensemble, une *topologie* sur X est un ensemble $\mathcal{T}$ de parties de X vérifiant les propriétés suivantes.

(i) L'ensemble vide $\emptyset$ et l'ensemble X sont des éléments de X.

(ii) L'ensemble $\mathcal{T}$ est stable par union quelconque.

(iii) L'ensemble $\mathcal{T}$ est stable par intersection finie.

Un *espace topologique* est un couple $(X, \mathcal{T})$ où X est un ensemble et $\mathcal{T}$ une topologie de X. Les éléments de $\mathcal{T}$ sont alors appelés *ouverts* de X et leurs complémentaires *fermés* de X.

Si X est un espace métrique, pour une distance d, on peut définir une topologie sur X en choisissant pour parties ouvertes les parties U de X telles que

$$\forall x \in U, \exists \varepsilon > 0, \{y \in X, d(x, y) < \varepsilon\} \subset U$$

autrement dit les parties qui sont voisinages de tous leurs points.

Si $(X, \mathcal{T})$ et $(X', \mathcal{T}')$ sont deux espaces topologiques, une application $f : X \to X'$ est dite *continue* si l'image réciproque d'un ouvert de X' par f est un ouvert de X. Si les topologies $\mathcal{T}$ et $\mathcal{T}'$ sont définies à partir de distances, la notion d'application continue de $(X, \mathcal{T})$ dans $(X', \mathcal{T}')$ coïncide avec la notion d'application continue entre espaces métriques.

La notion d'espace topologique est plus générale que celle d'espace métrique. En effet, toute distance définit une topologie mais toute topologie n'est pas définie par une distance. En géométrie algébrique, les topologies rencontrées ne sont en général pas définies par une distance.

Un espace topologique $(X, \mathcal{T})$ est dit *séparé* si, étant donné deux points distincts $x \neq y$ de X, il existe deux ouverts U et V tels que $x \in U$, $y \in V$ et $U \cap V = \emptyset$. Un espace métrique est toujours séparé.

Soit $(X, \mathcal{T})$ un espace topologique et soit $A \subset X$ une partie de X. L'intersection de toutes les parties fermées contenant A est un fermé et c'est le plus petit fermé de X contenant A, on l'appelle *adhérence* de A dans X et on le note $\overline{A}$. De façon analogue, l'union de toutes les parties ouvertes de X contenue dans A est un ouvert et c'est le plus grand ouvert inclus dans A. On l'appelle *intérieur* de A et on le note $\mathring{A}$.

Lorsque I parcourt les idéaux de $k[X_1, \ldots, X_n]$, l'ensemble des parties de la forme $k^n \setminus V(I)$ est une topologie sur k^n. Cette topologie est appelée *topologie de Zariski*. Les parties algébriques de k^n sont les fermés pour la topologie de Zariski.

Si X est une partie quelconque de k^n, la topologie induite sur X par la topologie de Zariski de k^n est appelée *topologie de Zariski* de X.

Pour $n \geqslant 1$, la topologie de Zariski sur k^n ne provient pas d'une distance. En effet, cette topologie n'est pas séparée. Supposons que U et V sont deux ouverts non vides de k^n tels que $U \cap V = \emptyset$. Il existe alors deux idéaux I et J de $k[X_1, \ldots, X_n]$ tels que $U = k^n \setminus V(I)$ et $V = k^n \setminus V(J)$. Ainsi

$$V(IJ) = V(I) \cup V(J) = k^n.$$

Cela signifie que si $f \in I$ et $g \in J$, alors $fg \in IJ$ s'annule sur k^n tout entier. Comme k est algébriquement clos, et en particulier infini, ceci implique que $fg = 0$. Comme l'anneau $k[X_1, \ldots, X_n]$ est intègre, $f = 0$ ou $g = 0$. On en déduit que l'idéal I ou l'idéal J est nul, c'est-à-dire que $U = \emptyset$ ou $V = \emptyset$, ce qui est absurde.

1.5 Le théorème des zéros de Hilbert

Commençons par considérer le cas où $n = 1$. Soit $I \subsetneq k[X]$ un idéal non trivial. Comme l'anneau $k[X]$ est principal, l'idéal I est de la forme (P) pour P un polynôme non constant (ou bien nul). Le théorème de d'Alembert-Gauss implique alors que P a au moins une racine $x \in k$. Ainsi $\{x\} \subset V(I)$ et en particulier $V(I) \neq \emptyset$. Le théorème des zéros de Hilbert est une sorte de généralisation de ce résultat en dimension supérieure.

Tout d'abord rappelons que si $I \subset J$, alors $V(J) \subset V(I)$. Pour obtenir de « petites » parties algébriques, il faut donc considérer de « grands » idéaux. Si A est un anneau, un idéal I de A est dit maximal si $I \neq A$ et s'il n'existe pas d'idéal J tel que $I \subsetneq J \subsetneq A$. Cela n'est pas complètement évident mais il existe toujours des idéaux maximaux.

Théorème 1.10 (Krull)**.** *Soit A un anneau. Soit I un idéal de A différent de A. Alors il existe un idéal maximal de A contenant I.*

Dans sa version la plus générale, ce résultat est une conséquence du lemme de Zorn, un résultat de théorie des ensembles. Comme nous ne rencontrerons que des anneaux noethériens dans ce cours, nous donnons la preuve uniquement dans le cas noethérien.

Démonstration du théorème 1.10 dans le cas noethérien. Soit A un anneau noethérien et I un idéal de A différent de A. Supposons par l'absurde qu'il n'existe pas d'idéal maximal de A contenant I. On peut alors construire une suite strictement croissante $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ d'idéaux de A contenant I. L'union $J = \bigcup_{n \geqslant 0} I_n$ est alors un idéal de A. Cet idéal est de type fini puisque A est noethérien. Il existe donc un indice n tel que I_n contient une famille génératrice de J. Ainsi $I_n = J$ et $I_n = I_m$ pour $m \geqslant n$. C'est une contradiction. □

Un idéal I de A est maximal si et seulement si A/I est un corps. Si A est une k-algèbre de type fini, et si I est un idéal maximal de A, alors A/I est une k-algèbre de type fini qui est également un corps. C'est ce que l'on appelle une *extension* de k. Il n'est pas complètement évident que cette extension soit finie. C'est pourtant vrai et c'est le résultat clef qui se cache derrière le théorème des zéros.

Théorème 1.11. *Soit k un corps et soit K une extension de k qui est également une k-algèbre de type finie. Alors K est un k-espace vectoriel de dimension finie et ses éléments sont algébriques sur k.*

Démonstration. Commençons par remarquer que si $x \in K$ et si x n'est pas algébrique sur k, alors le morphisme de k-algèbres $k[X] \to K$ envoyant $P(X)$ sur $P(x)$ est injectif. Ainsi la sous-k-algèbre de K engendrée par x est isomorphe à $k[X]$. Comme K est un corps, le plus petit sous-corps de K contenant $k[x]$ est le corps $k(x)$ isomorphe au corps des fractions $k(X)$ de $k[X]$.

Comme K est une k-algèbre de type fini, il existe des éléments $x_1, \ldots, x_n$ de K tels que $K = k[x_1, \ldots, x_n]$. Nous allons démontrer par récurrence sur n que tous les éléments x_i sont algébriques sur k. Supposons que $n = 1$. Supposons par l'absurde que x_1 n'est pas algébrique sur K. Alors $K = k[x_1]$ est isomorphe à $k[X]$. C'est absurde car $k[X]$ n'est pas un corps. Supposons donc le résultat démontré pour un entier n et considérons $x_1, \ldots, x_{n+1}$ tels que $K = k[x_1, \ldots, x_{n+1}]$. Supposons par l'absurde que les x_i ne sont pas tous algébriques sur k. Quitte à réordonner ces éléments, on peut supposer que x_1 n'est pas algébrique sur k. Le sous-corps $k(x_1) \subset K$ est alors isomorphe à $k(X)$ et $K = k(x_1)[x_2, \ldots, x_{n+1}]$. Par récurrence, on en déduit que K est un $k(X)$-espace vectoriel de dimension finie. Le lemme 8.35 implique alors que $k(X)$ est une k-algèbre de type fini. Montrons que ceci est absurde. Supposons en effet qu'il existe des fractions rationnelles $F_1, \ldots, F_r$ telles que tout élément de $k(X)$ soit un polynôme en $F_1, \ldots, F_r$. Soient $D_1, \ldots, D_r$ les dénominateurs des fractions rationnelles F_i écrites sous forme de fraction irréductible. Tout élément de $k(X)$ écrit sous forme de fraction irréductible a donc un dénominateur divisant une puissance du produit $D_1 \cdots D_r$. En appliquant cette observation à la fraction $1/P$, on en déduit que tout élément de $k[X]$ divise une puissance du produit $D_1 \cdots D_r$. On en conclut en particulier que $k[X]$ n'a qu'un nombre fini de polynômes irréductibles unitaires. Or un raisonnement analogue à celui d'Euclide pour l'anneau $\mathbb{Z}$ montre que l'anneau $k[X]$ possède une infinité de polynômes irréductibles et unitaires.

Pour conclure, nous avons montré que $K = k[x_1, \ldots, x_n]$ avec x_i algébrique sur k, on en conclut que K est de dimension finie sur k. □

Lorsque k est un corps algébriquement clos, on en déduit une description complète des idéaux maximaux de $k[X_1, \ldots, X_n]$.

Corollaire 1.12. *Soit k un corps algébriquement clos. L'application*

$$(a_1, \ldots, a_n) \longmapsto (X_1 - a_1, \ldots, X_n - a_n)$$

est une bijection de k^n sur l'ensemble des idéaux maximaux de $k[X_1, \ldots, X_n]$.

Démonstration. Considérons $\mathfrak{m}$ un idéal maximal de $k[X_1, \ldots, X_n]$ et posons $K \coloneqq k[X_1, \ldots, X_n]/\mathfrak{m}$. D'après le théorème 1.11, le corps K est une extension finie de k. Comme k est algébriquement clos, on a en fait $K = k$. Posons alors, pour $1 \leqslant i \leqslant n$, $a_i \coloneqq q_{\mathfrak{m}}(X_i) \in k$. On a $q_{\mathfrak{m}}(X_i - a_i) = 0$ donc $(X_1 - a_1, \ldots, X_n - a_n) \subset \mathfrak{m}$. Par maximalité de l'idéal $(X_1 - a_1, \ldots, X_n - a_n)$, on en déduit l'égalité $(X_1 - a_1, \ldots, X_n - a_n) = \mathfrak{m}$. □

Théorème 1.13 (Théorème des zéros, version faible)**.** *Si $I \neq k[X_1, \ldots, X_n]$ est un idéal, on a $V(I) \neq \emptyset$.*

Démonstration. D'après le théorème 1.10, il existe un idéal maximal $\mathfrak{m}$ contenant I. On a donc $V(\mathfrak{m}) \subset V(I)$. Par ailleurs le corollaire 1.12 implique que $\mathfrak{m}$ est de la forme $(X_1 - a_1, \ldots, X_n - a_n)$ et donc $\{(a_1, \ldots, a_n)\} \subset V(I) \neq \emptyset$. □

Remarque 1.14. Lorsque le corps k n'est pas supposé algébriquement clos, ce résultat n'est plus valide. On peut considérer l'idéal $(X^2 + 1) \subset \mathbb{R}[X]$. On a alors $V(I) = \emptyset$ et $I \subsetneq \mathbb{R}[X, Y]$.

1.6 Idéaux annulateurs

Définition 1.15. *Soit X une partie de k^n. On note*

$$I(X) \coloneqq \{P \in k[X_1, \ldots, X_n] \mid \forall x \in X,\, P(x) = 0\}.$$

Il s'agit d'un idéal de $k[X_1, \ldots, X_n]$ nommé idéal annulateur *de la partie X.*

Exemple 1.16.

a) Si $X \subset Y$, on a $I(Y) \subset I(X)$.

b) On a $I(\emptyset) = k[X_1, \ldots, X_n]$ et $I(k^n) = 0$.

Remarque 1.17. Ici encore certaines des propriétés précédentes peuvent être mises en défaut lorsque k n'est pas supposé algébriquement clos. Par exemple $I(\mathbb{F}_p) = (X^p - X)$.

Proposition 1.18. *Soit X une partie de k^n. On a toujours $X \subset V(I(X))$ avec égalité si et seulement si X est une partie algébrique de k^n. Plus généralement, l'ensemble $V(I(X))$ s'identifie à l'adhérence de X dans k^n pour la topologie de Zariski.*

Démonstration. Il s'agit essentiellement de vérifier que, lorsque X est une partie algébrique de k^n, on a $X \supset V(I(X))$. On peut écrire $X = V(J)$ pour un idéal J de $k[X_1, \ldots, X_n]$. Par définition $J \subset I(X)$ et donc $V(I(X)) \subset V(J) = X$. □

Si I est un idéal de $k[X_1, \ldots, X_n]$, on a $I \subset I(V(I))$. En général cette inclusion est stricte. Nous allons à présent étudier le cas d'égalité.

Définition 1.19. *Soit A un anneau et soit I un idéal de A. L'idéal I est dit* radical *si pour tout $x \in A$ tel qu'il existe $n \geqslant 0$ vérifiant $x^n \in I$, alors $x \in I$.*

On vérifie immédiatement qu'une intersection d'idéaux radicaux est un idéal radical. Étant donné un idéal I il existe donc un plus petit idéal radical contenant I : il s'agit de l'intersection de tous les idéaux radicaux contenant I, on la note $\sqrt{I}$ et on l'appelle *racine* de l'idéal I.

Proposition 1.20. *Soit I un idéal d'un anneau A. On a alors*

$$\sqrt{I} = \{x \in A \mid \exists n \geqslant 0,\, x^n \in I\}$$

Démonstration. Par définition, $\sqrt{I}$ est contenu dans tous les idéaux radicaux contenant I. Il suffit donc de prouver que $\sqrt{I}$ est un idéal radical. Il est clair que $\sqrt{I}$ est stable par multiplication par les éléments de A. Soient x et y dans $\sqrt{I}$. Il existe alors $n \geqslant 0$ et $m \geqslant 0$ tels que $x^n \in I$ et $y^m \in I$. On a alors

$$(x+y)^{n+m-1} = \sum_{\substack{0 \leqslant i,j \leqslant n+m \\ i+j=n+m-1}} \binom{n+m}{i} x^i y^{n+m-1-i}.$$

Si $i+j = n+m-1$, on a soit $i \geqslant n$ soit $j \geqslant m$ et donc $x^i y^j \in I$. Ainsi $(x+y)^{n+m-1} \in I$ et $x+y \in \sqrt{I}$. Ainsi $\sqrt{I}$ est un idéal, il est immédiat de vérifier qu'il est radical. □

Si I est un idéal de $k[X_1, \ldots, X_n]$, l'idéal $I(V(I))$ est radical, on a donc une inclusion $\sqrt{I} \subset I(V(I))$. Le théorème qui suit affirme que cette inclusion est une égalité lorsque k est un corps algébriquement clos. Il s'agit de la forme originale du théorème des zéros de Hilbert. La méthode consistant à le déduire de la forme faible porte le nom d'« astuce de Rabinowitsch ».

Théorème 1.21 (Théorème des zéros, version forte)**.** *Soit I un idéal de $k[X_1, \ldots, X_n]$. On a une égalité*

$$\sqrt{I} = I(V(I))$$

Démonstration. Soit $P \in I(V(I))$. Considérons l'idéal J de $k[X_1, \ldots, X_{n+1}]$ défini par

$$J = (X_{n+1}P - 1) + Ik[X_1, \ldots, X_{n+1}].$$

On vérifie que $V(J) = \emptyset$. Supposons par l'absurde que $V(J) \neq \emptyset$. On peut alors choisir un élément $x \in V(J)$. Soit $(x_1, \ldots, x_{n+1})$ son système de coordonnées. Comme $x \in V(Ik[X_1, \ldots, X_{n+1}])$, on a $(x_1, \ldots, x_n) \in V(I)$. Par définition $P(x_1, \ldots, x_n) = 0$ et x est donc annulé par $X_{n+1}P$. Comme par ailleurs $x \in V(X_{n+1}P - 1)$, on en déduit $1 = 0$ ce qui est absurde. Ainsi $V(J) = \emptyset$.

Le Nullstellensatz faible implique alors $J = k[X_1, \ldots, X_{n+1}]$ et on peut écrire

$$1 = \sum_{i=0}^{k} b_i X_{n+1}^i + a(X_{n+1}P - 1)$$

où $a \in k[X_1, \ldots, X_{n+1}]$ et les b_i sont dans I. On a alors

$$1 = \sum_i b_i X_{n+1}^i \mod (X_{n+1}P - 1).$$

En multipliant cette égalité par P^k, on en déduit

$$P^k = \sum_{i=0}^{k} b_{k-i} P^i \mod (X_{n+1}P - 1).$$

Soit $R = P^k - \sum_{i=0}^{k} b_{k-i}P^i$. D'une part $R \in k[X_1, \ldots, X_n]$ et d'autre part $R = (X_{n+1}P - 1)Q$ pour un certain $Q \in k[X_1, \ldots, X_{n+1}]$. En utilisant l'additivité des degrés en X_{n+1} on en conclut que $Q = R = 0$ et donc que $P^k \in I$, c'est-à-dire $P \in \sqrt{I}$. □

1.7 Variétés algébriques affines irréductibles

Définition 1.22. *Une variété algébrique affine $V \subset k^n$ est dite irréductible si V est non vide et si, pour toute égalité $V = V_1 \cup V_2$ où V_1 et V_2 sont des parties algébriques de k^n, on a nécessairement $V_1 = V$ ou $V_2 = V$.*

Du côté des idéaux, l'analogue des variétés irréductibles est la notion d'idéal premier. Un idéal I d'un anneau commutatif A est dit *premier* si et seulement si $I \neq A$ et pour $x, y \in A$ tels que $x \notin I$ et $y \notin I$, on a $xy \notin I$. On démontre qu'un idéal I est premier si et seulement si l'anneau quotient A/I est intègre.

Proposition 1.23. *Une variété algébrique affine V est irréductible si et seulement si son idéal annulateur $I(V)$ est premier.*

Démonstration. Soit $V \subset k^n$ une partie algébrique. Supposons que V n'est pas irréductible. Il existe alors V_1 et V_2 des parties algébriques de k^n telles que $V_1 \subsetneq V$, $V_2 \subsetneq V$ et $V = V_1 \cup V_2$. On a donc $I(V) \subsetneq I(V_1)$ et $I(V) \subsetneq I(V_2)$. En particulier on peut trouver $F \in I(V_1) \setminus I(V)$ et $G \in I(V_2) \setminus I(V)$. Comme $V = V_1 \cup V_2$, le polynôme FG s'annule sur V et donc $FG \in I(V)$. L'idéal $I(V)$ n'est donc pas premier.

Réciproquement si $I(V)$ n'est pas premier, on peut trouver F et G dans le complémentaire de $I(V)$ tels que $FG \in I(V)$. Posons $V_1 = V(I(V) + (F))$ et $V_2 = V(I(V) + (F_2))$. On a bien $V = V_1 \cup V_2$ avec $V_1 \subsetneq V$ et $V_2 \subsetneq V$ puisque F s'annule sur V_1 mais pas sur V tout entier (idem pour V_2). □

Définition 1.24. *Soit V une variété algébrique affine. Une composante irréductible de V est une partie algébrique irréductible maximale de V.*

Proposition 1.25. *Une variété affine non vide possède un nombre fini de composantes irréductibles et est égale à l'union de ses composantes irréductibles.*

Démonstration. Voir l'exercice 1.7. □

1.8 Applications polynomiales

On fixe un corps algébriquement clos k.

Définition 1.26. *Soit $V \subset k^n$ une variété algébrique affine. Une fonction sur V à valeurs dans k est dite* polynomiale *s'il s'agit de la restriction à V d'un élément de $k[X_1, \ldots, X_n]$.*

Si $W \subset k^m$ est une autre variété algébrique affine, une application de V dans W est dite polynomiale *si toutes ses coordonnées sont des fonctions polynomiales.*

La somme de deux fonctions polynomiales, le produit de deux fonctions polynomiales ainsi que la multiplication d'une fonction polynomiale par un élément de k sont des fonctions polynomiales. On vérifie ainsi que l'ensemble des fonctions polynomiales sur une variété algébrique affine V est une k-algèbre que l'on note $k[V]$.

Proposition 1.27. *La k-algèbre des fonctions polynomiales sur une variété algébrique affine $V \subset k^n$ est isomorphe à la k-algèbre $k[X_1, \ldots, X_n]/I(V)$.*

Démonstration. Par définition l'application de restriction donnée par $P \mapsto P|_V$ de $k[X_1, \ldots, X_n]$ dans $k[V]$ est surjective. C'est de plus un morphisme de k-algèbres. Son noyau est l'ensemble des polynômes P tels que $P|_V = 0$, c'est-à-dire $I(V)$. □

Corollaire 1.28. *Une variété algébrique affine V est irréductible si et seulement si son algèbre $k[V]$ est intègre.*

Démonstration. C'est une conséquence immédiate des propositions 1.23 et 1.27. □

Considérons $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques affines et $f : V \to W$ une application polynomiale. Si $g \in k[W]$, la fonction $g \circ f$ est une fonction polynomiale sur V. Notons la $f^*(g)$. On a ainsi défini une application f^* de $k[W]$ vers $k[V]$. On vérifie aisément que f^* est un morphisme de k-algèbres. Ce procédé permet en fait de caractériser algébriquement les applications polynomiales de V vers W.

Théorème 1.29. *Soient $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques affines. Soit φ un morphisme de k-algèbres de $k[W]$ vers $k[V]$. Il existe alors une* unique *application polynomiale f de V vers W telle que $\varphi = f^*$.*

Démonstration. Rappelons que les applications de restrictions $k[X_1, \ldots, X_n] \to k[V]$ et $k[Y_1, \ldots, Y_m] \to k[W]$ induisent des isomorphismes qui nous permettent d'identifier $k[V]$ et $k[X_1, \ldots, X_n]/I(V)$ ainsi que $k[W]$ et $k[Y_1, \ldots, Y_m]/I(W)$. Choisissons alors, pour tout $1 \leqslant i \leqslant m$, un polynôme $P_i \in k[X_1, \ldots, X_n]$ tel que $\varphi(Y_i) \equiv P_i \mod I(V)$ et posons $f \coloneqq (P_1, \ldots, P_m)|_V$. Par définition f est une application polynomiale de V dans

k^m. Par ailleurs elle ne dépend pas du choix des polynômes P_i. Vérifions que l'image de f est bien incluse dans W. Si $x \in V$ et si $g \in I(W)$, on a

$$\begin{aligned} g(f(x)) &= g(P_1(x), \ldots, P_m(x)) \\ &= g((\varphi(Y_1), \ldots, \varphi(Y_m)))(x) \\ &= \varphi(g(Y_1, \ldots, Y_m))(x) && \text{puisque } \varphi \text{ est un morphisme de } k\text{-algèbres} \\ &= 0 && \text{puisque } \varphi(g) \in I(V). \end{aligned}$$

Ainsi $f(x) \in V(I(W)) = W$. On vérifie alors que $\varphi = f^*$. Si $g \in k[W]$, on a

$$\varphi(g) = \varphi(g(Y_1, \ldots, Y_m)) = g(\varphi(Y_1), \ldots, \varphi(Y_m)) = g(P_1, \ldots, P_m) = f^*(g)$$

Il nous reste à vérifier l'unicité de f. On vérifie en fait que si f et h sont deux applications polynomiales de V dans W, l'égalité $f^* = h^*$ implique $f = h$. Cela résulte du fait que si $x \in V$, on a $f(x) = (y_1, \ldots, y_m)$ où chaque y_i est l'évaluation du polynôme $f^*(Y_i) = h^*(Y_i)$ en $(x_1, \ldots, x_n)$. □

Définition 1.30. *Soient V et W deux variétés algébrique affines. Un* isomorphisme *de V sur W est une application polynomiale f de V dans W telle qu'il existe une application polynomiale g de W dans V vérifiant $g \circ f = \mathrm{Id}_V$ et $f \circ g = \mathrm{Id}_W$.*

Remarque 1.31.

1) Une application polynomiale bijective n'est pas nécessairement un isomorphisme.

2) Lorsqu'une application polynomiale f est un isomorphisme, l'application polynomiale g dans la définition ci-dessus est unique et est appelée *inverse* de f.

Corollaire 1.32. *Deux variétés algébriques affines sont isomorphes si et seulement si leurs algèbres de fonctions polynomiales sont isomorphes.*

Corollaire 1.33. *Deux variétés algébriques affines isomorphes sont toutes deux irréductibles si et seulement l'une des deux est irréductible.*

Exemple 1.34.

a) Posons $V = k$ et $W = V(Y - X^2) \subset k^2$. Les variétés V et W sont isomorphes. Un isomorphisme de V sur W est donné par $t \mapsto (t, t^2)$. Son inverse est donné par $(x, y) \mapsto x$.

b) Si $V = k$ et $W = V(Y^2 - X^3) \subset k^2$. L'application $t \mapsto (t^2, t^3)$ est une application polynomiale et bijective. Cependant ce n'est pas un isomorphisme.

1.9 Fonctions rationnelles

Soit V une variété algébrique affine irréductible. D'après le corollaire 1.28, son algèbre $k[V]$ est un anneau intègre. On peut donc considérer son corps de fractions que l'on note $k(V)$. Les éléments de ce corps sont appelés *fonctions rationnelles* sur V. Par définition toute fonction rationnelle sur V s'écrit sous la forme $\frac{g}{h}$ où g et h sont deux éléments de $k[V]$ et où $h \neq 0$.

Définition 1.35. *Soit V une variété algébrique affine irréductible et soit $f \in k(V)$. Si $P \in V$, on dit que f est* définie en P *s'il existe $g \in k[V]$ et $h \in k[V] \smallsetminus \{0\}$ tels que $f = \frac{g}{h}$ et si $h(P) \neq 0$. On pose alors $f(P) \coloneqq \frac{g(P)}{h(P)}$, cet élément ne dépend pas du choix de g et h.*

Si $f \in k(V) \smallsetminus \{0\}$, l'ensemble des points $P \in V$ tels que f est définie en P est un ouvert non vide de Zariski. En effet, il s'agit du complémentaire de l'intersection des lieux des zéros de tous les éléments $h \in k[V] \smallsetminus \{0\}$ tels qu'il existe $g \in k[V]$ vérifiant $f = \frac{g}{h}$.

Définition 1.36. *Soit V une variété algébrique irréductible et soit $P \in V$. L'*anneau local *de V en P est l'ensemble des éléments $f \in k(V)$ qui sont définis en P. On le note $k[V]_P$.*

Comme son nom l'indique, l'anneau local de V en P est un sous-anneau de $k(V)$. Il contient clairement $k[V]$ de sorte que l'on a une suite d'inclusions

$$k[V] \subset k[V]_P \subset k(V).$$

Notons $\mathfrak{m}_P$ l'ensemble des éléments de $f \in k[V]_P$ tels que $f(P) = 0$. Il s'agit d'un idéal de $k[V]_P$ et l'application d'évaluation $f \mapsto f(P)$ induit un isomorphisme $k[V]_P/\mathfrak{m}_P \xrightarrow{\sim} k$. Ainsi $\mathfrak{m}_P$ est un idéal maximal de $k[V]_P$. Il s'agit de son unique idéal maximal. En effet si $f \in k[V]_P \smallsetminus \mathfrak{m}_P$, alors f est un élément inversible de $k[V]_P$. On dit que $k[V]_P$ est un anneau *local*, c'est-à-dire un anneau possédant un unique idéal maximal.

1.10 Espaces tangents

Rappelons qu'une droite affine de k^n est une partie de la forme

$$D = P + L$$

où $P = (a_1, \ldots, a_n) \in k^n$ et $L \subset k^n$ est un sous-k-espace vectoriel de dimension 1. Une droite affine est une partie algébrique de k^n car c'est l'ensemble des zéros de l'idéal engendré par $f_i - f_i(P)$ où $f_1, \ldots, f_{n-1}$ est un ensemble de formes linéaires définissant L. Si l'on choisit v un vecteur directeur de L, l'application $t \mapsto P + tv$ induit un isomorphisme de variétés algébriques affines entre $\mathbb{A}^1_k$ et D. D'après le théorème 1.29, le morphisme $\mathbb{A}^1_k \simeq D \subset k^n$ correspond à un morphisme de variété algébriques $\varphi_v : k[X_1, \ldots, X_n] \to k[T]$ donné explicitement par $\varphi_v(X_i) = a_i + v_i T$. Remarquons que ce morphisme est surjectif, en effet si $v_i \neq 0$, on a $\varphi(X_i) = v_i T + a_i$ et $v_i T + a_i$ engendre la k-algèbre $k[T]$.

Si $V \subset k^n$ est un fermé algébrique, l'image de l'idéal $I(V)$ est donc un idéal de $k[T]$. Comme tous les idéaux de $k[T]$ sont principaux, il existe $Q \in k[T]$ tel que $\varphi(I(V)) = (Q)$.

Supposons de plus que $P \in V$, on a alors $Q(0) = 0$ de sorte que $T \mid Q$. On note alors $m_P(V, D)$ la borne supérieure des entiers $n \geqslant 1$ tels que $T^n \mid Q$. On vérifie que l'élément

$m_P(V, D) \in \mathbb{N}^* \cup \{\infty\}$ ne dépend pas du choix de vecteur directeur v et on l'appelle la *multiplicité d'intersection* de D avec V.

On dit que P est un point d'intersection *simple* de D et V si $m_P(V, D) = 1$ et que D est *tangente* à V si P n'est pas simple.

Exemple 1.37. Dans k^2. Si $V = V(Y - X^2)$, la droite d'équation $Y = 0$ est tangente à V en $(0, 0)$ et la multiplicité d'intersection est 2.

Proposition 1.38. *L'ensemble des droites tangentes à une variété algébrique affine V en un point P est un sous-espace affine de k^n.*

Le sous-espace affine dont l'existence est assurée par la proposition 1.38 est appelé *espace tangent* en P à V et noté $T_P(V)$.

Démonstration. Soient $v \in k^n \setminus \{0\}$, D_v la droite de vecteur directeur v et $\varphi_v : k[X_1, \ldots, X_n] \to k[X]$. Soient $F_1, \ldots, F_r$ des générateurs de l'idéal $I(V)$. L'image de $I(V)$ est engendrée par les vecteurs $\varphi_v(F_1), \ldots, \varphi_v(F_r)$. Le polynôme en $\varphi_v(F_i) = F_i(a_1 + Tv_1, \ldots, a_n + Tv_n)$ peut également s'écrire

$$\begin{aligned}\varphi_v(F_i) &\equiv F_i(a_1, \ldots, a_n) + T(\varphi_v(F_i))'(0) \mod T^2 \\ &\equiv T(\varphi_v(F_i))'(0) \mod T^2.\end{aligned}$$

On en conclut que $\varphi_v(I(V)) \subset (T^2)$ si et seulement si $(\varphi_v(F_i))'(0) = 0$ pour tout $1 \leqslant i \leqslant r$. Ainsi D_v est tangent à V si et seulement si

$$\forall 1 \leqslant i \leqslant r, \quad (\varphi_v(F_i))'(0) = 0.$$

Puisque $\varphi_v(F_i)'(0) = \sum_{j=1}^n v_i \frac{\partial F_i}{\partial X_j}(P)$, on en conclut que $T_P(V)$ est le sous-espace affine passant par P et de direction donnée par le sous-espace vectoriel défini par le système

$$\begin{cases} v_1 \frac{\partial F_1}{\partial X_1}(P) + \cdots + v_n \frac{\partial F_1}{\partial X_n}(P) &= 0 \\ &\vdots \\ v_1 \frac{\partial F_r}{\partial X_1}(P) + \cdots + v_n \frac{\partial F_r}{\partial X_n}(P) &= 0. \end{cases}$$

□

1.11 Dimension d'une variété affine

Soit V une variété algébrique affine et soit $P \in V$. Soient $F_1, \ldots, F_r$ des générateurs de l'idéal $I(V)$. La preuve de la proposition 1.38 et le théorème du rang montrent que la dimension de l'espace $T_P(V)$ est donnée par $n - \mathrm{rg}(\mathrm{Jac}_P(F_1, \ldots, F_r))$ où $\mathrm{Jac}_P(F_1, \ldots, F_r)$ est la matrice jacobienne de $F_1, \ldots, F_r$ en P :

$$\mathrm{Jac}_P(F_1, \ldots, F_r) = \begin{pmatrix} \frac{\partial F_1}{\partial X_1}(P) & \cdots & \frac{\partial F_1}{\partial X_n}(P) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_r}{\partial X_1}(P) & \cdots & \frac{\partial F_r}{\partial X_n}(P) \end{pmatrix}.$$

Définition 1.39. *Soit V une variété affine irréductible. On appelle* dimension de V *l'entier*

$$\dim(V) = \inf\{\dim(T_P(V)) \mid P \in V\}.$$

On dit qu'un point $P \in V$ est lisse *si $\dim(T_P(V)) = \dim(V)$. La variété V est lisse si tous ses points sont lisses.*

Le résultat suivant montre que la dimension correspond bien à l'idée intuitive que « génériquement la dimension de l'espace tangent d'une variété de dimension n est de dimension n ».

Proposition 1.40. *Soit V une variété algébrique irréductible. L'ensemble des points lisses de V est un ouvert dense de V pour la topologie de Zariski.*

Démonstration. Si $t \leqslant \min(r, n)$, une matrice de taille $r \times n$ est de rang $\leqslant t-1$ si et seulement si tous ses mineurs de tailles $t \times t$ sont nuls. Comme l'application associant à P la valeur d'un mineur de taille $t \times t$ de $\mathrm{Jac}_P(F_1, \ldots, F_r)$ est polynomiale en les coordonnées de P, il s'agit d'une application continue pour la topologie de Zariski. Ainsi l'ensemble $\{P \in V \mid \dim(T_P(V)) \geqslant t\}$ est fermé pour tout $t \geqslant 0$.

On en conclut que l'ensemble des points $P \in V$ tels que $\dim(V) = \dim(T_P(V))$ est le complémentaire dans V de l'ensemble des points P tels que $\dim(T_P(V)) \geqslant \dim(V) + 1$, c'est donc un ouvert de V. Par définition de V, c'est un ouvert non vide. Comme V est irréductible, tout ouvert non vide de V est dense dans V pour la topologie de Zariski. □

Définition 1.41. *Si V est une variété algébrique affine, on appelle* dimension de V *la borne supérieure des dimensions de ses composantes irréductibles. Une variété algébrique affine est dite* équidimensionnelle *si toutes ses composantes irréductibles sont de même dimension.*

Une *courbe algébrique affine* est alors une variété affine équidimensionnelle de dimension 1.

1.12 Exercices

Exercice 1.1. Soit k un corps algébriquement clos. Est-ce que les ensembles suivants sont des variétés algébriques affines dans k^2 ?

a) $\{(x,x) \in k^2 \mid x \neq 0\}$

b) $k^2 \smallsetminus \{(0,0)\}$

Exercice 1.2. Soit k un corps algébriquement clos et soit

$$J = (X^2 + Y^2 - 1, Y - 1) \subset k[X,Y]$$

a) Déterminer l'ensemble $V(J)$.

b) Trouver une fonction $f \in I(V(J))$ telle que $f \notin J$.

c) Déterminer $I(V(J))$.

Exercice 1.3. Soit k un corps algébrique clos. Déterminer les composantes irréductibles des variétés algébriques suivantes ainsi que l'idéal annulateur de chacune des composantes.

a) $V(Y, Y^2 - XZ) \subset \mathbb{A}^3_k$;

b) $V(X(Y - X^2 + 1), Y(Y - X^2 + 1)) \subset \mathbb{A}^2_k$;

c) $V(X^2) \subset \mathbb{A}^2_k$;

d) $V(X^2 - YZ, XZ - X) \subset \mathbb{A}^3_k$.

Déterminer la dimension de chacune des composantes irréductibles obtenues ci-dessus.

Exercice 1.4. Soit k un corps. Montrer que le polynôme $P(X,Y) \coloneqq Y^2 - X(X-1)(X+1) \in k[X,Y]$ est irréductible.

Exercice 1.5. Soit k un corps algébriquement clos. Déterminer les idéaux annulateurs des variétés algébriques affines suivantes.

a) $V(X^2Y, (X-1)(Y+1)^2)$;

b) $V(Z - XY, Y^2 + XZ - X^2)$;

c) $V(XY^3 + X^3Y - X^2 + Y)$.

Exercice 1.6.

a) Soit $V = V(Y - X^2)$. Montrer que l'anneau $k[V]$ est k-isomorphe à l'anneau des polynômes en une variable.

b) Soit $V = V(XY - 1)$. Montrer que l'anneau $k[V]$ n'est pas k-isomorphe à l'anneau des polynômes en une variable.

Exercice 1.7. Soit k un corps algébriquement clos et soit $V = V(I) \subset k^n$ une variété algébrique affine non vide.

a) Soit C une composante irréductible de V. Montrer que C est un fermé de V. (on pourra commencer par considérer l'adhérence de C)

b) En déduire que les composantes irréductibles de V sont en bijection avec les idéaux premiers minimaux de $k[V]$.

c) En utilisant le lemme de Zorn, montrer que tout idéal premier d'un anneau A contient un idéal premier minimal. En déduire que V est égale à l'union de ses composantes irréductibles.

d) Montrer que V a un nombre fini de composantes irréductibles. (on pourra utiliser l'exercice 8.11)

Exercice 1.8. Soit $f : V \to W$ un morphisme entre deux variétés algébriques affines. Montrer que f est une application continue pour les topologies de Zariski.

Exercice 1.9. Soit k un corps.

a) Soit $\mathfrak{m}$ un idéal maximal de $k[X, Y]$. Montrer que $\mathfrak{m}$ n'est pas principal.

b) Soit $f \in k[X, Y] \smallsetminus k[X]$ un polynôme irréductible et soit $g \in k[X, Y]$. Montrer que si f divise g dans $k(X)[Y]$, alors f divise g dans $k[X, Y]$.

c) Soit f un élément irréductible de $k[X, Y]$ et soit $g \in k[X, Y]$. Montrer que si f ne divise pas g, alors on a $((f) + (g)) \cap k[X] \neq 0$.

d) Montrer que les idéaux premiers de $k[X, Y]$ sont de deux sortes : les idéaux principaux premiers et les idéaux maximaux.

Exercice 1.10. Soit $V \subset k^n$ une variété algébrique affine et soit $P \in V$. Montrer que si $f \in k[V]$ ne s'annule pas en P, alors f est inversible dans $k[V]_P$. En déduire que l'idéal $\mathfrak{m}_P$ est l'unique idéal maximal de $k[V]_P$.

Exercice 1.11. Soit $f : V \to W$ un morphisme entre deux variétés algébriques affines. Montrer que l'image par f d'une composante irréductible de V est contenue dans une composante irréductible de W.

Exercice 1.12. Soit k un corps algébriquement clos. Si $V \subset k^n$ et $W \subset k^m$ sont deux variétés algébriques affines, montrer que $V \times W \subset k^{n+m}$ est une variété algébrique affine. Déterminer l'idéal $I(V \times W)$ en fonction de $I(V)$ et $I(W)$.

Exercice 1.13. Soit k un corps algébriquement clos. Montrer que le polynôme $\det \in k[X_{i,j},\ 1 \leqslant i, j \leqslant n]$ est irréductible (on pourra remarquer que toute matrice de déterminant nul est conjuguée à une matrice dont la première colonne est nulle).

Exercice 1.14. Soit k un corps algébriquement clos. On note $\mathcal{N}$ l'ensemble des matrices nilpotentes de $M_n(k)$.

a) Montrer que $\mathcal{N}$ est une variété algébrique affine et que son idéal de définition est engendré par n éléments. Les expliciter lorsque $n = 2$ et $n = 3$.

b) Montrer que $\mathcal{N}$ est l'adhérence de Zariski de l'ensemble des matrices nilpotentes de rang $n - 1$.

c) Montrer que $\mathcal{N}$ est irréductible.

Chapitre 2

Variétés algébriques projectives

2.1 Espaces projectifs

Définition 2.1. *Soit k un corps et soit E un k-espace vectoriel de dimension finie. L'ensemble $\mathbb{P}(E)$ des droites vectorielles de E est appelé* espace projectif *associé à E. Par convention, l'espace projectif associé à l'espace vectoriel nul est l'ensemble vide : $\mathbb{P}(0) = \emptyset$.*

On définit une relation d'équivalence sur $E \setminus \{0\}$:

$$x \sim y \Leftrightarrow kx = ky \Leftrightarrow \exists a \in k^\times,\ y = ax.$$

On note p l'application $E \setminus \{0\}$ vers $\mathbb{P}(E)$ définie par $p(x) \coloneqq kx$. Elle induit une bijection de $(E \setminus \{0\})/\sim$ sur $\mathbb{P}(E)$.

Par convention, la dimension de l'espace projectif $\mathbb{P}(E)$ est $\dim_k E - 1$ et on note $\mathbb{P}^n_k \coloneqq \mathbb{P}(k^{n+1})$.

Définition 2.2. *Un* sous-espace projectif *de $\mathbb{P}(E)$ est une partie de la forme $\mathbb{P}(V)$ où V est un sous-k-espace vectoriel de E.*

On vérifie qu'une intersection de sous-espaces projectifs est toujours un sous-espace projectif. En effet, pour $(V_i)_{i\in I}$ une famille de sous-k-espaces vectoriels de E, on a

$$\bigcap_{i\in I} \mathbb{P}(V_i) = \mathbb{P}(\bigcap_{i\in I} V_i).$$

On peut donc définir le sous-espace projectif projectif engendré par une partie quelconque de $S \subset \mathbb{P}(E)$. On le note $\mathbb{P}(S)$.

Théorème 2.3. *Soient L et L' deux sous-espaces projectifs de $\mathbb{P}(E)$. On a alors*

$$\dim L + \dim L' = \dim(L \cap L') + \dim \mathbb{P}(L \cup L').$$

Démonstration. En posant $L = \mathbb{P}(V)$ et $L' = \mathbb{P}(V')$, on a $L \cap L' = \mathbb{P}(V \cap V')$ et $\mathbb{P}(L \cup L') = \mathbb{P}(V + V')$, l'égalité est alors une conséquence immédiate de l'égalité

$$\dim_k V + \dim_k V' = \dim_k(V \cap V') + \dim_k(V + V'). \qquad \square$$

Corollaire 2.4. *Si L et L' sont deux sous-espaces projectifs de $\mathbb{P}(E)$ tels que $\dim L + \dim L' \geqslant \dim \mathbb{P}(E)$, alors $L \cap L' \neq \emptyset$.*

On appelle *droite projective* un espace projectif de dimension 1, *plan projectif* un espace projectif de dimension 2, etc. En particulier, dans le plan projectif, le corollaire ci-dessus implique que l'intersection de deux droites projectives est toujours non vide. Plus généralement, un *hyperplan projectif* de $\mathbb{P}^n_k$ est un sous-espace projectif de dimension $n - 1$.

2.2 Coordonnées homogènes

Soit $\underline{e} = (e_0, \ldots, e_n)$ une base de E. On a donc ici $n = \dim \mathbb{P}(E)$. Soit $x \in \mathbb{P}(E)$. On peut noter $x = p(y)$ pour $y \in E \smallsetminus \{0\}$.

Définition 2.5. *Un* système de coordonnées homogènes *de x est un $(n+1)$-uplet $(x_0, \ldots, x_n) \in k^{n+1} \smallsetminus \{0\}$ tel que $x = p(x_0 e_0 + \cdots + x_n e_n)$.*

Dans une base donnée, il n'y a pas unicité du système de coordonnées homogènes de x. Si $(x_0, \ldots, x_n)$ est un système de coordonnées homogènes de x, les autres systèmes de coordonnées homogènes de x sont les $(n+1)$-uplets $(ax_0, \ldots, ax_n)$ où $a \in k^\times$.

On note $(x_0 : \ldots : x_n)$ le point de $\mathbb{P}(E)$ dont $(x_0, \ldots, x_n)$ est un système de coordonnées homogènes. Pour tout $a \in k^\times$, on a donc

$$(x_0 : \ldots : x_n) = (ax_0 : \ldots : ax_n).$$

Réciproquement, si $(x_0 : \ldots : x_n) = (y_0 : \ldots : y_n)$, il existe $a \in k^\times$ tel que $y_i = ax_i$ pour tout $0 \leqslant i \leqslant n$.

Si $a \in k^\times$, remplacer la base $\underline{e}$ par la base $a\underline{e}$ ne change pas les systèmes de coordonnées homogènes associés aux point de $\mathbb{P}(E)$. La base $\underline{e}$ est entièrement déterminée, à homothétie près, par les $n+2$-points

$$p(e_0), \ldots, p(e_n), p(e_0 + \cdots + e_n).$$

Ces $(n+2)$ points ont la propriété particulière que $n+1$ quelconques d'entre eux ne sont jamais dans un même hyperplan. Réciproquement, une famille de $n+2$ points vérifiant cette propriété détermine entièrement une classe d'homothétie de bases de E. Il est donc légitime d'introduire la définition suivante.

Définition 2.6. *Un* repère projectif *de $\mathbb{P}(E)$ est la donnée de $n+2$ points tels que $n+1$-quelconques d'entre eux n'appartiennent jamais à un même hyperplan.*

On a en fait démontré le résultat suivant.

Proposition 2.7. *L'ensemble des bases de E à homothétie près est en bijection naturelle avec les repères projectifs de $\mathbb{P}(E)$.*

En d'autres termes, si on fixe un repère projectif $P_0, \ldots, P_{n+1}$ de $\mathbb{P}(E)$, on identifie $\mathbb{P}(E)$ à $\mathbb{P}(k^{n+1})$ de telle sorte que P_i corresponde au point $(0 : \ldots : 0 : 1 : 0 : \ldots : 0)$ (le 1 étant à la i-ème place) et P_{n+1} au point $(1 : \ldots : 1)$.

Exemple 2.8. Un repère projectif de $\mathbb{P}^2_k$ et constitué de 4 points tels que 3 d'entre eux ne sont jamais alignés.

2.3 Homographies

Soit $u \in \mathrm{GL}(E)$ une application linéaire bijective de E sur lui-même. L'automorphisme u induit une permutation $\mathbb{P}(u)$ de $\mathbb{P}(E)$ définie par $kx \mapsto ku(x)$ et appelée *homographie*.

Si u et v sont dans $\mathrm{GL}(E)$, on a $v \circ u \in \mathrm{GL}(E)$ et $\mathbb{P}(v \circ u) = \mathbb{P}(v) \circ \mathbb{P}(u)$ de sorte que l'ensemble G des homographies de $\mathbb{P}(E)$ forme un groupe et que l'application $\mathbb{P} : \mathrm{GL}(E) \to G$ est un morphisme surjectif de groupes. Si $\dim_k E \geqslant 2$, on vérifie aisément que $\mathbb{P}(u) = \mathrm{Id}_{\mathbb{P}(E)}$ si et seulement si u est une homothétie de sorte que le morphisme $\mathbb{P}$ identifie le groupe $\mathrm{PGL}(E) \coloneqq \mathrm{GL}(E)/k^\times$ au groupe G des homographies de $\mathbb{P}(E)$.

Étudions l'effet des homographies sur les repères projectifs.

Théorème 2.9. *Soient $(P_0, \ldots, P_{n+1})$ et $(Q_0, \ldots, Q_{n+1})$ deux repères projectifs de $\mathbb{P}(E)$. Il existe une homographie h de $\mathbb{P}(E)$ telle que $h(P_i) = Q_i$ pour $0 \leqslant i \leqslant n+1$. Autrement dit le groupe $\mathrm{PGL}(E)$ opère simplement et transitivement sur l'ensemble des repères projectifs de $\mathbb{P}(E)$.*

Démonstration. Il existe une base $\underline{e} = (e_0, \ldots, e_n)$ de E telle que $P_i = p(e_i)$ et $P_{n+1} = p(e_0 + \cdots + e_n)$. De même il existe une base $\underline{f} = (f_0, \ldots, f_n)$ telle que $Q_i = p(f_i)$ et $Q_{n+1} = p(f_0 + \cdots + f_n)$. Il existe alors une unique application linéaire $u \in \mathrm{GL}(E)$ telle que $u(e_i) = f_i$ pour $0 \leqslant i \leqslant n$. Comme les bases $\underline{e}$ et $\underline{f}$ sont déterminées de façon unique à homothétie près, il en est de même de u. □

Exactement comme en géométrie affine, nous avons deux points de vue équivalents en géométrie projective : changer de repère projectif ou appliquer une homographie.

2.4 Espaces affines et espaces projectifs

Soit $n \geqslant 1$. Dans l'espace projectif $\mathbb{P}^n_k$, considérons H_0 l'hyperplan projectif défini par l'équation $x_0 = 0$. Si P est un point de $\mathbb{P}^n_k \smallsetminus H_0$, il existe un unique n-uplet $(y_1, \ldots, y_n) \in$

k^n tel que

$$P = (1 : y_1 : \ldots : y_n).$$

On a donc une bijection entre k^n et $\mathbb{P}^n_k \smallsetminus H_0$ donnée par $(y_1, \ldots, y_n) \mapsto (1 : y_1 : \ldots : y_n)$.

Par ce procédé on plonge $\mathbb{A}^n_k$ dans $\mathbb{P}^n_k$ en l'identifiant au complémentaire de l'hyperplan H_0. Pour cette raison, on appelle H_0 *l'hyperplan à l'infini* de $\mathbb{A}^n_k$.

Remarque 2.10. Comme le groupe des homographies d'un espace projectif $\mathbb{P}(E)$ agit transitivement sur les hyperplans projectifs, étant donné un hyperplan H de $\mathbb{P}(E)$, on peut toujours trouver un repère projectif de $\mathbb{P}(E)$ dans lequel H s'identifie à l'hyperplan à l'infini de l'espace affine $\mathbb{A}^n_k$.

Exemple 2.11.

a) On peut plonger $\mathbb{A}^1_k$ dans $\mathbb{P}^1_k$ par $x \mapsto (1 : x)$. Dans ce cas, le complémentaire de $\mathbb{A}^1_k$ est le point à l'infini $(0 : 1)$. De sorte que

$$\mathbb{P}^1_k = \mathbb{A}^1_k \cup \{(0 : 1)\}.$$

b) Plongeons $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k = \{(x : y : z)\}$ via l'application $(x, y) \mapsto (x : y : 1)$. La droite à l'infini, H_∞ est alors l'ensemble $\{(x : y : 0)\}$. Soit D une droite de $\mathbb{A}^2_k$ d'équation $aX + bY + c = 0$ où $(a, b) \neq (0, 0)$. Il existe alors une unique droite projective L de $\mathbb{P}^2_k$ telle que $L \cap \mathbb{A}^2_k = D$. Il s'agit de la droite d'équation $aX + bY + cZ = 0$. Calculons l'intersection de L avec la droite à l'infini H_∞

$$\begin{aligned} L \cap H_\infty &= \{(x : y : z),\ ax + by + cz = 0,\ z = 0\} \\ &= \{(x : y : 0) \mid ax + by = 0\} \\ &= \{(-b : a : 0)\}. \end{aligned}$$

Ainsi L et la droite H_∞ s'intersectent en un unique point. La droite L s'appelle la clôture projective de D. Le calcul qui précède montre que deux droites affines D_1 et D_2 sont parallèles si et seulement si elles ont le même point à l'infini : deux droites parallèles s'intersectent à l'infini !

c) Plus généralement si on plonge $\mathbb{A}^n_k$ dans $\mathbb{P}^n_k$ et que l'on note H_∞ son complémentaire dans $\mathbb{P}^n_k$, l'intersection d'un hyperplan projectif $H \neq H_\infty$ avec $\mathbb{A}^n_k$ est un hyperplan affine et tout hyperplan affine de $\mathbb{A}^n_k$ s'obtient de façon unique par ce procédé.

On peut encore essayer de généraliser le dernier exemple en remplaçant les équations linéaires des hyperplans par des équations polynomiales. On entre ainsi dans le cadre de la géométrie algébrique projective. Il faut cependant prendre garde au fait suivant. Si $F \in k[X_0, \ldots, X_n]$ est un polynôme, on peut avoir $P(x_0, \ldots, x_n) = 0$ mais $P(ax_0, \ldots, ax_n) \neq 0$ pour un certain $a \in k^\times$. Cependant, cette mésaventure ne se produit pas lorsque P est un polynôme *homogène* de $k[X_0, \ldots, X_n]$, autrement dit lorsque tous ses monômes ont le même degré total. Ce degré est alors appelé le degré du polynôme P. En effet, si P est un polynôme homogène de degré d, on a, pour tout $a \in k$,

$$P(aX_0, \ldots, aX_n) = a^d P(X_0, \ldots, X_n).$$

2.5 Variétés algébriques projectives

Pour la raison que l'on vient de voir, il est préférable, dans le cas projectif, de se limiter à la considération des objets homogènes. On fixe dans toute cette partie un corps k algébriquement clos.

Soit $n \geqslant 1$. Un polynôme *homogène* de degré d de $k[X_0, \ldots, X_n]$ est un élément du sous-k-espace vectoriel engendré par les monômes de degré d. On peut montrer qu'un polynôme $P \in k[X_0, \ldots, X_n]$ est homogène de degré d si et seulement si, pour tout $a \in k^\times$, on a $P(aX_0, \ldots, aX_n) = a^d P(X_0, \ldots, X_n)$.

Un idéal de $k[X_0, \ldots, X_n]$ est dit *homogène* s'il est engendré par des éléments homogènes de $k[X_0, \ldots, X_n]$.

Exemple 2.12. L'idéal (X, Y^2) de $k[X, Y]$ est homogène. L'idéal $(X + Y^2)$ ne l'est pas.

Définition 2.13. *Soit $I \subset k[X_0, \ldots, X_n]$ un idéal homogène. On note $V_p(I)$ la partie de $\mathbb{P}_k^n$ définie par*

$$V_p(I) \coloneqq \{(x_0 : \ldots : x_n) \in \mathbb{P}_k^n \mid \forall F \in I,\, F(x_0, \ldots, x_n) = 0\}.$$

Une partie de $\mathbb{P}_k^n$ de la forme $V_p(I)$ est appelée partie algébrique *de $\mathbb{P}_k^n$ ou encore* variété algébrique projective.

Exactement comme dans le cas affine, on a les propriétés suivantes :

— $I \subset J \Rightarrow V_p(J) \subset V_p(I)$;
— $V_p(I + J) = V_p(I) \cap V_p(J)$;
— $V_p(IJ) = V_p(I \cap J) = V_p(I) \cup V_p(J)$;
— $V_p(0) = \mathbb{P}_k^n$ et $V_p(k[X_0, \ldots, X_n]) = V_p(X_0, \ldots, X_n) = \emptyset$.

La seule véritable nouveauté vient de l'égalité $V_p(X_0, \ldots, X_n) = \emptyset$ alors que $(X_0, \ldots, X_n) \subsetneq k[X_0, \ldots, X_n]$. On a de même une version projective du théorème des zéros.

Théorème 2.14 (Théorème des zéros projectif)**.** *Soit I un idéal homogène de $k[X_0, \ldots, X_n]$. On a alors*

$$\begin{aligned} V_p(I) = \emptyset &\Leftrightarrow \exists m \geqslant 0,\, (X_0, \ldots, X_n)^m \subset I \\ &\Leftrightarrow (X_0, \ldots, X_n) \subset \sqrt{I}. \end{aligned}$$

Démonstration. On se ramène au cas affine. Remarquons que $V_p(I) = p(V(I) \smallsetminus \{(0, \ldots, 0)\})$. D'où

$$\begin{aligned} V_p(I) = \emptyset &\Leftrightarrow V(I) \subset \{(0, \ldots, 0)\} = V(X_0, \ldots, X_n) \\ &\Leftrightarrow (X_0, \ldots, X_n) \subset \sqrt{I}. \end{aligned}$$

□

Définition 2.15. *Soit $W \subset \mathbb{P}_k^n$. On note $I_p(W)$ l'idéal homogène de $k[X_0, \ldots, X_n]$ engendré par les polynômes homogènes de degré > 0 s'annulant sur W.*

Comme dans le cas affine, on a $W = V_p(I_p(W))$ si et seulement si W est une variété algébrique projective et, pour un idéal homogène $I \subsetneq k[X_0, \ldots, X_n]$, on a $\sqrt{I} = I_p(V_p(I))$.

Remarque 2.16. Remarquons que si $W = \emptyset$, alors par définition $I_p(W) = k[X_0, \cdots, X_n]$.

Définition 2.17. *Une variété algébrique projective W est dite* irréductible *si elle est non vide et si $W = W_1 \cup W_2$ avec W_1 et W_2 des variétés algébriques projectives, on a $W = W_1$ ou $W = W_2$.*

Proposition 2.18. *Une variété algébrique projective $W \subset \mathbb{P}^n_k$ est irréductible si et seulement si $I_p(W)$ est un idéal premier différent de $(X_0, \ldots, X_n)$. De plus, si $I \subsetneq k[X_0, \ldots, X_n]$ est un idéal homogène premier différent de $(X_0, \ldots, X_n)$, alors $V_p(I)$ est une variété algébrique projective irréductible.*

L'ensemble des parties algébriques projectives de $\mathbb{P}^n_k$ est l'ensemble des fermés d'une topologie appelée *topologie de Zariski* sur $\mathbb{P}^n_k$. Si W est une partie de $\mathbb{P}^n_k$, l'adhérence de W dans $\mathbb{P}^n_k$ pour la topologie de Zariski est l'ensemble $V_p(I_p(W))$.

Si $H \subset \mathbb{P}^n_k$ est un hyperplan projectif, il existe une homographie h de $\mathbb{P}^n_k$ telle que $h(H_0) = H$ où H_0 est l'hyperplan projectif d'équation $X_0 = 0$. La composition de la bijection $\mathbb{A}^n_k \simeq \mathbb{P}^n_k \smallsetminus H_0$ donnée par $(y_1, \ldots, y_n) \mapsto (1 : y_1 : \ldots : y_n)$ avec h induit une bijection $\mathbb{A}^n_k \simeq \mathbb{P}^n_k \smallsetminus H$. C'est un isomorphisme pour les différentes topologies de Zariski que l'on appelle aussi *carte affine*.

Remarque 2.19. Soit $F \in k[X_0, \ldots, X_n]$ un polynôme homogène de degré $d > 0$. Décomposons $F = F_1 \cdots F_r$ en produit de polynômes irréductibles. On vérifie facilement que tous les F_i sont homogènes de degrés > 0. On a alors

$$V_p(F) = V_p(F_1) \cup \cdots \cup V_p(F_r).$$

Ainsi $V_p(F)$ est irréductible si et seulement si les F_i sont identiques à un scalaire près, autrement dit si et seulement si $F = aF_1^r$ pour un certain $a \in k^\times$. Dans ce cas on a $\sqrt{(F)} = (F_1)$.

2.6 Intersection avec une carte affine

Soit k un corps algébriquement clos. On plonge $\mathbb{A}^n_k$ dans $\mathbb{P}^n_k$ via la carte affine $(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$. De sorte que l'hyperplan projectif d'équation $X_0 = 0$ s'identifie à l'hyperplan à l'infini de $\mathbb{A}^n_k$. Soit $F \in k[X_0, \ldots, X_n]$ un polynôme homogène de degré $d > 0$. On définit le polynôme « déshomogénéisé » :

$$F_*(X_1, \ldots, X_n) \coloneqq F(1, X_1, \ldots, X_n).$$

Réciproquement si $G \in k[X_1, \ldots, X_n]$ est un polynôme non nul, on définit « l'homogénéisé » :

$$G^*(X_0, \ldots, X_n) \coloneqq X_0^d G\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right).$$

où d désigne le degré total de G. Le polynôme G^* est alors homogène de degré d.

Soit $I \subset k[X_0, \ldots, X_n]$ un idéal homogène. On définit alors

$$I_* \coloneqq \{F_*,\, F \in I\}.$$

Il s'agit d'un idéal de $k[X_1, \ldots, X_n]$.

Les démonstrations des deux résultats qui suivent fournissent de bons exercices pour se familiariser avec la géométrie algébrique projective.

Proposition 2.20. *On a $V_p(I) \cap \mathbb{A}_k^n = V(I_*)$. De plus, si $V_p(I)$ est irréductible et si $V(I_*)$ est non vide, alors $V_p(I) \cap \mathbb{A}_k^n$ est une variété algébrique affine irréductible.*

Proposition 2.21. *Soit $G \in k[X_1, \ldots, X_n]$ un polynôme non nul. L'adhérence de Zariski de $V(G)$ dans $\mathbb{P}_k^n$ est $V_p(G^*)$. Si de plus $V(G)$ est irréductible, il en est de même de $V_p(G^*)$.*

Remarque 2.22. Il faut prendre garde au fait que si W est une variété algébrique projective, l'irréductibilité de la variété affine $W \cap \mathbb{A}_k^n$ n'implique pas l'irréductibilité de W. Par exemple si W est l'union $H \cup H_\infty$ de deux hyperplans où H_∞ est l'hyperplan à l'infini et si $H \neq H_\infty$, on a $W \cap \mathbb{A}_k^n = H \cap \mathbb{A}_k^n$ qui est irréductible alors que W ne l'est manifestement pas.

Par ailleurs, si $W = V(F, G) \subset \mathbb{A}_k^n$, il n'est pas toujours vrai que l'adhérence de Zariski projective de W coïncide avec $V_p(F^*, G^*)$.

Notons que l'image d'une partie algébrique projective par une homographie est encore une partie algébrique projective. Ainsi la nature algébrique d'une partie de l'espace projectif n'est pas affectée par un changement de repère projectif.

2.7 Dimension d'une variété projective

Supposons que k est algébriquement clos. Soit $V \subset \mathbb{P}_k^n$ une variété projective irréductible. On choisit une carte affine $i : \mathbb{A}_k^n \hookrightarrow \mathbb{P}_k^n$ telle que $V \cap i(\mathbb{A}_k^n)$ est non vide. L'image réciproque $i^{-1}(V)$ est alors un fermé de $\mathbb{A}_k^n$, c'est-à-dire une variété affine. D'après la proposition 2.20, la variété affine $i^{-1}(V)$ est irréductible. Si $P \in V \cap i(\mathbb{A}_k^n)$, on appelle *espace tangent* à V en P, l'adhérence de $i(T_{i^{-1}(P)}(i^{-1}(V)))$. Il s'agit d'un sous-espace projectif de $\mathbb{P}_k^n$ dont la dimension est la dimension de $T_{i^{-1}(P)}(i^{-1}(V))$. On le note $T_P(V)$. C'est un petit exercice de vérifier que $T_P(V)$ ne dépend que de P et de V et non du choix de i. Comme tout point de V est contenu dans une certaine carte affine, on a ainsi défini l'espace tangent en tout point de V.

Définition 2.23. *On appelle* dimension *d'une variété projective irréductible V la borne inférieure des dimensions de ses espaces tangents. On appelle* dimension *d'une variété*

projective la borne supérieure des dimensions de ses composantes irréductibles. Une variété projective est dite équidimensionnelle si toutes ses composantes irréductibles ont la même dimension.

On dit qu'un point $P \in V$ d'une variété projective irréductible est lisse *si* $\dim(V) = \dim(T_P(V))$. *La variété V est lisse si tous ses points le sont.*

Proposition 2.24. *L'ensemble des points lisses d'une variété projective irréductible est un ouvert dense de V.*

Démonstration. Si V est une variété projective irréductible et si $i : \mathbb{A}_k^n \hookrightarrow \mathbb{P}_k^n$ est une carte affine telle que $V \cap i(\mathbb{A}_k^n) \neq \emptyset$ alors $V \cap i(\mathbb{A}_k^n)$ est un ouvert de V, dense par irréductibilité de V. Si $P \in V$ est un point tel que $\dim(T_P(V)) = \dim(V)$ et si j est une carte affine telle que $V \cap j(\mathbb{A}_k^d) \neq \emptyset$, on a donc $V \cap i(\mathbb{A}_k^n) \cap j(\mathbb{A}_k^d) \neq \emptyset$, ce qui implique que $\dim(V) = \dim(i^{-1}(V))$. De plus, on en déduit que les points lisses de $V \cap i(\mathbb{A}_k^n)$ sont les images par i des points lisses de $i^{-1}(V)$, ils forment donc une partie ouverte de $V \cap i(\mathbb{A}_k^n)$. L'ensemble des points lisses de V est donc une union d'ouverts de V et est donc un ouvert de V. Cet ouvert est non vide, donc dense par irréductibilité de V. □

Remarque 2.25. Si V est une variété projective irréductible et si $i : \mathbb{A}_k^n \hookrightarrow \mathbb{P}_k^n$ est une carte affine telle que $V \cap i(\mathbb{A}_k^n) \neq \emptyset$ alors les variétés $i^{-1}(V)$ et V ont la même dimension.

2.8 Fonctions rationnelles sur les variétés projectives

Soit k un corps algébriquement clos. Soit $V \subset \mathbb{P}_k^n$ une variété algébrique projective irréductible. D'après la proposition 2.18, l'idéal homogène $I_p(V)$ est alors premier et l'anneau $A[V] \coloneqq k[X_0, \ldots, X_n]/I_p(V)$ est intègre. Contrairement au cas des variétés affines, les éléments de $A[V]$ ne peuvent pas être naturellement identifiés à des fonctions définies sur V. En effet si $P = (x_0 : \ldots : x_n) \in V$ et si $f \in k[X_0, \ldots, X_n]$ est un élément de degré d, on a

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n).$$

Cependant l'évaluation du *quotient* de deux éléments *de même degré* de $A[V]$ en $(x_0, \ldots, x_n)$ ne dépend que du point associé de $\mathbb{P}_k^n$. Il est donc naturel de poser la définition suivante.

Définition 2.26. *Soit $V \subset \mathbb{P}_k^n$ une variété algébrique projective irréductible. On appelle* corps des fonctions rationnelles *de V l'ensemble $k(V)$ des éléments f du corps des fractions de $A[V] \coloneqq k[X_0, \ldots, X_n]/I_p(V)$ qui peuvent s'écrire sous la forme $\frac{g}{h}$ où g et h sont les images dans $A[V]$ de deux éléments homogènes de même degré de $k[X_0, \ldots, X_n]$.*

On vérifie que $k(V)$ est un sous-corps du corps des fractions de l'anneau intègre $A[V]$. Si $f \in k(V)$ on définit l'*ensemble de définition de f* comme l'ensemble des points $P = (x_0 : \ldots : x_n) \in V$ pour lesquels il existe g et h éléments homogènes de même degré

de $k[X_0, \ldots, X_n]$ tels que $f = \frac{g}{h}$ dans $k(V)$ et $h(x_0, \ldots, x_n) \neq 0$. La *valeur* de f en P est alors définie par

$$f(P) \coloneqq \frac{g(x_0, \ldots, x_n)}{h(x_0, \ldots, x_n)}.$$

Comme g et h sont homogènes de même degré, cette valeur ne dépend pas du choix de système de coordonnées homogènes de P. Elle ne dépend pas non plus du choix de g et h.

On définit alors l'*anneau local de* V en un point P comme étant l'ensemble des éléments $f \in k(V)$ qui sont définis en P. Il s'agit d'un sous-anneau de $k(V)$, noté $k[V]_P$. Il s'agit d'un anneau local dont l'unique idéal maximal est l'ensemble $\mathfrak{m}_P$ des fonctions s'annulant en P. On a de plus

$$k[V]_P/\mathfrak{m}_P \xrightarrow{\sim} k.$$

Le théorème suivant est l'analogue algébrique du « principe du maximum » et indique que l'on peut penser aux variétés algébriques projectives comme à des objets topologiquement « compacts ».

Théorème 2.27. *Soit $V \subset \mathbb{P}^n_k$ une variété algébrique projective irréductible. Les seules fonctions rationnelles sur V qui sont définies partout sont les fonctions constantes.*

Démonstration. Soit $f \in k(V)$ une fonction rationnelle définie sur V tout entier. Pour tout point $P \in V$, il existe deux polynômes homogènes de même de degré, g_P et h_P tels que $f = \frac{g_P}{h_P}$ et tels que $h_P(P) \neq 0$. Ainsi on a, dans $\mathbb{P}^n_k$,

$$\bigcap_{P \in V} V(h_P) \cap V = \emptyset.$$

On en conclut, d'après le théorème 2.14, que

$$(X_0, \ldots, X_n) \subset \sqrt{I_p(V) + (h_P;\, P \in V)}.$$

Il existe donc $M \geqslant 1$ tel que, pour tout $0 \leqslant i \leqslant n$, $X_i^M \in I_p(V) + (h_P;\, P \in V)$. Soit L le corps des fractions de l'anneau $A[V]$. Par définition de g_P et h_P, on sait que, pour tout $P \in V$, $h_P f$ est l'image dans $A[V]$ d'un polynôme homogène de même degré que g_P et h_P. On en conclut que, pour tout $0 \leqslant i \leqslant n$, $X_i^M f$ est l'image dans $A[V]$ d'un polynôme homogène de degré M. Comme tout polynôme homogène de degré $N \coloneqq Mn$ appartient à l'idéal $(X_0^N, \ldots, X_n^N)$ de $k[X_0, \ldots, X_n]$, on en conclut que pour tout polynôme homogène h de degré N, hf est l'image dans $A[V]$ d'un polynôme homogène de degré N. En notant $A_N[V]$ le sous-anneau image dans $A[V]$ engendré par les images des monômes de degré N, on en conclut que $A_N[V]f \subset A_N[V]$. Par récurrence, $A_N[V]f^m \subset A_N[V]$ pour tout $m \geqslant 1$, en particulier le sous-$A_N[V]$-module de L engendré par $(f^i)_{i \geqslant 0}$ est inclus dans $X_0^{-N} A_N[V]$ qui est un $A_N[V]$-module de type fini. Comme l'anneau $A_N[V]$ est le quotient d'un anneau de polynômes en un nombre fini de variables, il s'agit d'un anneau noethérien. On en conclut que la suite croissante de sous-modules $\left(\sum_{i=0}^k A_N[V] f^i\right)_{k \geqslant 0}$

de $X_0^{-N} A_N[V]$ est stationnaire et donc qu'il existe $q \geqslant 1$, ainsi que $a_0, \ldots, a_{q-1}$ dans $A_N[V]$ vérifiant

$$f^q + \sum_{i=0}^{q-1} a_i f^i = 0.$$

Soit g et h deux polynômes homogènes de même degré de $k[X_0, \ldots, X_n]$ tels que $f = \frac{g}{h}$ et soient $\tilde{a}_i$ des éléments de $k[X_0, \ldots, X_n]$ relevant les éléments a_i, cette relation peut se réécrire

$$g^q + \sum_{i=0}^{q-1} \tilde{a}_i g^i h^{q-i} \in I_p(V).$$

En utilisant le fait que $I_p(V)$ est un idéal homogène, on remarque que cette égalité reste vraie en remplaçant chaque polynôme $\tilde{a}_i$ par son terme constant. En réduisant modulo $I_p(V)$, on en conclut que l'on peut supposer $a_i \in k$ et donc que f est un élément de L qui est algébrique sur k. Comme k est algébriquement clos, on a nécessairement $f \in k$. □

Si $f \in k(V)$ est définie et s'annule en un point $P \in k(V)$, on dit que P est un *zéro* de f. Si, au contraire, la fonction f n'est pas définie en P, on dit que P est un *pôle* de f.

Remarque 2.28. Le théorème 2.27 implique que toute fonction rationnelle non constante sur V a au moins un pôle et un zéro.

2.9 Morphismes de variétés projectives

Pour étudier les fonctions sur les variétés projectives, il semble donc judicieux de ne pas se limiter aux fonctions définies partout. C'est pourquoi on introduit la définition suivante.

Définition 2.29. *Soit V une variété projective irréductible et soit $U \subset V$ un ouvert de V. Une fonction $f : U \to k$ est dite* régulière *s'il existe $F \in k(V)$ telle que pour tout $P \in U$, $F \in k[V]_P$ et $f(P) = F(P)$.*

On peut alors définir un morphisme de variétés projectives.

Définition 2.30. *Soient V et W deux variétés projectives irréductibles. Un* morphisme *de V vers W est une application continue $\phi : V \to W$ telle que, pour tout ouvert $U \subset W$, et toute fonction régulière f définie sur U, la fonction $f \circ \phi$ est une fonction régulière sur l'ouvert $\phi^{-1}(U) \subset V$.*

On vérifie facilement que la restriction d'une fonction régulière sur un ouvert U est aussi régulière en restriction à un ouvert $U' \subset U$. De plus si $U = \bigcup_{i=1}^{r} U_i$ est une union finie d'ouverts et si $f : U \to k$ est une fonction, alors pour que f soit régulière il faut et il suffit que sa restriction à chaque ouvert U_i soit régulière. On en déduit facilement le critère suivant.

Proposition 2.31. *Soit $\phi : V \to W$ une application continue entre variétés projectives irréductibles. Alors ϕ est un morphisme si et seulement si il existe des recouvrement ouverts $V = \bigcup_{i=1}^{r} V_i$ et $W = \bigcup_{i=1}^{r} W_i$ tels que $\phi(V_i) \subset W_i$ et tels que si f est régulière sur W_i, alors $f \circ \phi$ est régulière sur V_i.*

Exemple 2.32. Soient $P_1, \ldots, P_m$ des polynômes homogènes de même degré de $k[X_1, \ldots, X_n]$. On suppose que pour tout $x \in V$, les éléments $P_1(x), \ldots, P_m(x)$ ne sont pas tous nuls et que $(P_1(x), \ldots, P_m(x)) \in W$. Alors l'application

$$(x_1, \ldots, x_n) \longmapsto (P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n))$$

est un morphisme de V dans W.

Exemple 2.33. Considérons $V = V_p(Y^2Z - X^3 - XZ^2 - Z^3) \subset \mathbb{P}^2_k$ et $W = \mathbb{P}^1_k$. Posons

$$\phi(x : y : z) = \begin{cases} (x : z) & \text{si } z \neq 0 \\ (1 : 0) & \text{si } x = z = 0. \end{cases}$$

Si $xz \neq 0$, on a

$$\phi(x : y : z) = (x^3 : zx^2) = (y^2z - xz^2 - z^3 : zx^2) = (y^2 - xz - z^2 : x^2).$$

Ainsi on peut écrire

$$\phi(x : y : z) = \begin{cases} (y^2 - xz - z^2 : x^2) & \text{si } y^2 - xz - z^2 \neq 0 \\ (0 : 1) & \text{si } y^2 - xz - z^2 = 0. \end{cases}$$

Posons $V_1 = \{(x : y : z) \in V \mid z \neq 0\}$ et $V_2 = \{(x : y : z) \in V \mid y^2 - xz - z^2 \neq 0\}$, $W_1 = \{(x : z) \in \mathbb{P}^1_k \mid z \neq 0\}$ et $W_2 = \{(x : z) \mid x \neq 0\}$, on vérifie facilement que ϕ induit des applications polynomiales de V_1 dans W_1 et de V_2 dans W_2. Comme $V = V_1 \cup V_2$, on en conclut que ϕ est bien un morphisme de V dans W.

Un *automorphisme* d'une variété projective V est un morphisme f de V dans V tel qu'il existe un morphisme g de V dans V vérifiant $g \circ f = f \circ g = \mathrm{Id}_V$.

2.10 Points rationnels

On suppose dans cette partie que k est un corps *parfait* non nécessairement algébriquement clos.

On rappelle qu'un corps est *parfait* s'il est de caractéristique 0 ou de caractéristique p, avec p un nombre premier, et que l'endomorphisme $x \mapsto x^p$ de k dans k est surjectif (et donc bijectif).

Les corps algébriquement clos et les corps finis sont des corps parfaits.

Fixons $\overline{k}$ une clôture algébrique de k. On note $\mathrm{Gal}(\overline{k}/k)$ le *groupe de Galois* de k. Il s'agit du groupe des automorphismes de corps σ de $\overline{k}$ tels que $\sigma|_k = \mathrm{Id}_k$. Le théorème fondamental de la théorie de Galois est le suivant.

Théorème 2.34. *On a* $\overline{k}^{\mathrm{Gal}(\overline{k}/k)} = k$.

Attention, ce résultat devient faux si k n'est pas supposée parfait.

Définition 2.35. *Soit I un idéal de $\overline{k}[X_1, \ldots, X_n]$. On dit que I est* défini sur k *si I est engendré par une famille d'éléments de $k[X_1, \ldots, X_n]$.*

Remarque 2.36.

1) Si un idéal I est défini sur k, l'idéal I est en fait engendré par une famille *finie* d'éléments de $k[X_1, \ldots, X_n]$.

2) Si un idéal I est homogène et défini sur k, il est engendré par une famille finie de polynômes homogènes de $k[X_1, \ldots, X_n]$.

3) Le groupe $\mathrm{Gal}(\overline{k}/k)$ agit sur $\overline{k}[X_1, \ldots, X_n]$ par

$$\sigma\left(\sum_{(i_1,\ldots,i_n)} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right) = \sum_{(i_1,\ldots,i_n)} \sigma(a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n}.$$

Un idéal de $\overline{k}[X_1, \ldots, X_n]$ est défini sur k si et seulement s'il est stable sous l'action de $\mathrm{Gal}(\overline{k}/k)$.

Définition 2.37. *Une variété algébrique affine (resp. projective) est dite* définie sur k *si elle est de la forme $V(I)$ (resp. $V_p(I)$) où I est un idéal (resp. idéal homogène) défini sur k. Si $V \subset \overline{k}^n$ est une variété algébrique définie sur k, l'ensemble de ses* points rationnels *est l'ensemble*

$$\begin{aligned} V(k) &\coloneqq \{x \in k^n \mid \forall F \in I,\, F(x) = 0\} \\ &= V \cap k^n. \end{aligned}$$

De façon analogue on définit l'ensemble des points rationnels d'une variété algébrique projective $V \subset \mathbb{P}^n_{\overline{k}}$ définie sur k comme étant

$$V(k) \coloneqq V \cap \mathbb{P}^n_k\,.$$

Exemple 2.38.

a) Les variétés $\mathbb{A}^n_{\overline{k}}$ et $\mathbb{P}^n_{\overline{k}}$ sont définies sur k. Leurs ensembles de points rationnels sont respectivement $\mathbb{A}^n_k$ et $\mathbb{P}^n_k$.

b) Si $k = \mathbb{R}$ et $\overline{k} = \mathbb{C}$, alors $\{i, -i\} \subset \mathbb{C}$ est définie sur k, mais $\{i\}$ ne l'est pas.

c) La courbe plane $C = V(X^2 + Y^2 + 1) \subset \mathbb{A}^2_{\overline{\mathbb{Q}}}$ est définie sur $\mathbb{Q}$ et $C(\mathbb{Q}) = \emptyset$.

Proposition 2.39. *Si V est une variété algébrique définie sur k, alors $I(V)$ (resp. $I_p(V)$) est un idéal défini sur k.*

Le groupe $\mathrm{Gal}(\overline{k}/k)$ agit sur $\mathbb{A}^n_{\overline{k}}$ et $\mathbb{P}^n_{\overline{k}}$ coordonnée par coordonnée. Une variété algébrique V est alors définie sur k si et seulement si elle est stable sous l'action de $\mathrm{Gal}(\overline{k}/k)$. On a alors

$$V(k) = V^{\mathrm{Gal}(\overline{k}/k)}.$$

2.11 Exercices

Exercice 2.1. Soit k un corps algébriquement clos. Soit $P \in k[X_0, \ldots, X_n]$. Montrer que P est un polynôme homogène de degré d si et seulement si, pour tout $a \in k^\times$, on a $P(aX_0, \ldots, aX_n) = a^d P(X_0, \ldots, X_n)$.

Exercice 2.2. Soit k un corps algébriquement clos. Soit $F(X, Y, Z) \in k[X, Y, Z]$ un polynôme homogène degré 2. Montrer que $V_p(F)$ est soit l'union de deux droites, éventuellement confondues, soit une conique irréductible, isomorphe à $V_p(XY + YZ + XZ)$.

Exercice 2.3. Soit k un corps algébriquement clos. Si $F \in k[X_1, \ldots, X_n]$ est un polynôme non nul, on pose $F^*(X_0, \ldots, X_n) \coloneqq X_0^d F(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$ où d est le degré de F. Si I est un idéal de $k[X_1, \ldots, X_n]$, on note I^* l'idéal de $k[X_0, \ldots, X_n]$ engendré par les éléments F^* où F parcourt les éléments non nuls de I. On plonge $\mathbb{A}_k^n$ dans $\mathbb{P}_k^n$ via $(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$. Montrer que l'adhérence de Zariski de $V(I)$ dans $\mathbb{P}_k^n$ est $V_p(I^*)$.

Exercice 2.4. Soit k un corps algébriquement clos. On note ϕ l'application de $\mathbb{A}_k^1$ vers $\mathbb{A}_k^3$ définie par $\phi(t) \coloneqq (t, t^2, t^3)$. On note W l'image de ϕ.

a) Montrer que W est une partie algébrique de $\mathbb{A}_k^3$. Déterminer l'idéal $I(W)$. Montrer qu'il est engendré par deux éléments.

b) Déterminer l'adhérence de Zariski de W dans $\mathbb{P}_k^3$. Montrer que

$$I_p(W) = (XY - TZ, Y^2 - XZ, X^2 - YT) \subset k[T, X, Y, Z]$$

c) Montrer que $I_p(W)$ ne peut pas être engendré par deux éléments homogènes.

d) En déduire que si $J = (F_1, \ldots, F_r)$, alors il n'est pas toujours vrai que $J^* = (F_1^*, \ldots, F_r^*)$.

Exercice 2.5. Soit k un corps algébriquement clos. On considère l'application $\Phi_{n,m}$ de $\mathbb{P}_k^n \times \mathbb{P}_k^m$ vers $\mathbb{P}_k^{nm+n+m}$ définie par

$$((x_0, \ldots, x_n), (y_0, \ldots, y_m)) \mapsto (x_i y_j)_{0 \leqslant i \leqslant n, 0 \leqslant j \leqslant m}$$

Montrer que $\Phi_{n,m}$ induit une bijection de $\mathbb{P}_k^n \times \mathbb{P}_k^m$ sur une partie algébrique de $\mathbb{P}_k^{nm+n+m}$.

Exercice 2.6. Soit k un corps algébriquement clos et soit $V \in \mathbb{P}_K^n$ une variété algébrique projective irréductible. Soit $H \subset \mathbb{P}_k^n$ un hyperplan projectif tel que $V \neq H$. On identifie alors $\mathbb{P}_k^n \smallsetminus H$ à l'espace affine $\mathbb{A}_k^n$. Montrer qu'il existe un isomorphe de k-algèbres $k(V) \simeq k(V \cap \mathbb{A}_k^n)$ et que, si $P \in V \cap \mathbb{A}_k^n$, cet isomorphisme identifie $k[V]_P$ et $k[V \cap \mathbb{A}_k^n]_P$.

Exercice 2.7. Soit A un anneau et soient I et J deux idéaux de A tels que $I + J = A$. Montrer que $IJ = I \cap J$ et que le morphisme canonique de A/IJ vers $A/I \oplus A/J$ est un isomorphisme. Donner une interprétation géométrique de ce résultat lorsque $A = k[X_1, \ldots, X_n]$, $I = I(V)$ et $J = I(W)$.

Exercice 2.8.

a) Soit I un idéal de $k[X_1, \ldots, X_n]$ et $A = k[X_1, \ldots, X_n]/I$. Montrer que l'intersection des idéaux maximaux de A est exactement l'ensemble des éléments nilpotents de A.

b) Soit A une k-algèbre de *dimension* finie sur k. Montrer que A possède un nombre fini d'idéaux maximaux (on pourra remarquer que si le produit de deux idéaux I et J est contenu dans un idéal premier $\mathfrak{p}$ alors $I \subset \mathfrak{p}$ ou $J \subset \mathfrak{p}$). Si $\mathfrak{m}$ est un idéal maximal de A, montrer qu'il existe un unique entier $e = e_{\mathfrak{m}} \geqslant 1$ tel que $\mathfrak{m}^e = \mathfrak{m}^{e+1}$ et $\mathfrak{m}^{e-1} \neq \mathfrak{m}^e$.

c) Soient $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ les idéaux maximaux de A. Montrer que $\prod_{i=1}^r \mathfrak{m}_i^{e_{\mathfrak{m}_i}} = 0$.

d) Montrer que le morphisme canonique $A \to \bigoplus_{i=1}^r A/\mathfrak{m}_i^{e_{\mathfrak{m}_i}}$ est un isomorphisme.

Exercice 2.9. Soient F et G deux éléments non nuls et premiers entre eux de $k[X, Y]$. Posons $d_1 = \deg F$ et $d_2 = \deg G$ les degrés totaux de F et G.

a) Soit $d \geqslant 0$ et soit $k[X, Y]_d$ l'ensemble des polynômes de $k[X, Y]$ de degré total inférieur ou égal à d. Calculer la dimension du k-espace vectoriel $k[X, Y]_d$.

b) Soit $d \geqslant d_1 + d_2$. On note $W_d \subset k[X, Y]_d$ l'ensemble des éléments de la forme $AF + BG$ où $\deg A \leqslant d - d_1$ et $\deg B \leqslant d - d_2$. Calculer la dimension de W_d et en conclure que $\dim_k k[X, Y]/(F, G) \leqslant d_1 d_2$.

c) On note F_{d_1} et G_{d_2} les termes dominants de F et G. Montrer que si $V(F)$ et $V(G)$ ne s'intersectent pas à l'infini, les polynômes F_{d_1} et G_{d_2} sont premiers entre eux.

d) Montrer que si $V(F)$ et $V(G)$ ne s'intersectent pas à l'infini, on a

$$\dim_k k[X, Y]/(F, G) \geqslant d_1 d_2$$

Exercice 2.10. Soit p un nombre premier et soit q une puissance de p. On note $\mathbb{F}_q$ le corps fini à q éléments. Si $n \geqslant 1$, calculer le cardinal de l'ensemble $\mathbb{P}^n_{\mathbb{F}_q}$.

Exercice 2.11. Soit k un corps algébriquement clos de caractéristique p, où p est un nombre premier. Soit $I \subset k[X_1, \ldots, X_n]$ un idéal engendré par des éléments de $\mathbb{F}_p[X_1, \ldots, X_n]$. Montrer que l'application $(x_1, \ldots, x_n) \mapsto (x_1^p, \ldots, x_n^p)$ induit une application polynomiale bijective de $V(I)$ dans $V(I)$ mais que c'est un isomorphisme si et seulement si $V(I)$ est fini.

Chapitre 3

Courbes planes et courbes elliptiques

Sauf mention du contraire, la lettre k désigne un corps algébriquement clos.

3.1 Courbes planes

Définition 3.1. *On appelle* courbe projective plane *une partie algébrique de $\mathbb{P}^2_k$ qui est équidimensionnelle de dimension* 1*.*

De même, on appelle courbe affine plane *une partie algébrique de $\mathbb{A}^2_k$ qui est équidimensionnelle de dimension* 1*.*

Proposition 3.2. *Une* courbe projective plane *est une variété projective de la forme $V_p(F) \subset \mathbb{P}^2_k$ où $F \in k[X,Y,Z]$ est un polynôme homogène de degré $d > 0$. De même, on appelle* courbe affine plane *une variété affine de la forme $V(F) \subset \mathbb{A}^2_k$ où F est un polynôme non constant de $k[X,Y]$.*

Démonstration. Commençons par le cas affine. Soit $F \in k[X,Y]$ un polynôme non inversible. Comme $k[X,Y]$ est factoriel, on peut écrire $F = F_1^{\alpha_1} \cdots F_r^{\alpha_r}$ avec F_i des polynômes irréductibles, on en conclut que $V(F)$ est l'union des $V(F_i)$ avec $V(F_i)$ irréductible. Il suffit donc de prouver que si F est irréductible, la partie algébrique $V(F)$ est de dimension 1. Comme $k[X,Y]$ est factoriel, l'idéal (F) est premier et on a donc $I(V(F)) = (F)$. Montrons que $\frac{\partial F}{\partial X}$ et $\frac{\partial F}{\partial Y}$ ne sont pas identiquement nuls sur F. Si c'était le cas, on aurait $F \mid \frac{\partial F}{\partial X}$ et $F \mid \frac{\partial F}{\partial Y}$. Pour des raisons de degré, on a donc $\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = 0$. Ceci implique soit que F est une constante, ce qui est faux, soit que le corps k est de caractéristique p, pour un nombre premier p, et qu'il existe un polynôme G tel que $F(X,Y) = G(X^p, Y^p)$. Si

$$G = \sum_{i,j} a_{i,j} X^i Y^j,$$

comme le corps k est algébriquement clos, il existe des éléments $b_{i,j} \in k$ tels que $a_{i,j,k} = b_{i,j}^p$ et finalement

$$F(X,Y) = \left(\sum_{i,j} b_{i,j} X^i Y^j \right)^p$$

Ceci contredit le fait que F est irréductible. Il existe donc un point $P \in V(F)$ pour lequel la matrice jacobienne est de rang 1 et donc $\dim(T_P V(F)) = 1$. Comme la matrice jacobienne de F en un point est de rang au plus 1, on a $\dim(T_P(F)) \geqslant 1$ en tout point de $V(F)$, ce qui prouve que $V(F)$ est de dimension 1.

Réciproquement si C est une partie algébrique irréductible de $\mathbb{A}_k^2$ qui est de dimension 1, il existe $F \in I(C)$ non inversible, donc $C \subset V(F)$. Comme C est irréductible, elle est contenue dans une des composantes irréductibles de $V(F)$. On a vu plus haut que ces composantes irréductibles sont de la forme $V(G)$ avec G irréductible. Il existe donc G irréductible tel que $C \subset V(G)$. Si $C \subsetneq V(G)$, le résultat de l'exercice 1.9 montre que $I(C)$ est un idéal maximal de $k[X,Y]$ et donc que C est réduit à un point par le théorème des zéros. En particulier C est de dimension 0, c'est une contradiction. Ainsi $C = V(G)$.

Le cas projectif est une conséquence des propositions 2.20 et 2.21. □

Soit $C = V_p(F)$ une courbe projective plane. Le Nullstellensatz fort implique que $I_p(C) = \sqrt{(F)}$. Soient $F_1, \ldots, F_r$ les diviseurs irréductibles de F. Ce sont des polynômes homogènes et on a $\sqrt{(F)} = (F_1 \cdots F_r)$. Il existe donc un polynôme homogène G, unique à multiplication près par un élément de $k^\times$, tel que $I_p(C) = (G)$. Les composantes irréductibles de C sont alors en bijection avec les diviseurs irréductibles de G et cette bijection est donnée par $D \mapsto V_p(D)$.

Définition 3.3. *Si C est une courbe projective plane, le* degré *de C est par définition le degré d'un polynôme homogène F tel que $I_p(C) = (F)$.*

Nous allons à présent démontrer une petite partie du théorème de Bezout : la finitude de l'ensemble $C_1 \cap C_2$.

Proposition 3.4. *Soient F_1 et F_2 deux polynômes non nuls de $k[X,Y]$, sans diviseur irréductible commun, alors $V(F_1) \cap V(F_2)$ est un ensemble fini.*

Démonstration. Il suffit de prouver que $(F_1, F_2) \cap k[X] \neq 0$. Supposons en effet ce fait prouvé. Par symétrie on a également $(F_1, F_2) \cap k[Y] \neq 0$. Il existe alors deux polynômes non nuls à une variable, $G(X)$ $H(Y)$, tels que $(G(X), H(Y)) \subset k[X,Y]$. Alors $k[X,Y]/(G(X), H(Y))$ est un k-espace vectoriel de dimension finie, car engendré par la famille finie $(X^i Y^j)$, où $0 \leqslant i \leqslant \deg G - 1$ et $0 \leqslant j \leqslant \deg H - 1$, c'est donc aussi le cas de $k[X,Y]/(F_1, F_2)$. Comme les points de $V(F_1) \cap V(F_2) = V(F_1, F_2)$ sont en bijection avec les idéaux maximaux de $k[X,Y]/(F_1, F_2)$, on en conclut que $V(F_1) \cap V(F_2)$ est fini puisque une k-algèbre de dimension finie possède un nombre fini d'idéaux maximaux (voir par exemple l'exercice 2.8).

Il reste à prouver que $(F_1, F_2) \cap k[X] \neq 0$. Supposons que $F_1 \notin k[X]$ et $F_2 \notin k[X]$ sinon il n'y a rien à faire. En particulier les polynômes F_1 et F_2 ne sont pas inversibles dans $k(X)[Y]$ et sont premiers entre eux dans $k(X)[Y]$. De sorte que $(F_1) + (F_2) = k(X)[Y]$. Il existe donc $\frac{A_1}{B_1}$ et $\frac{A_2}{B_2}$ dans $k(X)$ tels que $1 = \frac{A_1}{B_1}F_1 + \frac{1_2}{B_2}F_2$ et donc $B_1(X)B_2(X) = A_1B_2F_1 + A_2B_1F_2 \in (F_1, F_2)$. □

Corollaire 3.5. *Soient F_1 et F_2 deux polynômes homogènes sans diviseur premier en commun de $k[X, Y, Z]$. L'ensemble $V_p(F_1) \cap V_p(F_2)$ est fini.*

Démonstration. Commençons par vérifier que si H est un hyperplan de $\mathbb{P}^2_k$, l'ensemble $V_p(F_1) \cap V_p(F_2) \cap (\mathbb{P}^2_k \smallsetminus H)$ est fini. On peut se ramener au cas où H est l'hyperplan à l'infini du plongement de $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k$. Il suffit de traiter le cas où $V_p(F_1) \not\subset H$ et $V_p(F_2) \not\subset H$ de sorte que les polynômes $F_{1,*}$ et $F_{2,*}$ de $k[X, Y]$ ne sont pas inversibles. Ils sont premiers entre eux dans $k[X, Y]$, on peut donc appliquer la proposition 3.4 qui implique la finitude de l'ensemble

$$V_p(F_1) \cap V_p(F_2) \cap \mathbb{A}^2_k = V(F_{1,*}) \cap V(F_{2,*}).$$

On remarque qu'il existe trois hyperplans H_0, H_1, H_2 de $\mathbb{P}^2_k$ tels que $H_0 \cap H_1 \cap H_2 = \emptyset$ (prendre par exemple les hyperplans $V_p(X_i)$)). L'ensemble ci-dessous est alors fini

$$V_p(F_1) \cap V_p(F_2) = \bigcup_{i=0}^{2} (V_p(F_1) \cap V_p(F_2) \cap (\mathbb{P}^2_k \smallsetminus H_i)).$$ □

Dans la preuve ci-dessus, comme l'ensemble $V_p(F_1) \cap V_p(F_2)$ est fini, on peut trouver un hyperplan de $\mathbb{P}^2_k$ tel que $V_p(F_1) \cap V_p(F_2) \cap H = \emptyset$. Quitte à faire un changement de repère projectif, on peut supposer que l'hyperplan H est l'hyperplan à l'infini du plongement de $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k$ et donc que les courbes $C_1 \coloneqq V_p(F_1)$ et $C_2 \coloneqq V_p(F_2)$ ne s'intersectent pas à l'infini.

Proposition 3.6. *Soit C une courbe projective plane irréductible. Les fermés algébriques de C sont C ainsi que les parties finies de C.*

Démonstration. Soit $S \subsetneq C$ une partie algébrique de C. Alors par définition $S = V_p(I)$ pour un idéal homogène I. Il existe donc des polynômes homogènes $F_1, \ldots, F_r$ tels que $I = (F_1, \ldots, F_r)$ et donc que $S = V_p(F_1) \cap \cdots \cap V_p(F_r)$. Comme $S \subsetneq C$, il existe i tel que $C \not\subset V_p(F_i)$. Or le corollaire 3.5 implique que $C \cap V_p(F_i)$ est fini, donc S est fini. □

3.2 Courbes lisses

Soit $C \in \mathbb{A}^2_k$ une courbe affine plane. Soit $F \in k[X, Y]$ tel que $I(C) = (F)$. Si $P \in C$, la courbe C est *lisse* au point P si et seulement si le vecteur $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P)\right)$ est non nul. Un point de C qui n'est pas lisse est dit *singulier*. Si P est un point lisse de C, la

tangente T_pC à C en P est alors la droite affine vecteur directeur $\left(-\frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial X}(P)\right)$ et passant par P.

Dans le cas projectif, si C est une courbe projective plane et si $P \in C$, le point P est un point *lisse* de C si et seulement si le vecteur $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right)$ est non nul[1]. Un point de C qui n'est pas lisse est dit *singulier*. Si P est un point lisse de C, sa tangente $T_P(C)$ à C en P est la droite projective d'équation

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0.$$

Si C est une courbe projective plane, on note C^{sing} l'ensemble de ses points singuliers.

Proposition 3.7. *Soit C une courbe projective plane irréductible. L'ensemble C^{sing} est une partie finie de C.*

Démonstration. Ainsi C^{sing} est une partie algébrique de C. Comme l'ensemble des points lisses de C est non vide (et même dense), C^{sing} est un fermé strict de C. D'après la proposition 3.6, c'est une partie finie. □

On a également la caractérisation algébrique suivante des courbes projectives planes lisses.

Proposition 3.8. *Soit $C \subset \mathbb{P}^2_k$ une courbe projective plane irréductible. Un point $P \in C$ est lisse si et seulement si l'idéal maximal $\mathfrak{m}_P$ de l'anneau local $k[C]_P$ est principal.*

Démonstration. On se ramène facilement au cas affine (voir par exemple l'exercice 2.6). On peut donc supposer que $C = V(F)$ pour $F \in k[X,Y]$ irréductible et on note $P = (x_P, y_P)$. Quitte à échanger les rôles de X et Y, on peut supposer que $\frac{\partial F}{\partial Y}(P) \neq 0$. Nous allons montrer que l'idéal $\mathfrak{m}_P$ est engendré par l'image de la fonction $X - x_P$ dans $k[C]_P$. Soit donc $f \in k[C]_P$ tel que $f(P) = 0$. On peut écrire $f = \frac{g}{h}$ avec $h(P) \neq 0$ et $g(P) = 0$. Il suffit donc de prouver que g appartient à l'idéal principal de $k[C]_P$ engendré par $(X - x_P)$. Soit $\tilde{g}$ un relevé de g dans $k[X,Y]$. Alors $\tilde{g}(P) = 0$, ce qui implique que $\tilde{g}$ appartient à l'idéal $(X - x_P, Y - y_P)$ de $k[X,Y]$. Il suffit donc de prouver que l'image de $Y - y_P$ dans $k[C]_P$ appartient à $k[C]_P(X - x_P)$. En effectuant la division euclidienne de F par $Y - y_P$ dans $k[X,Y]$, on voit que l'on peut écrire

$$F(X,Y) = A(X,Y)(Y - y_P) + B(X)$$

où $A(X,Y) \in k[X,Y]$ et $B(X) \in k[X]$. Comme de plus $F(x_P, y_P) = 0$, on a $B(x_P) = 0$, ce qui implique qu'il existe $C(X) \in k[X]$ tel que

$$F(X,Y) = A(X,Y)(Y - y_P) + C(X)(X - x_P).$$

1. Le lecteur attentif aura remarqué que l'évaluation du polynôme homogène $\frac{\partial F}{\partial X}$ au point P n'est pas définie, sa valeur dépend d'un choix de coordonnées homogènes pour P. Cependant son annulation ou non ne dépend pas de ce choix de système de coordonnées.

En appliquant l'opérateur $\frac{\partial}{\partial Y}$, on obtient

$$\frac{\partial F}{\partial Y}(P) = A(x_P, y_P) \neq 0,$$

ce qui implique que $A(X,Y)(Y - y_P) = -C(X)(X - x_P)$ dans $k[C]$. Comme $A(P) \neq 0$, on a $-\frac{C(X)}{A(X,Y)} \in k[C]_P$ et donc $Y - y_P \in k[C]_P(X - x_P)$.

Supposons inversement que l'idéal maximal de $k[C]_P$ est principal. Comme cet idéal est engendré par $X - x_P$ et $Y - x_P$, il est engendré par l'un de ces deux éléments. Supposons qu'il s'agisse de $X - x_P$. Par définition de $k[C]_P$, il existe alors $A(X,Y)$ et $B(X,Y)$ dans $k[X,Y]$ tels que $B(P) \neq 0$ et

$$B(X,Y)(Y - y_P) - A(X,Y)(X - x_P) \in k[X,Y]F(X,Y).$$

On peut donc écrire $D(X,Y)F(X,Y) = B(X,Y)(Y - y_P) - A(X,Y)(X - x_P)$ pour un certain $D(X,Y) \in k[X,Y]$. En appliquant $\frac{\partial}{\partial Y}$ et en évaluant en P, on obtient

$$D(P)\frac{\partial F}{\partial Y}(P) = B(P) \neq 0$$

donc $\frac{\partial F}{\partial Y}(P) \neq 0$, ce qui permet de conclure que $C = V(F)$ est lisse en P. □

3.3 Un cas particulier du théorème de Bezout

Soit $F \in k[X,Y]$ un polynôme de degré $d > 0$. Soit $D \subset \mathbb{A}^2_k$ une droite affine. On désire étudier l'intersection des parties $V(F)$ et D. Quitte à effectuer un changement de coordonnées, on peut supposer que $D = V(Y)$. On a donc

$$V(F) \cap D = \{(x,0) \mid F(x,0) = 0\}$$

Il y a deux possibilités, soit Y divise F et $D \subset V(F)$, soit le polynôme $F(X,0)$ est non nul et a un nombre fini de zéros $x_1, \ldots, x_r$. On a alors

$$F(X,0) = \prod_{i=1}^{r} (X - x_i)^{m_i}$$

où m_i est la multiplicité d'intersection de la droite D avec la courbe $V(F)$ au point $(x_i, 0)$ (étudiée dans la section 1.10). Il faut remarquer que la somme des multiplicités d'intersection $\sum_{i=1}^{r} m_i$ est égale au degré du polynôme $F(X,0)$ qui est inférieur à d, mais peut parfois être strictement inférieur !

Les multiplicités manquantes sont évidemment à rechercher à l'infini. On identifie désormais le plan affine $\mathbb{A}^2_k$ à une partie du plan projectif $\mathbb{P}^2_k$ via le plongement $(x,y) \mapsto (x : y : 1)$. Considérons le polynôme $F^* \in k[X,Y,Z]$, qui est homogène de degré d, de sorte que la clôture projective de $V(F)$ dans $\mathbb{P}^2_k$ est $V_p(F^*)$. De même la clôture projective

de D dans $\mathbb{P}^2_k$ est la droite projective $V_p(Y)$. Calculons alors l'intersection de $V_p(F^*)$ et $V_p(Y)$ à l'infini :

$$V_p(F^*) \cap V_p(Y) \cap V_p(Z) \subset \{(1:0:0)\}$$

Comme Y ne divise pas F, il ne divise pas non plus F^*. On en conclut que le polynôme $G(X,Z) \coloneqq F^*(X,0,Z)$ est homogène de degré d. Le point $(1:0:0)$ est dans l'intersection $V_p(F) \cap V_p(Y)$ si et seulement si $G(1,0) = 0$, c'est-à-dire si et seulement si le monôme X^d n'apparaît pas dans F. Écrivons $G(X,Z) = Z^m H(X,Z)$ où $H(1,0) \neq 0$. Ainsi $(1:0:0) \in V_p(F) \cap V_p(Y)$ si et seulement si $m \geqslant 1$. L'entier m mérite le nom de multiplicité d'intersection des courbes $V_p(F)$ et $V_p(Y)$ au point $(1:0:0)$. Comme le degré du polynôme $F^*(X,0,1)$ est exactement le degré du polynôme H, on a bien

$$m + \sum_{i=1}^{r} m_i = m + \deg H = d = \deg F.$$

En tenant compte de tous les points de l'espace projectif et de leur multiplicité, l'intersection d'une droite avec une courbe « de degré d » est bien égale à d. Cette situation sera généralisée plus tard par le théorème de Bezout.

3.4 Multiplicités d'intersections et théorème de Bezout

Soit C une courbe projective plane irréductible. Supposons C lisse en P et soit $t \in k(C)_P$ une fonction rationnelle définie en P et engendrant l'idéal maximal de $k[C]_P$. Une telle fonction t est appelée une *uniformisante* de C en P. Fixons une uniformisante t de C en P. Tout élément $f \in k[C] \smallsetminus \{0\}$ peut alors s'écrire de façon unique sous la forme ut^n où $u \in k[C]_P^\times$ et $n \geqslant 0$. Plus généralement, tout élément $f \in k(C)^\times$ peut s'écrire de façon unique sous la forme ut^n où $n \in \mathbb{Z}$. L'entier n ainsi obtenu ne dépend pas du choix de l'uniformisante t mais uniquement de f et P. Cet entier est appelé *ordre* de f en P, on le note $\mathrm{ord}_P(f)$.

On vérifie aisément que l'ordre en P est une fonction multiplicative. Si f et g sont deux éléments de $k(C)^\times$, on a $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$. De plus on retrouve $k[C]_P$ via l'égalité

$$k[C]_P = \{f \in k(C) \mid \mathrm{ord}_P(f) \geqslant 0\},$$

et l'idéal maximal $\mathfrak{m}_P \subset k[C]_P$ via

$$\mathfrak{m}_P = \{f \in k(C) \mid \mathrm{ord}_P(f) > 0\}.$$

Remarque 3.9. Soit C une courbe affine plane lisse irréductible. Les seuls idéaux premiers non nuls de $k[C]$ sont les idéaux de la forme $\mathfrak{m}_P$. Comme les anneaux locaux $k[C]_P$ sont tous principaux, on en conclut que l'anneau $k[C]$ est un *anneau de Dedekind*.

Définition 3.10. *Soit C une courbe projective plane irréductible. Soit $F \in k[X,Y,Z]$ un polynôme homogène de degré $d \geqslant 1$ ne s'annulant pas sur C. Si $P \in C$ est un point*

lisse *de C, on définit l'*ordre de F en P *par la formule*

$$\mathrm{ord}_P(F|_C) \coloneqq \mathrm{ord}_P\left(\frac{F}{L^d}\right)$$

où L est un polynôme homogène de degré 1 *tel que $P \notin V(L)$. L'entier positif ainsi défini* $\mathrm{ord}_P(F|_C)$ *ne dépend pas du choix de L.*

Soient C et C' deux courbes projectives lisses irréductibles. Posons $I_p(C) = (F)$ et $I_p(C') = (F')$ où F et F' sont deux polynômes homogènes irréductibles. Soit $P \in C \cap C'$, on peut ainsi définir la *multiplicité d'intersection de C et C' en P* comme l'entier

$$m_P(C, C') \coloneqq \mathrm{ord}_P(F'|_C).$$

L'énoncé suivant est appelé « théorème de Bezout pour les courbes lisses ».

Théorème 3.11 (Théorème de Bezout)**.** *Soient C et C' deux courbes projectives lisses irréductibles et distinctes. Alors $C \cap C'$ est un ensemble fini et on a*

$$\sum_{P \in C \cap C'} m_P(C, C') = (\deg C)(\deg C').$$

De plus on a $m_P(C, C') = m_P(C', C)$ pour tout point $P \in C \cap C'$.

Le même énoncé est vrai plus généralement pour des courbes qui ne sont pas nécessairement lisses, mais il faut alors donner une autre définition des multiplicités d'intersection $m_P(C, C')$.

Si C est une courbe projective plane, on note $\mathrm{Div}(C)$ le groupe abélien libre dont une base est donnée par les points de C. Un élément du groupe $\mathrm{Div}(C)$ est appelé *diviseur* et est représenté par une somme formelle finie $\sum_{P \in C} m_P(P)$ où les symboles m_P représentent des éléments de $\mathbb{Z}$. Le fait qu'une telle somme est finie se traduit par le fait que tous les m_P sont nuls sauf un nombre fini. Si C' est une autre courbe projective plane différente C, on note $C \cdot C'$ le *produit d'intersection* de la courbe C avec C'. Il s'agit d'un élément de $\mathrm{Div}(C)$ défini par la formule

$$C \cdot C' \coloneqq \sum_{P \in C} m_P(C, C')(P).$$

Exemple 3.12. Soit L une droite projective différente de C, alors $m_P(C, L)$ est la multiplicité d'intersection étudiée dans la section 3.3. Si la courbe C intersecte la droite L en trois points P, Q, R avec multiplicité 1, on a $C \cdot L = (P) + (Q) + (R)$. Si elle intersecte L en P avec multiplicité 2 et Q avec multiplicité 1, on a $C \cdot L = 2(P) + (Q)$, cependant cette quantité peut également s'écrire $(P) + (P) + (Q)$ dans le groupe $\mathrm{Div}(C)$.

On définit un morphisme de groupes de $\mathrm{Div}(C)$ dans $\mathbb{Z}$ appelé *degré* par la formule $\deg(\sum_P m_P(P)) = \sum_P m_P$. Le théorème de Bezout peut alors se reformuler de façon compacte sous la forme

$$\deg(C \cdot C') = \deg(C) \deg(C').$$

3.5 Morphismes entre courbes projectives lisses

Proposition 3.13. *Supposons que C et C' sont deux courbes projectives lisses irréductibles. Soit $\varphi : C \to C'$ une application continue pour la topologie de Zariski. Supposons qu'il existe un ouvert non vide $U \subset C$ tel que pour tout ouvert $U' \subset C'$, l'application $f \mapsto f \circ \phi$ transforme une fonction régulière sur U' en une fonction régulière sur $\phi^{-1}(U') \subset U$. Alors φ est un morphisme de courbes projectives.*

Démonstration. Soit $P \notin U$ et soit V un ouvert de C contenant P. Comme $C \smallsetminus U$ est fini d'après la proposition 3.6, quitte à rétrécir V, on peut supposer que $U \cap V = V \smallsetminus \{P\}$. On se ramène aisément à prouver que si f est une fonction continue de V dans k dont la restriction à $U \cap V$ est régulière, alors f est régulière. Soit $F \in k(C)$ la fonction rationnelle définissant de domaine de définition contenant $U \cap V$ et induisant f sur $U \cap V$. Il suffit de prouver que $F \in k[C]_P$. Comme C est lisse, il existe $x_P \in k(C)$ une uniformisante de C en P. Quitte à rétrécir V, on peut encore supposer que le domaine de définition de x_P contient V. Supposons par l'absurde $F \notin k[C]_P$ et soit $n = -\operatorname{ord}_P(F)$. On a alors $x_P^n F \in k[C]_P \smallsetminus \mathfrak{m}_P$ et définit une fonction régulière sur V qui ne s'annule pas en P et coïncide avec $x_P^n f$ sur $V \smallsetminus \{P\}$. Par continuité, on doit donc avoir $(x_P^n F)(Q) = x_P(Q)^n f(Q)$ pour tout $Q \in V$. C'est absurde car x_P s'annule en P et f est bien définie en P. □

3.6 Courbes elliptiques

Une courbe projective de degré 2 est appelée *conique*, une courbe projective de degré 3 est appelée *cubique*.

Définition 3.14. *Une* courbe elliptique *est une cubique plane lisse irréductible.*

Soit E une courbe elliptique. Fixons 0 un point de E. Soient P et Q deux points de E. Le théorème de Bezout implique qu'il existe une unique droite projective L et un unique point R de E tels que, dans $\operatorname{Div}(E)$,

$$E \cdot L = (P) + (Q) + (R)$$

En effet, si P et Q sont distincts, la droite L est l'unique droite projective contenant P et Q. Si $P = Q$, la droite L est la tangente à E au point P. On note $P * Q$ le point R. Ainsi le point $P * Q$ est l'unique point de E tel que

$$E \cdot L = (P) + (Q) + (P * Q).$$

On en déduit facilement que $P * Q = R \Leftrightarrow Q = P * R$.

De même, il existe une unique droite projective L' et un unique point $S \in E$ tels que

$$E \cdot L' = (0) + (P * Q) + (S)$$

On note $P +_0 Q$ le point S. Autrement dit $P +_0 Q$ est le point $(0 * (P * Q))$. On a ainsi défini une loi de composition interne sur E.

Théorème 3.15. *La loi de composition $+_0$ fait du couple $(E, +_0)$ un groupe abélien d'élément neutre 0.*

Remarque 3.16. La loi $+_0$ dépend vraiment du point 0 puisque c'est son élément neutre. Cependant, dans la plupart des cas, on note simplement $+$ la loi de groupe sur E.

Démonstration. La loi $+_0$ est clairement commutative. Vérifions que le point 0 est un élément neutre. Par définition, si $P \in E$, il existe une droite L et une droite L' telles que

$$E \cdot L = (0) + (P) + (0 * P) \quad E \cdot L' = (0) + (0 * P) + (0 +_0 P)$$

Ainsi $L = L'$ et $0 +_0 P = P$.

Si $P \in E$, vérifions qu'il existe $Q \in E$ tel que $P +_0 Q = 0$. Soit L la droite projective tangente à E en 0. On a alors

$$E \cdot L = 2(0) + (0 * 0)$$

On remarque au passage que l'on a $0 * (0 * 0) = 0$. Soit L' l'unique droite passant par P et $0 * 0$ (la tangente en P s'il se trouve que $P = 0 * 0$) et soit Q le troisième point d'intersection de L' avec E, on a alors

$$E \cdot L' = (P) + (Q) + (0 * 0)$$

On en déduit que $P * Q = 0 * 0$ donc

$$P +_0 Q = 0 * (0 * 0) = 0$$

L'associativité de la loi $+_0$ est la propriété la plus difficile à démontrer. La démonstration est repoussée à plus tard. □

Théorème 3.17. *Supposons que le corps k est de caractéristique différente de 2 et 3. Soit E une courbe elliptique. Quitte à faire un changement de repère projectif, il existe $(a, b) \in k^2$ tels que $4a^3 + 27b^2 \neq 0$ et*

$$E = V_p(Y^2Z - X^3 - aXZ^2 - bZ^3)$$

Démonstration. Comme E est de degré 3, la courbe E possède au moins un point d'inflexion P (voir exercice 3.9). Choisissons l'axe $Z = 0$ tel que la droite $Z = 0$ soit tangente à E en P. D'après le théorème de Bezout, la droite $Z = 0$ coupe alors E uniquement en P. Ceci implique que l'équation de E est de la forme

$$F = X^3 + ZG(X, Y, Z)$$

où G est un polynôme homogène de degré 2. Ainsi E pour équation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6$$

Le changement de variable $Y \mapsto Y - \frac{1}{2}(a_2X - a_3Z)$ permet d'éliminer a_1 et a_3. Ensuite le changement de variable $X \mapsto X - \frac{1}{3}a_2Z$ permet d'éliminer a_2.

Lorsque la caractéristique du corps k est différente de 2, on vérifie alors que la courbe d'équation $Y^2Z - X^3 - aXZ^2 - bZ^3$ est lisse si et seulement si le polynôme $X^3 + aX + b$ n'a pas de racine multiple, autrement dit si et seulement si son discriminant est non nul, c'est-à-dire si et seulement si $4a^3 + 27b^2 \neq 0$. □

3.7 Courbes elliptiques sur les corps parfaits

Nous supposons désormais que le corps k est un corps parfait, non nécessairement algébriquement clos.

Définition 3.18. *Une courbe elliptique définie sur k est une cubique lisse E définie sur k telle que $E(k) \neq \emptyset$.*

Soit E une courbe elliptique définie sur k et soit $0 \in E(k)$. On considère la loi de groupe $+_0$.

Proposition 3.19. *Si E est une courbe elliptique définie sur k et si $0 \in E(k)$, l'ensemble $E(k)$ est un sous-groupe de $(E, +_0)$.*

Démonstration. Comme $0 \in E(k)$ et que $P +_0 Q = 0 * (P * Q)$, il suffit de prouver que si $P \in E(k)$ et $Q \in E(k)$, alors $P * Q \in E(k)$. Soit L l'unique droite contenant P et Q si $P \neq Q$ et tangente à E en P si $P = Q$. Comme E est définie sur k et que P et Q sont dans $E(k)$, la droite L est définie sur k. On a alors

$$E \cdot L = (P) + (Q) + (P * Q)$$

En appliquant un automorphisme $\sigma \in \mathrm{Gal}(\overline{k}/k)$, on a $\sigma(E) = E$ et $\sigma(L) = L$ d'où

$$\sigma(E) \cdot \sigma(L) = (P) + (Q) + (P * Q)$$

Par ailleurs on vérifie facilement que

$$\sigma(E) \cdot \sigma(L) = (\sigma(P)) + (\sigma(Q)) + (\sigma(P * Q))$$

Comme $\sigma(P) = P$ et $\sigma(Q) = Q$, on a $\sigma(P * Q) = P * Q$. Cette égalité étant valable pour tout $\sigma \in \mathrm{Gal}(\overline{k}/k)$, on a $P * Q \in E(k)$. □

Soit $Y^2-X^3-aX-b \in k[X,Y]$ et supposons $4a^3+27b^2 \neq 0$. La clôture projective de $V(Y^2-X^3-aX-b)$ dans $\mathbb{P}^2_{\overline{k}}$ est $V_p(Y^2Z-X^3-aXZ^2-bZ^3)$. Il s'agit d'une cubique lisse (en caractéristique différente de 2) E définie sur k. Comme le point $(0:1:0)$ appartient à $E(k)$, la courbe E est en fait une courbe elliptique définie sur k. Dans la suite du cours, sauf mention explicite du contraire, on la munit toujours de la loi de groupe $+_{(0:1:0)}$ et on utilisera l'abus de langage suivant : « soit E la courbe elliptique définie par l'équation $Y^2 = X^3 + aX + b$ ».

Si E est définie par l'équation de Weierstraß

$$Y^2 = X^3 + aX + b,$$

on peut donner des formules explicites pour l'addition de deux points. Soit $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ deux points de $E \smallsetminus \{0\}$. On a alors $-P = (x_P, -y_P)$ et, si $P \neq \pm Q$, on a $P + Q = (x_{P+Q}, y_{P+Q})$, avec

$$x_{P+Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - (x_P + x_Q) = \left(\frac{x_P^2 + x_P x_Q + x_Q^2 + a}{y_P + y_Q}\right)^2 - (x_P + x_Q) \tag{3.1}$$

$$y_{P+Q} = -\left(y_P + \frac{y_Q - y_P}{x_Q - x_P}(x_{P+Q} - x_P)\right). \tag{3.2}$$

On peut également montrer que, si $P + P \neq 0$, alors

$$x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}.$$

3.8 Le théorème des neuf points

Dans cette section k est un corps algébriquement clos. Nous allons démontrer un théorème de géométrie projective qui est la clef de l'associativité de la loi de groupe d'une courbe elliptique. On commence par démontrer les deux premiers cas du théorème de Bézout.

Lemme 3.20. *Soit $C \subset \mathbb{P}^2_k$ une courbe définie par un polynôme homogène de degré d et soit $L \subset \mathbb{P}^2_k$ une droite non contenue dans C. Alors $C \cap L$ est composé de d points comptés avec multiplicités.*

Démonstration. Il s'agit d'une conséquence directe de la discussion du §3.3. □

Lemme 3.21. *Soit $C \subset \mathbb{P}^2_k$ une courbe définie par un polynôme homogène de degré d et soit $D \subset \mathbb{P}^2_k$ une conique non contenue dans C. Alors $C \cap D$ est composé de $2d$ points comptés avec multiplicités.*

Démonstration. Soit $F(X,Y,Z) = 0$ l'équation homogène de degré d qui définit la courbe C. Si la conique D est réductible, D est l'union de deux droites. Quitte à faire un

changement linéaire en coordonnées, on peut supposer que la conique est donnée par l'équation $XY-Z^2=0$, i.e. que D est l'image de morphisme $\mathbb{P}^1 \to \mathbb{P}^2, (u:v) \mapsto (u^2 : v^2 : uv)$ (voir l'exercice 2.2). Le polynôme $f(u,v) = F(u^2, v^2, uv)$ est un polynôme homogène non nul (car D n'est pas contenue dans C) de degré $2d$. Comme k est algébriquement clos, on a donc une factorisation $f(Y,Z) = \alpha \prod_i (Y - \alpha_i Z)^{m_i}$ avec $\sum m_i = 2d$. Les points d'intersection de D et C sont donnés par la condition $f(u,v) = 0$. Comptés avec multiplicité, ces points sont donc au nombre de $\sum m_i = 2d$. □

Le but des énoncés suivants est de décrire les courbes de degré donné qui passant par un certain nombre de points donnés. De façon générale, l'ensemble des hypersurfaces de degré d dans $\mathbb{P}^N_k$ forme aussi un espace projectif, dont les coordonnées correspondent aux coefficients des équations de ces hypersurfaces. Par exemple, une conique dans $\mathbb{P}^2_k$ est donnée par une équation homogène $q(X,Y,Z) = \sum a_{ijs} X^i Y^j Z^s$ avec $i+j+s=2$, il y a donc 6 coefficients. On associe à la conique le vecteur de ses coefficients. L'ensemble de toutes les formes $q(X,Y,Z)$ forme donc un espace vectoriel de dimension 6. Pour que deux formes définisssent la même conique il faut et il suffit qu'elles ne diffèrent que par multiplication par un scalaire non nul. L'ensemble des coniques est donc un espace projectif $\mathbb{P}^5_k$.

Lemme 3.22. *Soient $P_1, \ldots, P_5$ des points distincts de $\mathbb{P}^2_k$. Il existe une conique dans $\mathbb{P}^2_k$ qui passe par ces points. De plus, si quatre de ces points ne sont jamais alignés, la conique est unique.*

Démonstration. Une conique C dans $\mathbb{P}^2_k$ est donnée par une équation homogène de la forme $q(X,Y,Z) = \sum_{i+j+s=2} a_{ijs} X^i Y^j Z^s$. Le k-espace vectoriel V des équations de coniques est donc de dimension 6. L'appartenance d'un point à la conique C est caractérisée par une forme linéaire sur cet espace. L'ensemble des équations de coniques passant par 5 points fixés est donc l'espace des solutions d'un système de 5 équations linéaires dans un espace de dimension 6. Un système de 5 équations linéaires à 6 inconnues possède toujours une solution non nulle. Étant donnés 5 points fixés, il existe donc toujours une conique passant par ces 5 points. Il existe donc au moins une conique C passant par les points $P_1, \ldots, P_5$.

Supposons que 3 points, disons P_1, P_2, P_3 sont alignés. Soit L la droite (P_1P_2). L'équation q de la conique C est donc divisible par l'équation de L, ainsi q s'annule en P_4 et P_5. Comme P_4 et P_5 ne sont pas sur L, la conique C est l'union des deux droites L et (P_4P_5) .

Supposons qu'aucun triplet parmi les points $P_1, \ldots, P_5$ n'est aligné. Soit P_6 un point sur la droite $L = P_1P_2$, différent de P_1 et de P_2. Supposons par l'absurde que la dimension sous-k-espace vectoriel des équations de coniques passant par les points $P_1, \ldots, P_5$ est au moins égale à 2. Il existe alors une conique contenant les points $P_1, \ldots, P_6$. En effet la condition qu'une conique passe par un point donné est une condition linéaire. Puisque P_1, P_2, P_6 sont alignés, C est l'union de $L = (P_1P_2)$ et une autre droite. On en conclut que

les points $P_3, \ldots, P_5$ doivent être alignés, c'est une contradiction. L'espace des équations de coniques passant par les points $P_1, \ldots, P_5$ est donc de dimension 1. □

Lemme 3.23. *Soient $P_1, \ldots, P_8$ des points distincts de $\mathbb{P}^2_k$, tels que quatre d'entre eux ne sont jamais alignés et que sept d'entre eux n'appartiennent jamais à la même conique. Soit V le k-espace vectoriel des polynômes homogènes de degré 3 s'annulant en $P_1, \ldots, P_8$. Alors* $\dim V = 2$.

Démonstration. Le k-espace vectoriel W des équations de cubiques (polynômes homogènes de degré 3) est de dimension 10, ainsi $\dim V \geqslant 10 - 8 = 2$. La démonstration se découpe en plusieurs étapes.

Supposons dans un premier temps qu'il existe une droite L incluse dans toutes les coniques passant par les points $P_1, \ldots, P_8$. Sous nos hypothèses, cette droite contient au plus 3 points parmi $P_1, \ldots, P_8$. On peut donc supposer que $P_4, \ldots, P_8$ n'appartiennent pas à L. Toute conique passant par les points $P_1, \ldots, P_8$ s'écrit donc sous la forme $C = L \cup Q$ où Q est une quadratique. Les points $P_4, \ldots, P_8$ sont donc sur Q. D'après le lemme 3.22, il n'existe qu'une seule telle conique. Ainsi $\dim V = 1$, ce qui contredit le fait que $\dim V \geqslant 2$. Ainsi une conique passant par les points $P_1, \ldots, P_8$ ne contient aucune droite.

Supposons à présent que P_1, P_2, P_3 sont alignés, soit L l'unique droite les contenant. Soit $q \in V$. Comme q ne s'annule pas en tous les points de L, on peut trouver un point $P_9 \in L$ tel que $q(P_9) \neq 0$. L'espace vectoriel des cubiques qui passent par les neuf points $P_1, \ldots, P_9$ est donc de dimension $\dim V - 1$. Si une cubique C passe par $P_1, \ldots, P_9$, alors l'intersection de C et L contient au moins 4 points. Ainsi C et L ont une composante irréductible commune. On en conclut que C est de la forme $L \cup Q$ pour Q une conique. D'après les hypothèses, Q contient $P_4, \ldots, P_8$. D'après le lemme 3.22, il n'existe qu'une seule telle conique. Ainsi $\dim V - 1 \leqslant 1$, d'où le résultat.

Supposons que $P_1, P_2, \ldots, P_6$ sont sur une conique Q. Soit P_9 un autre point de cette conique. D'après le lemme 3.21, toute cubique C qui contient $P_1, \ldots P_9$ a 7 points d'intersections distincts avec Q et doit donc contenir Q. Elle s'écrit donc sous la forme $C = Q \cup L$ où L est une droite. Sous nos hypothèses, $L = (P_7P_8)$. On a donc encore $\dim V - 1 \leqslant 1$, d'où le résultat.

Supposons finalement que trois points parmi $P_1, \ldots, P_8$ ne sont jamais alignés et que six points parmi $P_1, \ldots, P_8$ ne sont jamais sur une même conique. Soient P_9, P_{10} deux points distincts de la droite $L = (P_1P_2)$ choisis distincts de P_1 et P_2. Supposons par l'absurde $\dim V > 2$. Le sous-espace des équations de cubiques s'annulant sur P_9 et P_10 est de codimension inférieure ou égale à 2, il possède donc une intersection non nulle avec V. Il existe alors une cubique C qui passe par les points $P_1, \ldots, P_{10}$. D'après le lemme 3.20, cette cubique contient la droite L et elle est donc l'union de L et d'une conique. Étant donné notre hypothèse sur $P_1, \ldots, P_8$, c'est une contradiction. □

Théorème 3.24. *Soient C_1 et C_2 deux cubiques dans $\mathbb{P}^2_k$. Supposons C_1 irréductible et que C_1 et C_2 ont neuf points d'intersection distincts $P_1, \ldots P_9$, tels que les points*

$P_1, \ldots, P_8$ sont distincts. Si une cubique C passe par les points $P_1, \ldots, P_8$, alors elle passe par le point P_9.

Démonstration. La cubique C_1 ne contient pas 4 points alignés. En effet d'après le lemme 3.20, on en conclurait que C_1 contient une droite, ce qui n'est pas possible car C_1 est irréductible. De même, le lemme 3.21 montre que C_1 ne contient pas 7 points appartenant à une même conique. Les points $P_1, \ldots, P_8$ satisfont donc les hypothèses du lemme 3.23 et le k-espace vectoriel des polynômes homogènes de degré 3 s'annulant en $P_1, \ldots, P_8$ est de dimension 2. Il est donc engendré par C_1 et C_2. Ainsi, l'équation de la cubique C est une combinaison linéaire des équations de C_1 et C_2, en particulier, elle s'annule en P. □

3.9 Associativité de la loi de groupe

Soit k un corps algébriquement clos et soit E une courbe elliptique définie sur k. Nous allons achever la preuve du théorème 3.15.

Soient $P, Q, R \in E$ trois points distincts.

- Soit L_1 la droite (PQ) et soit $T = P * Q$ le troisième point d'intersection de L_1 avec E.
- Soit L_2 la droite $(T0_E)$ et soit $T' = P + Q$ le troisième point d'intersection de L_2 avec E.
- Soit L_3 la droite (RT') et soit $U = (P+Q) * R$ le troisième point d'intersection de L_3 avec E.
- Soit M_1 la droite (QR) et soit $S = Q * R$ le troisième point d'intersection de M_1 avec E.
- Soit M_2 la droite $(S0_E)$ et soit $S' = Q + R$ le troisième point d'intersection de M_2 avec E ;
- Soit M_3 la droite (PS') et soit $V = P * (Q + R)$ le troisième point d'intersection de M_3 avec E.

Par construction, on a $(P+Q)+R = -U$ et $P+(Q+R) = -V$ et on veut donc montrer que $U = V$.

Soient $C_1 = L_1 + M_2 + L_3$ et $C_2 = M_1 + L_2 + M_3$ deux cubiques. On a $E \cap C_1 = \{P, Q, R, 0_E, T, T', S, S', U\}$ et $E \cap C_2 = \{P, Q, R, 0_E, T, T', S, S', V\}$. Supposons que les points $P, Q, R, 0_E, T, T', S, S', U$ sont tous distincts. D'après le lemme 3.24 appliqué à E et à C_1, on a alors $U = V$.

Nous allons finir la démonstration en utilisant un argument de continuité.

Remarquons dans un premier temps que E est une courbe projective irréductible. Ses fermés sont E et les parties finies de E. En particulier, si $\alpha : E \to E$ est bijective, alors α est continue pour la topologie de Zariski. En effet, l'image réciproque d'une partie finie

est finie donc fermée. L'image réciproque d'un fermé est fermé, donc α est continue. Si $Q \in E$, l'application $P \mapsto P * Q$ est une involution, donc une bijection et d'après ce qui précède un homéomorphisme de E. Ainsi l'application $P \mapsto P + Q = (P * Q) * 0_E$ est un homéomorphisme de E sur E. Supposons alors que les points Q et R sont choisis tels que

$$Q, R, Q * R, Q + R, 0_E$$

sont distincts. L'ensemble des points P tels que

$$P, Q, R, P * Q, P + Q, Q + R, Q * R, (P + Q) * R, 0_E$$

sont distincts est un ouvert non vide de E, donc une partie dense de E. Les deux fonctions $P \mapsto (P + Q) + R$ et $P \mapsto P + (Q + R)$ sont continues et coïncident sur une partie dense de E, elles sont donc égales pour toute valeur de P. Ainsi, on a prouvé l'égalité $(P + Q) + R = P + (Q + R)$ pour toutes valeurs de P, Q, R telles que les points $Q, R, Q + R, Q + R, 0_E$ sont distincts. Supposons désormais $R \neq 0_E$, alors le même argument de continuité nous permet de conclure que, à P et $R \neq 0$ fixés, on a $P+(Q+R) = (P+Q)+R$ pour toute valeur de Q. Il reste à traiter le cas $P = Q = R = 0_E$ qui est immédiat.

3.10 Le théorème d'Abel-Jacobi

Soit k un corps algébriquement clos et soit E une courbe elliptique définie sur k. Si $f \in k(E)$, on note $\mathrm{div}(f)$ l'élément de $\mathrm{Div}(E)$ défini par

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

Notons $\mathrm{Div}^0(E)$ le sous-groupe de $\mathrm{Div}(E)$ défini comme le noyau de l'application $\deg : \mathrm{Div}(E) \to \mathbb{Z}$. Alors le théorème de Bezout implique que $\mathrm{div}(f) \in \mathrm{Div}^0(E)$. Le théorème suivant nous permet de construire des fractions rationnelles sur E.

Théorème 3.25. *Soit $D = \sum_P m_P(P) \in \mathrm{Div}^0(E)$. Si on a $\sum_P m_P P = 0$ dans E, alors il existe une fonction $f \in k(E)$ telle que $\mathrm{div}(f) = D$. De plus la fonction f est uniquement déterminée à multiplication près par un élément de $k^\times$.*

3.11 Exercices

Dans tous les exercices, k désigne un corps algébriquement clos de caractéristique différente de 2 et 3.

Exercice 3.1.

a) Soit $F \in k[X_0, \ldots, X_n]$ un polynôme homogène de degré $d \geqslant 1$. Démontrer l'identité d'Euler

$$dF = \sum_{i=0}^{n} X_i \frac{\partial F}{\partial X_i}$$

b) Soit C une courbe projective plane. Soit $F \in k[X, Y, Z]$ tel que $I_p(C) = (F)$. Si la caractéristique de k ne divise pas le degré de F, montrer que

$$C^{\text{sing}} = V_p\left(\frac{\partial F}{\partial X}\right) \cap V_p\left(\frac{\partial F}{\partial Y}\right) \cap V_p\left(\frac{\partial F}{\partial Z}\right)$$

Exercice 3.2. Montrer que la cubique d'équation $Y^2Z = X^3 + aXZ^2 + bZ^3$ est lisse si et seulement si $4a^3 + 27b^2 \neq 0$.

Exercice 3.3. Soit $P \in k[X]$ un polynôme simplement scindé de degré $d \geqslant 3$. Soit W l'adhérence de Zariski de $V(Y^2 - P(X)) \subset \mathbb{A}^2_k$ dans $\mathbb{P}^2_k$. Déterminer les points lisses de W.

Exercice 3.4. Soit E une courbe elliptique définie sur k d'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, d'élément neutre $0 = (0 : 1 : 0)$. Montrer que l'ensemble

$$\{P \in E,\ [2]P = 0\}$$

est de cardinal 4. En déduire qu'il s'agit d'un sous-groupe de E isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 3.5. Soit E une courbe elliptique définie sur k d'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, d'élément neutre $0 = (0 : 1 : 0)$. Soit $P = (x, y) \in E \smallsetminus \{0\}$.

a) Calculer les coordonnées du point $[2]P$.

b) En déduire que l'application $P \mapsto [2]P$ de E dans E est surjective.

Exercice 3.6. Soit E une courbe elliptique définie sur k d'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, d'élément neutre $0 = (0 : 1 : 0)$.

a) Soit $P = (x, y) \in E \smallsetminus \{0\}$. Montrer que $P \in E[3]$ si et seulement si x est racine de l'équation

$$3x^4 + 6ax^2 + 12bx - a^2 = 0. \tag{3.3}$$

b) Montrer que l'équation (3.3) n'a que des racines simples et en déduire le cardinal ainsi que la structure du groupe $E[3]$.

c) Déterminer le sous-groupe de 3-torsion de la courbe elliptique E définie par l'équation $Y^2 = X^3 + 1$ et déterminer $E(\mathbb{Q})[3]$.

Exercice 3.7. Montrer que la courbe projective d'équation $X^3 + Y^3 = Z^3$ est lisse. Expliciter la loi de groupe en choisissant pour élément neutre le point $(1 : 0 : 1)$.

Exercice 3.8. Soit C une courbe projective plane lisse. Montrer que les composantes irréductibles de C sont deux à deux disjointes. En déduire qu'elle est irréductible.

Exercice 3.9 (Points d'inflexion)**.** Soit C une courbe projective plane lisse définie sur k. Un point P de C est un *point d'inflexion* si et seulement si la multiplicité d'intersection en P de C avec sa tangente en P est $\geqslant 3$.

a) Montrer qu'une conique lisse n'a pas de point d'inflexion.

b) Posons $I_p(C) = (F)$. Soit $H(X, Y, Z)$ le déterminant de la matrice

$$M(X,Y,Z) = \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X Y} & \frac{\partial^2 F}{\partial X Z} \\ \frac{\partial^2 F}{\partial X Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y Z} \\ \frac{\partial^2 F}{\partial X Z} & \frac{\partial^2 F}{\partial Y Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}$$

Soit d le degré de C. Montrer que

$$Z^2 H(X,Y,Z) = \begin{vmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X Y} & (d-1)\frac{\partial F}{\partial X} \\ \frac{\partial^2 F}{\partial X Y} & \frac{\partial^2 F}{\partial Y^2} & (d-1)\frac{\partial F}{\partial Y} \\ (d-1)\frac{\partial F}{\partial X} & (d-1)\frac{\partial F}{\partial Y} & d(d-1)F(X,Y,Z) \end{vmatrix}$$

(on pourra utiliser l'identité d'Euler prouvée dans l'exercice 3.1).

c) Si k est de caractéristique 0, montrer que P est un point d'inflexion de C si et seulement si $H(P) = 0$.

d) En déduire qu'une courbe plane lisse de degré $d \geqslant 3$ a toujours des points d'inflexion.

e) Supposons que C est une cubique irréductible. Montrer que P est un point d'inflexion de C si et seulement si P est le seul point d'intersection de C avec sa tangente en P.

f) Soit E une courbe elliptique. Supposons que 0 est un point d'inflexion de E. Montrer que P est un point d'inflexion de E si et seulement si $[3]P = 0$ et que le nombre de points d'inflexion de E est égal à 1, 3 ou 9.

g) Montrer que le nombre de points d'inflexion d'une courbe elliptique E est exactement égal à 9.

Dans tous les exercices, k désigne un corps de caractéristique différente de 2 ou 3.

Exercice 3.10. On suppose k algébriquement clos.

a) Soit E une courbe elliptique sur k donnée par l'équation $Y^2 = X^3 + AX + B$. Montrer que $(x, y) \to (x, -y)$ est un endomorphisme de groupes de E.

b) Soit E une courbe elliptique sur k donnée par l'équation $Y^2 = X^3 + B$. Montrer que $(x, y) \to (\zeta x, -y)$, où $\zeta^3 = 1$ une racine primitive de l'unité, est un endomorphisme de E.

c) Soit E une courbe elliptique sur k donnée par l'équation $Y^2 = X^3 + AX$. Montrer que $(x, y) \to (-x, iy)$ est un endomorphisme de E dans lui-même.

Exercice 3.11. On suppose k algébriquement clos. Soit E une courbe elliptique donnée par une équation $Y^2 = X^3 + AX + B$. On définit le j-invariant de E par la formule

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

a) Soient E_1 et E_2 deux courbes elliptiques données par des équations $y^2 = x^3 + A_i x + B_i$. Montrer que si $j(E_1) = j(E_2)$, alors il existe $\mu \in k^\times$ tel que $A_2 = \mu^4 A_1$ et $B_2 = \mu^6 B_1$.

b) En déduire que l'application $(x, y) \mapsto (\mu^2 x, \mu^3 y)$ induit un isomorphisme de groupes de E_1 sur E_2.

Exercice 3.12. Soit $a \in \mathbb{Z}$ un entier qui n'est divisible par aucune puissance quatrième (sauf 1) et soit E une courbe elliptique $Y^2 = X^3 + aX$. On se propose de trouver tous les points d'ordre 2^n de $E(\mathbb{Q})$.

a) Déterminer tous les points d'ordre 2.

b) Soient $(x, y), (u, v) \in E$ avec $(x, y) = [2](u, v)$. Montrer que $x = (u^2 - a)^2/4v^2$.

c) Soit $P \in E(\mathbb{Q})$ un point d'ordre 2. Montrer que $P = [2]Q$ implique $a = 4$. Trouver les points d'ordre 4.

d) Conclure.

Exercice 3.13.

a) Montrer que $C = V_p(X^2 + Y^2 - 3Z^2)$ est une variété algébrique projective définie sur $\mathbb{Q}$ mais que $C(\mathbb{Q}) = \emptyset$ (on pourra considérer un point à coefficients dans $\mathbb{Z}$ et le réduire modulo 3).

b) Soit p un nombre premier. À quelle condition sur p, la variété algébrique $V_p(X^2 + Y^2 - pZ^2)$ a-t-elle des points sur $\mathbb{Q}$?

Exercice 3.14. Soit p un nombre premier. Si $\frac{m}{n} \in \mathbb{Q}$, on pose $v_p(\frac{m}{n}) = v_p(m) - v_p(n)$. Soit E une courbe elliptique définie sur $\mathbb{Q}$ par l'équation $Y^2 = X^3 + aX + b$.

a) Soit $(x, y) \in E \setminus \{0\}$. On suppose que $v_p(x) < 0$. Montrer qu'il existe $\nu > 0$ tel que $v_p(x) = -2\nu$ et $v_p(y) = -3\nu$.

b) Montrer que l'ensemble

$$E(\nu) := \{0\} \cup \{(x, y) \in E(\mathbb{Q}),\ v_p(x) \leqslant -2\nu\}$$

est un sous-groupe de $E(\mathbb{Q})$.

Exercice 3.15.

a) Soit $F = \frac{P}{Q} \in k(X)$ où P et Q sont deux éléments premiers entre eux de $k[X]$. On pose $\deg F = \max(\deg P, \deg Q)$. Si $F \neq 0$, montrer que le corps $k(X)$ est un extension finie de $k(F)$ et que $[k(X) : k(F)] = \deg F$.

b) Soit E une courbe elliptique définie sur k. Soient α et β deux endomorphismes de E. Montrer que $\deg(\alpha \circ \beta) = \deg(\alpha)\deg(\beta)$. En déduire que $\mathrm{End}(E)$ est un anneau intègre.

Exercice 3.16. Soit k un corps parfait et soit $\overline{k}$ une clôture algébrique de k. Montrer qu'un idéal de $\overline{k}[X]$ est défini sur k si et seulement si il est stable sous l'action du groupe $\mathrm{Gal}(\overline{k}/k)$.

Exercice 3.17. Démontrer le théorème 3.25.
Indication : on pourra procéder par récurrence descendante sur le degré de $\sum_{m_P>0} m_P(P)$.

Chapitre 4

Courbes elliptiques sur $\mathbb{C}$

4.1 Fonctions elliptiques

Un *réseau* de $\mathbb{C}$ est un sous-groupe de $\mathbb{C}$ qui est un $\mathbb{Z}$-module libre de rang 2 et qui engendre $\mathbb{C}$ comme $\mathbb{R}$-espace vectoriel. Si Λ est un réseau de $\mathbb{C}$, il existe alors deux éléments ω_1 et ω_2 tels que $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Le choix de la base (ω_1, ω_2) est bien sûr loin d'être unique.

Si Λ est un réseau de $\mathbb{C}$, on appelle *maille élémentaire* de ce réseau une partie de $\mathbb{C}$ de la forme

$$M(\alpha, \omega_1, \omega_2) \coloneqq \{\alpha + t_1\omega_1 + t_2\omega_2 \mid (t_1, t_2) \in [0, 1[^2\},$$

où α est un élément de $\mathbb{C}$ et (ω_1, ω_2) une base du réseau. Une maille élémentaire $M(\alpha, \omega_1, \omega_2)$ est alors un système de représentants pour l'action de Λ sur $\mathbb{C}$ par translation, c'est-à-dire que tout élément $z \in \mathbb{C}$ s'écrit de façon unique sous la forme $z = p + \omega$ avec $p \in M(\alpha, \omega_1, \omega_2)$ et $\omega \in \Lambda$, ou encore

$$\mathbb{C} = \coprod_{\omega \in \Lambda} (\omega + M(\alpha, \omega_1, \omega_2)).$$

Définition 4.1. *Une fonction elliptique relativement à Λ est une fonction méromorphe f sur $\mathbb{C}$ telle que*

$$\forall z \in \mathbb{C},\ \forall \lambda \in \Lambda,\ f(z + \lambda) = f(z).$$

Si f est une fonction elliptique relativement à Λ, l'ensemble des zéros et l'ensemble des pôles de f sont des parties de $\mathbb{C}$ stables par translation par les éléments de Λ.

Le principe des zéros isolés implique que si f est une fonction elliptique non nulle, l'ensemble des zéros et l'ensemble des pôles de f sont des parties discrètes et fermées de $\mathbb{C}$. En particulier, si A est une partie bornée de $\mathbb{C}$, la fonction f n'a qu'un nombre fini de zéros et de pôles dans A.

Si $P \in \mathbb{C}$, il existe un voisinage ouvert U de $\mathbb{C}$ contenant P, une fonction holomorphe g sur U telle que $g(0) \neq 0$ ainsi qu'un entier $n \in \mathbb{Z}$ tel que

$$\forall z \in U,\ f(z) = (z-P)^n g(z).$$

L'entier n ne dépend que du point P et de la fonction f et s'appelle l'ordre de f en P. On le note $\mathrm{ord}_P(f)$. Le point P est un zéro de f si et seulement si $\mathrm{ord}_P(f) > 0$ et est un pôle de f si et seulement si $\mathrm{ord}_P(f) < 0$.

On vérifie facilement que

$$\forall P \in \mathbb{C},\ \forall \lambda \in \Lambda,\ \mathrm{ord}_{P+\lambda}(f) = \mathrm{ord}_P(f).$$

Définition 4.2. *Si f est une fonction elliptique non nulle sur $\mathbb{C}$, on appelle* degré *de la fonction f, l'entier*

$$\deg(f) \coloneqq \sum_{Q \in M(P,\omega_1,\omega_2),\, \mathrm{ord}_Q(f)>0} \mathrm{ord}_Q(f).$$

L'entier $\deg(f)$ est bien défini car toute maille élémentaire du réseau Λ est une partie bornée de $\mathbb{C}$. De plus l'entier $\deg(f)$ ne dépend pas de la maille élémentaire choisie pour le définir.

Proposition 4.3. *Si M est une maille élémentaire du réseau Λ et f une fonction elliptique, on a*

$$\sum_{Q \in M} \mathrm{ord}_Q(f) = 0.$$

Démonstration. La somme $\sum_{Q\in M} \mathrm{ord}_Q(f)$ ne dépend pas de la maille élémentaire M. On peut donc faire le calcul avec n'importe quelle maille élémentaire. Une partie bornée de $\mathbb{C}$ ne contient qu'un nombre fini de zéros et de pôles de f, on peut donc choisir la maille M de sorte qu'aucun pôle ni zéro de f n'appartienne au bord de $\overline{M}$, l'adhérence de M. On applique alors le théorème des résidus à la fonction $\frac{f'}{f}$ sur un contour parcourant le bord de $\overline{M}$. Notons que notre choix de f implique que la fonction $\frac{f'}{f}$ n'a pas de pôle sur ce contour. On obtient

$$\sum_{Q \in M} \mathrm{ord}_Q(f) = \frac{1}{2\mathrm{i}\pi}\left(\int_P^{P+\omega_1} \frac{f'(z)}{f(z)}\,\mathrm{d}z + \int_{P+\omega_1}^{P+\omega_1+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z + \int_{P+\omega_1+\omega_2}^{P+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z + \int_{P+\omega_2}^{P} \frac{f'(z)}{f(z)}\,\mathrm{d}z\right) = 0.$$

En effet le caractère elliptique de f implique que

$$\int_P^{P+\omega_1} \frac{f'(z)}{f(z)}\,\mathrm{d}z = \int_{P+\omega_2}^{P+\omega_1+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z$$

et

$$\int_P^{P+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z = \int_{P+\omega_1}^{P+\omega_1+\omega_2} \frac{f'(z)}{f(z)}\,\mathrm{d}z.$$

□

Corollaire 4.4. *Une fonction elliptique non nulle est de degré* 0 *si et seulement si elle est constante.*

Démonstration. Soit f une fonction elliptique telle que $\deg f = 0$. Par définition, la fonction f n'a pas de zéro sur $\mathbb{C}$. La proposition 4.3 implique que f n'a pas non plus de pôle sur $\mathbb{C}$. En particulier, la fonction f est une fonction holomorphe sur $\mathbb{C}$, invariante par translation par Λ. On en déduit

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\overline{M}} |f(z)|$$

où M désigne une maille élémentaire de Λ. Comme $\overline{M}$ est un compact et f continue, la fonction f est bornée sur $\overline{M}$, donc sur $\mathbb{C}$. La fonction f est holomorphe sur $\mathbb{C}$ et bornée, elle est donc constante. □

Proposition 4.5. *Si M est une maille élémentaire du réseau Λ et f une fonction elliptique, on a*

$$\sum_{Q\in M} Q \operatorname{ord}_Q(f) \in \Lambda.$$

Démonstration. On applique cette fois-ci la formule des résidus à la fonction $z \mapsto z\frac{f'(z)}{f(z)}$. □

Corollaire 4.6. *Il n'existe pas de fonction elliptique non nulle de degré* 1.

Démonstration. Soit f une fonction elliptique de degré 1. Si M est une maille élémentaire du réseau Λ, la fonction f a un unique zéro, disons z_0, dans M, ainsi qu'un unique pôle z_1 dans M. La proposition 4.5 implique alors $z_0 - z_1 \in \Lambda$. Par définition de M, on en déduit $z_0 = z_1$, ce qui est absurde. □

Proposition 4.7. *Soit f une fonction elliptique non constante et soit $c \in \mathbb{C}$. On a alors*

$$\sum_{P\in f^{-1}(c)} \operatorname{ord}_P(f - c) = \deg f.$$

En particulier, l'ensemble $f^{-1}(c)$ est non vide et, si A désigne l'ensemble des pôles de f, on a $f(\mathbb{C} \smallsetminus A) = \mathbb{C}$.

Démonstration. Si la fonction f est non constante, elle possède au moins un pôle. De plus, si P est un pôle de f, alors P est aussi un pôle de $f-c$ et f et $f-c$ ont le même ordre en P. On en déduit que $\deg(f-c)=\deg(f)$. Ainsi

$$\deg f = \deg(f-c) = \sum_{P\in f^{-1}(c)} \operatorname{ord}_P(f-c).$$

□

4.2 La fonction de Weierstraß

Si $\lambda\in\Lambda$, et $z\neq\lambda$, on a

$$\left|\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right| = \left|\frac{z(2\lambda-z)}{\lambda^2(z-\lambda)^2}\right| \sim_{|\lambda|\to+\infty} 2\frac{|z|}{|\lambda|^3}.$$

On en déduit que, pour $z\notin\Lambda$, la série

$$\mathfrak{p}(z) \coloneqq \frac{1}{z^2}+\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)$$

converge absolument.

L'égalité

$$\left|\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right| = \left|\frac{z(2\lambda-z)}{z^2(z-\lambda)^2}\right|$$

montre en fait que la série de fonctions définissant $\mathfrak{p}$ est normalement convergente sur tout compact de $\mathbb{C}\backslash\Lambda$. Comme il s'agit d'une série de fonctions holomorphes sur $\mathbb{C}\smallsetminus\Lambda$, on en conclut que $\mathfrak{p}$ est une fonction holomorphe sur $\mathbb{C}\smallsetminus\Lambda$ et que, pour $z\notin\Lambda$, on a

$$\mathfrak{p}'(z) = -2\sum_{\lambda\in\Lambda}\frac{1}{(z-\lambda)^3}.$$

Théorème 4.8. *La fonction $\mathfrak{p}$ est une fonction elliptique non nulle sur $\mathbb{C}$. De plus on a $\deg\mathfrak{p}=2$ et $\deg\mathfrak{p}'=3$.*

Démonstration. On a déjà prouvé que la fonction $\mathfrak{p}$ est holomorphe sur $\mathbb{C}\smallsetminus\Lambda$. De plus la fonction $\mathfrak{p}'$ est clairement invariante par translation par Λ et l'ouvert $\mathbb{C}\smallsetminus\Lambda$ de $\mathbb{C}$ est connexe. Ainsi, pour $\mu\in\Lambda$, il existe une constante $C(\mu)$ telle que

$$\forall z\in\mathbb{C}\smallsetminus\Lambda,\ \mathfrak{p}(z+\mu)=\mathfrak{p}(z)+C(\mu). \tag{4.1}$$

On vérifie facilement que la fonction $\mathfrak{p}$ est paire. On a alors

$$C(\mu)=\mathfrak{p}(\mu/2)-\mathfrak{p}(-\mu/2)=0$$

ce qui prouve la périodicité de $\mathfrak{p}$.

Remarquons à présent que la série $\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)$ est absolument convergente sur tout compact de $(\mathbb{C}\smallsetminus\Lambda)\cup\{0\}$. En particulier, la fonction $z\mapsto\mathfrak{p}(z)-\frac{1}{z^2}$ est homolorphe en 0. Ceci implique que la fonction $\mathfrak{p}$ est méromorphe en 0 et y possède un pôle d'ordre 2. Par périodicité de $\mathfrak{p}$, la fonction $\mathfrak{p}$ possède un pôle d'ordre 2 en tout point de Λ, il s'agit donc d'une fonction méromorphe sur $\mathbb{C}$. Fixons (ω_1,ω_2) une base de Λ. On vient de voir que la fonction $\mathfrak{p}$ possède un unique pôle d'ordre 2 dans l'ensemble $M(0,\omega_1,\omega_2)$, on a donc

$$\deg\mathfrak{p}=2.$$

Le même raisonnement nous permet de calculer le degré de $\mathfrak{p}'$. □

Calculons à présent un développement de Laurent de la fonction $\mathfrak{p}$ en 0. On commence par utiliser la formule

$$\frac{1}{(\lambda-z)}=\frac{1}{\lambda}\sum_{n\geqslant 0}\left(\frac{z}{\lambda}\right)^n$$

valable pour $|z|<|\lambda|$. En dérivant cette expression, on obtient

$$\frac{1}{(\lambda-z)^2}=\sum_{n\geqslant 0}(n+1)\frac{z^n}{\lambda^{n+2}}$$

Posons alors $r=\inf\{|\lambda|,\ \lambda\in\Lambda\smallsetminus\{0\}\}$. On a bien $r>0$, étant donné que $\Lambda\smallsetminus\{0\}$ est une partie fermée de $\mathbb{C}$ ne contenant pas 0. La convergence absolue de la série

$$\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\sum_{n\geqslant 1}(n+1)\frac{|z|^n}{|\lambda|^{n+2}}$$

pour $|z|<r$ permet d'invertir les signes sommes et d'obtenir l'égalité suivante

$$\begin{aligned}\mathfrak{p}(z)&=\frac{1}{z^2}+\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)\\&=\frac{1}{z^2}+\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\sum_{n\geqslant 1}(n+1)\frac{z^n}{\lambda^{n+2}}\\&=\frac{1}{z^2}+\sum_{n\geqslant 1}(n+1)\left(\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\frac{1}{\lambda^{n+2}}\right)z^n.\end{aligned}$$

Posons, pour $n\geqslant 3$,

$$G_n(\Lambda):=\sum_{\lambda\in\Lambda\smallsetminus\{0\}}\frac{1}{\lambda^n}.$$

Alors, soit en utilisant la parité de $\mathfrak{p}$, soit en remarquant que $G_n(\Lambda)=0$ pour n impair, on obtient

$$\mathfrak{p}(z)=\frac{1}{z^2}+\sum_{n\geqslant 1}(2n+1)G_{2n+2}(\Lambda)z^{2n}.$$

Théorème 4.9. *Les fonctions $\mathfrak{p}$ et $\mathfrak{p}'$ vérifient l'équation*

$$\mathfrak{p}'^2 = 4\mathfrak{p}^3 - 60G_4(\Lambda)\mathfrak{p} - 140G_6(\Lambda).$$

Démonstration. On calcule les premiers termes du développement de $\mathfrak{p}'^2$ en 0. On obtient

$$\mathfrak{p}'(z)^2 = 4z^{-6} - 24G_4(\Lambda)z^{-2} - 80G_6(\Lambda) + O(z).$$

Et donc

$$\mathfrak{p}'(z)^2 - 4\mathfrak{p}(z)^3 = -24G_4(\Lambda)z^{-2} - 80G_6(\Lambda) - 36G_4(\Lambda)z^{-2} - 60G_6(\Lambda) + O(z).$$

La fonction $\mathfrak{p}'^2 - 4\mathfrak{p}^3 + 60G_4(\Lambda)\mathfrak{p} + 140G_6(\Lambda)$ est donc une fonction elliptique sur $\mathbb{C}$, sans pôle et s'annulant en 0, il s'agit donc de la fonction nulle, ce qui prouve l'égalité

$$\mathfrak{p}'^2 = 4\mathfrak{p}^3 - 60G_4(\Lambda)\mathfrak{p} - 140G_6(\Lambda).$$

□

Proposition 4.10. *La fonction $\mathfrak{p}'$ a exactement trois zéros dans une maille élémentaire. De plus, ces trois zéros sont simples.*

Démonstration. Soit $M = M(P, \omega_1, \omega_2)$ une maille élémentaire du réseau Λ. La fonction $\mathfrak{p}'$ étant impaire, elle s'annule aux points $\omega_1/2$, $\omega_2/2$ et $(\omega_1 + \omega_2)/2$. Comme de plus $\mathfrak{p}'$ est une fonction elliptique de degré 3, ces trois points sont les seuls zéros de $\mathfrak{p}'$ et ce sont des zéros simples. □

Corollaire 4.11. *L'équation $Y^2Z = 4X^3 - g_4(\Lambda)XZ^2 - g_6(\Lambda)Z^3$ définit une courbe elliptique.*

Démonstration. Il suffit de vérifier que le polynôme $P_\Lambda(X) \coloneqq 4X^3 - g_4(\Lambda)X - g_6(\Lambda)$ a exactement trois racines dans $\mathbb{C}$. Soit (ω_1, ω_2) une base de Λ. D'après le théorème 4.9, les nombres $\mathfrak{p}(\omega_1/2)$, $\mathfrak{p}(\omega_2/2)$ et $\mathfrak{p}((\omega_1+\omega_2)/2)$ sont des racines de P_Λ. Il suffit donc de vérifier que ces nombres sont deux à deux distincts. Si $z \in \{\omega_1, \omega_2, (\omega_1 + \omega_2)/2\}$, on a $\mathfrak{p}'(z) = 0$, donc z est un zéro de $\mathfrak{p} - \mathfrak{p}(z)$ d'ordre au moins 2. Comme par ailleurs, $\deg(\mathfrak{p} - \mathfrak{p}(z)) = 2$, cet ordre est exactement 2, et z est l'unique zéro de $\mathfrak{p} - \mathfrak{p}(z)$ dans la maille élémentaire $M(0, \omega_1, \omega_2)$. On en déduit que les nombres $\mathfrak{p}(\omega_1)$, $\mathfrak{p}(\omega_2/2)$ et $\mathfrak{p}((\omega_1 + \omega_2)/2)$ sont deux à deux distincts. □

Soit E_Λ la courbe elliptique définie sur $\mathbb{C}$ par l'équation

$$Y^2Z = 4X^3 - g_4(\Lambda)XZ^2 - g_6(\Lambda)Z^3.$$

On étend alors l'application $z \mapsto (\mathfrak{p}(z), \mathfrak{p}'(z))$ en une application ψ_Λ de $\mathbb{C}/\Lambda$ dans $E_\Lambda(\mathbb{C})$ en posant

$$\psi_\Lambda(z) \coloneqq \begin{cases} (\mathfrak{p}(z) \colon \mathfrak{p}'(z) \colon 1) & \text{si } z \notin \Lambda; \\ (0 \colon 1 \colon 0) & \text{si } z \in \Lambda. \end{cases}$$

Théorème 4.12. *L'application ψ_Λ est bijective.*

Démonstration. Commençons par prouver que ψ_Λ est injective. Par définition, il suffit de vérifier que pour z_1 et z_2 dans $\mathbb{C} \smallsetminus \Lambda$,

$$\psi_\Lambda(z_1) = \psi_\Lambda(z_2) \Rightarrow z_2 - z_1 \in \Lambda.$$

On peut supposer que $\psi_\Lambda(z_1) = \psi_\Lambda(z_2)$ et que z_1 et z_2 sont tous deux dans une même maille élémentaire M. Par ailleurs, le cas où $\mathfrak{p}'(z_1) = 0$ a déjà été traité dans la preuve du corollaire 4.11. On peut donc supposer que $\mathfrak{p}'(z_1) = \mathfrak{p}'(z_2) \neq 0$. On raisonne alors comme dans la preuve du corollaire 4.11 sauf que cette fois-ci z_1 est un zéro simple de la fonction elliptique $\mathfrak{p} - \mathfrak{p}(z_1)$. Cette fonction est de degré 2 et a donc deux zéros simples dans la maille élémentaire M. Par parité de $\mathfrak{p}$ ces deux zéros sont z_1 et $-z_1$. Comme $\mathfrak{p}'(-z_1) = -\mathfrak{p}'(z_1) \neq \mathfrak{p}'(z_1)$, on a nécessairement $z_2 = z_1$.

Prouvons à présent la surjectivité de ψ_Λ. Soit $P = (x\colon y\colon 1)$ un point de $E_\Lambda(\mathbb{C})$. Comme $\mathfrak{p}$ est une fonction elliptique non constante, la proposition 4.7 implique qu'il existe $z \in \mathbb{C}$ tel que $\mathfrak{p}(z) = x$. On a alors $\mathfrak{p}'(z) \in \{y, -y\}$. Comme $\mathfrak{p}(-z) = \mathfrak{p}(z)$ et $\mathfrak{p}'(-z) = -\mathfrak{p}'(z)$, on a $\psi_\Lambda(z) = P$ ou $\psi_\Lambda(-z) = P$. □

Proposition 4.13. *Pour z_1 et z_2 dans $\mathbb{C}$, on a*

$$\psi_\Lambda(z_1 + z_2) = \psi_\Lambda(z_1) +_{E_\Lambda} \psi_\Lambda(z_2).$$

Démonstration. Soit L une droite projective de $\mathbb{P}^2(\mathbb{C})$. Et posons

$$L \cap E_\Lambda(\mathbb{C}) = P_1 + P_2 + P_3.$$

Soient $(z_1, z_2, z_3) \in \mathbb{C}^3$ tels que $\psi_\Lambda(z_i) = P_i$ pour $1 \leqslant i \leqslant 3$. Il suffit de prouver que $z_1 + z_2 + z_3 \in \Lambda$. Soit F un polynôme homogène de degré 1 tel que $L = V_p(F)$. Posons $f = \frac{F}{Z} \in \mathbb{C}(E_\Lambda)$. Il s'agit d'une fraction rationnelle. De plus, la fonction $g \coloneqq f \circ \psi_\Lambda$ est une fonction elliptique sur $\mathbb{C}$. On voit que les pôles de g sont les éléments de Λ et sont d'ordre 3. De plus, les zéros de f sont donnés, dans une maille élémentaire, par z_1, z_2 et z_3 comptés avec multiplicité. On déduit alors de la proposition 4.5 que

$$z_1 + z_2 + z_3 - 3 \cdot 0 \in \Lambda,$$

ce qu'il fallait démontrer. □

Corollaire 4.14. *La loi de composition $+_{E_\Lambda}$ sur l'ensemble $E_\Lambda(\mathbb{C})$ est une loi de groupe commutatif et ψ_Λ induit un isomorphisme de groupes*

$$\psi_\Lambda : (\mathbb{C}/\Lambda, +) \xrightarrow{\sim} (E_\Lambda(\mathbb{C}), +_{E_\Lambda}).$$

4.3 Un petit détour du côté des formes modulaires

Les fonctions $\Lambda \mapsto g_4(\Lambda)$ et $\Lambda \mapsto g_6(\Lambda)$ sont définis sur l'ensemble des réseaux et ont la propriété remarquable suivante

$$\forall a \in \mathbb{C},\ g_4(a\Lambda) = a^{-4} g_4(\Lambda),\ g_6(a\Lambda) = a^{-6} g_6(\Lambda).$$

La fonction $\Delta \coloneqq g_4^3 - 27 g_6^2$ possède le même genre de propriété. De plus la proposition 4.11 implique que $\Delta(\Lambda) \neq 0$ quelque soit le réseau Λ. On peut donc définir, pour tout réseau Λ, le nombre complexe

$$j(\Lambda) \coloneqq 1728 \frac{g_4(\Lambda)^3}{\Delta(\Lambda)}.$$

On vérifie immédiatement que ce nombre complexe ne dépend pas de la classe d'homothétie du réseau Λ et est donc un invariant de la classe d'isomorphisme de la courbe elliptique E_Λ.

Si Λ est un réseau de $\mathbb{C}$, il existe un nombre complexe $\tau \in \mathbb{C}$ tel que $\operatorname{Im} \tau > 0$ et tel que Λ soit homothétique au réseau $\mathbb{Z} \oplus \mathbb{Z}\tau$. On définit alors des fonctions sur le demi-plan de Poincaré

$$\mathbb{H} \coloneqq \{z \in \mathbb{C},\ \operatorname{Im} z > 0\}$$

en posant

$$\forall \tau \in \mathbb{H},\ g_4(\tau) \coloneqq g_4(\mathbb{Z} \oplus \mathbb{Z}\tau),\ g_6(\tau) \coloneqq g_6(\mathbb{Z} \oplus \mathbb{Z}\tau).$$

Les propriétés de semi-invariante des fonctions de réseau g_4 et g_6 impliquent la propriété remarquable

$$\forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}),\ \forall \tau \in \mathbb{H},\ g_4\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^4 g_4(\tau),\ g_6\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^6 g_6(\tau).$$

On en déduit immédiatement que la fonction j est invariante sous l'action du groupe $\mathrm{SL}_2(\mathbb{Z})$. Autrement dit

$$\forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}),\ j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

Plus généralement considérons un entier $k \in \mathbb{Z}$ ainsi qu'une fonction holomorphe f de $\mathbb{H}$ dans $\mathbb{C}$ vérifiant

$$\forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}),\ f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau). \tag{4.2}$$

Une telle fonction est en particulier périodique de période 1 :

$$\forall \tau \in \mathbb{H},\ f(\tau + 1) = f(\tau).$$

On en déduit qu'il existe une unique fonction holomorphe F de $\{q \in \mathbb{C},\ 0 < |q| < 1\}$ telle que

$$\forall \tau \in \mathbb{H},\ f(\tau) = F(e^{2\mathrm{i}\pi\tau}).$$

Exemple 4.15. On a

$$G_{2k}(\tau) \coloneqq \sum_{(c,d)\in\mathbb{Z}\smallsetminus\{(0,0)\}} \frac{1}{(c\tau+d)^{2k})} = 2\zeta(2k) + 2\frac{(2\mathrm{i}\pi)^{2k}}{(2k-1)!}\sum_{n\geqslant 1}\left(\sum_{d|n} d^{k-1}\right) q^n.$$

Définition 4.16. *Si $k \in \mathbb{Z}$, on appelle forme modulaire de poids k une fonction holomorphe $f : \mathbb{H} \to \mathbb{C}$ vérifiant la relation* (4.2) *et ayant un q développement holomorphe, autrement dit s'il existe une fonction holomorphe F sur le disque unité ouvert vérifiant*

$$\forall \tau \in \mathbb{H},\ f(\tau) = F(e^{2\mathrm{i}\pi\tau}).$$

Pour $k \geqslant 2$, la fonction G_{2k} est une forme modulaire de poids $2k$. On en déduit facilement que la fonction Δ est une forme modulaire de poids 12. La fonction j n'est pas une forme modulaire, en effet elle est *méromorphe à l'infini* :

$$j(\tau) = \frac{1}{q} + \cdots .$$

On vérifie facilement qu'il ne peut exister de formes modulaire de poids k impair. En fait, il n'existe de formes modulaire de poids k que pour k pair et $\geqslant 4$ ou $k = 0$. Dans ce cours, nous aurons uniquement besoin du cas particulier où $k = 0$.

Proposition 4.17. *Les seules formes modulaires de poids* 0 *sont les fonctions constantes sur $\mathbb{H}$.*

Démonstration. En effet, soit f une forme modulaire de poids 0. Considérons son q-développement

$$f(\tau) = \sum_{n\geqslant 0} a_n q^n.$$

Nous allons prouver que la fonction $g \coloneqq f - a_0$ est nulle. Posons

$$\mathcal{F} \coloneqq \left\{\tau \in \mathbb{H} \mid |\tau| \geqslant 1,\ -\frac{1}{2} \leqslant \mathrm{Re}(\tau) \leqslant \frac{1}{2}\right\}.$$

L'ensemble $\mathcal{F}$ est un domaine fondamental pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$. En particulier, on a

$$\mathbb{H} = \bigcup_{M\in\mathrm{SL}_2(\mathbb{Z})} M\mathcal{F}$$

(voir l'exercice 4.3 pour une preuve de cette égalité). Comme g est une forme modulaire de poids 0, elle est invariante sous l'action de $\mathrm{SL}_2(\mathbb{Z})$ et donc

$$\sup_{\mathbb{H}} |g| = \sup_{\mathcal{F}} |g|.$$

Par ailleurs, un examen du q-développement de la fonction g montre que pour tout $\varepsilon > 0$, il existe $A_\varepsilon > 0$ tel que

$$\operatorname{Im}\tau > A_\varepsilon \Rightarrow |g(\tau)| < \varepsilon.$$

Supposons alors $g \neq 0$. Il existe donc $A > 0$ tel que

$$\sup_{\mathbb{H}}|g| = \sup_{\mathcal{F}}|g| = \sup_{\mathcal{F}\cap\{\operatorname{Im}\tau\leqslant A\}}|g|.$$

La partie $\mathcal{F}\cap\{\operatorname{Im}\tau \leqslant A\}$ étant compacte, la fonction continue $|g|$ y atteint son maximum. Ainsi la fonction g est une fonction holomorphe atteignant son maximum sur un ouvert connexe de $\mathbb{C}$. Le principe du maximum implique qu'il s'agit d'une fonction constante. On en conclut que f est également une fonction constante. □

Théorème 4.18. *La fonction j induit une surjection de $\mathbb{H}$ sur $\mathbb{C}$.*

Démonstration. Il s'agit de prouver que si $c \in \mathbb{C}$, il existe $\tau \in \mathbb{H}$ tel que $j(\tau) = c$ ou encore tel que $g_4(\tau)^3 - c\Delta(\tau) = 0$. L'idée de la preuve est de supposer par l'absurde qu'un tel τ n'existe pas et d'en déduire une contradiction. Supposons que la fonction $g_4^3 - c\Delta$ ne s'annule pas sur $\mathbb{H}$. Comme $\zeta(4) = \frac{\pi^4}{90} > 0$, le terme constant de son q-développement ne s'annule pas. On en conclut que la fonction $\frac{g_4^3}{g_4^3 - c\Delta}$ est une forme modulaire de poids 0 sur $\mathbb{H}$. La proposition 4.17 implique alors qu'il s'agit d'une constante non nulle. Il existe donc $d \neq 0$ tel que $g_4^3 = dg_4^3 - dc\Delta$ et donc

$$(1 - d + dc)g_4^3 = 27dcg_6^2.$$

Une comparaison des premiers termes des q-développements de g_4^3 et g_6^2 montre que ces formes ne sont pas proportionnelles, d'où $dc = 0$, $d = 1$ et donc $c = 0$. Ce qui est encore une fois absurde puisque g_4, et donc j, s'annule en $e^{\frac{2i\pi}{3}}$. □

Corollaire 4.19. *Soit $(a, b) \in \mathbb{C}^2$ tel que $4a^3 + 27b^2 \neq 0$. Alors il existe un réseau $\Lambda \subset \mathbb{C}$ tel que $(g_4(\Lambda), g_6(\Lambda)) = (a, b)$. Autrement dit, toute courbe elliptique sur $\mathbb{C}$ est de la forme E_Λ pour un certain réseau $\Lambda \subset \mathbb{C}$.*

4.4 Exercices

Exercice 4.1. Soit Λ un réseau de $\mathbb{C}$. Soit f une fonction elliptique (relativement à Λ) paire.

a) Si $a \in \mathbb{C}$ vérifie $2a \notin \Lambda$, montrer que $\mathrm{ord}_a(f) = \mathrm{ord}_{-a}(f)$. Si $2a \in \Lambda$, montrer que $\mathrm{ord}_a(f)$ est pair.

b) Montrer qu'il existe une fraction rationnelle $F(X) \in \mathbb{C}(X)$ telle que $f = F(\mathfrak{p}_\Lambda)$. *Indication* : on pourra considérer une suite $u_1, \dots, u_r$ de points de $\mathbb{C}$ contenant exactement un élément de chaque partie $\{u, -u \mod \Lambda\}$ où u est un zéro ou pôle de f et poser $m_i = \mathrm{ord}_{u_i}(f)$ si $2u_i \notin \Lambda$ et $m_i = \frac{1}{2}\mathrm{ord}_{u_i}(f)$ si $2u_i \in \Lambda$, puis considérer la fonction $g(z) = \prod_{i=1}^r (\mathfrak{p}_\Lambda(z) - \mathfrak{p}_\Lambda(u_i))^{m_i}$.

c) En déduire que si f est une fonction elliptique, il existe une fraction rationnelle $F(X,Y) \in \mathbb{C}(X,Y)$ telle que $f = F(\mathfrak{p}_\Lambda, \mathfrak{p}'_\Lambda)$. *Indication* : on pourra commencer par décomposer f comme somme d'une fonction elliptique paire et d'une fonction elliptique impaire.

Exercice 4.2. Soit $\Lambda \subset \mathbb{C}$ un réseau. On pose, pour $z \in \mathbb{C}$,

$$\sigma_\Lambda(z) \coloneqq \prod_{\omega \in \Lambda \smallsetminus \{0\}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2}.$$

a) Montrer que σ_Λ est une fonction holomorphe sur $\mathbb{C}$ et que possède un zéro simple en chaque point de Λ et ne s'annule hors de Λ.

b) Calculer $\frac{d^2}{dz^2}\log\sigma$ et en déduire qu'il existe des constantes $a, b \in \mathbb{C}$ telles que

$$\forall z \in \mathbb{C}, \quad \sigma_\Lambda(z + \omega) = e^{az+b}\sigma(z).$$

c) Soient $n_1, \dots, n_r \in \mathbb{Z}$ et $z_1, \dots, z_r \in \mathbb{C}$ tels que $\sum_i n_i = 0$ et $\sum_i n_i z_i \in \Lambda$. Montrer alors qu'il existe une fonction elliptique f relativement à Λ telle que

$$\mathrm{div}(f) = \sum_i n_i(z_i).$$

Indication : on pourra considérer la fonction

$$\prod_i \sigma(z - z_i)^{n_i}.$$

Exercice 4.3. Soit $\tau \in \mathbb{H}$.

a) Si $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, calculer la partie imaginaire de $M\tau \coloneqq \frac{a\tau+b}{c\tau+d}$.

b) Montrer qu'il existe $M \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\mathrm{Im}(M\tau)$ soit maximal.

c) En déduire qu'il existe $M \in \mathrm{SL}_2(\mathbb{Z})$ tel que

$$M\tau \in \left\{\tau \in \mathbb{H} \mid \tau \geqslant 1,\ -\frac{1}{2} \leqslant \mathrm{Re}(\tau) \leqslant \frac{1}{2}\right\}.$$

Chapitre 5

Points de torsion des courbes elliptiques

Sauf mention du contraire, la lettre k désigne toujours un corps de caractéristique différente de 2 et 3.

Définition 5.1. *Si E est une courbe elliptique et si $N \geqslant 1$, on note $[N]$ l'application de E dans E définie par*

$$[N](P) = \underbrace{P + \cdots + P}_{N}$$

C'est un morphisme de groupes dont le noyau est noté $E[N]$.

Le but de cette partie est d'étudier la structure du groupe $E[N]$.

5.1 Le cas des courbes elliptiques complexes

Théorème 5.2. *Soit E une courbe elliptique définie sur $\mathbb{C}$. Alors le sous-groupe $E[N]$ de $E(\mathbb{C})$ est un groupe abélien fini isomorphe à $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.*

Démonstration. D'après le théorème 4.19, il existe un réseau $\Lambda \subset \mathbb{C}$ tel que le groupe $E(\mathbb{C})$ est isomorphe au groupe $\mathbb{C}/\Lambda$. Il est alors immédiat de vérifier que le noyau $E[N]$ de la multiplication par N est isomorphe au quotient $N^{-1}\Lambda/\Lambda$ qui est isomorphe au groupe $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. □

5.2 Endomorphismes des courbes elliptiques

Définition 5.3. *Soit k un corps algébriquement clos et soient E_1 et E_2 deux courbes elliptiques définies sur k par des équations de Weierstraß. Un* morphisme *de la courbe*

elliptique E_1 vers la courbe E_2 est un morphisme de groupes α qui est également un morphisme de courbes projectives. Un endomorphisme *d'une courbe elliptique E est un morphisme de E dans E.*

Proposition 5.4. *Si α et β sont deux morphismes de courbes elliptiques $E_1 \to E_2$, alors $\alpha + \beta$ est un morphisme de E_1 vers E_2. Si $E_1 = E_2$, alors $\beta \circ \alpha$ est aussi un endomorphisme de E_1.*

Démonstration. C'est clair pour $\beta\circ\alpha$. Pour $\alpha+\beta$, on peut utiliser la proposition 3.13. En effet, si $\alpha = -\beta$, c'est immédiat. Sinon les formules explicites d'additions (3.1) montrent que $\alpha+\beta$ est un morphisme en restriction à l'ouvert non vide $\{P \in E_1 \mid \alpha(P) \neq -\beta(P)\}$. Pour appliquer la proposition 3.13, il reste donc à vérifier que $\alpha + \beta$ est continue pour la topologie de Zariski. Autrement dit, il faut montrer que pour tout $Q \in E_2$, l'ensemble $\{P \in E_1 \mid \alpha(P) + \beta(P) = Q\}$ est égal à E_1 ou est fini. Il ne peut être égal à E_1 que si $\alpha = -\beta$ et $Q = 0$. Supposons donc $\{P \in E_1 \mid \alpha(P) + \beta(P) = Q\}$ infini. Alors les applications continues α et $Q - \beta$ coïncident sur une partie infinie. Par continuité elles coïncident sur E_1 et donc $\alpha = -\beta$. □

Ainsi, si E est une courbe elliptique, l'ensemble $\operatorname{End} E$ de ses endomorphismes est un sous-anneau de l'anneau des endomorphismes du *groupe* E. En particulier, pour tout $N \in \mathbb{Z}$, on a $[N] \in \operatorname{End} E$.

Si $\alpha : E_1 \to E_2$ est un morphisme de E_1 dans E_2, il existe deux fractions rationnelles R_1 et R_2 sur E_1 telles que si $P = (x_P, y_P) \in E_1 \smallsetminus \{0\}$, et si P n'annule pas les dénominateur de R_1 et R_2, alors

$$\alpha(P) = (R_1(x_p, y_P) : R_2(x_P, y_P) : 1) \in E_2.$$

Les fractions rationnelles R_1 et R_2 ne sont pas uniques. En effet si $(x : y : 1) \in E$, on a $y^2 = x^3 + ax + b$. On ne change pas α en remplaçant y^2 par $x^3 + ax + b$ dans R_1 et R_2. On peut donc supposer R_1 et R_2 de la forme

$$R_i(x, y) = \frac{p_1^i(x) + p_1^i(x)y}{q_1^i(x) + q_2^i(x)y} = \frac{(p_1^i(x) + p_2^i(x)y)(q_1^i(x) - q_2^i(x)y)}{(q_1^i(x)^2 - q_2^i(x)^2(x^3 + ax + b))} = \frac{r_1^i(x) + r_2^i(x)y}{q^i(x)},$$

où r_1^i, r_2^i et q^i sont des polynômes de $k[X]$. Comme α est un endomorphisme de groupes, on a en particulier $\alpha(x, -y) = -\alpha(x, y)$, c'est-à-dire $p_2^1 = 0$ et $q_1^2 = 0$. On peut donc choisir R_1 et R_2 de la forme

$$R_1(x, y) = \frac{P(x)}{Q(x)}, \quad R_2(x, y) = \frac{R(x)}{S(x)}y.$$

Une telle écriture pour R_1 et R_2, avec P et Q premiers entre eux et R et S premiers entre eux, est unique et ne dépend que de α. On l'appelle *l'écriture canonique* de α. On déduit alors de la continuité de α que *pour tout* $(x, y) \in E \smallsetminus \{0\}$ tel que $Q(x) \neq 0$, on a $\alpha(x, y) \neq 0$ et

$$\alpha(x, y) = \left(\frac{P(x)}{Q(x)}, \frac{R(x)}{S(x)}y\right).$$

Remarque 5.5. La relation $R_2^2 = R_1^3 + aR_1 + b$ s'écrit alors

$$\frac{(x^3+ax+b)R(x)^2}{S(x)^2} = \frac{P(x)^3 + aP(x)Q(x)^2 + bQ(x)^3}{Q(x)^3},$$

ou encore

$$(x^3+ax+b)R(x)^2Q(x)^3 = (P(x)^3 + aP(x)Q(x)^2 + bQ(x)^3)S(x)^2.$$

Définition 5.6. *Le* degré *de l'endomorphisme α est alors, par définition,*

$$\deg \alpha = \max(\deg P, \deg Q)$$

On convient aussi que le degré de l'endomorphisme constant égal à 0 est 0.

On dit qu'un endomorphisme non nul α est séparable *si $\left(\frac{P}{Q}\right)' \neq 0$.*

On peut définir de la même façon le degré d'un morphisme d'une courbe elliptique E_1 vers une courbe elliptique E_2.

Le phénomène d'inséparabilité n'apparaît que lorsque k est de caractéristique p pour p un nombre premier.

Exemple 5.7. Soit E une courbe elliptique définie sur $\mathbb{F}_q$ par une équation de Weierstrass. L'endomorphisme de Frobenius, ϕ_q défini par $(x,y) \mapsto (x^q, y^q)$ n'est pas séparable et est de degré q.

Le degré d'un endomorphisme non nul est lié au cardinal des fibres $\alpha^{-1}(Q)$.

Proposition 5.8. *Soit α un endomorphisme non nul d'une courbe elliptique E, on a*

$$|\alpha^{-1}(0)| \leqslant \deg \alpha$$

avec égalité si et seulement si α est séparable.

Démonstration. Supposons $\alpha \neq 0$ et écrivons α sous la forme

$$\alpha(x,y) = (R_1(x), R_2(x,y)) = \left(\frac{P(x)}{Q(x)}, \frac{R(x)}{S(x)}y\right)$$

avec P et Q premiers entre eux, ainsi que R et S. Supposons α séparable. Soit $\mathcal{S} = \{x \in k,\ (P'Q - PQ')(x) = 0\}$. Comme α est séparable, $\mathcal{S}$ est une partie finie de k. Comme de plus, la fonction R_1 prend une infinité de valeurs, il existe un point $(c,d) \in E$ tel que

— $c \neq 0$, $d \neq 0$, $c \notin R_1(\mathcal{S})$ et $(c,d) \in \alpha(E)$;

— $\deg(P - cQ) = \deg \alpha$.

Comme α est un morphisme de groupes, on a $|\alpha^{-1}(0)| = |\alpha^{-1}((c,d))|$. Nous allons montrer que $|\alpha^{-1}((c,d))| = \deg\alpha$. Un point (x,y) vérifie $\alpha(x,y) = (c,d)$ si et seulement si

$$P(x) = cQ(x), \quad R_2(x)y = d.$$

Puisque $d \neq 0$, on a $R_2(x) \neq 0$ et alors $y = \frac{d}{R_2(x)}$. Ainsi le cardinal de $|\alpha^{-1}((c,d))|$ est égal au nombre de racines du polynôme $P - cQ$. Comme ce polynôme est de degré $\deg\alpha$, il suffit de prouver que ce polynôme n'a que des racines simples. Or une racine double de $P - cQ$ est automatique racine de $P'Q - PQ' = (P' - cQ')Q - (P - cQ)Q'$. L'existence d'une racine double de $P - cQ$ contredirait $c \notin R_1(\mathcal{S})$.

Si maintenant α n'est pas séparable, alors le polynôme $P - cQ$ a toujours des racines doubles. □

Proposition 5.9. *Un endomorphisme non nul d'une courbe elliptique est surjectif.*

Démonstration. Le point $P = 0$ est toujours l'image de 0. On fixe donc un point $P = (c,d) \in E \setminus \{0\}$ et on cherche $(x,y) \in E$ tel que $\alpha(x,y) = (c,d)$. Soit $(\frac{P}{Q}, \frac{R}{S}Y)$ l'écriture canonique de α. Posons $F(X) = P(X) - cQ(X)$. Séparons deux cas.

1. Si le polynôme F n'est pas constant, fixons x_0 une racine de F. Comme P et Q sont premiers entre eux, on a nécessairement $Q(x_0) \neq 0$. Soit y_0 une racine carré de $x_0^3 + ax_0 + b$. Alors $\alpha(x_0, y_0) = (c, d')$ avec $d' \in k$. Comme (c,d') est un point de E, on a nécessairement $d = \pm d'$ et donc $(c,d) = \alpha(x_0, \pm y_0)$.

2. Supposons à présent que F est un polynôme constant. Comme $\mathrm{Ker}(\alpha)$ est fini, la fraction $\frac{P}{Q}$ n'est pas constante, l'élément c est donc l'unique élément de k tel que $P - cQ$ est constant. D'après l'étude du cas précédent, il existe donc au plus deux points qui ne sont pas dans l'image de α et ces deux points sont de la formes $(c, \pm d)$ où $d^2 = c^3 + ac + b$. Comme E est infini, choisissons (c_1, d_1) tel que $(c_1,d_1) + (c,d) \neq \pm(c, \pm d)$. Comme (c_1,d_1) et $(c_1,d_1) + (c,d)$ sont dans l'image de α, c'est aussi le cas de (c,d) puisque α est un morphisme de groupes. □

Corollaire 5.10. *L'anneau des endomorphismes* $\mathrm{End}\, E$ *d'une courbe elliptique* E *est intègre.*

Démonstration. Supposons en effet que $\alpha \circ \beta = 0$. Si $\beta \neq 0$, alors $\beta(E) = E$, donc $\alpha = 0$. □

5.3 Les polynômes de division

Si l'on veut déterminer le degré de l'endomorphisme $[N]$, il faut déterminer des polynômes φ_N et ψ_N tels que $[N](x,y) = (\frac{\varphi_N(x)}{\psi_N(x)}, \dots)$. C'est ce que nous allons faire dans cette partie. Nous avons décidé de suivre l'approche historique et de dériver ce calcul de la méthode analytique complexe.

Soit E une courbe elliptique définie sur $\mathbb{C}$ et soit Λ un réseau de $\mathbb{C}$ tel que $E \simeq E_\Lambda$. On cherche à étudier les polynômes dont les racines sont les coordonnées des points de $E[N]$. On est naturellement amené à étudier la fonction

$$z \longmapsto N^2 \prod_{\omega \in E[N] \smallsetminus \{0\}} (\mathfrak{p}(z) - \mathfrak{p}(\omega)).$$

Il existe un polynôme $P_N \in \mathbb{C}[X]$ tel que

$$N^2 \prod_{\omega \in E[N] \smallsetminus \{0\}} (\mathfrak{p}(z) - \mathfrak{p}(\omega)) = \begin{cases} P_N(\mathfrak{p}(z))^2 & \text{si } N \text{ est impair;} \\ \left(\frac{1}{2}\mathfrak{p}'(z)\right)^2 P_N(\mathfrak{p}(z))^2 & \text{si } N \text{ est pair.} \end{cases}$$

On déduit du théorème 5.2 que le polynôme P_N est un polynôme de degré $\frac{N^2-1}{2}$ si N est impair et $\frac{N^2-4}{2}$ si N est pair. Son coefficient dominant est égal à N.

Le polynôme P_N ainsi défini est appelé N-ième *polynôme de division.*

On posera également

$$\psi_N(z) := \begin{cases} P_N(\mathfrak{p}(z)) & \text{si } N \text{ est impair;} \\ \frac{1}{2}\mathfrak{p}'(z) P_N(\mathfrak{p}(z)) & \text{si } N \text{ est pair.} \end{cases}$$

De sorte que ψ_N^2 est toujours un polynôme de degré $N^2 - 1$ en $\mathfrak{p}$.

Proposition 5.11. *Pour tout $N \geqslant 2$, on a la relation suivante entre fonctions elliptiques*

$$\mathfrak{p}(Nz) = \mathfrak{p}(z) - \frac{\psi_{N-1}(z)\psi_{N+1}(z)}{\psi_N(z)^2}.$$

Démonstration. La fonction $z \mapsto \mathfrak{p}(Nz) - \mathfrak{p}(z)$ a, en dehors des points de Λ, un pôle d'ordre 2 en tout zéro de ψ_N^2. Par ailleurs cette fonction a un zéro exactement aux points de $\mathbb{C} \smallsetminus \Lambda$ tels que $Nz = \pm z$. De plus ces zéros ont multiplicité un. En effet si ce n'était pas le cas, la dérivée de la fonction $z \mapsto \mathfrak{p}(Nz) - \mathfrak{p}(z)$ s'annulerait en un tel point, on aurait donc $N\mathfrak{p}'(Nz) = \mathfrak{p}'(z)$, ce qui est absurde si $Nz = \pm z \mod \Lambda$. On en conclut que la fonction méromorphe

$$z \mapsto \frac{\psi_N(z)^2(\mathfrak{p}(Nz) - \mathfrak{p}(z))}{\psi_{N+1}(z)\psi_{N-1}(z)}$$

n'a de zéros et pôles que sur Λ, elle est donc constante. En calculant sa limite en 0, on obtient l'égalité recherchée. □

De la proposition 5.11, on peut déduire une relation de récurrence permettant de calculer les fonctions ψ_N ainsi que les polynômes P_N. Fixons en effet $M > N$. La fonction $z \mapsto \mathfrak{p}(Mz) - \mathfrak{p}(Nz)$ a un zéro d'ordre un en tous les points $u \in \mathbb{C}$ tels que $Mu \equiv \pm Nu \not\equiv 0 \mod \Lambda$. Comme ni ψ_N ni ψ_M ne peut s'annuler en de tels points, on en conclut que ce sont des zéros de la fonction $\psi_{N+1}\psi_{N-1}\psi_M^2 - \psi_{M+1}\psi_{M-1}\psi_N^2$. Ce sont

également les zéros avec multiplicité un de la fonction $\psi_{M+N}\psi_{M-N}$. Comme ces deux fonctions sont des polynômes de même degré en $\mathfrak{p}_\Lambda$ ayant les mêmes zéros, on en conclut l'égalité

$$\psi_{M+N}\psi_{M-N} = \psi_{M+1}\psi_{M-1}\psi_N^2 - \psi_{N+1}\psi_{N-1}\psi_M^2. \tag{5.1}$$

Corollaire 5.12. *On a les formules de récurrence suivantes*

$$\begin{aligned} P_{2N+1} &= \begin{cases} P_{N+2}P_N^3 - P_{N+1}^3 P_{N-1}(X^3+AX+B)^2 & \text{pour } N \text{ impair;} \\ (X^3+AX+B)^2 P_{N+2}P_N^3 - P_{N+1}^3 P_{N-1} & \text{pour } N \text{ pair;} \end{cases} \\ P_{2N} &= \frac{1}{2}P_N(P_{N+2}P_{N-1}^2 - P_{N-2}P_{N+1}^2). \end{aligned} \tag{5.2}$$

On en conclut en particulier que $P_N \in \mathbb{Z}[A,B][X]$ *où* $A = -\frac{1}{4}g_4(\Lambda)$ *et* $B = -\frac{1}{4}g_6(\Lambda)$.

Soit k un corps parfait de caractéristique différente de 2 ou 3 et fixons a et b dans k tels que $4a^3 + 27b^2 \neq 0$. On note E la courbe elliptique définie par l'équation de Weierstraß $Y^2 = X^3 + aX + b$. Définissons alors par récurrence la suite d'éléments suivants $P_N \in k[X]$. On pose

$$\begin{aligned} P_1 &= 1, \quad P_2 = 2 \\ P_3 &= 3X^4 + 6aX^2 + 12bX - a^2 \\ P_4 &= 4(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3) \\ P_{2N+1} &= \begin{cases} P_{N+2}P_N^3 - P_{N+1}^3 P_{N-1}4(X^3+aX+b)^2 & \text{pour } N \text{ impair;} \\ (X^3+aX+b)^2 P_{N+2}P_N^3 - P_{N+1}^3 P_{N-1} & \text{pour } N \text{ pair;} \end{cases} \\ P_{2N} &= \frac{1}{2}P_N(P_{N+2}P_{N-1}^2 - P_{N-2}P_{N+1}^2). \end{aligned} \tag{5.3}$$

On définit alors des éléments ψ_N, φ_N et ω_N dans $k[X,Y]/(Y^2 - X^3 - aX - b)$ par les formules

$$\begin{aligned} \psi_N &= P_N(X) \text{ si } N \text{ est impair;} \\ \psi_N &= YP_N(X) \text{ si } N \text{ est pair;} \\ \varphi_N &= X\psi_N^2 - \psi_{N-1}\psi_{N+1} \\ 4Y\omega_N &= \psi_{N+2}\psi_{N-1}^2 - \psi_{N-2}\psi_{N+1}^2. \end{aligned}$$

On remarque que, pour tout $N \geqslant 1$, l'élément ψ_N^2 est dans l'image de $k[X]$.

Proposition 5.13. *Alors pour tout* $(x,y) \in E \smallsetminus \{0\}$ *tel que* $\psi_N(x,y) \neq 0$, *on a*

$$[N](x,y) = \left(\frac{\varphi_N(x,y)}{\psi_N(x,y)^2}, \frac{\omega_N(x,y)}{\psi_N(x,y)^3}\right).$$

De plus, les polynômes $\varphi_N(X)$ *et* $\psi_N(X)^2$ *sont premiers entre eux. En particulier* $\deg[N] = N^2$.

Soit A un anneau principal et soit $\mathfrak{p}$ un idéal premier non nul de A. Il s'agit alors d'un idéal maximal. Notons $k = A/\mathfrak{p}$ son corps résiduel et K le corps des fractions de A. On peut alors définir de façon canonique une application de « réduction modulo $\mathfrak{p}$ » allant de $\mathbb{P}^n(K)$ vers $\mathbb{P}^n(k)$. En effet tout élément x de $\mathbb{P}^n(K)$ possède un système de coordonnées homogènes $(x_0 : \ldots : x_n)$ tel que $(x_0, \ldots, x_n) \in A^{n+1}$ et tel que les éléments $x_0, \ldots, x_n$ sont premiers entre eux dans leur ensemble. On peut donc définir la réduction de x modulo $\mathfrak{p}$ par la formule

$$\mathrm{red}_{\mathfrak{p}}(x) \coloneqq ((x_0 \mod \mathfrak{p}) : \ldots : (x_n \mod \mathfrak{p})) \in \mathbb{P}^n(k).$$

On vérifie immédiatement que cette définition ne dépend du choix de $(x_0 : \ldots : x_n)$.

Supposons à présent donnée une courbe elliptique E définie sur K par une équation de Weierstraß $Y^2 = X^3 + aX + b$ où a et b sont deux éléments de A tels que

$$4a^3 + 27b^2 \not\equiv 0 \mod \mathfrak{p}.$$

Cela implique que la courbe plane définie sur k par l'équation $Y^2 = X^3 + \overline{a}X + \overline{b}$ est une courbe elliptique. De plus l'application de réduction $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$ envoie $E(K)$ dans $E(k)$. On vérifie, par exemple sur les formules explicites d'addition, que cette application est en fait un morphisme de groupes.

Démonstration de la proposition 5.13. Si k est un corps de caractéristique 0, on plonge le sous-corps de k engendré par $\mathbb{Q}$, a et b dans $\mathbb{C}$ et on se ramène au cas d'une courbe elliptique définie sur $\mathbb{C}$ qui est un exercice à partir de la proposition 5.11. Soit donc k un corps de caractéristique p différente de 2 et 3, E une courbe elliptique définie sur k par l'équation $Y^2 = X^3 + aX + b$ ainsi que $P = (x, y) \in E(k) \smallsetminus \{0\}$ un point de $E(k)$ tel que $\psi_N(x, y) \neq 0$. Nous admettons ici qu'il existe A un anneau principal dont le corps des fractions est de caractéristique 0 et muni d'un morphisme d'anneaux $h : A \mapsto k$, de noyau $\mathfrak{p}$ ainsi que d'éléments $\tilde{a}$, $\tilde{b}$, $\tilde{x}$ et $\tilde{y}$ s'envoyant respectivement sur a, b, x et y via h tels que $\tilde{P} \coloneqq (\tilde{x}, \tilde{y}) \in E(K)$. La construction d'un tel anneau, lorsque k est un corps fini, est esquissée un peu plus loin (proposition 8.10). En particulier on obtient une courbe elliptique $\tilde{E}$ définie sur K par l'équation $Y^2 = X^3 + \tilde{a}X + \tilde{b}$ et h induit un morphisme de groupes $E(K) \to E(k)$ envoyant $\tilde{P}$ sur P. Comme de plus φ_N, ψ_N et ω_N sont les réductions modulo $\mathfrak{p}$ des polynômes analogues à coefficients dans A, on en conclut que

$$[N](P) = \mathrm{red}_{\mathfrak{p}}([N](\tilde{P})) = \mathrm{red}_{\mathfrak{p}}\left(\frac{\tilde{\varphi}_N(\tilde{x}, \tilde{y})}{\tilde{\psi}_N(\tilde{x}, \tilde{y})^2}, \frac{\tilde{\omega}_N(\tilde{x}, \tilde{y})}{\tilde{\psi}_N(\tilde{x}, \tilde{y})^3}\right) = \left(\frac{\varphi_N(x, y)}{\psi_N(x, y)^2}, \frac{\omega_N(x, y)}{\psi_N(x, y)^3}\right),$$

le cas du corps K de caractéristique 0 ayant déjà été traité. □

Nous admettrons que, sur tout corps de caractéristique différente de 2 ou 3, les polynômes φ_N et ψ_N^2 sont premiers entre eux.

Corollaire 5.14. *Si k est un corps de caractéristique p avec $p \notin \{2, 3\}$ et si E est une courbe elliptique définie sur k. Alors $[N]$ est un morphisme séparable si et seulement si $p \nmid N$.*

Démonstration. On se ramène facilement au cas où N est un nombre premier. Le morphisme $[N]$ est séparable si et seulement si $\left(\frac{\varphi_N}{\psi_N^2}\right)' \neq 0$. On a

$$\left(\frac{\varphi_N}{\psi_N^2}\right)' = 0 \Leftrightarrow \varphi_N'\psi_N^2 = (\psi_N^2)'\varphi_N.$$

Comme φ_N et ψ_N^2 sont premiers entre eux, cette égalité est encore équivalente à $\psi_N' = \varphi_N' = 0$, ce qui implique que leur degré est un multiple de p. On conclut en remarquant que $\deg[N] = \max(\deg \varphi_N, \psi_N^2)$. □

5.4 Structure du sous-groupe des points de torsion

Théorème 5.15.

(i) Si $(n, car.k) = 1$, alors $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$.

(ii) Si $p = car.k \mid n$, alors $E[n] = \mathbb{Z}/n' \oplus \mathbb{Z}/n'$ ou $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n'$, où $n = p^r n'$ et $(n', p) = 1$.

Démonstration. (i) D'après les propositions 5.13 et 5.14, on a $E[n] = deg\,([n]) = n^2$. Le groupe $E[n]$ est un groupe abélien fini d'ordre n^2. D'après le théorème de structure, on a donc

$$E[n] = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2 \oplus \ldots \oplus \mathbb{Z}/n_s$$

avec $n_i | n_{i+1}, 1 \leqslant i \leqslant s-1$. Soit l un premier qui divise n_1. On a donc l^s divise l'ordre de $E[n]$. Or $\#E[l] = l^2$. On obtient $s = 2$ et

$$E[n] = \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2, n_1 | n_2.$$

Par ailleurs, ce groupe est annulé par n, d'où $n_2 | n$. Comme $\#E[n] = n^2 = n_1 n_2$, on déduit que $n_1 = n_2 = n$.

(ii) On va d'abord déterminer la structure du groupe $E[p^s]$ pour tout $s > 0$. Comme le morphisme de multiplication par p n'est pas séparable, $\#E[p] < p^2$. Tout élément de $E[p]$ est d'ordre 1 ou p, on a donc $\#E[p]$ est une puissance de p, et donc c'est 1 ou p. Si $\#E[p] = 1$, alors $\#E[p^s] = 1$ pour tout $s > 0$ (on utilise que si $Q \in E[p^s]$, alors $p^{s-1}Q \in E[p]$). Supposons $\#E[p] = p$. Soit $Q \in E[p^s]$. On a donc $pQ \in E[p^{s-1}]$. Par récurrence, $E[p^s]$ est cyclique d'ordre p^s.

Écrivons maintenant $n = p^r n'$. On a alors $E[n] = E[n'] \oplus E[p^r]$. Comme $E[n'] = \mathbb{Z}/n' \oplus \mathbb{Z}/n'$, $E[p^r] = 1$ ou $\mathbb{Z}/p^r$ et $\mathbb{Z}/n' \oplus \mathbb{Z}/p^r \simeq \mathbb{Z}/n'p^r = \mathbb{Z}/n$, on obtient la formule de l'énoncé. □

De façon analogue, on démontre le théorème de structure pour les points d'une courbe elliptique sur un corps fini :

Théorème 5.16. *Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. On a*

$$E(\mathbb{F}_q) = \mathbb{Z}/n \text{ ou } \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$$

où $n \geqslant 1$ et $n_1, n_2 \geqslant 1$ sont des entiers, avec $n_1 \mid n_2$.

5.5 L'accouplement de Weil

Soit k un corps parfait et soit E une courbe elliptique définie sur k.

Théorème 5.17. *Soit $N \geqslant 2$ un entier premier à la caractéristique de k. Il existe alors une application $e_N : E[N] \times E[N] \to \mu_N$ vérifiant les propriétés suivantes :*

- *l'application e_N est bilinéaire ;*
- *l'application e_N est alternée, ce qui signifie que $e_N(P, P) = 1$ pour tout $P \in E[N]$;*
- *l'application e_N est non dégénérée, c'est-à-dire que si $P \in E[N]$ et si $e_N(P, Q) = 1$ pour tout $Q \in E[N]$, alors $P = 0$;*
- *l'application e_N est compatible à l'action du groupe de Galois*

$$\forall \sigma \in \mathrm{Gal}(\overline{k}/k) \forall (P, Q) \in E[N]^2, \quad e_N(\sigma(P), \sigma(Q)) = \sigma(e_N(P, Q));$$

- *si $f \in \mathrm{End}\, E$, alors*

$$\forall (P, Q) \in E[N]^2, \quad e_N(f(P), f(Q)) = e_N(P, Q)^{\deg f}.$$

La preuve de ce résultat est reportée à l'exercice 5.3.

Corollaire 5.18. *Sous les hypothèses du théorème 5.17, soit (S, T) une base du $\mathbb{Z}/N\mathbb{Z}$-module $E[N]$. Alors $e_N(S, T)$ est une racine primitive N-ième de l'unité*

5.6 Exercices

Exercice 5.1. Soit k un corps algébriquement clos et E une courbe elliptique définie sur k. Soit $\alpha \in \operatorname{End} E$ un endomorphisme séparable.

a) Soit $P \in E \smallsetminus E[2]$. Montrer que la fonction rationnelle $X - x_P$ est une uniformisante de E en P.

b) Montrer que si $P \in E \smallsetminus f^{-1}(E[2])$, en déduire que $\operatorname{ord}_{f(P)}(f \circ \alpha) = \operatorname{ord}_P(f)$.

c) En déduire que pour tout $P \in E$, on a $\operatorname{ord}_{f(P)}(f \circ \alpha) = \operatorname{ord}_P(f)$.

Exercice 5.2. Soit k un corps algébriquement clos ainsi que E et E' deux courbes elliptiques définie sur k. Soit $\alpha \in \operatorname{Hom}(E, E')$.

a) Montrer qu'il existe $n \geqslant 0$ et $\beta \in \operatorname{Hom}(E^{(p^n)}, E')$ séparable tels que $\alpha = \beta \circ \phi_p^n$.

b) En déduire que si $P \in E$, et $f \in k(E')$, alors $\operatorname{ord}_P(f \circ \alpha) = p^n \operatorname{ord}_{f(P)}(f)$.

Exercice 5.3. Soit k un corps algébriquement et soit E une courbe elliptique définie sur k. Soit $N \in \mathbb{N}_{\geqslant 1}$ premier à la caractéristique de k.

a) Soit $T \in E[N]$ et soit $T' \in E$ tel que $[N](T') = T$. Montrer qu'il existe deux fonctions $f_T, g_T \in k(E)$ telles que

$$\operatorname{div}(f_T) = \sum_{P \in E[N]} (N[T] - N[0]), \quad \operatorname{div}(g_T) = \sum_{P \in E[N]} ([T' + P] - [P]).$$

b) Montrer qu'il existe $\lambda \in k^\times \smallsetminus \{0\}$ tel que $g_T^N = \lambda(f_T \circ [N])$.

c) En déduire que pour tout $S \in E[N]$, il existe un unique $e_N(S, T) \in \mu_N$ tel que

$$g_T(X + S) = e_N(S, T) g_T(X).$$

d) Montrer que l'application e_N est linéaire à gauche.

e) Si T_1 et T_2 sont deux points de $E[N]$, notons $h \in k(E)$ telle que $\operatorname{div}(h) = (T_1 + T_2) - (T_1) - (T_2) + (0)$. Montrer alors qu'il existe des éléments non nuls c et c' de k tels que

$$f_{T_1+T_2} = c f_{T_1} f_{T_2} h^N, \quad g_{T_1+T_2} = c' g_{T_1} g_{T_2} (h \circ [N]).$$

En déduire que e_N est linéaire à droite.

f) En considérant son diviseur, montrer que la fonction rationnelle $\prod_{i=0}^{N-1} f(X + [i]T)$ est constante. En déduire qu'il en est de même de la fonction $\prod_{i=0}^{N-1} g(X + [i]T')$.

g) Montrer que pour tout $T \in E[N]$, on a $e_N(T, T) = 1$.

h) Soient $\alpha \in \operatorname{End} E$ de degré premier à N, $T \in E[N]$ et $[N]T = T'$. Si g' vérifie

$$\operatorname{Div}(g') = \sum_{P \in E[N]} [\alpha(T') + P] - [P],$$

montrer que $g' \circ \alpha = g^{\deg \alpha}$.

i) En déduire que $e_N(\alpha(S), \alpha(T)) = e_N(S, T)^{\deg \alpha}$.

Chapitre 6

Courbes elliptiques sur les corps finis

6.1 Le théorème de Hasse

Soit k un corps fini. La caractéristique du corps k est un nombre premier p et le cardinal $|k|$ du corps k est une puissance de p. Réciproquement, si $q = p^f$ est une puissance d'un nombre premier p, il existe un unique, à isomorphisme près, corps fini de cardinal q. On note $\mathbb{F}_q$ ce corps.

L'application $\phi_p : x \mapsto x^p$ est un automorphisme du corps $\mathbb{F}_q$ appelé automorphisme de Frobenius. Plus généralement, on définit $\phi_{p^f} \coloneqq \phi_p^f$. On rappelle la proposition suivante, issue du cours de théorie de Galois.

Proposition 6.1. *Si $\mathbb{F}_q \subset \mathbb{F}_{q'}$, alors il existe $n \geqslant 1$ tel que $q' = q^n$, l'extension $\mathbb{F}_{q'}/\mathbb{F}_q$ est galoisienne et le groupe $\mathrm{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q)$ est cyclique engendré par ϕ_q.*

Proposition 6.2. *Si k est un corps fini, le groupe $k^\times$ est un groupe cyclique.*

Considérons à présent E une courbe elliptique définie par une équation de Weierstrass $Y^2 = X^3 + aX + b$ où a et b sont des éléments d'un corps fini $\mathbb{F}_q$. Si $x \in \mathbb{F}_q$, il y a au plus deux éléments $y \in \mathbb{F}_q$ tels que $y^2 = x^3 + ax + b$, on obtient donc une estimation grossière du cardinal du groupe fini $E(\mathbb{F}_q)$:

$$|E(\mathbb{F}_q)| \leqslant 2q + 1$$

En réalité on peut faire beaucoup mieux. Le théorème suivant est dû à Helmut Hasse.

Théorème 6.3 (Hasse)**.** *Soit E une courbe elliptique définie sur $\mathbb{F}_q$, alors*

$$||E(\mathbb{F}_q)| - (q+1)| \leqslant 2\sqrt{q}$$

Proposition 6.4. *Il existe un polynôme unitaire de degré 2 annulant ϕ_q.*

6.2 Le degré vu comme forme quadratique

Si E est une courbe elliptique définie sur un corps algébriquement clos, on note $\operatorname{End} E$ l'anneau de ses endomorphismes.

La preuve du théorème de Hasse dans le cas général repose sur le résultat suivant.

Proposition 6.5. *L'application* deg *de* $\operatorname{End} E$ *vers* $\mathbb{N}$ *est une forme quadratique. Autrement dit, pour tout* $(\alpha, \beta) \in (\operatorname{End} E)^2$ *et* $(r, s) \in \mathbb{Z}^2$*, on a*

$$\deg(r\alpha + s\beta) = r^2 \deg \alpha + s^2 \deg \beta + rs(\deg(\alpha + \beta) - \deg \alpha - \deg \beta)$$

Plusieurs preuves de ce résultat existent. Nous choisissons ici de présenter la preuve basée sur l'existence de l'accouplement de Weil.

Proposition 6.6. *Soit* k *un corps parfait et soit* ℓ *un nombre premier différent de la caractéristique de* k*. Soit* E *une courbe elliptique définie sur* k*. Si* $f \in \operatorname{End} E$*, notons* $\det_\ell f$ *déterminant de l'endomorphisme* $\mathbb{F}_\ell$*-linéaire de* $E[\ell]$ *induit par* f*. On a alors*

$$\deg f \equiv \det_\ell f \mod \ell.$$

Démonstration. Soit (e_1, e_2) une base du $\mathbb{F}_\ell$-espace vectoriel $E[\ell]$. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice, dans la base (e_1, e_2), de l'endomorphisme de $E[\ell]$ induit par f. En utilisant le caractère alterné de l'accouplement e_ℓ, on obtient

$$e_\ell(f(e_1), f(e_2)) = e_\ell(ae_1 + ce_2, be_1 + de_2) = e_\ell(e_1, e_2)^{ad-bc}.$$

Par ailleurs, on a aussi

$$e_\ell(f(e_1), f(e_2)) = e_\ell(e_1, e_2)^{\deg f}.$$

Comme e_ℓ est non dégénérée, l'élément $e_\ell(e_1, e_2)$ est une racine primitive ℓ-ième de l'unité. On en conclut que

$$\deg f \equiv ad - bc = \det_\ell f \mod \ell. \qquad \square$$

Démonstration de la proposition 6.5. Soit ℓ un nombre premier. Si M_1 et M_2 sont deux éléments de $\mathcal{M}_2(\mathbb{F}_\ell)$, l'espace des matrices de taille 2×2 à coefficients dans $\mathbb{F}_\ell$, on a

$$\det(rM_1 + sM_2) = r^2 \det(M_1) + s^2 \det(M_2) + rs(\det(M_1 + M_2) - \det(M_1) - \det(M_2)),$$

en remarquant par exemple que l'application $(M_1, M_2) \mapsto \det(M_1 + M_2) - \det(M_1) - \det(M_2)$ est une forme bilinéaire (symétrique). On en conclut que, pour f_1 et f_2 dans $\operatorname{End} E$, on a

$$\deg(rf_1 + sf_2) \equiv r^2 \deg(f_1) + s^2 \deg(f_2) + rs(\deg(f_1 + f_2) - \deg(f_1) - \deg(f_2)) \mod \ell$$

pour tout nombre premier ℓ différent de la caractéristique de k. Comme deux nombres entiers congrus modulo une infinité de nombres premiers sont nécessairement égaux, on obtient l'égalité recherchée. $\square$

6.3 Démonstration du théorème de Hasse

Soit q une puissance d'un nombre premier p et soit E une courbe elliptique définie sur $\mathbb{F}_q$. On rappelle que ϕ_q désigne l'endomorphisme de E défini par $(x, y) \mapsto (x^q, y^q)$. Il s'agit d'un endomorphisme inséparable de degré q.

Lemme 6.7. *L'endomorphisme $\phi_q - 1$ est séparable.*

Démonstration. La formule d'addition nous montre que l'endomorphisme $\phi_q - 1$ est donné par la formule

$$(x, y) \longmapsto \left((x^3 + ax + b) \left(\frac{(x^3 + ax + b)^{\frac{q-1}{2}} - 1}{x^q - x} \right)^2 - (x^q + x), \cdots \right).$$

Supposons par l'absurde que $\phi_q - 1$ n'est pas séparable. Mettons la coordonnée en X de $\phi_q - 1$ sous forme irréductible

$$(X^3 + aX + b) \left(\frac{(X^3 + aX + b)^{\frac{q-1}{2}} - 1}{X^q - X} \right)^2 - (X^q + X) = \frac{P(X)}{Q(X)}$$

avec P et Q deux polynômes premiers entre eux. On a alors $P'Q - PQ' = 0$, donc $P \mid P'$ et $Q \mid Q'$, ce qui implique, pour des raisons de degré, que $P' = Q' = 0$. On en conclut que Q est de la forme $Q_1(X^p)$. Comme par ailleurs $Q \mid (X^q - X)^2$ et que $p > 2$, on en conclut que $Q(X) = 1$ et donc la relation

$$(X^q - X)^2 \mid (X^3 + aX + b)((X^3 + aX + b)^{\frac{q-1}{2}} - 1)^2.$$

Rappelons que le polynôme $X^q - X$ est à racines simples. Supposons dans un premier temps que le polynôme $X^3 + aX + b$ est scindé sur $\mathbb{F}_q$. Dans ce cas, ce dernier polynôme divise $X^q - X$. Par ailleurs les deux polynômes $X^3 + aX + b$ et $((X^3 + aX + b)^{\frac{q-1}{2}} - 1)$ sont premiers entre eux, on en conclut que $(X^q - X)^2$ divise $X^3 + aX + b$, ce qui contredit le fait que ce dernier est à racines simples. On en conclut que $\phi_q - 1$ est séparable si $X^3 + aX + b$ est scindé dans $\mathbb{F}_q$.

Dans le cas général, on peut trouver une extension $\mathbb{F}_{q'}$ de $\mathbb{F}_q$ dans laquelle $X^3 + aX + b$ est scindé. On en conclut que l'endomorphisme $\phi_{q'} - 1$ est séparable. Posons $q' = q^f$ (en fait on peut choisir $f = 2$ ou $f = 3$). La factorisation

$$\phi_{q'} - 1 = (\phi_q^{f-1} + \phi_q^{f-2} + \cdots + \phi_q + 1) \circ (\phi_q - 1)$$

implique que $\phi_q - 1$ est séparable. □

Démonstration du théorème 6.3. Comme le morphisme $\phi_q - 1$ est séparable, on a

$$|E(\mathbb{F}_q)| = |\mathrm{Ker}(\phi_q - 1)| = \deg(\phi_q - 1).$$

Par ailleurs, pour tout $(r,s) \in \mathbb{Z}^2$, on a

$$0 \leqslant \deg(r\phi_q + s) = r^2 \deg(\phi_q) + s^2 + rs(\deg(\phi_q - 1) - \deg\phi_q - 1) = \\ = qr^2 + s^2 + rs(\deg(\phi_q - 1) - q - 1).$$

Posons $a_q \coloneqq \deg(\phi_q - 1) - (q+1)$. On en déduit que pour tout rationnel $\frac{r}{s}$, on a

$$q\frac{r}{s}^2 + a_q\frac{r}{s} + 1 \geqslant 0.$$

On obtient un polynôme de degré 2 prenant des valeurs positives en tous les nombres rationnels, on en déduit que son discriminant est négatif, c'est-à-dire $a_q^2 \leqslant 4q$, ce qui nous donne exactement l'inégalité recherchée. □

6.4 La fonction zêta

Soit E une courbe elliptique définie sur $\mathbb{F}_q$ et posons $a_q \coloneqq (q+1) - |E(\mathbb{F}_q)|$. Le résultat suivant est démontré dans l'exercice 6.6.

Proposition 6.8. *Dans l'anneau* $\operatorname{End} E$*, on a l'égalité*

$$\phi_q^2 - [a_q]\phi_q + [q] = 0.$$

Cette proposition nous apprend que l'élément ϕ_q est un entier quadratique dans l'anneau intègre $\operatorname{End} E$. Le théorème de Hasse affirme alors que le corps des fractions de l'anneau $\mathbb{Z}[\phi_q]$ est soit $\mathbb{Q}$, soit un corps quadratique imaginaire. En d'autres termes, si α et β désignent les racines dans $\overline{\mathbb{Q}}$ du polynôme $X^2 - a_qX + q$, α et β sont des nombres complexes conjugués et

$$|\alpha| = |\beta| = \sqrt{q}.$$

On déduit alors de la proposition 6.8 (voir exercice 6.6) le résultat suivant nous permettant de calculer $|E(\mathbb{F}_{q^n})|$ pour tout $n \geqslant 1$.

Corollaire 6.9. *Pour tout* $n \geqslant 1$*, on a*

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - (\alpha^n + \beta^n).$$

Définition 6.10. *Soit* X *une variété algébrique projective définie sur* $\mathbb{F}_q$*. On définit la* fonction zêta *de* X *comme la série formelle*

$$Z(X/\mathbb{F}_q, T) \coloneqq \exp\left(\sum_{n\geqslant 1} \frac{|X(\mathbb{F}_{q^n})|}{n} T^n\right) \in \mathbb{Q}[[T]].$$

Si $X = \mathbb{P}^1_{\mathbb{F}_q}$, alors $|X(\mathbb{F}_{q^n})| = q^n + 1$, on en déduit

$$Z(\mathbb{P}^1/\mathbb{F}_q, T) = \exp\left(\sum_{n\geqslant 1}\frac{T^n}{n} + \sum_{n\geqslant 1}\frac{q^n}{n}T^n\right)$$
$$= \exp\left(-\log(1+T) - \log(1+qT)\right) = \frac{1}{(1-T)(1-T^q)}.$$

Le corollaire 6.9 nous permet de calculer la fonction zêta d'une courbe elliptique E. On a

$$Z(E/\mathbb{F}_q, T) = \frac{1 - a_q T + qT^2}{(1-T)(1-qT)}.$$

Plus généralement, André Weil a démontré que si C est une courbe projective lisse définie sur $\mathbb{F}_q$, alors

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1-T)(1-qT)}$$

où $P(T) \in \mathbb{F}_q[T]$ est un polynôme de degré pair dont les racines sont des nombres complexes de norme $\sqrt{q}$. De plus cette fonction vérifie l'équation fonctionnelle

$$Z\left(C/\mathbb{F}_q, \frac{1}{qT}\right) = qT^2 Z(C/\mathbb{F}_q, T).$$

Ces résultats ont par la suite été généralisés par Pierre Deligne (1974) à toutes les variétés projectives lisses définies sur les corps finis.

Remarque 6.11. Le nom « fonction zêta » donné à ces séries provient de la remarque suivante. Considérons le produit suivant, où $s \in \mathbb{C}$, portant sur tous les nombres premiers

$$\prod_p Z(\mathbb{P}^1/\mathbb{F}_p, p^{-s}) = \prod_p \frac{1}{1-p^{-s}} \prod_p \frac{1}{1-p^{-s+1}} = \zeta(s)\zeta(s-1).$$

On retrouve alors une expression dépendant de la fonction zêta de Riemann.

6.5 Factorisation

Si N est un entier, un problème important consiste à étudier les algorithmes permettant de déterminer les facteurs premiers de N. La sécurité des cryptosystèmes modernes dépend en particulier du fait que ce problème est très difficile à résoudre en pratique. Dans cette partie on présente une approche qui utilise les courbes elliptiques : l'algorithme **ECM** (« Elliptic Curve Method »), introduit par H. Lenstra dans les années 1980 et développé par R. Brent, P. Montgomery et autres. Cet algorithme est à nos jours le plus efficace en termes de la taille des facteurs de N trouvés (et non pas de N) : sa complexité est en $exp(c\sqrt{log\, p(loglog\, p)})$, où p est le plus petit facteur de N. Un des derniers facteurs trouvés [1] est de 74 chiffres : c'est le facteur suivant de $12^{284}+1$ trouvé le 26 octobre 2014 par B. Dodson :

$$267211945319738489547677723511141522030835772068139431494848756286233094 73$$

1. au moment de l'écriture de ce cours...

6.5.1 Algorithme $p-1$ de Pollard

Pour commencer, on rappelle l'algorihme $(p-1)$ de Pollard, dont les idées sont aussi utilisées dans l'algorithme ECM. Supposons que N possède un facteur premier p tel que

$$p-1 = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}.$$

Si les facteurs q_i vérifient

$$q_i \leqslant B, 1 \leqslant i \leqslant r$$

on dit que $p-1$ est B**-lisse**. L'algorithme suivant permet de trouver un facteur p si $p-1$ est B-lisse.

1. On prend $2 \leqslant a < N$ et on pose $x = a$.
2. Pour $i = 1, 2, \dots s$:

(a) $x \to x^i \bmod N$ (notons qu'ici on calcule $a^{i!} \bmod N$)

(b) $d := (x-1, N)$

(c) si $1 < d < N$, on a trouvé un facteur d de N

3. retour à la première étape.

Soit $s = max\, e_j q_j$. Alors $q_j^{e_j}$ divise $s!$, i.e. $(p-1)|s!$. On a donc $a^{s!} \equiv 1 \bmod p$. Il est peu probable que $a^{s!} \equiv 1 \bmod N$ et on espère donc trouver un facteur de N.

6.5.2 Algorithme ECM

Courbes elliptiques modulo N

Soit E une courbe elliptique donnée par une équation homogène $Y^2Z = X^3 + aXZ^2 + bZ^3$ où les coefficients $a, b \in \mathbb{Z}/N$ et le derminant $\Delta(E)$ sont inversibles. On définit

$$E(\mathbb{Z}/N) = \{(X:Y:Z), X, Y, Z \in \mathbb{Z}/N, pgcd(N, X, Y, Z) = 1, \\ Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

Si N était premier, on pourrait toujours trouver la somme $P+Q$ pour tous deux points $P, Q \in E(\mathbb{Z}/N)$ par les formules de la loi explicite (Proposition 3.1). Dans ces formules on est amenés à inverser $x_P - x_Q$. Si cela n'est pas possible, et si $x_P \neq x_Q$, on a nécessairement que $(x_P - x_Q, N) > 1$ et on trouve donc un facteur de N. On obtient donc l'algorithme suivant. Pour l'efficacité l'on utilise souvent plusieurs courbes à la fois.

L'algorithme

1. On fixe un entier m (souvent $10 < m < 20$) et un entier B (par exemple, d'ordre 10^8).

2. On choisit m courbes elliptiques aléatoires E_i modulo N :

$$E_i : Y^2Z = X^3 + a_iXZ^2 + b_iZ^3$$

et un point $P_i \in E_i$. Pour ce faire, on choisit de façon aléatoire a_i, $P_i = (x_{i,0}, y_{i,0})$ et on pose $b_i = y_{i,0}^2 - x_{i,0}^3 - ax_{i,0}$.

3. Pour tout i on calcule successivement $(B!)P_i$ sur E_i. Si une des opérations d'inversion est impossible, on trouve un facteur de N.

4. Sinon, on change B ou les courbes E_i et on revient à la première étape.

L'opération d'inversion échoue si $B!P_i = O$ dans $E_i(\mathbb{F}_p)$ où p est un facteur de N. C'est le cas si l'ordre $\#E_i(\mathbb{F}_p)$ divise $B!$. Or $\#E_i(\mathbb{F}_p)$ varie dans l'intervalle $]p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}[$, alors que, par exemple, dans la méthode de Pollard, l'ordre $p - 1$ est fixé. On s'attend donc à ce que l'algorithme soit plus efficace.

6.6 L'algorithme de Schoof

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. D'après le théorème de Hasse 6.3, le nombre $\#E(\mathbb{F}_q)$ satisfait une inégalité

$$|\#E(\mathbb{F}_q) - q - 1| \leqslant 2\sqrt{q}.$$

Dans cette section on va décrire un algorithme, du à Schoof, qui permet de calculer $\#E(\mathbb{F}_q)$ en temps $O((log\, q)^c)$, pour c une constante convenable. Soit

$$a_q = q + 1 - \#E(\mathbb{F}_q).$$

Pour déterminer a_q on va déterminer a_q modulo ℓ pour beaucoup de nombres premiers ℓ.

On prend donc ℓ un premier. Soit $P \in E(\overline{\mathbb{F}}_q)[\ell]$. D'après le théorème 6.8, on a

$$a_q\phi_q(P) = \phi_q^2(P) + qP,$$

où ϕ_q est le morphisme de Frobenius. Par ailleurs, comme $\ell P = O_E$, on a

$$[a_q]_\ell\, \phi_q(P) = \phi_q^2(P) + [q]_\ell P, \tag{6.1}$$

où $[a_q]_\ell$ et $[q]_\ell$ sont des restes modulo ℓ. De plus, l'égalité 6.1 détermine $[a_q]_\ell$ de facon unique.

D'après la proposition 5.13, on a $P \in E(\overline{\mathbb{F}}_q)[\ell] \Leftrightarrow \psi_\ell(P) = O_E$ pour un polynôme ψ_ℓ défini de façon récursive. Ce polynôme est de degré $\frac{\ell^2-1}{2}$. Pour trouver des multiples de P, on peut donc travailler dans l'anneau

$$R_\ell = \mathbb{F}_q[x, y]/(\psi_l(x), y^2 - x^3 - ax - b)$$

de telle sorte qu'on n'a jamais de puissances de y^r pour $r > 1$ et de x^r pour $r > \frac{\ell^2-3}{2}$.

On peut maintenant décrire l'algorithme de Schoof.

L'algorithme

1. Soient $A = 1$, $\ell = 3$.
2. si $A < 4\sqrt{q}$:

(a) pour $n = 0, \dots \ell - 1$ on vérifie l'égalité (dans l'anneau R_ℓ) :

$$(x^{q^2}, y^{q^2}) + [q]_\ell(x, y) = n(x^q, y^q)$$

Si l'égalité est vérifiée, on sauvegarde $n_\ell = n$ et l'on passe à l'étape suivante.

(b) On change $A \to \ell A$, et on change ℓ par un nombre premier suivant.

3. On trouve a_q comme unique entier $|a_q| \leqslant 2q$ tel que $a_q \equiv n_\ell$ pour tout ℓ.

Remarque 6.12. À la dernière étape de l'algorithme on utilise le théorème des restes chinois pour trouver a avec les conditions $a_q \equiv n_\ell$. Puisque $A = \prod \ell > 4\sqrt{q}$ et $a_q \in]-2q, +2q[$ par le théorème de Hasse, un tel entier est unique.

6.7 Primalité

Les algorithmes à la base des courbes elliptiques sont utilisés pour tester (et prouver) la primalité de très grands entiers (plus que 20000 chiffres), qui ont déjà passés d'autres tests de primalité. Un des records les plus récents est le nombre

$$(2^{83339} + 1)/3$$

qui est donc premier et qui a 25088 chiffres. Cet algorithme marche en temps d'ordre $O((log\, N)^4)$.

On va présenter ici le test de primalité de Goldwasser-Kilian. On y utilise les deux énoncés qui suivent.

Proposition 6.13. *Soit N un entier premier à 6 et soit E une courbe à coefficients dans $\mathbb{Z}/N$. Supposons qu'il existe*

(i) un entier m et un premier q, $q|m$ et $q > (\sqrt[4]{N} + 1)^2$;

(ii) un point $P \in E(\mathbb{Z}/N)$ tel que $mP = O_E$ et $(m/q)P = (x : y : z)$ avec z inversible dans $\mathbb{Z}/N$.

Alors N est premier.

Démonstration. Supposons que N n'est pas premier : on a donc un facteur premier l de N tel que $l \leqslant \sqrt{N}$. On note $\bar{E}$ la courbe obtenue en réduisant les coefficients a, b de E modulo l. La réduction modulo l du point P donne un point $\bar{P}$ de $\bar{E}$ d'ordre divisible par q (par la condition (ii)). On a donc $q \leqslant \#\bar{E}(\mathbb{F}_l) \leqslant (\sqrt{l} + 1)^2$ par le théorème de Hasse. Or $l \leqslant \sqrt{N}$. On obtient donc une contradiction avec la condition (i). □

Proposition 6.14. *Soit N un nombre premier, $(N,6)=1$ et soit E une courbe elliptique donnée par une équation homogène $Y^2Z = X^3+aXZ^2+bZ^3$ où les coefficients $a, b \in \mathbb{Z}/N$ et le déterminant $\Delta(E)$ sont inversibles. Soit $m = \#E(\mathbb{Z}/N)$. Supposons qu'il existe un nombre premier q tel que $q|m$ et $q > (\sqrt[4]{N}+1)^2$. Alors il existe un point $P \in E(\mathbb{Z}/N)$ tel que $mP = O_E$ et $(m/q)P = (x:y:z)$ avec z inversible dans $\mathbb{Z}/N$.*

Démonstration. Supposons que pour tout point P de $E(\mathbb{Z}/N)$ on a $(m/q)P = O_E$. Ainsi l'ordre de $E(\mathbb{Z}/N)$ divise m/q. D'après le théorème 5.16 on a $E(\mathbb{Z}/N) = \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2, d_1|d_2$, d'où $d_2|(m/q)$. Comme $m \leqslant d_2^2$, on obient $m \leqslant (m/q)^2$. Or $m \leqslant (\sqrt{N}+1)^2$ par le théorème de Hasse, on obtient une contradiction avec l'hypothèse sur q. □

Comme conséquence des deux propriétés ci-dessus, on obtient donc que si l'on trouve une courbe elliptique E telle que l'ordre m de $E(\mathbb{Z}/N)$ admet un grand facteur premier q (i.e. $q > (\sqrt[4]{N}+1)^2$), alors N est premier si et seulement s'il existe un point $P \in E(\mathbb{Z}/N)$ tel que $mP = O_E$ et $(m/q)P = (x:y:z)$ avec z inversible dans $\mathbb{Z}/N$. Pour une courbe elliptique donnée, on peut utiliser l'algorithme de Schoof pour déterminer son ordre m. Ensuite, pour tester si q est premier, on réitère encore la même procédure. On obtient donc l'algorithme suivant.

L'algorithme

1. On choisit une courbe elliptique E et on calcule $m = \#E(\mathbb{Z}/N)$.

2. On divise m par des petits nombres premiers dont on note m_0 le produit et on cherche $q = m/m_0$ qui vérifie $q > (\sqrt[4]{N}+1)^2$ et qui passe des tests classiques de primalité. Si cela n'est pas achevé, on revient à la première étape.

3. On choisit $x \in \mathbb{Z}/N$ tel que x^3+ax+b est un carré dans $\mathbb{Z}/N$. On obtient donc un point P de la courbe E. On vérifie si $mP = 0_E$ et $(m/q)P = (x:y:z)$ avec z inversible dans $\mathbb{Z}/N$. Si c'est le cas, on sait que N est premier si q est premier. On revient donc à la première étape avec q à la place de N. Sinon, on change le point P et l'on continue.

6.8 Cryptographie avec les courbes elliptiques

On considère généralement le contexte suivant pour les systèmes cryptographiques à clé publique : deux personnes, Alice et Bob veulent s'échanger des messages de façon sécurisée. Eva veut lire leurs messages, elle a l'accès au canal public de la transmission des messages d'Alice et Bob. Dans ce système, on distingue trois algorithmes de base : l'échange de clés, le chiffrement et la signature numérique. Dans la procédure d'échange de clés, Alice et Bob produisent une clé commune (qui n'est connue que par eux), pour utiliser cette clé dans la suite. La procédure de la signature numérique permet à Bob de s'assurer que le message qu'il reçoit est bien envoyé par Alice. Les schémas que l'on décrit ci-dessous peuvent aussi être utilisés dans n'importe quel groupe. On décrit ensuite des aspects spécifiques aux courbes elliptiques.

6.8.1 L'échange de clés : schéma Diffie-Hellman

1. Données publiques : E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et un point $P \in E(\mathbb{F}_q)$ d'ordre suffisamment grand.

2. Choix secret d'Alice : un entier a.

3. Choix secret de Bob : un entier b.

4. Alice envoie $P_a = aP$ à Bob.

5. Bob calcule $P_b = bP$ et l'envoie à Alice ;

6. Alice calcule $aP_b = abP$ et Bob calcule $bP_a = abP$. La clé commune est une certaine fonction du même point abP.

Définition 6.15. *On appelle* **problème de Diffie-Hellman** *le problème suivant :*

étant donné P, aP et bP dans $E(\mathbb{F}_q)$, trouver abP.

La difficulté à résoudre ce problème pour une courbe elliptique E garantit la sécurité du schéma Diffie-Hellman.

6.8.2 Cryptosystème ElGamal

Pour recevoir un message d'Alice, Bob choisit une courbe elliptique E sur un corps fini $\mathbb{F}_q$ et point $P \in E$. Il choisit aussi un entier secret s et il calcule $B = sP$. Les données publiques sont les suivantes

$$E, P, B.$$

La clé secrète de Bob est l'entier s.

Pour coder un message, Alice utilise l'algorithme suivant :

1. Elle représente son message comme un point $M \in E(\mathbb{F}_q)$.

2. Elle choisit un entier secret k au hasard et calcule $M_1 = kP$, $M_2 = M + kB$.

3. Alice envoie les points M_1, M_2 à Bob.

Pour retrouver le message d'Alice, Bob calcule

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

6.8.3 Signature numérique

Le principe de la signature numérique est l'inverse de celui de codage : tout le monde peut vérifier si la signature est correcte, mais seulement Alice peut signer un document. On présente ici l'algorithme que l'on utilise dans le standard ECDSA.

Pour signer son document, Alice choisit une courbe elliptique E sur un corps fini $\mathbb{F}_q$, telle que $\#E(\mathbb{F}_q) = fr$, où r est un grand premier et où f est un entier, généralement

$f = 1, 2$ ou 4. Elle choisit un point $P \in E$ d'ordre r. Elle choisit aussi un entier secret s et calcule $Q = sP$. Les informations suivantes

$$E, r, P, Q$$

sont visibles par tous.

Pour signer son message m (qu'on voit comme un entier cette fois-ci), Alice choisit un entier k au hasard et calcule $R = kP = (x, y)$ et $z = k^{-1}(m + sx) \bmod r$. Ensuite Alice signe le document

$$m, R, z.$$

Pour vérifier la signature, Bob utilise la procédure suivante.

1. Il calcule $u_1 = z^{-1}m \bmod r$ et $u_2 = z^{-1}x \bmod r$.
2. Il calcule $V = u_1P + u_2Q$.
3. Il décide que la signature est correcte si $V = R$.

On laisse en exercice la vérification qu'on doit effectivement avoir que $V = R$ si le document est bien signé par Alice.

6.9 Logarithme discret

Définition 6.16. *Soit G un groupe. Dans le problème du* **logarithme discret** *dans G on demande de trouver, pour $x, y \in G$ un entier m tel que $x^m = y$ (si un tel entier existe).*

La difficulté à résoudre ce problème dans le cas où $G = E(\mathbb{F}_q)$ est à la base de la sécurité des algorithmes ci-dessus. En général, pour G un groupe d'odre n, les algorithmes actuels pour résoudre ce problème marchent en temps $O(\sqrt{N})$ (ce qui est beaucoup !). On discute ici brièvement deux algorithmes généraux pour le problème du logarithme discret, ainsi qu'un algorithme, dû à Menezes, Okamoto et Vanstone, qui s'applique à certaines courbes elliptiques et utilise l'accouplement de Weil.

6.9.1 Babystep-Giantstep

Soit G un groupe, $x, y \in G$ et soit n l'ordre de x. Soit N un entier $N = \lceil \sqrt{n} \rceil$.

L'algorithme

1. on sauvegarde la liste suivante d'éléments de G : $x, x^2, x^3, \ldots x^N$;
2. on pose $z = (x^N)^{-1}$ et on sauvegarde $yz, yz^2, yz^3, \ldots yz^N$.
3. on cherche des coïncidences dans ces deux listes : si $x^i = yz^j$, on a trouvé $y = x^{i+jN}$.

Le problème de cet algorithme est qu'on a besoin de suvegarder les deux listes. La méthode de Pollard permet de résoudre ce problème.

6.9.2 ρ-méthode de Pollard

Soient G un groupe, $x, y \in G$ et soit n l'ordre de x. On cherche m tel que $x^m = y$. Pour ce faire, on va trouver des entiers i, j, i_1, j_1 tels que

$$x^i y^j = x^{i_1} y^{j_1}. \tag{6.2}$$

On aura donc $x^{i-i_1} = y^{j_1-j}$, ce qui permet de trouver m si $j - j_1$ est premier à l'ordre de x dans G (ce que l'on peut toujours supposer quitte à se restreindre à x d'ordre premier).

Soit $G = A \cup B \cup C$ l'union disjointe, où A, B, C sont de même cardinal (à quelques éléments près). On pose $f : G \to G$ la fonction

$$f(z) = \begin{cases} xz & z \in A \\ z^2 & z \in B \\ yz & z \in C. \end{cases}$$

Soit $x_0 = x \in G$. Pour tout $i > 1$ on définit $x_i = f(x_{i-1})$. Soit t le plus grand entier tel que x_{t-1} n'apparait qu'une fois dans la suite $(x_i)_{i \geqslant 0}$ et soit l le plus petit entier tel que $x_{t+l} = x_t$. Alors, on peut montrer que $t+l$ est d'ordre $O(\sqrt{n})$ et qu'il existe $1 \leqslant i < t+l$ tel que $x_{2i} = x_i$, ce qui permet de trouver la collision 6.2.

6.9.3 L'attaque MOV

Dans l'algorithme de Menezes, Okamoto et Vanstone on réduit le problème de logarithme discret dans $E(\mathbb{F}_q)$ à un problème de logarithme discret dans le groupe $\mathbb{F}_{q^d}$ pour certain d.

Définition 6.17. *Soit m un entier. Le* **degré de plongement** *de m dans un corps fini $\mathbb{F}_q$ est le plus petit entier d tel que*

$$q^d \equiv 1 (\ mod\ m).$$

Remarque 6.18. La condition ci-dessus est équivalente à la condition $\mu_m \subset \mathbb{F}_{q^d}$.

Lemme 6.19. *Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et soit $m \geqslant 1$ un entier premier à q et à $q-1$. Soit d le degré de plongement de m dans $\mathbb{F}_q$. Si $E(\mathbb{F}_q)$ contient un point d'ordre exact m, alors $E[m] \subset E(\mathbb{F}_{q^d})$.*

Démonstration. Soit P le point d'ordre exact m et soit $T \in E(\overline{\mathbb{F}}_q)[m]$ tel que $\{P, T\}$ est une base de $E(\overline{\mathbb{F}}_q)[m] = \mathbb{Z}/m \oplus \mathbb{Z}/m$. Soit ϕ_q l'endomorphisme de Frobenius. On a

$$\phi_q(P) = P, \phi_q(T) = uP + vT, u, v \in \mathbb{Z}/m.$$

D'après les propriétés de l'accouplement de Weil

$$e_m(P,T)^q = e_m(\phi_q(P), \phi_q(T)) = e_m(P,P)^u e_m(P,T)^v = e_m(P,T)^v.$$

Puisque $e_m(P,T)$ est une racine ℓ-ième primitive de l'unité (corollaire 5.18), on en déduit que $v \equiv q \pmod m$, i.e.

$$\phi_q(T) = uP + qT.$$

On en déduit

$$\phi_{q^d}(T) = u(1+q+q^2+\ldots+q^{d-1})P + q^dT.$$

Par définition de d, on a $q^d \equiv 1 \pmod m$, d'où $q^dT = T$ et $(1+q+q^2+\ldots+q^{d-1})P = O_E$. On a donc $\phi_{q^d}(T) = T$, d'où $T \in E(\mathbb{F}_{q^d})$. □

L'algorithme

Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et soit m un entier, $(m,q) = 1$. Soient P, Q deux points d'ordre m et soit d le degré de plongement de m dans $\mathbb{F}_q$.

1. On prend $T \in E(\overline{\mathbb{F}}_q)[m]$ tel que P, T engendrent $E[m]$. D'après le lemme ci-dessus, $T \in E(\mathbb{F}_{q^d})$.

2. D'après la proposition 5.18, $e_m(P,T)$ est une racine m-ième primitive de l'unité. D'après la définition de d, on a $e_m(P,T) \in \mathbb{F}_{q^d}$. On dispose des algorithmes pour calculer l'accouplement de Weil (dans $E(\mathbb{F}_{q^d})$) : on trouve alors $e_m(Q,T)$. Puisque $e_m(P,T)$ est une racine n-ième primitive de l'unité, on a que

$$Q = rP \Leftrightarrow e_m(Q,T) = e_m(P,T)^r.$$

On trouve donc le problème de logarithme discret dans $\mathbb{F}_{q^d}$.

6.9.4 Courbes supersingulières

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique $p \geqslant 5$. Rappelons (cf. théorème 5.15) que le groupe $E(\bar{\mathbb{F}}_p)[p]$ est soit réduit à un point O_E, soit $E(\bar{\mathbb{F}}_p)[p] \simeq \mathbb{Z}/p$.

Définition 6.20. *On dit que E est* **supersingulière** *si $E(\bar{\mathbb{F}}_p)[p] = \{O_E\}$.*

Proposition 6.21. *Soit $a = q+1-\#E(\mathbb{F}_q)$. Les assertions suivantes sont équivalentes :*

(i) E est supersingulière ;

(ii) $a \equiv 0 \ (mod\ p)$;

(iii) $\#E(\mathbb{F}_q) \equiv 1 \ (mod\ p)$.

Démonstration. Soient α, β les racines du polynôme $x^2 - ax + q = 0$. Soit $s_n = \alpha^n + \beta^n$. On a $s_0 = 2, s_1 = a$ et on vérifie par récurrence :

$$s_{n+1} = as_n - qs_{n-1}.$$

D'après la définition de a, on a $(ii) \Leftrightarrow (iii)$.

Supposons (ii). On a alors $s_n \equiv 0 \pmod p$, d'où $\#E(\mathbb{F}_{q^n}) \equiv 1 \pmod p$ pour tout n (cf. théorème 6.8). On n'a donc pas de point d'ordre p dans le groupe $E(\mathbb{F}_{q^n})$, d'où (i).

Supposons que E est supersingulière. Supposons que $a \neq 0 \pmod p$. On a donc $s_{n+1} \equiv as_n \pmod p$ et

$$\#E(\mathbb{F}_q) = q^n + 1 - s_n \equiv 1 - a^n \pmod p.$$

Ainsi, pour $n = p - 1$ on obtient que $p|\#E(\mathbb{F}_q)$ et donc E n'est pas supersingulière. Contradiction. □

Corollaire 6.22. *Une courbe elliptique E sur $\mathbb{F}_p$ est supersingulière si et seulement si $\#E(\mathbb{F}_p) = p + 1$.*

Démonstration. D'après le théorème de Hasse, $|a| \leqslant 2\sqrt{p}$. Dans la proposition précédente on a donc $a = 0 \Leftrightarrow a \equiv 0 \pmod p \Leftrightarrow \#E(\mathbb{F}_p) = p + 1$. □

De point de vue algorithmique, les opérations artihmétiques sur les courbes supersingulières se calculent très facilement. Supposons $a = 0$. On a alors pour tout $P = (x, y) \in E(\bar{\mathbb{F}}_p)$:

$$q(x, y) = -\phi_q(x, y) = (x^{q^2}, -y^{q^2}).$$

Soit m un entier. Pour calculer mP, on procède comme suit :

1. on décompose $m = m_0 + m_1 q + m_2 q^2 + \ldots + m_r q^r$ avec $0 \leqslant m_i < q$;

2. on calcule $m_i P = (x_i, y_i)$, puis $q^i m_i P = (x_i^{q^{2i}}, (-1)^i y_i^{q^{2i}})$, en enfin on calcule la somme de tous ces points.

Par ailleurs, comme le montre la proposition ci-dessous, l'attaque MOV s'applique à E et le problème de logarithme discret sur E peut être réduit au logarithme discret dans $\mathbb{F}_{q^2}$, ce qui est beaucoup plus simple.

Proposition 6.23. *Soit E une courbe elliptique supersingulière sur $\mathbb{F}_q$ et soit $N > 0$ un entier. Supposons $a = q + 1 - \#E(\mathbb{F}_q) = 0$. S'il existe un point $P \in E(\mathbb{F}_q)$ d'ordre N, alors $E(\bar{\mathbb{F}}_q)[N] \subset E(\mathbb{F}_{q^2})$.*

Démonstration. Soit $Q \in E(\bar{\mathbb{F}}_q)[N]$. Puisque $\#E(\mathbb{F}_q) = q + 1$, on a $N|q + 1$. Puisque E est supersingulière et $a = 0$, on a $\phi_q^2(S) = -qS = S$. Ainsi Q est fixé par ϕ_{q^2}, d'où $Q \in E(\mathbb{F}_{q^2})$. □

6.10 Exercices

Dans tous les exercices, la lettre p désigne un nombre premier différent de 2 et la lettre q une puissance de p.

Exercice 6.1. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Montrer que le groupe $E(\mathbb{F}_q)$ est isomorphe au groupe $\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$ pour certains $n_1 \geqslant 1$ et $n_2 \geqslant 1$ tels que $n_1 \mid n_2$.

Exercice 6.2. Soit E la courbe elliptique $Y^2 = X^3 + X + 1$ sur $\mathbb{F}_5$.

a) Montrer que $|E(\mathbb{F}_5)| = 9$.

b) Montrer que $[3](0,1) = (2,1)$ sur E.

c) Montrer que $(0,1)$ engendre le groupe $E(\mathbb{F}_5)$.

Exercice 6.3. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Supposons que $E(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/n \oplus \mathbb{Z}/n$.

a) Montrer que $(n,p) = 1$.

b) Montrer que $E(\overline{\mathbb{F}_q})[n] \subset E(\mathbb{F}_q)$. En déduire que $\mu_n \subset \mathbb{F}_q$.

c) Soit $a = q + 1 - |E(\mathbb{F}_q)|$. Montrer que $a \equiv 2 \mod n$.

d) Montrer que $q = n^2 + 1$ ou $q = n^2 \pm n + 1$ ou $q = (n \pm 1)^2$.

Exercice 6.4. Soit E une courbe elliptique définie sur un corps algébriquement clos k, de caractéristique différente de 2 et 3. Rappelons que $E[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$ pour tout entier n premier à la caractéristique de k. Soit (T_1, T_2) une base de $E[n]$.

a) Soit $\zeta = e_n(T_1, T_2)$ et soit d un entier tel que $\zeta^d = 1$. Montrer que $e_n(T_1, dT_2) = 1$ et que $e_n(T_2, dT_2) = 1$. En déduire que, pour tout $S \in E[n]$, on a $e_n(S, dT_2) = 1$.

b) Montrer que $e_n(T_1, T_2)$ est une racine n-ième primitive de l'unité.

Exercice 6.5. Soit E la courbe elliptique définie par

$$Y^2 = X^3 - 4X^2 + 16$$

a) Déterminer pour quels nombres premiers p, la courbe E est une courbe elliptique sur $\mathbb{F}_p$. On note M_p le cardinal de $E(\mathbb{F}_p)$.

b) Calculer M_p pour les nombres premiers $3 \leqslant p \leqslant 13$.

c) Soit $F(q)$ la série formelle

$$F(q) = q \prod_{n=1}^{\infty} \left((1-q^n)^2(1-q^{11n})^2\right) = q + a_2 q^2 + \cdots + a_n q^n + \cdots$$

Calculer a_n pour $n \leqslant 13$, et pour $3 \leqslant p \leqslant 13$, calculer $a_p + M_p$.

d) Qu'est-on amené à conjecturer ? Vérifier cette conjecture à l'aide d'un ordinateur pour de plus grande valeurs de p.

Exercice 6.6.

a) Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$, $q = p^r$, et soit $a_q = q+1-|E(\mathbb{F}_q)|$. On note ϕ_q le morphisme de Frobenius sur E et pour tout entier m premier à q on note $(\phi_q)_m$ l'endomorphisme induit par ϕ_q sur $E(\overline{\mathbb{F}_q})[m]$. Montrer que

$$\det(\phi_q)_m \equiv q \mod m \text{ et } \mathrm{Tr}(\phi_q)_m \equiv a_q \mod m$$

(On rappelle que $|\mathrm{Ker}(\phi_q - 1)| = \deg(\phi_q - 1) = q + 1 - a_q$).

b) En déduire que l'endomorphisme $\phi_q^2 - a_q\phi_q + q$ est identiquement nul sur $E(\overline{\mathbb{F}_q})[m]$.

c) Montrer que le noyau de l'endomorphisme $\phi_q^2 - a_q\phi_q + q$ est infini ; en déduire que le polynôme $g(x) = x^2 - a_q x + q$ annule ϕ_q.

d) Supposons que b est un entier tel que le polynôme $x^2 - bx + q$ annule ϕ_q. En déduire que $(a_q - b)$ annule $E(\overline{\mathbb{F}_q})$ et enfn que $a_q = b$.

e) Soient α, β les racines du polynôme $g(x)$ et soit $g_n(x)$ le polynôme

$$g_n(x) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n.$$

Montrer que $g(x)$ divise $g_n(x)$ pour tout n. En déduire que

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = 0.$$

f) En déduire que $E(\mathbb{F}_{q^n})$ est de cardinal $q^n + 1 - (\alpha^n + \beta^n)$.

g) On définit la fonction zêta de la courbe E par

$$Z(E/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} |E(\mathbb{F}_{q^n})| \frac{T^n}{n}\right).$$

Montrer que $Z(E/\mathbb{F}_q, T)$ est la fraction rationnelle

$$\frac{1 - a_q T + qT^2}{(1-T)(1-qT)}.$$

Exercice 6.7. Soit E une courbe elliptique sur $\mathbb{F}_q$ avec $q = p^{2m}$. Supposons que $|E(\mathbb{F}_q)| = q + 1 - 2\sqrt{q}$.

a) Montrer que $(\phi_q - p^m)^2 = 0$.

b) En déduire que $\phi_q - p^m = 0$.

c) Montrer que ϕ_q agit comme l'identité sur $E(\overline{\mathbb{F}_q})[p^m - 1]$. En déduire que

$$E(\overline{\mathbb{F}_q})[p^m - 1] \subset E(\mathbb{F}_q).$$

d) Montrer que $E(\mathbb{F}_q) = \mathbb{Z}/(p^m - 1) \oplus \mathbb{Z}/(p^m - 1)$.

Exercice 6.8. Soit E la courbe elliptique définie sur $\mathbb{F}_7$ par $Y^2 = X^3 + 2$.

a) Déterminer la structure du groupe $E(\mathbb{F}_7)$.

b) Déterminer la structure du groupe $E(\mathbb{F}_{49})$.

Exercice 6.9. Soit $p > 2$ un nombre premier tel que $p \equiv 2 \mod 3$. Soit E la courbe elliptique définie par l'équation $Y^2 = X^3 + b$ sur $\mathbb{F}_p$.

a) Soit $n \geqslant 1$ un entier tel que (n, p)=1. Supposons $E[n] \subset E(\mathbb{F}_p)$. Montrer que $n \mid p - 1$ et $n^2 \mid p + 1$. En déduire $n \leqslant 2$.

b) Montrer que $E[2] \not\subseteq E(\mathbb{F}_p)$.

c) Montrer que le groupe $E(\mathbb{F}_p)$ est cyclique. Quel est l'ordre de ce groupe ?

Exercice 6.10. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Supposons $E(\mathbb{F}_q) = \mathbb{Z}/n \oplus \mathbb{Z}/mn$.

a) Montrer que $n \mid q - 1$. En déduire que l'on peut écrire

$$q = mn^2 + kn + 1 \tag{6.3}$$

pour certain entier k.

b) Montrer que $|k| \leqslant 2\sqrt{m}$ et que $mn \geqslant \sqrt{m}(\sqrt{q} - 1)$.

c) Montrer que si $m \geqslant 17$ et q est suffisamment grand, alors $E(\mathbb{F}_q)$ admet un point d'ordre $N > 4\sqrt{q}$.

d) Soit $m \geqslant 1$ fixé. Montrer que, lorsque N tend vers $+\infty$, la proportion des entiers q puissance de nombres premiers ne sont pas de la forme (6.3) parmi les entiers $q \leqslant N$ puissances de nombres premiers tend vers 0 (on peut utiliser la conséquence suivante du théorème des nombres premiers : le nombre de $q = p^r$ avec p premier, $r > 0$ (non fixés) tels que $q \leqslant x$ est environ $x/\log x$.)

e) Montrer que pour la plupart des entiers q puissances de nombres premiers, toute courbe elliptique sur $\mathbb{F}_q$ admet un point d'ordre $N > 4\sqrt{q}$.

Exercice 6.11. Soit E la courbe elliptique d'équation $Y^2 = X^3 - X + 19$ sur $\mathbb{F}_{23}$.

a) Montrer que $P = (2, 5)$ est bien un point de E. En admettant que $4P = (-2, 6)$, calculer $8P$, puis $9P$. En déduire que $17P = 0_E$.

b) Montrer que $|E(\mathbb{F}_{23})| < 34$. En déduire le cardinal de $E(\mathbb{F}_{23})$ et donner les générateurs de ce groupe.

c) En déduire que $X^3 - X + 19$ est irréductible dans $\mathbb{F}_{23}[X]$ et que $E(\mathbb{F}_{23^2})[2] = 0$.

d) Que vaut $|E(\mathbb{F}_{23^2})|$ et quelle est la structure du groupe $E(\mathbb{F}_{23^2})$?

Exercice 6.12. Soit $p > 2$ un nombre premier et soit $E : Y^2 = X^3 + AX + B$ une courbe elliptique définie sur $\mathbb{F}_p$. On définit $m \mid M$ tels que $E(\mathbb{F}_p) = \mathbb{Z}/m \oplus \mathbb{Z}/M$. Pour $d \in (\mathbb{F}_p) \smallsetminus (\mathbb{F}_p^\times)^2$, on définit une *tordue* de E comme une courbe elliptique E' donnée par l'équation $Y^2 = X^3 + Ad^2X + Bd^3$. Soient $a = p + 1 - |E(\mathbb{F}_p)|$ et $a' = p + 1 - |E'(\mathbb{F}_p)|$. On écrit aussi $E'(\mathbb{F}_p) = \mathbb{Z}/n \oplus \mathbb{Z}/N$, où $n \mid N$.

a) Montrer qu'après un changement linéaire en coordonnées on peut écrire E' sous la forme $dy^2 = x^3 + Ax + B$. En déduire que $a = -a'$.

b) Montrer que $(m^2, n^2) \mid 2a$.

c) Montrer que $a \equiv 2 \mod m$ et que $a \equiv -2 \mod n$ (on pourra utiliser que $E(\overline{\mathbb{F}_p})[m] \subset E(\mathbb{F}_p)$).

d) En déduire que $(m^2, n^2) \mid 16$ et finalement que $(m^2, n^2) \mid 4$.

e) Montrer que la restriction du Frobenius ϕ_p sur $E'(\overline{\mathbb{F}_p})[n^2]$ est donnée par une matrice $\begin{pmatrix} 1+sn & tn \\ un & 1+vn \end{pmatrix}$ avec $a \equiv 2 + (s+v)n \mod n^2$ et $p \equiv 1 + (s+v)n \mod n^2$. En déduire que $4p \equiv a^2 \mod n^2$.

f) Montrer que $\frac{m^2n^2}{4} \leqslant 4p - a^2$.

g) En déduire que pour p suffisamment grand, soit la courbe E, soit la courbe E' admet un point d'ordre plus grand que $4\sqrt{p}$.

Exercice 6.13. Soit $p \geqslant 7$ un nombre premier. Soit E une courbe elliptique définie sur $\mathbb{F}_p$ telle que $E(\mathbb{F}_p)$ possède un élément d'ordre p. Montrer que $|E(\mathbb{F}_p)| = p$.

Exercice 6.14. Soit $N = 199843247$. En utilisant la courbe elliptique d'équation $Y^2 = X^3 + 59X - 59$ et le point $(1, 1)$ déterminer un diviseur non trivial de N au moyen de l'algorithme de Lenstra.

Exercice 6.15. Soit q une puissance d'un nombre premier et soit $n \geqslant 1$. Calculer la fonction zêta de $\mathbb{P}^n_{\mathbb{F}_q}$.

Chapitre 7

Le groupe des points rationnels

7.1 Le Théorème de Mordell

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation de Weierstrass $Y^2 = X^3 + aX + b$.

Le résultat suivant a été conjecturé par Poincaré et démontré par Mordell en 1922.

Théorème 7.1 (Mordell)**.** *Le groupe $E(\mathbb{Q})$ est un groupe abélien de type fini.*

En conséquence le groupe $E(\mathbb{Q})$ est isomorphe à $E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$ où $E(\mathbb{Q})_{\text{tors}}$ est un groupe abélien fini et $r \geqslant 0$ est un entier appelé le *rang* de la courbe elliptique.

Remarque 7.2. 1. Plus généralement si K est un corps de nombres et E est une courbe elliptique définie sur K, le groupe $E(K)$ est de type fini. Cette généralisation est due à André Weil et porte le nom de *théorème de Mordell-Weil*.

2. Le groupe $E(\mathbb{Q})_{\text{tors}}$ est en général plus facile à calculer que le rang r. De façon générale, on ne connaît pas d'algorithme permettant de calculer le rang d'une courbe elliptique.

7.2 Calcul du groupe $E(\mathbb{Q})_{\text{tors}}$

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation de Weierstrass $Y^2 = X^3 + aX + b$. Quitte à faire un changement de variable, on peut supposer que $(a, b) \in \mathbb{Z}^2$. C'est ce que nous ferons dans la suite. On note $\Delta = -16(4a^3 + 27b^2)$, c'est le *discriminant* de la courbe elliptique E.

Fixons p un nombre premier ne divisant pas 2Δ et notons $\overline{a}$ et $\overline{b}$ les images de a et b dans $\mathbb{F}_p$. L'équation $Y^2 = X^3 + \overline{a}X + \overline{b}$ définit alors une courbe elliptique E_p sur $\mathbb{F}_p$.

Si P est un point de $\mathbb{P}^2(\mathbb{Q})$, il existe (x, y, z) dans $\mathbb{Z}^3$, avec x, y et z premiers entre eux, tel que $P = (x : y : z)$. Si de plus $P \in E(\mathbb{Q})$, le point $(\overline{x} : \overline{y} : \overline{z})$ est un point

de $E_p(\mathbb{F}_p) \subset \mathbb{P}^2(\mathbb{F}_p)$. On vérifie facilement que ce point ne dépend pas du système de coordonnées homogènes (x, y, z) de P. On a ainsi défini une application $P \mapsto \overline{P}$ de $E(\mathbb{Q})$ dans $E_p(\mathbb{F}_p)$ appelée application de *réduction modulo p*. Comme les réductions modulo p de trois points alignés de $E(\mathbb{Q})$ forment trois points alignés de $E_p(\mathbb{F}_p)$, l'application de réduction modulo p est un morphisme de groupes abéliens de $E(\mathbb{Q})$ vers $E_p(\mathbb{F}_p)$.

Le résultat suivant est très pratique pour calculer $E(\mathbb{Q})_{\text{tors}}$.

Théorème 7.3. *Si N est un entier, le morphisme de réduction modulo p induit une injection de $E[N] \cap E(\mathbb{Q})$ dans $E_p(\mathbb{F}_p)$.*

Remarque 7.4. Ce théorème ne sera pas démontré dans ce cours, le cas où $N = 2$ est proposé en exercice.

Le résultat suivant est également très utile pour calculer $E(\mathbb{Q})_{\text{tors}}$.

Théorème 7.5 (Lutz-Nagell)**.** *Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation de Weierstrass $Y^2 = X^3 + aX + b$ avec $(a, b) \in \mathbb{Z}^2$. Si $P \in E(\mathbb{Q})_{\text{tors}} \smallsetminus \{0\}$ alors $P = (x, y)$ avec $(x, y) \in \mathbb{Z}^2$. De plus on a $y = 0$ ou $y^2 \mid (4a^3 + 27b^2)$.*

7.3 Principe de la preuve du théorème de Mordell

L'idée de la preuve est d'utiliser le principe de la *descente infinie* qui remonte à Fermat. Il repose sur les deux résultats intermédiaires suivants.

1) Le groupe $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini. Ce résultat porte également le nom de *théorème de Mordell-Weil faible*.

2) Il existe une application *hauteur* sur $E(\mathbb{Q})$, c'est-à-dire une application $h_E : E(\mathbb{Q}) \to \mathbb{R}$ ayant les propriétés suivantes

— pour tout point $P_0 \in E(\mathbb{Q})$, il existe $C_1 > 0$ tel que

$$\forall P \in E(\mathbb{Q}),\ h_E(P + P_0) \leqslant 2h_E(P) + C_1$$

— il existe $C_2 > 0$ tel que

$$\forall P \in E(\mathbb{Q}),\ |h_E([2](P)) - 4h_E(P)| \leqslant C_2$$

— pour tout $C > 0$, l'ensemble $\{P \in E(\mathbb{Q}),\ h_E(P) \leqslant C\}$ est fini.

Nous allons prouver que les assertions 1) et 2) impliquent le théorème de Mordell.

Preuve du théorème de Mordell. D'après 1), il existe un ensemble fini $S_0 \in E(\mathbb{Q})$ tel que l'application quotient $S_0 \to E(\mathbb{Q})/2E(\mathbb{Q})$ est surjective. Soit

$$C = \max\{h_E(s) \mid s \in S_0\}$$

et soit $S = \{x \in E(\mathbb{Q}) \mid h_E(x) \leqslant C\}$. Les propriétés de h_E impliquent que S est un ensemble fini. Nous allons prouver que S engendre le groupe $E(\mathbb{Q})$.

Tout d'abord, comme $S_0 \subset S$, l'application quotient $S \to E(\mathbb{Q})/2E(\mathbb{Q})$ est surjective. Soit $P \in E(\mathbb{Q})$. Soit $P_1 \in S$ tel que $P - P_1 \in 2E(\mathbb{Q})$. On peut donc écrire $P = P_1 + 2Q_2$. De même, il existe $P_2 \in S$ tel que $Q_2 = P_2 + 2Q_3$. On construit ainsi deux suites (P_n) et (Q_n) telles que $P_n \in S$ et $Q_n = P_n + 2Q_{n+1}$. Soit C_1 tel que $h_E(Q+P) \leqslant 2h_E(Q) + C_1$ et $h_E(2Q) \geqslant 4h_E(Q) - C_1$ pour tout $Q \in E(\mathbb{Q})$ et tout $P \in S$ (on utilise ici le fait que S est fini). On a alors, pour tout $n \geqslant 1$,

$$h_E(Q_{n+1}) \leqslant \frac{1}{4}(h_E(Q_n - P_n) + C_1) \leqslant \frac{1}{4}(2h_E(Q_n) + 2C_1) \leqslant \frac{1}{2}h_E(Q_n) + \frac{1}{2}C_1$$

Ainsi

$$h(Q_n) \leqslant \frac{1}{2^n}h_E(P) + \frac{1}{2}C_1 + \frac{1}{4}C_1 + \cdots + \frac{1}{2^n}C_1 \leqslant \frac{1}{2^n}h(P) + C_1.$$

Pour n suffisamment grand, on a donc $Q_n \in S' \coloneqq \{Q \in E(\mathbb{Q}) \mid h_E(Q) \leqslant C_1 + 1\}$. Comme $S \subset S'$, P appartient au sous-groupe engendré par S'. On en conclut que $E(\mathbb{Q})$ est le groupe engendré par l'ensemble fini S'. □

7.4 Existence de la fonction hauteur

Nous allons à présent prouver la propriété 2) nécessaire à la preuve du théorème de Mordell.

Définition 7.6. *Soit $P \in \mathbb{P}^n(\mathbb{Q})$. On appelle* hauteur *de P l'entier*

$$H(P) \coloneqq \max_{0 \leqslant i \leqslant n}(|x_i|)$$

où $P = (x_0 : \ldots : x_n)$ avec $(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ et $(x_0, \ldots, x_n)$ premiers entre eux dans leur ensemble. La hauteur logarithmique *de P est donnée par $h(P) \coloneqq \ln H(P)$.*

Si $x \in \mathbb{Q}$, on note $H(x) \coloneqq H((x : 1))$ et $h(x) = h((x : 1))$. Autrement dit $h(x) = \ln(\max(|p|, |q|))$ si $x = \frac{p}{q}$ avec p et q premiers entre eux. Il est immédiat de vérifier que, pour tout $C > 0$, l'ensemble $\{x \in \mathbb{Q} \mid h(x) \leqslant C\}$ est fini.

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation de Weierstrass $Y^2 = X^3 + aX + b$ avec $(a, b) \in \mathbb{Z}^2$. Soit $P \in E(\mathbb{Q})$. On définit alors

$$h_E(P) \coloneqq \begin{cases} 0 \text{ si } P = 0 \\ h(x_P) \text{ si } P = (x_P, y_P) \end{cases}$$

La fonction h_E est la fonction hauteur recherchée.

Lemme 7.7. *Soit $P \in \mathbb{Q}[X]$ un polynôme de degré d. Il existe alors $C > 0$ tel que*

$$\forall x \in \mathbb{Q},\ H(P(x)) \leqslant CH(x)^d$$

Démonstration. On peut supposer que $P \in \mathbb{Z}[X]$. En effet, si $P \in \mathbb{Q}[X]$, il existe $a \in \mathbb{Z}$ tel que $aP \in \mathbb{Z}[X]$. On a alors, pour $x \in \mathbb{Q}$,

$$H(P(x)) = H(a^{-1}aP(x)) \leqslant H(a)H(aP(x))$$

Supposons donc que $P \in \mathbb{Z}[X]$. On peut écrire $P(X) = a_d X^d + \cdots + a_0$ avec $a_d \neq 0$. Si $x = \frac{p}{q} \in \mathbb{Q}$, on a

$$H\left(P\left(\frac{p}{q}\right)\right) = H\left(\frac{a_d p^d + a_{d-1}p^{d-1}q + \cdots + a_0 q^d}{q^d}\right)$$
$$\leqslant \max(|q|^d, |a_d p^d|, \ldots, |a_0 q^d| \leqslant AH\left(\frac{p}{q}\right)^d$$

où $A = \max(|a_i|)$. □

Lemme 7.8. *Soient P et Q deux polynômes de $\mathbb{Q}[X]$ premiers entre eux. Soit $d = \max(\deg P, \deg Q)$. Il existe $C > 0$ tel que*

$$\forall x \in \mathbb{Q},\ H\left(\frac{P(x)}{Q(x)}\right) \geqslant CH(x)^d$$

Démonstration. Comme dans la preuve du lemme précédent, on peut supposer que P et Q sont dans $\mathbb{Z}[X]$. Si $x = \frac{p}{q} \in \mathbb{Q}$, on a

$$F\left(\frac{p}{q}\right) = q^{\deg Q - \deg P}\frac{P^*(p,q)}{Q^*(p,q)}$$

où $P^*(X,Z)$ et $Q^*(X,Z)$ sont les polynômes homogénéisés de P et Q. Si $\deg P \geqslant \deg Q$, on pose $A(X,Z) \coloneqq P^*(X,Z)$ et $B(X,Z) \coloneqq X^{\deg P - \deg Q}Q^*(X,Z)$ et si $\deg Q \geqslant \deg P$, on pose $A(X,Z) \coloneqq X^{\deg Q - \deg P}P^*(X,Z)$ et $B(X,Z) \coloneqq Q(X,Z)$. De sorte que

$$\forall \frac{p}{q} \in \mathbb{Q},\ F\left(\frac{p}{q}\right) = \frac{A(p,q)}{B(p,q)}$$

où A et B sont des polynômes homogènes de même degré $d = \max(\deg P, \deg Q)$. Comme P et Q sont premiers entre eux, on vérifie facilement que les polynômes A et B sont premiers entre eux. On déduit alors du Nullstellensatz projectif qu'il existe $N \geqslant 0$ tel que

$$(X,Z)^N \subset (A,B)$$

Il existe donc des polynômes U_1, V_1, U_2, V_2 dans $\mathbb{Z}[X,Z]$, ainsi qu'un entier α tels que

$$U_1 A + V_1 B = \alpha X^N$$
$$U_2 A + V_2 B = \alpha Z^N$$

Comme A et B sont homogènes de degré d, on peut choisir U_1, V_1, U_2 et V_2 de degré $N - d$.

Soit $x \in \mathbb{Q}$. On peut écrire $x = \frac{p}{q}$ où p et q sont des entiers premiers entre eux. Soit δ le PGCD de $A(p,q)$ et $B(p,q)$. On a donc $\delta \mid \alpha p^N$ et $\delta \mid \alpha q^N$. Comme p et q sont premiers entre eux, on en déduit $\delta \mid \alpha$. Au final,

$$H\left(F\left(\frac{p}{q}\right)\right) \geqslant H(\alpha)^{-1} \max(A(p,q), B(p,q))$$

et il existe une constante $C > 0$ telle que

$$H(p)^N \leqslant CH\left(\frac{p}{q}\right)^{N-d} \max(|A(p,q)|, |B(p,q)|)$$
$$H(q)^N \leqslant CH\left(\frac{p}{q}\right)^{N-d} \max(|A(p,q)|, |B(p,q)|)$$

D'où finalement

$$H\left(F\left(\frac{p}{q}\right)\right) \geqslant H(\alpha)^{-1} C^{-1} H\left(\frac{p}{q}\right)^d. \qquad \square$$

Proposition 7.9. *Soit E une courbe elliptique définie sur $\mathbb{Q}$.*

(i) Soit $P_0 \in E(\mathbb{Q})$. Il existe alors $C_1 > 0$ tel que

$$\forall P \in E(\mathbb{Q}),\ h_E(P + P_0) \leqslant 2h_E(P) + C_1$$

(ii) Il existe $C_2 > 0$ tel que

$$\forall P \in E(\mathbb{Q}),\ 4h_E(P) - C_2 \leqslant h_E(2P) \leqslant 4h_E(P) + C_2$$

(iii) Pour tout $C > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid h_E(P) \leqslant C\}$ est fini.

Démonstration. Commençons par prouver (i). Le cas où $P_0 = 0$ est évident, on suppose donc $P_0 \neq 0$. Quitte à élargir C_1, on peut sans problème exclure un nombre fini de possibilités pour P et donc supposer $P \notin \{0, P_0, -P_0\}$. Posons $P_0 = (x_{P_0}, y_{P_0})$ et $P = (x_P, y_P)$. La formule d'addition nous donne

$$\begin{aligned} x_{P+P_0} &= \left(\frac{y_P - y_{P_0}}{x_P - x_{P_0}}\right)^2 - (x_P + x_{P_0}) = \frac{(y_P - y_{P_0})^2 - (x_P - x_{P_0})^2(x_P + x_{P_0})}{(x_P - x_{P_0})^2} \\ &= \frac{x_P^3 + x_{P_0}^3 + ax_P + ax_{P_0} + 2b - 2y_P y_{P_0} + (x_P + x_{P_0})(x_P - x_{P_0})^2}{(x_P - x_{P_0})^2} \\ &= \frac{(x_P + x_{P_0})(x_P^2 + x_{P_0}^2 - x_P x_{P_0} - x_P^2 - x_{P_0}^2 + 2x_P x_{P_0} + a) + 2b - 2y_P y_{P_0}}{(x_P - x_{P_0})^2} \\ &= \frac{(x_P + x_{P_0})(x_P x_{P_0} + a) + 2(b - y_P y_{P_0})}{(x_P - x_{P_0})^2} \end{aligned}$$

On remarque alors que l'on peut écrire $x_P = \frac{u}{d^2}$, $y_P = \frac{v}{d^3}$, $x_{P_0} = \frac{u_0}{d_0^2}$ et $y_{P_0} = \frac{v_0}{d_0^3}$, où u et d, v et d, u_0 et d_0, v_0 et d_0 sont premiers entre eux. On obtient

$$x_{P+P_0} = \frac{(d_0^2 u + d^2 u_0)(uu_0 + a(dd_0)^2) + 2(b(dd_0)^3 - vv_0)}{(ud_0^2 - u_0 d^2)^2}$$

On en déduit

$$H(x_{P+P_0}) \leqslant \max(|(d_0^2u + d^2u_0)(uu_0 + a(dd_0)^2) + 2(b(dd_0)^3 - vv_0)|, |(ud_0^2 - u_0d^2)^2|)$$

Or il existe $A_1 > 0$ tel que

$$\forall (u,d) \in \mathbb{Z}^2,\ |(ud_0^2 - u_0d^2)^2| \leqslant A_1 \max(|u|, |d|^2)^2$$

et $A_2 > 0$ tel que

$$\forall (u,v,d) \in \mathbb{Z}^3,\ |(d_0^2u + d^2u_0)(uu_0 + a(dd_0)^2) + 2(b(dd_0)^3 - vv_0)| \leqslant A_2 \max(|u|^2, |d|^4, |v|)$$

Cependant on a $v^2 = u^3 + aud^4 + b$, d'où l'existence de $A_3 > 0$, ne dépendant que de a et b, tel que $|v| \leqslant A_3 \max(|u|, |d|^2)^{3/2}$. En remarquant que $H_P(x_P) = \max(|u|, |d|^2)$, on en déduit le résultat désiré.

Pour prouver (ii), on peut supposer que $2P \neq 0$. On a alors

$$x_{2P} = \frac{(3x_P^2 + a)^2 - 8x_P(x_P^3 + ax_P + b)}{4(x_P^3 + ax_P + b)} = \frac{x_P^4 - 6ax_P^2 + bX_P - a^2}{4(x_P^3 + ax_P + b)}$$

Comme $X^3 + aX + b$ est à racines distinctes, les polynômes $X^3 + aX + b$ et $X^4 - 6aX^2 + bX - a^2$ sont premiers entre eux. Le résultat est alors une conséquence direct des deux lemmes.

La propriété (iii) est alors une conséquence du fait que le nombre de $x \in \mathbb{Q}$ tels que $h(x) \leqslant C$ est fini et qu'il y a au plus deux points de $E(\mathbb{Q})$ vérifiant $x_P = x_0$ pour un x_0 donné. □

Remarque 7.10. Si $P \in E(\mathbb{Q})$, on peut montrer que la suite $\frac{1}{4^n} h_E([2^n](P))$ converge vers un nombre réel $\hat{h}_E(P)$. La fonction $\hat{h}_E$ est appelée *hauteur de Néron-Tate*. Elle vérifie toutes les propriétés de la proposition 7.9. En fait il existe une constante $\alpha \geqslant 0$ telle que $|\hat{h}_E - h_E| \leqslant \alpha$. Cependant la fonction $\hat{h}_E$ a de meilleures propriétés que h_E : c'est une forme quadratique. Autrement dit la fonction

$$(P,Q) \mapsto \langle P,Q \rangle \coloneqq \hat{h}_E(P+Q) - \hat{h}_E(P) - \hat{h}_E(Q)$$

est bilinéaire alternée. Cette forme bilinéaire alternée s'étend naturellement au $\mathbb{R}$-espace vectoriel $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ (de dimension finie d'après le théorème de Mordell) et est définie positive, il s'agit donc d'un produit scalaire.

7.5 Exercices

Exercice 7.1. Pour les courbes elliptiques suivantes, déterminer le groupe $E(\mathbb{Q})_{\text{tors}}$.

a) $Y^2 = X^3 - 7X + 13$;

b) $Y^2 = X^3 - 2$, $Y^2 = X^3 - 8$, $Y^2 = X^3 + 25$, $Y^2 = X^3 + 1$;

c) $Y^2 = X^3 - 43X + 166$ (on pourra remarquer que $(3, 8) \in E(\mathbb{Q})$).

Exercice 7.2. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par l'équation

$$Y^2 = X^3 + 17$$

a) Calculer $E(\mathbb{Q})_{\text{tors}}$.

b) En déduire que l'ensemble $E(\mathbb{Q})$ est de cardinal infini.

Exercice 7.3. Soit E une courbe elliptique définie par $Y^2 = X^3+aX+b$ avec $(a, b) \in \mathbb{Z}^2$. On note $\Delta = 4a^3+27b^2$. On note $f(X) \coloneqq X^3+aX+b \in \mathbb{Z}[X]$. Soit p un nombre premier. On note $\overline{f}(X)$ l'image de f dans $\mathbb{F}_p[X]$ par l'application de réduction modulo p.

a) Soit $P = (x, y) \in E[2] \cap E(\mathbb{Q})$. Montrer que $(x, y) \in \mathbb{Z}^2$.

b) Si p ne divise pas 2Δ, montrer que le polynôme $\overline{f}(X)$ est séparable.

c) En déduire que, si p ne divise pas 2Δ, l'application de réduction modulo p induit une injection de $E[2] \cap E(\mathbb{Q})$ dans $E(\mathbb{F}_p)$.

Exercice 7.4. Soit G un groupe abélien. Soit q une fonction de $G \times G$ dans $\mathbb{R}$ telle que

$$\forall (x, y) \in G^2,\ q(x + y) + q(x - y) = 2q(x) + 2q(y)$$

a) Montrer que $q(0) = 0$ et que, pour tout $x \in G$, on a $q(-x) = q(x)$.

b) Montrer que q est une forme quadratique.

Exercice 7.5. Soit G un groupe abélien. Soit $q : G \to \mathbb{R}$ une forme quadratique. On suppose que $G/2G$ est un groupe fini et que, pour tout $C > 0$, l'ensemble $\{x \in G \mid q(x) \leqslant C\}$ est fini. Montrer que G est de type fini.

Exercice 7.6. Soit $(x, y) \in \mathbb{Q}^2$.

a) Montrer que $H(xy) \leqslant H(x)H(y)$.

b) Montrer que $H(x + y) \leqslant 2H(x)H(y)$.

c) Montrer que $H(x)H(y) \leqslant 2\max(H(x + y), H(xy))$.

Exercice 7.7. Soit E une courbe elliptique définie sur $\mathbb{Q}$ par l'équation $Y^2 = X^3+aX+b$ avec $(a, b) \in \mathbb{Z}^2$.

a) Soit $(P, Q) \in E(\mathbb{Q})^2$. On suppose que $P \neq 0$ et $Q \notin \{0, \pm P\}$. On pose ainsi $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$. Montrer que

$$x_{P+Q} + x_{P-Q} = \frac{2(x_P + x_Q)(a - x_P x_Q) + 4b}{(x_P + x_Q)^2 - 4x_P x_Q},\ x_P x_Q = \frac{(x_P x_Q - a)^2 - 4b(x_P + x_Q)}{(x_P + x_Q)^2 - 4x_P x_Q}$$

b) Montrer qu'il existe $c > 0$ tel que

$$\forall (P, Q) \in E(\mathbb{Q}),\ h_E(P+Q) + h_E(P-Q) \leqslant 2h_E(P) + 2h_E(Q) + c$$

c) Montrer qu'il existe $c' > 0$ tel que

$$\forall (P, Q) \in E(\mathbb{Q}),\ |h_E(P+Q) + h_E(P-Q) - 2h_E(P) - 2h_E(Q)| \leqslant c'$$

(on pourra utiliser l'inégalité précédente ainsi que la borne du cours concernant $|h_E([2](P) - 4h_E(P)|$).

d) Montrer que la fonction $\hat{h}_E$ sur $E(\mathbb{Q})$ définie par

$$\hat{h}_E(P) \coloneqq \lim_{n \to +\infty} \frac{1}{4^n} h_E([2^n](P))$$

est une forme quadratique, c'est-à-dire que l'application

$$(P, Q) \mapsto \langle P, Q \rangle \coloneqq \hat{h}_E(P+Q) - \hat{h}_E(P) - \hat{h}_E(Q)$$

est bilinéaire symétrique.

e) Montrer que pour tout $P \in E(\mathbb{Q})$ et $m \in \mathbb{Z}$, on a $\hat{h}_E([m](P)) = m^2 \hat{h}_E(P)$. En déduire que $\hat{h}_E(P) = 0$ si et seulement si P est un point de torsion.

f) Montrer que pour tout $A > 0$, l'ensemble $\{P \in E(\mathbb{Q}) \mid \hat{h}_E(P) \leqslant A\}$ est fini.

g) En utilisant le théorème de Mordell, montrer que $\langle -, - \rangle$ se prolonge à $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ en une forme quadratique définie positive (on pourra utiliser la classification de Sylvester des formes quadratiques réelles ainsi que le théorème suivant de Minkowski : soit V un espace vectoriel réel de dimension finie et soit Λ un réseau de V, toute partie convexe symétrique de volume assez grand contient un point de Λ).

h) Montrer que

$$|\{P \in E(\mathbb{Q}),\ h_E(P) \leqslant n\}| \sim_{n \to +\infty} d n^{\frac{r}{2}}$$

où r désigne le rang de $E(\mathbb{Q})$ et un certain réel $d > 0$.

Chapitre 8

Le rang d'une courbe elliptique

8.1 Anneaux d'entiers des corps de nombres

Soit K un corps de nombres, c'est-à-dire une extension finie du corps des nombres rationnels $\mathbb{Q}$. Un élément $x \in K$ est dit entier s'il est annulé par un polynôme *unitaire* de $\mathbb{Z}[X]$. L'ensemble des entiers de K forme un sous-anneau de K noté $\mathcal{O}_K$. Le résultat suivant est dû à Dedekind.

Théorème 8.1. *Tout idéal non nul de $\mathcal{O}_K$ s'écrit de façon unique comme produit fini d'idéaux premiers de $\mathcal{O}_K$.*

Soit $\mathcal{I}$ l'ensemble des idéaux non nuls de $\mathcal{O}_K$. On munit l'ensemble $\mathcal{I}$ d'une relation d'équivalence définie par

$$I \sim J \Leftrightarrow \exists a \in K^\times,\ J = aI$$

On vérifie que si $I_1 \sim J_1$ et $I_2 \sim J_2$, on a $I_1 I_2 \sim J_1 J_2$. Le quotient de $\mathcal{I}/\sim$ est noté $\mathrm{Cl}(\mathcal{O}_K)$. C'est un groupe pour la relation de multiplication.

Théorème 8.2. *Le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est fini.*

Remarque 8.3. L'anneau $\mathcal{O}_K$ est un anneau principal si et seulement si le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est trivial. De plus si I est un idéal non nul de $\mathcal{O}_K$, il existe $n \geqslant 1$ tel que l'idéal I^n est principal.

Exemple 8.4. Si $d \in \mathbb{Z}$ est sans facteur carré et si $K = \mathbb{Q}(\sqrt{d})$, alors K est un corps de nombres et l'anneau $\mathcal{O}_K$ est de la forme $\mathbb{Z}[x]$ avec

$$x = \begin{cases} \sqrt{d} & \text{si } d \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \mod 4 \end{cases}$$

On peut montrer que les anneaux $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ sont principaux mais que l'anneau $\mathbb{Z}[\sqrt{-5}]$ ne l'est pas. Le groupe $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$ est de cardinal 2, engendré par la classe de l'idéal premier $(2, 1+\sqrt{-5})$.

Définition 8.5. *Soit S un ensemble fini d'idéaux premiers de $\mathcal{O}_K$. On définit*

$$\mathcal{O}_{K,S} = \{x \in K \mid \exists a \in \bigcap_{\mathfrak{p} \notin S} (\mathcal{O}_K \smallsetminus \mathfrak{p}),\ ax \in \mathcal{O}_K\}$$
$$= \left\{ \frac{a}{b} \mid a \in \mathcal{O}_K,\ b \in \bigcap_{\mathfrak{p} \notin S} (\mathcal{O}_K \smallsetminus \mathfrak{p}) \right\}$$

Il s'agit d'un sous-anneau de K appelé anneau des S-entiers *de K.*

Exemple 8.6. Si $K = \mathbb{Q}$ et si $S = \{p_1, \ldots, p_r\}$, l'anneau $\mathbb{Z}_S$ est l'anneau des fractions dont le dénominateur n'a que des diviseurs premiers appartenant à S.

Si I est un idéal de $\mathcal{O}_{K,S}$, l'idéal $I \cap \mathcal{O}_K$ est un idéal de $\mathcal{O}_K$ et l'application $I \mapsto I \cap \mathcal{O}_K$ est une injection de l'ensemble des idéaux de $\mathcal{O}_{K,S}$ dans l'ensemble des idéaux de $\mathcal{O}_K$. On vérifie qu'elle induit une bijection entre l'ensemble des idéaux premiers de $\mathcal{O}_{K,S}$ et l'ensemble des idéaux premiers de $\mathcal{O}_K$ qui n'appartiennent pas à S.

Corollaire 8.7. *Tout idéal non nul de l'anneau $\mathcal{O}_{K,S}$ s'écrit de façon unique comme un produit d'idéaux premiers.*

On vérifie de plus que l'application $I \mapsto I\mathcal{O}_{K,S}$ induit un morphisme de groupes surjectif $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_{K,S})$. Les éléments de S sont dans le noyau de ce morphisme.

Corollaire 8.8. *Il existe une partie finie $S' \supset S$ telle que l'anneau $\mathcal{O}_{K,S'}$ est principal.*

Si K est un corps de nombres, il y a exactement $[K : \mathbb{Q}]$ morphismes de corps de K dans $\mathbb{C}$. Un tel morphisme τ est dit *réel* si $\tau(K) \subset \mathbb{R}$, il est dit *complexe* dans le cas contraire. Remarquons que si τ est un plongement complexe, son conjugué $\overline{\tau}$ en est un autre. Le cardinal de l'ensemble des plongements complexes de K est donc pair. Notons le $2r_2$ et notons r_1 le nombre de plongements réels. On a ainsi $[K : \mathbb{Q}] = r_1 + 2r_2$.

L'ingrédient principal du théorème de Mordell-Weil faible est le résultat suivant.

Théorème 8.9. *Soit K un corps de nombres et soit S un ensemble fini d'idéaux premiers de $\mathcal{O}_K$. Le groupe $\mathcal{O}_{K,S}^\times$ est un groupe de type fini. On a de plus un isomorphisme*

$$\mathcal{O}_{K,S}^\times \simeq (\mathcal{O}_{K,S}^\times)_{\mathrm{tors}} \times \mathbb{Z}^{r_1+r_2-1+|S|}$$

Démonstration. Nous démontrons juste la finitude qui est le seul ingrédient utilisé dans la preuve du théorème de Mordell-Weil faible. Si $S \subset S'$, on a $\mathcal{O}_{K,S}^\times \subset \mathcal{O}_{K,S'}^\times$. Pour prouver que $\mathcal{O}_{K,S}^\times$ est de type fini, il suffit de prouver que $\mathcal{O}_{K,S'}^\times$ est de type fini. On peut donc supposer que $\mathcal{O}_{K,S}$ est un anneau principal. Si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_{K,S}$, il existe $\pi_\mathfrak{p} \in \mathfrak{p}$ tel que $\mathfrak{p} = (\pi_\mathfrak{p})$. Pour tout $x \in K^\times$, on note $v_\mathfrak{p}(x)$ la valuation de l'élément x en $\pi_\mathfrak{p}$. L'application $v_\mathfrak{p}$ de $K^\times$ dans $\mathbb{Z}$ est alors un morphisme de groupes.

On définit alors le morphisme de groupes suivant

$$\Phi_K : \begin{array}{ccc} \mathcal{O}_{K,S}^\times & \longrightarrow & \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} \times \mathbb{R}^{|S|} \\ x & \longmapsto & ((\ln|\tau_1(x)|)_{1\leqslant i\leqslant r_1}, (\ln|\sigma_i(x)|)_{1\leqslant i\leqslant r_2}, (v_\mathfrak{p}(x))_{\mathfrak{p}\in S}) \end{array}$$

Il s'agit clairement d'un morphisme de groupes. Son noyau est constitué des éléments $x \in \mathcal{O}_K$ tels que $|\tau(x)| = 1$ pour tout plongement τ de K dans $\mathbb{C}$, il s'agit du groupe des racines de l'unité présentes dans K, c'est-à-dire un groupe fini.

Pour conclure, il suffit donc de prouver que l'image de Φ_K est un sous-groupe discret de $\mathbb{R}^{r_1+r_2+|S|}$. Pour ce faire, il suffit de prouver qu'il existe une boule ouverte centrée en zéro de $\mathbb{R}^{r_1+r_2+|S|}$ contenant un nombre fini d'éléments de l'image de Φ_K. Soit donc $0 < \varepsilon < 1$. Si $|\Phi_K(x)|_\infty < \varepsilon$ et si $\mathfrak{p} \in S$, on a $|v_\mathfrak{p}(x)| < 1$, donc $v_\mathfrak{p}(x) = 0$. Ainsi $x \in \mathcal{O}_K^\times$. De plus, on a $|\tau(x)| < \exp(\varepsilon)$ pour tout plongement τ de K dans $\mathbb{C}$. Par ailleurs le polynôme

$$P_x(X) = \prod_\tau (X - \tau(x))$$

est un polynôme unitaire de $\mathbb{Z}[X]$ et ses coefficients sont bornés par un réel $C(\varepsilon) = 2^n \exp(n\varepsilon)$. Il y a un nombre fini de tels polynômes, donc un nombre fini de $x \in \mathcal{O}_K$ tels que $|\Phi_K(x)| < \varepsilon$.

On en déduit de plus que le rang du groupe $\Phi_K(\mathcal{O}_{K,S}^\times)$ est $\leqslant r_1 + r_2 + |S|$. □

On peut montrer que le rang de $\mathcal{O}_{K,S}^\times$ est en fait inférieur à $r_1 + r_2 - 1 + |S|$ en utilisant la formule du produit. Si $x \in K$, on a

$$\prod_{i=1}^{r_1} |\tau_i(x)| \prod_{i=1}^{r_2} |\sigma_i(x)|^2 \prod_\mathfrak{p} q_\mathfrak{p}^{-v_\mathfrak{p}(x)} = 1$$

où $q_\mathfrak{p}$ est le cardinal du corps $\mathcal{O}_K/\mathfrak{p}$.

Les considérations ci-dessus permettent de démontrer une assertion déjà utilisée dans ce cours.

Proposition 8.10. *Soit k un corps fini. Il existe un alors anneau principal A dont le corps des fractions est de caractéristique 0 ainsi qu'un idéal premier $\mathfrak{p}$ de A tel que $A/\mathfrak{p} \simeq k$.*

Equisse de démonstration. Supposons que k est le corps fini à $q = p^f$ éléments pour un nombre premier p. Il est en particulier isomorphe au corps $\mathbb{F}_p[X]/(P(X))$ où $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré f. Soit $\tilde{P}(X) \in \mathbb{Z}[X]$ un polynôme unitaire dont l'image dans $\mathbb{F}_p[X]$ est $P(X)$. Soit K le corps de rupture de $\tilde{P}$. Il s'agit d'un corps de nombres K. De plus l'idéal de son anneau d'entiers $\mathcal{O}_K$ engendré par p est un idéal premier et $\mathcal{O}_K/(p) \simeq \mathbb{F}_q$. On peut alors choisir un ensemble fini S d'idéaux premiers de $\mathcal{O}_K$ ne contenant pas p et tel que $\mathcal{O}_{K,S}$ est principal. On vérifie alors que $\mathcal{O}_{K,S}/(p) \simeq \mathbb{F}_q$. □

8.2 Le théorème de Mordell-Weil faible

Le but de cette partie est de prouver le résultat suivant.

Théorème 8.11. *Soit K un corps de nombres et soit E une courbe elliptique définie sur K. Le groupe $E(K)/2E(K)$ est fini.*

Démonstration. Dans un premier temps, on va se ramener au cas où $E[2] \subset E(K)$. Il suffit de prouver le résultat intermédiaire suivant : si L est une extension galoisienne finie de K alors si $E(L)/2E(L)$ est fini, l'ensemble $E(K)/2E(K)$ est fini. Il suffit de prouver que le noyau Φ de l'application $E(K)/2E(K) \to E(L)/2E(L)$ est fini. Soit $P \in \Phi$. Par définition il existe $Q \in E(L)$ tel que $[2](Q) = P$. Si $\sigma \in \mathrm{Gal}(L/K)$, on pose $c_P(\sigma) \coloneqq \sigma(Q) - Q$. On a $[2](c_P(\sigma)) = \sigma(P) - P$ donc $[2](c_P(\sigma)) = 0$. L'application c_P est donc une application de $\mathrm{Gal}(L/K)$ dans $E[2]$. Montrons que l'application $P \mapsto c_P$ est injective. Si $c_P = c_{P'}$, on a, pour tout $\sigma \in \mathrm{Gal}(L/K)$,

$$\sigma(Q' - Q) = Q' - Q$$

Le point $Q' - Q$ est donc dans $E(K)$, ce qui prouve que $P' - P$ est dans $2E(K)$. Le groupe Φ est donc fini.

On peut donc supposer que $E[2] \subset E(K)$. La courbe elliptique est définie par l'équation

$$Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

et on a $E[2] = \{0, P_1, P_2, P_3\}$ avec $P_i = (\alpha_i, 0)$. Pour tout $P \in E(K)$ et $1 \leqslant i \leqslant 3$, on définit un élément $\phi_i(P)$ de $K^\times/K^{\times 2}$ par

$$\phi_i(P) = \begin{cases} 1 & \text{si } P = 0 \\ x_P - \alpha_i & \text{si } P \notin \{0, P_i\} \\ (\alpha_{i+1} - \alpha_i)(\alpha_{i-1} - \alpha_i) & \text{si } P = P_i \end{cases}$$

On note alors ϕ l'application (ϕ_1, ϕ_2, ϕ_3) de $E(K)$ dans $(K^\times/K^{\times 2})^3$.

Montrons que ϕ est un morphisme de groupes. Pour cela, il suffit de prouver que chaque application ϕ_i est un morphisme de groupes. Il suffit de prouver que

$$P + Q + R = 0 \Rightarrow \phi_i(P)\phi_i(Q)\phi_i(R) = 1$$

Supposons dans un premier temps que $R = 0$. Alors $Q = -P$ et $\phi_i(P)\phi_i(Q) = \phi_i(P)^2 = 1$ dans $K^\times/K^{\times 2}$. On peut donc supposer que les points P, Q et R sont différents de 0. Ils sont donc alignés sur une droite d'équation $Y = \lambda X + \mu$. Les nombres $x_P - \alpha_i$, $x_Q - \alpha_i$, $x_R - \alpha_i$ sont alors solutions (en comptant les multiplicités) de l'équation

$$(\lambda(X + \alpha_i) + \mu)^2 = (X + \alpha_i)^3 + a(X + \alpha_i) + b.$$

Le produit des racines de ce polynômes est égal à l'opposé de son terme constant, on obtient donc

$$(x_P - \alpha_i)(x_Q - \alpha_i)(x_R - \alpha_i) = -(\alpha_i^3 + a\alpha_i + b) + (\lambda\alpha_i + \mu)^2 = (\lambda\alpha_i + \mu)^2.$$

On a donc $\phi_i(P)\phi_i(Q)\phi_i(R) = 1$ dans $K^\times/K^{\times 2}$.

Montrons à présent que $2E(K)$ est exactement le noyau de ϕ. Comme $K^\times/K^{\times 2}$ est un 2-groupe, on a $2E(K) \subset \operatorname{Ker}\phi$. Réciproquement soit $P \in \operatorname{Ker}\phi$. Supposons que $P \notin E[2]$. On a alors

$$\begin{cases} x_P - \alpha_1 = z_1^2 \\ x_Q - \alpha_2 = z_2^2 \\ x_R - \alpha_3 = z_3^2 \end{cases}$$

La matrice

$$D = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix}$$

est inversible. Il existe donc $(u, v, w) \in K^3$ tel que

$$\begin{cases} z_1 = u + v\alpha_1 + w\alpha_1^2 \\ z_2 = u + v\alpha_2 + w\alpha_2^3 \\ z_3 = u + v\alpha_3 + w\alpha_3^2 \end{cases}$$

En développant les carrés, une identification terme à terme (loisible puisque D est inversible) nous donne le système

$$\begin{cases} x_P = u^2 - 2bvw \\ 0 = 2uv - 2avw - bw^2 + 1 \\ 0 = v^2 + 2uw - aw^2 \end{cases}$$

Les deux dernières équations montrent que $w \neq 0$ et que le point $Q = (\frac{v}{w}, \frac{1}{w})$ est dans $E(\mathbb{Q})$. On calcule alors $[2](x_Q)$, on trouve

$$\begin{aligned} x_{[2](Q)} &= \frac{x_Q^4 - 2ax_Q^2 - 8bx_Q + a^2}{4(x_Q^3 + ax_Q + b)} \\ &= \frac{v^4 - 2av^2w^2 - 8bvw^3 + a^2w^4}{4w^2} \\ &= \frac{v^4 - 2av^2w^2 + a^2w^4}{4w^2} - 2bvw \\ &= \left(\frac{v^2}{2w} - \frac{aw}{2}\right)^2 - 2bvw = u^2 - 2bvw \\ &= x_P \end{aligned}$$

On en conclut que $[2](Q) = \pm P$ et donc que $P = [2](\pm Q)$ et donc $P \in 2E(K)$.

Il reste à prouver que l'image de ϕ dans $K^\times/K^{\times 2}$ est un groupe fini, ce qui achèvera la preuve du théorème. Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$ contenant l'ensemble des idéaux premiers de $\mathcal{O}_K$ divisant $2(4a^3+37b^2)$. Comme $-4a^3-27b^2 = ((\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3))^2$, on en conclut que 2, $\alpha_1-\alpha_2$, $\alpha_2-\alpha_3$ et $\alpha_1-\alpha_3$ sont des éléments inversibles de $\mathcal{O}_{K,S}$. Notons que l'on peut de plus choisir S suffisamment grand de sorte que $\mathcal{O}_{K,S}$ soit principal.

Soit $P \in E(K)$. On peut écrire $P = (\frac{u}{t}, \frac{v}{s})$ avec u et t premiers entre eux et v et s premiers entre eux. La relation $P \in E(K)$ implique que

$$v^2t^3 = s^2(u-\alpha_1 t)(u-\alpha_2 t)(u-\alpha_3 t)$$

Comme s et v sont premiers entre eux, on a $s^2 \mid t^3$. Par ailleurs comme t et u sont premiers entre eux, t et $(u-\alpha_i t)$ sont premiers entre eux pour $1 \leqslant i \leqslant 3$ et donc $t^3 \mid s^2$. Comme $\mathcal{O}_{K,S}$ est un anneau principal, quitte à modifier t et s par des inversibles de $\mathcal{O}_{K,S}$, on peut supposer $t^3 = s^2$ ainsi que l'existence d'un élément $d \in \mathcal{O}_{K,S}$ tel que $t = d^2$ et $s = d^3$. De plus, d et u, ainsi que d et v sont premiers entre eux. On obtient donc l'équation

$$v^2 = (u-\alpha_1 d^2)(u-\alpha_2 d^2)(u-\alpha_3 d^2)$$

Notons enfin que les nombres $(u-\alpha_i d^2)$ pour $1 \leqslant i \leqslant 3$ sont premiers entre eux deux à deux. En effet si δ divise $u-\alpha_1 d^2$ et $u-\alpha_2 d^2$, il divise $2u$ et $d^2(\alpha_1-\alpha_2)$. Comme 2 et $\alpha_1-\alpha_2$ sont inversibles dans $\mathcal{O}_{K,S}$, on en conclut que δ divise u et d^2, donc que δ est inversible. Ainsi, pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_{K,S}$, on a $v_\mathfrak{p}(u-\alpha_i d^2)$ pair. Il existe donc un élément inversible $\gamma_i \in \mathcal{O}_{K,S}^\times$ ainsi qu'un élément $z_i \in K^{\times 2}$ tel que $u-\alpha_i d^2 = \gamma_i z_i^2$. On en conclut que $x_P - \alpha_i = \gamma_i d^{-2} z_i^2$, donc que $\phi_i(P)$ appartient à $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$.

Il reste à traiter le cas où $P = P_i$. Dans ce cas $\phi_i(P_i) = (\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1}) \in \mathcal{O}_{K,S}^\times$ par définition de S. □

Remarque 8.12. On remarque qu'on a en fait $\phi_1(P)\phi_2(P)\phi_3(P) = 1$ pour tout $P \in E(K)$. En particulier l'application (ϕ_1, ϕ_2) induit un morphisme de groupes injectif

$$E(K)/2E(K) \hookrightarrow (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^2$$

pour S assez grand. Si $E[2] \subset E(K)$, on en déduit la majoration suivante pour le rang r de E :

$$r \leqslant 2(r_1 + r_2 - 1 + |S|).$$

8.3 Exercices

Exercice 8.1. Soit S un ensemble fini de nombres premiers.

a) Montrer que l'inclusion de $\mathbb{Z}_S$ dans $\mathbb{R}$ induit un morphisme surjectif de groupes

$$\psi : \mathbb{Z}_S^\times/\mathbb{Z}_S^{\times 2} \longrightarrow \mathbb{R}^\times/\mathbb{R}^{\times 2}$$

Quel est le cardinal de $\mathbb{R}^\times/\mathbb{R}^{\times 2}$?

b) Soit E une courbe elliptique définie sur $\mathbb{Q}$ par l'équation

$$Y^2 = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3) = X^3 + aX + b$$

avec $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Q}^3$. On suppose que S contient tous les diviseurs premiers de $2(4a^3 + 27b^2)$. Supposons pour fixer les idées $\alpha_1 < \alpha_2 < \alpha_3$. Pour $1 \leqslant i \leqslant 3$, on note $\phi_i = \phi_{\alpha_i}$ le morphisme de groupes de $E(\mathbb{Q})$ vers $\mathbb{Z}_S^\times/\mathbb{Z}_S^{\times 2}$ construit en cours. Montrer que l'image de $(\psi \circ \phi_1, \psi \circ \phi_2)$ dans $(\mathbb{R}^\times/\mathbb{R}^{\times 2})^2$ ne contient ni $(-1, 1)$ ni $(-1, -1)$. Si r désigne le rang de E, en déduire que

$$r \leqslant 2|S| - 1$$

Exercice 8.2. Soit E la courbe elliptique définie sur $\mathbb{Q}$ par l'équation $Y^2 = X^3 - X$.

a) Montrer que $E[2] \subset E(\mathbb{Q})$.

b) Montrer que le groupe $G \coloneqq \mathbb{Z}_{\{2\}}^\times/\mathbb{Z}_{\{2\}}^{\times 2}$ est un 2-groupe de cardinal 4 engendré par 2 et -1.

c) Déterminer le sous-groupe $\phi(E[2])$ de G^3.

d) Montrer que le point $(1, 2, 2)$ n'appartient pas à l'image de ϕ.

e) En déduire $E(\mathbb{Q})$.

Exercice 8.3. Soit E la courbe elliptique définie sur $\mathbb{Q}$ par l'équation $Y^2 = X^3 - 25X$.

a) Montrer que $(-4, 6) \in E(\mathbb{Q})$. Que peut-on en déduire sur le rang de E ?

b) Soit $(b_1, b_2) \in \mathbb{Q}^2$ tel que $v_2(b_1) = 0$ et $v_2(b_2) = 1$. Montrer que le système

$$\begin{cases} b_1X^2 - b_2Y^2 = 5 \\ b_1X^2 - b_1b_2Z^2 = 10 \end{cases}$$

n'a pas de solution dans $\mathbb{Q}^3$.

c) Montrer que le système

$$\begin{cases} X^2 - 5Y^2 = 5 \\ X^2 - 5Z^2 = 10 \end{cases}$$

n'a pas de solution dans $\mathbb{Q}^3$.

d) Déterminer la structure du groupe $E(\mathbb{Q})$.

Exercice 8.4. Déterminer la structure du groupe $E(\mathbb{Q})$ lorsque E est la courbe elliptique définie sur $\mathbb{Q}$ par l'équation

$$Y^2 = X^3 - 12X^2 + 20X$$

Exercice 8.5. Soit E une courbe elliptique définie sur $\mathbb{Q}$ par l'équation $Y^2 = P(X)$ où $P(X)$ est un polynôme irréductible de degré 3 de $\mathbb{Q}[X]$. Soit α une racine de P et soit $K = \mathbb{Q}(\alpha)$. Si $P \in E(\mathbb{Q})$, on note $\phi(P)$ l'élément de $K^\times/K^{\times 2}$ défini par

$$\phi(P) = \begin{cases} 1 & \text{si } P = 0 \\ x_P - \alpha & \text{si } P \neq 0 \end{cases}$$

a) Montrer que ϕ est un morphisme de groupes de $E(\mathbb{Q})$ dans $K^\times/(K^\times)^2$.

b) Montrer que l'image de ϕ est incluse dans le sous-groupe

$$\{x \in K^\times/K^{\times 2} \mid N_{K/\mathbb{Q}}(x) \in \mathbb{Q}^{\times 2}\}$$

où $N_{K/Q}$ désigne la norme de $K/\mathbb{Q}$.

c) Montrer que le noyau de ϕ est le sous-groupe $2E(\mathbb{Q})$.

d) Soit r le rang de la courbe elliptique définie sur $\mathbb{Q}$ par l'équation $Y^2 = X^3 + 2$. Montrer que

$$1 \leqslant r \leqslant 3$$

(on pourra utiliser le fait que l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{2})$ est $\mathbb{Z}[\sqrt[3]{2}]$ et qu'il est principal).

Exercice 8.6. Soit K un corps de nombres.

a) Soit M l'ensemble des entiers $x \in \mathcal{O}_K$ tels que pour tout plongement τ de K dans $\mathbb{C}$ on a $|\tau(x)| = 1$. Montrer que M est un ensemble fini.

b) En remarquant que M est stable par l'opération $x \mapsto x^2$, montrer que M est l'ensemble des racines de l'unité de K.

Appendice

Anneaux de polynômes

Généralités

Soit A un anneau. Si $n \geqslant 1$ est un entier, on note $A[X_1, \ldots, X_n]$ l'anneau des polynômes en n-variables. Ses éléments sont par définition les sommes formelles finies

$$\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_n^{i_n}$$

où $(i_1, \ldots, i_n)$ parcourt les n-uplets d'entiers positifs et les $a_{(i_1,\ldots,i_n)}$ des éléments de A. Si $\underline{i} = (i_1, \ldots, i_n)$ est un n-uplet d'entiers positifs, on note $X^{\underline{i}}$ l'élément $X_1^{i_1} \cdots X_n^{i_n}$ appelé *monôme* de *multidegré* $\underline{i}$. Le *degré total* du monôme de multidegré $(i_1, \ldots, i_n)$ est alors l'entier $i_1 + \cdots + i_n$.

L'ensemble des polynômes $A[X_1, \ldots, X_n]$ peut être muni d'une structure d'anneau en posant

$$\left(\sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}} X^{\underline{i}}\right) + \left(\sum_{\underline{i}\in\mathbb{N}^n} b_{\underline{i}} X^{\underline{i}}\right) = \sum_{\underline{i}\in\mathbb{N}^n} (a_{\underline{i}} + b_{\underline{i}}) X^{\underline{i}}$$

et

$$\left(\sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}} X^{\underline{i}}\right) \cdot \left(\sum_{\underline{i}\in\mathbb{N}^n} b_{\underline{i}} X^{\underline{i}}\right) = \sum_{\underline{i}\in\mathbb{N}^n} \left(\sum_{\substack{(\underline{j},\underline{k})\in\mathbb{N}^n\times\mathbb{N}^n \\ \underline{j}+\underline{k}=\underline{i}}} a_{\underline{j}} b_{\underline{k}} \right) X^{\underline{i}}.$$

On vérifie de façon élémentaire que le triplet $(A, +, \cdot)$ est un anneau commutatif dont l'élément unité est $X^{\underline{0}}$ où $\underline{0} = (0, \ldots, 0)$, on le note donc 1.

L'application de A vers $A[X_1, \ldots, X_n]$ envoyant a sur $a \cdot 1$ est un morphisme injectif d'anneaux identifiant A à un sous-anneau de $A[X_1, \ldots, X_n]$. On munit ainsi $A[X_1, \ldots, X_n]$ d'une structure de A-algèbre et en particulier de A-module. En tant que A-module, $A[X_1, \ldots, X_n]$ est libre et la famille $(X^{\underline{i}})_{\underline{i}\in\mathbb{N}^n}$ en forme une base.

En particulier si A est un corps k, le k-espace vectoriel $k[X_1, \ldots, X_n]$ est de dimension infinie.

Si $P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$, on définit le *degré total* comme étant le maximum des degrés totaux de monômes apparaissant avec un coefficient non nul dans P, c'est-à-dire

$$\deg\left(\sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}} X^{\underline{i}}\right) = \max\{i_1 + \cdots + i_n \mid a_{(i_1,\ldots,i_n)} \neq 0\}.$$

On adopte la convention de noter $-\infty$ le minimum de l'ensemble vide. Ainsi la fonction degré prend ses valeurs dans l'ensemble $\mathbb{N} \cup \{-\infty\}$ ordonné de telle sorte que $-\infty$ est inférieur à tous les éléments de $\mathbb{N}$. On convient de plus que $-\infty + a = -\infty$ pour tout $a \in \mathbb{N} \cup \{-\infty\}$. Ainsi $\deg P = -\infty$ si et seulement si $P = 0$.

La A-algèbre $A[X_1, \ldots, X_n]$ vérifie la propriété universelle suivante.

Proposition 8.13. *Soit B une A-algèbre et soient $b_1, \ldots, b_n$ des éléments de B. Il existe alors un unique morphisme de A-algèbres $f : A[X_1, \ldots, X_n] \to B$ tel que, pour $1 \leqslant i \leqslant n$, on a $f(X_i) = b_i$.*

Démonstration. Étant donné B une A-algèbre et $(x_1, \ldots, x_n)$ un n-uplet d'éléments de B. On pose

$$f\left(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_n^{i_n}\right) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} x_1^{i_1} \cdots x_n^{i_n}.$$

Il faut alors vérifier que f est bien un morphisme de A-algèbres et que c'est l'unique morphisme de A-algèbres envoyant X_i sur x_i pour tout $1 \leqslant i \leqslant n$. □

Si $P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ et $(x_1, \ldots, x_n)^n$, on notera $P(x_1, \ldots, x_n)$ l'élément $f(P)$ construit dans la démonstration ci-dessus.

Le cas des polynômes d'une variable

On s'intéresse maintenant au cas où $n = 1$. On note $A[X]$ la A-algèbre ainsi obtenue. Ainsi tout élément de $A[X]$ s'écrit de façon unique $a_m X^m + a_{m_1} X^{m-1} + \cdots + a_1 X + a_0$. Le degré de P est alors le plus grand entier m tel que $a_m \neq 0$, $a_m X^m$ est appelé le *terme dominant* de P et l'élément $a_{\deg P}$ est appelé le *coefficient dominant* de P. Un polynôme $P \in A[X]$ est dit *unitaire* s'il est non nul et si son terme dominant est $X^{\deg P}$ (c'est-à-dire si $a_{\deg P} = 1$).

Il n'est pas toujours vrai que $\deg(PQ) = \deg(P) + \deg(Q)$. Cependant c'est vrai si le coefficient dominant de P n'est pas diviseur de 0 dans A, en particulier si le coefficient dominant de P est inversible dans A.

Lorsque A est un anneau quelconque, on peut toujours effectuer la division euclidienne par un polynôme unitaire. Plus précisément, on a le résultat suivant.

Proposition 8.14. *Soit $P(X) \in A[X]$ et soit $Q(X) \in A[X]$ un polynôme de coefficient dominant inversible. Il existe alors unique couple $(R(X), S(X))$ où $R(X)$ et $S(X)$ sont deux polynômes tels que*

$$P(X) = R(X)Q(X) + S(X) \quad et \quad \deg S < \deg Q.$$

Démonstration. The existence of $R(X)$ and $S(X)$ can be proved induction on the degree of P. For the unicity, assume that $R_1(X)Q(X) + S_1(X) = R_2(X)Q(X) + S_2(X)$ with $\deg S_1, \deg S_2 < \deg Q$, then $S_1 - S_2 = (R_1 - R_2)Q$. Comme le coefficient dominant de Q est inversible dans A, on a $\deg(S_1 - S_2) = \deg(R_1 - R_2) + \deg Q$. Comme $\deg(S_1 - S_2) < \deg Q$, on a nécessairement $R_1 - R_2 = 0$ et donc $S_1 - S_2 = 0$. □

Si k est un corps, tout polynôme non nul de $k[X]$ a un coefficient dominant inversible dans k, on peut donc effectuer la division euclidienne par tout polynôme non nul de $k[X]$. À titre d'illustration, voici une application bien connue de la division euclidienne.

Proposition 8.15. *Soit k un corps. L'anneau $k[X]$ est principal.*

Démonstration. En effet l'anneau est $k[X]$ est intègre. Montrons que tous ses idéaux sont principaux. Soit I un idéal non nul de $k[X]$. Soit $Q(X) \in I$ un polynôme de degré minimal parmi les polynômes non nuls de I. Si $P(X) \in I$, on peut effectuer la division euclidienne de P par Q, on obtient $P(X) = R(X)Q(X) + S(X)$ avec $\deg S < \deg Q$. Comme I est un idéal de $k[X]$ contenant P et Q, on a $S \in I$. Comme $\deg S < \deg Q$, la minimalité de $\deg Q$ implique que $S = 0$ et donc que $P \in (Q)$. Comme évidemment $(Q) \subset I$, on en déduit que $I = (Q)$. □

Polynômes multivariés vus comme polynôme univariés

Soit $n \geqslant 1$ et soit $1 \leqslant i \leqslant n$. Alors il existe un isomorphisme de A-algèbres

$$A[X_1, \ldots, X_n] \simeq A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n][X_i]$$

envoyant X_j sur X_j pour tout $1 \leqslant j \leqslant n$. Cela peut se vérifier formellement en utilisant les propriétés universelles de ces deux anneaux. Il est plus simple d'y penser sous la forme suivante : à partir d'un polynôme de $A[X_1, \ldots, X_n]$, on regroupe les termes ayant la même puissance de X_i. Par exemple si $n = 2$, le polynôme $X_1^3 + X_1^2X_2 + X_1^7X_2 + X_2^5$ correspond au polynôme $X_2^5 + (X_1^2 + X_1^7)X_2 + X_1^3$ de $A[X_1][X_2]$. On peut également, pour $1 \leqslant i \leqslant n$, définir le *degré partiel en la variable* X_i de P, il s'agit du degré $\deg_{X_i} P$ de P vu comme élément de l'anneau de polynômes en une variable $A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n][X_i]$.

Cette identification est très pratique car elle permet de démontrer des résultats par récurrence sur le nombre de variable.

On peut remarquer par exemple que si A est un anneau intègre, alors l'anneau $A[X]$ est intègre. En effet soient P et Q sont deux éléments non nuls de $A[X]$. Comme leurs

termes dominants sont non nuls, ce ne sont pas des diviseurs de zéro dans A puisque A est intègre. Ainsi $\deg(PQ) = \deg(P)+\deg(Q)$. On en conclut que $PQ \neq 0$. En raisonnant par récurrence sur n, on en déduit :

Proposition 8.16. *Soit A un anneau intègre. Alors pour tout $n \geqslant 1$, l'anneau $A[X_1, \ldots, X_n]$ est intègre.*

Ainsi, lorsque A est intègre, les fonctions degré total et degré partiel sont multiplicatives : $\deg(PQ) = \deg P + \deg Q$ et $\deg_{X_i}(PQ) = \deg_{X_i} P + \deg_{X_i} Q$.

Corps des fractions d'un anneau intègre

Soit A un anneau intègre. Pour construire l'anneau des *fractions* de A, on peut procéder comme suit. On considère l'ensemble E des couples $(a, b) \in A \times (A \setminus \{0\})$. On définit sur l'ensemble E la relation d'équivalence

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1.$$

On note alors $\operatorname{Frac} A$ l'ensemble des classes d'équivalence pour cette relation. Si $(a, b) \in E$, on note $\frac{a}{b}$ sa classe d'équivalence. On vérifie sans difficulté que $\operatorname{Frac} A$ peut être muni d'une structure d'anneau en posant

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{cd}, \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd},$$

l'élément nul étant donné par la classe de $(0, 1)$ et l'élément neutre par la classe de $(1, 1)$. On vérifie de plus que l'application de A dans $\operatorname{Frac} A$ définie par $a \mapsto \frac{a}{1}$ est un morphisme injectif d'anneaux que l'on utilise pour identifier A à un sous-anneau de $\operatorname{Frac} A$. Enfin, l'anneau $\operatorname{Frac} A$ est en fait un corps. En effet, un élément $\frac{a}{b}$ est non nul si et seulement si $a \neq 0$ ($b \neq 0$ est toujours vérifié), et son inverse est donné par $\frac{b}{a}$.

Le corps $\operatorname{Frac} A$ possède la propriété universelle suivante.

Proposition 8.17. *Soit K un corps et soit $f : A \to K$ un morphisme d'anneaux. Il existe alors un unique morphisme d'anneaux $\tilde{f} : \operatorname{Frac} A \to K$.*

Démonstration. Il suffit de poser $\tilde{f}(\frac{a}{b}) = f(a)f(b)^{-1}$. Il faut vérifier que cette application est bien définie et est un morphisme d'anneaux. C'est de plus l'unique morphisme d'anneaux prolongeant f. □

Remarquons qu'un morphisme de corps est toujours injectif, le morphisme $\tilde{f}$ de l'énoncé précédent est donc injectif et permet d'identifier $\operatorname{Frac} A$ à un sous-corps de K. C'est pourquoi on dit aussi que $\operatorname{Frac} A$ est le plus petit corps contenant A.

Quelques classes d'anneaux

Définition 8.18. *Un anneau A est dit principal s'il est intègre et si tous ses idéaux sont principaux.*

Exemple 8.19.

a) Les anneaux $\mathbb{Z}$ et $k[X]$, pour k un corps, sont principaux.

b) Si $n \geqslant 2$, l'anneau $k[X_1, \ldots, X_n]$ n'est pas principal.

Définition 8.20. *Soit A un anneau et soit $x \in A$. L'élément x est dit* irréductible *si x n'est pas inversible dans A et si $x = ab$ implique $a \in A^\times$ ou $b \in A^\times$.*

Exemple 8.21. Dans l'anneau $k[X, Y]$, les polynômes X et Y sont irréductibles.

Définition 8.22. *Un anneau A est dit* factoriel *s'il est intègre et si tout élément non nul de A s'écrit comme un produit d'éléments irréductibles avec unicité de cette écriture à permutation près et multiplication par des inversibles. Plus précisément si*

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

avec $p_1, \ldots, p_n, q_1, \ldots, q_m$ irréductibles, on a $n = m$ et il existe une bijection σ de $\{1, \ldots, n\}$ sur $\{1, \ldots, m\}$ ainsi que des éléments inversibles $a_1, \ldots, a_n$ tels que, pour tout $1 \leqslant i \leqslant n$, on a $p_i = a_i q_{\sigma(i)}$.

Les anneaux factoriels ont les propriétés suivantes.

Proposition 8.23. *Soit A un anneau factoriel et soit $x \in A$. Alors l'idéal principal (x) est premier si et seulement si x est irréductible.*

La propriété suivante est plus difficile à démontrer mais est bien pratique.

Proposition 8.24. *Soit A un anneau factoriel et soit K son corps des fractions. Un polynôme $P \in A[X]$ est irréductible si et seulement si il est*

— *soit de degré 0 et irréductible dans A ;*

— *soit irréductible dans $K[X]$ et ses coefficients sont premiers entre eux dans leur ensemble dans A.*

Exemple 8.25.

a) Un anneau principal est factoriel.

b) Si A est factoriel, l'anneau $A[X]$ est factoriel.

c) L'anneau $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ est intègre mais n'est pas factoriel.

Théorème 8.26. *Soit A un anneau factoriel. Alors l'anneau $A[X]$ est factoriel.*

Corollaire 8.27. *Soit k un corps. Alors pour tout $n \geqslant 1$, l'anneau $k[X_1, \ldots, X_n]$ est factoriel.*

Anneaux quotients

Soient A et B deux anneaux et soit f un morphisme d'anneaux de A vers B. Le noyau $\operatorname{Ker} f$ de f est toujours un idéal de A. Réciproquement, la construction qui va suivre montre que tout idéal de I est le noyau d'un morphisme surjectif entre anneaux.

Soit I un idéal de A. On définit une relation d'équivalence sur A en posant $x \sim_I y$ si et seulement si $x - y \in I$. On note A/I l'ensemble des classes d'équivalence pour la relation $\sim_I$. Si $x \in A$, on note $[x]$ la classe de x, autrement dit l'ensemble $x + I$. On peut munir l'ensemble A/I d'une structure d'anneau en posant $[x] + [y] = [x + y]$ et $[x][y] = [xy]$. Il est important de vérifier que cette définition est cohérente, c'est-à-dire que les classes $[x + y]$ et $[xy]$ sont indépendantes des choix faits pour les représentants x et y des classes $[x]$ et $[y]$. Cette vérification est laissée au lecteur, de même que la preuve de la proposition suivante.

Proposition 8.28. *L'application $q_I : x \mapsto [x]$ est un morphisme surjectif d'anneaux de A vers A/I dont le noyau est égal à l'idéal I.*

Remarque 8.29. La construction de la relation d'équivalence $\sim_I$ est une généralisation de la notion de congruence. En effet, si on considère l'anneau $A = \mathbb{Z}$ et l'idéal $I = \mathbb{Z}n$ alors la relation d'équivalence $\sim_I$ est exactement la relation de congruence modulo n et l'anneau quotient A/I est l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exemple 8.30. Soit k un corps et soit A l'anneau $k[X, Y]$ des polynômes en deux variables à coefficients dans k. On considère I l'idéal des multiples de Y. L'anneau A/I est alors isomorphe à l'anneau $k[X]$ des polynômes en une variable. Il suffit en effet de considérer le morphisme envoyant un polynôme $P(X, Y)$ sur le polynôme $P(X, 0)$ en une variable. En termes imagés, on a « ajouté la relation $Y = 0$ à l'anneau A ».

Anneaux noethériens

Définition 8.31. *Un anneau A est dit* noethérien *si tous ses idéaux sont de type fini.*

Une autre façon de caractériser les anneaux noethériens est la suivante : un anneau A est noethérien si et seulement si toute suite croissante d'idéaux de A est stationnaire (exercice).

Les anneaux noethériens sont ainsi nommés d'après Emmy Noether qui a été la première à étudier en toute généralité les anneaux munis de cette *condition de chaîne ascendante*.

Plus généralement on peut considérer la propriété suivante.

Définition 8.32. *Un A-module est dit* noethérien *si tous ses sous-A-modules sont de type fini.*

Comme précédemment, on peut vérifier qu'un A-module M est noethérien si et seulement si toute suite croissante de sous-A-modules de M est stationnaire. Ainsi un anneau A est noethérien si et seulement si A, vu comme A-module, est un A-module noethérien.

Proposition 8.33. *Soit M un A-module.*

(i) Si M est noethérien tout sous-A-module de M et tout quotient de M est noethérien.

(ii) Réciproquement si M' est un sous-A-module de M tel que M' et M/M' sont noethérien, alors M est noethérien.

(iii) Si A est un anneau noethérien, tout A-module de type fini est noethérien.

Démonstration. Si M est noethérien et si M' est un sous-module de M, tout sous-module de M' est en particulier un sous-module de M et est donc de type fini. Ainsi M' est noethérien. On prouve de façon analogue qu'un quotient de M est un A-module noethérien, ce qui prouve (i). Prouvons alors (ii). Soit $(N_i)_{i\geqslant 0}$ une suite croissante de sous-A-modules de M. Notons $\overline{N}_i$ l'image de N_i dans M/M'. Comme M/M' est noethérien, il existe i_0 tel que $\overline{N}_i = \overline{N}_{i_0}$ pour $i \geqslant i_0$. En considérant les images réciproques de ces modules dans M, cela signifie que $N_i + M' = N_{i_0} + M'$ pour $i \geqslant i_0$. De même, en utilisant le fait que M' est noethérien, il existe $i_1 \geqslant i_0$ tel que $N_i \cap M' = N_{i_1} \cap M'$ pour $i \geqslant 1$. Comme $N_{i_1} \subset N_i$ pour $i \geqslant i_1$, les égalités $N_{i_1} + M' = N_i + M'$ et $N_{i_1} \cap M' = N_i \cap M'$ prouvent que $N_{i_1} = N_i$ et que la suite (N_i) est stationnaire. Ainsi M est un A-module noethérien. Enfin prouvons (iii). Si M est de type fini, il existe une surjection $A^m \twoheadrightarrow M$. Par la propriété (i), il suffit de prouver que A^n est noethérien. Par la propriété (ii), il suffit de prouver que A est A-module noethérien, ce qui est équivalent au fait que A est anneau noethérien. □

Le théorème suivant est un des outils les plus utilisés pour construire des anneaux noethériens. En particulier, il implique directement, par récurrence, le théorème 1.8.

Théorème 8.34. *Si A est un anneau noethérien, l'anneau $A[X]$ est noethérien. Plus généralement, toute A-algèbre de type fini est un anneau noethérien.*

Démonstration. Soit I un idéal de $A[X]$. Pour $n \geqslant 0$, on note I_n l'ensemble des polynômes de I qui sont de degré inférieur ou égal à n et J_n l'ensemble des $a \in A$ pour lesquels il existe $Q \in A_{n-1}[X]$ tel que $aX^n + Q \in I$. L'ensemble J_n est clairement un idéal de A. Si $a \in J_n$, il existe $P(X) = aX^n + \sum_{i=0}^{n-1} a_i X^i \in I$. Mais alors $XP(X) \in I$, ce qui implique que $a \in J_{n+1}$. Ceci montre que la suite $(J_n)_{n\geqslant 0}$ est une suite croissante d'idéaux de A. L'ensemble $J \coloneqq \bigcup_{n\geqslant 0} J_n$ est alors un idéal de A. Comme l'anneau A est noethérien, cette suite est stationnaire, autrement dit il existe $p \geqslant 0$ tel que $J_n = J_p$ pour $n \geqslant p$.

On va alors montrer que I est l'idéal de A engendré par I_p. Plus précisément soit I' l'idéal de I engendré par I_p. On montre par récurrence sur $n \geqslant p$ que $I_n \subset I'$. Le cas où $n = p$ est évident. Supposons donc $n > p$ et soit $P \in I$ de degré n. Soit a_n le coefficient

dominant de P. Comme $J_n = J_p$, il existe un polynôme $Q \in I$ de degré p et de coefficient dominant a_n. On a alors

$$P - X^{n-p}Q \in I_{n-1} \subset I'$$

où la deuxième inclusion résulte de l'hypothèse de récurrence. On a donc finalement $I = I'$.

Pour conclure, on remarque I_p est un sous-A-module de l'ensemble des polynômes de $A[X]$ de degré inférieur ou égal à p, ensemble qui forme un A-module de type fini. Comme A est un anneau noethérien, le A-module I_p est de type fini. Une famille de générateurs du A-module I_p engendre I comme $A[X]$-module, ce qui permet de conclure que I est un $A[X]$-module de type fini. Ainsi $A[X]$ est noethérien.

La dernière assertion est alors une conséquence du fait que $A[X_1, \ldots, X_n]$ est noethérien pour tout $n \geqslant 0$ et qu'un quotient d'un anneau noethérien est un anneau noethérien. □

Le résultat technique qui suit nous servira dans la preuve du théorème des zéros de Hilbert.

Lemme 8.35 (Lemme d'Artin-Tate)**.** *Soit C un anneau et soient A et B deux sous-anneaux de C tels que $A \subset B \subset C$. On suppose que A est un anneau noethérien, que C est une A-algèbre de type fini et que C est un B-module de type fini. Alors B est une A-algèbre de type fini.*

Démonstration. Soit f un morphisme surjectif de $A[X_1, \ldots, X_n]$ vers C. Pour tout $1 \leqslant i \leqslant n$, posons $x_i = f(X_i)$. Quitte à agrandir n, on peut supposer que la famille $(x_i)_{1 \leqslant i \leqslant n}$ engendre le B-module C. Pour $1 \leqslant i, j \leqslant n$, il existe alors des éléments $b_{i,j}^k \in B$ tels que

$$x_i x_j = \sum_{k=1}^{n} b_{i,j}^k x_k.$$

Soit B' la sous-A-algèbre de B engendrée par les $(b_{i,j}^k)_{1 \leqslant i,j,k \leqslant n}$. On vérifie alors que la famille $(x_i)_{1 \leqslant i \leqslant n}$ engendre C comme B'-module. En particulier C est un B'-module de type fini. L'algèbre B' est une A-algèbre de type fini, le théorème 8.34 implique donc qu'il s'agit d'un anneau noethérien. Comme B est un sous-B'-module de C et que C est de type fini sur B', on peut en conclure que B est un B'-module de type fini. En résumé, B est un B'-module de type fini et B' est une A-algèbre de type fini, donc B est une A-algèbre de type fini. □

8.4 Exercices

Exercice 8.7. Soit A un anneau commutatif unitaire. Soit I un idéal de A.

a) Montrer que I est premier si et seulement si $I \neq A$ et

$$\forall x, y \in A, \quad (xy \in I \Rightarrow x \in I \quad \text{ou} \quad y \in I)$$

b) Montrer que I est maximal si et seulement si $I \neq A$ et si pour tout idéal J tel que $I \subset J \subset A$ on a $J = I$ ou $J = A$.

c) Soient $\mathfrak{p}$ un idéal premier de A ainsi que I_1 et I_2 deux idéaux de A. Si $I_1 I_2 \subset \mathfrak{p}$, montrer que $I_1 \subset \mathfrak{p}$ ou $I_2 \subset \mathfrak{p}$.

Exercice 8.8. Soit k un corps. Montrer que les idéaux premiers de $k[X]$ sont l'idéal nul et les idéaux maximaux.

Exercice 8.9. Soit k un corps et soit $n \geqslant 1$. On fixe $(a_1, \ldots, a_n) \in k^n$. Montrer que l'idéal $(X_1 - a_1, \ldots, X_n - a_n)$ de $k[X_1, \ldots, X_n]$ est maximal. (On pourra considérer l'application $k[X_1, \ldots, X_n] \to k$ définie par $P \mapsto P(a_1, \ldots, a_n)$ et déterminer son noyau.)

Exercice 8.10.

a) Soit $f : A \to B$ un morphisme *surjectif* d'anneaux. Montrer que si I est un idéal de A alors $f(I)$ est un idéal de B. Est-ce toujours vrai si f est un morphisme d'anneaux non nécessairement surjectif ?

b) Soient I et J deux idéaux d'un anneau A. On note q_I le morphisme canonique $A \to A/I$ et on note $\overline{J} = q_I(J)$. Montrer que les anneaux $(A/I)/\overline{J}$ et $A/(I + J)$ sont isomorphes.

c) Montrer que les idéaux (2) et (3) ne sont pas premiers dans $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ (on pourra commencer par prouver que $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ est isomorphe à $\mathbb{Z}[X]/(X^2 + 5)$).

d) Montrer que l'anneau $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ n'est pas factoriel (on pourra montrer que les éléments 2 et 3 sont irréductibles).

Exercice 8.11. Soit A un anneau noethérien.

a) Soit I un idéal de A. Montrer qu'il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I$.

b) En déduire qu'il n'existe qu'un nombre fini d'idéaux premiers qui sont minimaux pour la relation d'inclusion.

Exercice 8.12. Soit $f : A \to B$ un morphisme d'anneaux.

a) Soit $\mathfrak{p}$ un idéal premier de B. Montrer que $f^{-1}(\mathfrak{p})$ est un idéal premier de A.

b) Soit k un corps. On suppose que A et B sont des k-algèbres de type fini (on rappelle qu'une k-algèbre de type fini est un anneau de la forme $k[X_1, \ldots, X_n]/I$ pour un idéal I). Montrer que si $\mathfrak{m}$ est un idéal maximal de B, alors $f^{-1}(\mathfrak{m})$ est un idéal maximal de A.

c) Donner un contre exemple à l'énoncé b) lorsque A et B ne sont pas des k-algèbres de type fini.